УДК 442.95
DOI https://doi.org/10.32782/2524-0374/2022-8/71

ПОВНОВАЖЕННЯ ПРАВООХОРОННИХ ОРГАНІВ ПРИ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

POWERS OF LAW ENFORCEMENT AGENCIES IN THE IMPLEMENTATION OF STATE POLICY ON ENSURING INFORMATION SECURITY

Макарчук В.В., к.ю.н.,
доцент кафедри конституційного права та теоретико-правових дисциплін
Білоцерківський національний аграрний університет

Стаття присвячена аналізу повноважень правоохоронних органів при реалізації державної політики щодо забезпечення інформаційної безпеки. Досліджено правову базу та державну політику стосовно безпеки в інформаційній сфері. Визначені групи повноважень правоохоронних органів при реалізації ними державної політики в інформаційній безпеці. Акцентовано на дослідженні компетенції та повноважень правоохоронних органів стосовно інформаційної безпеки, що є необхідним, оскільки тільки так можна розкрити зміст діяльності владного суб'єкта, його реальні функції, а як наслідок – вносити обґрунтовані рекомендації та пропозиції щодо адміністративно-правового статусу органу, зміни та доповнення чинного законодавства. Особливу роль у прогнозуванні, виявленні, визначенні загроз національній безпеці та обороні та протидії їм відіграють суб'єкти формування та реалізації державної політики у вказаній сфері. Їх можливості, повноваження та діяльність повинні забезпечувати ефективність реалізації безпекової функції держави. Провідними такими суб'єктами виступають правоохоронні органи. Тому саме компетенція та повноваження є важливим елементом їхнього адміністративно-правового статусу.

Встановлено, що у вітчизняному законодавстві повноваження правоохоронних органів в конкретних секторах національної безпеки та оборони не конкретизуються, а лише дублюють їх статус, що визначений у статутних актах законодавства. З метою реалізації державної політики у сфері національної безпеки та оборони України необхідно використовувати можливості космічних інформаційних технологій й правоохоронними органами. Однак використання таких технологій правоохоронними органами у своїй діяльності можуть виплинути на права людини. Тому такі повноваження мають бути чітко визначені законодавчо з обов'язковою деталізацією процедури реалізації. Для цього необхідно розробити й прийняти ряд нормативно-правових актів, в тому числі програмних.

Ключові слова: кібербезпека, інформація, інформаційні системи, державна стратегія, національна безпека.

The article is devoted to the analysis of the powers of law enforcement agencies in the implementation of the state policy on ensuring information security. The legal framework and state policy regarding security in the information sphere have been studied. Defined groups of powers of law enforcement agencies in their implementation of state policy in information security. Emphasis is placed on the study of the competence and powers of law enforcement agencies in relation to information security, which is necessary, because this is the only way to reveal the content of the activity of a powerful entity, its real functions, and as a result - to make reasonable recommendations and proposals regarding the administrative and legal status of the body, changes and supplementing the current legislation. A special role in forecasting, detection, identification of threats to national security and defense and countermeasures is played by subjects of formation and implementation of state policy in the specified sphere. Their capabilities, powers and activities must ensure the effectiveness of the implementation of the security function of the state. Law enforcement agencies are the leading such subjects. Therefore, competence and authority are an important element of their administrative and legal status.

It was established that the domestic legislation does not specify the powers of law enforcement agencies in specific sectors of national security and defense, but only duplicates their status, which is defined in statutory acts of legislation. In order to implement the state policy in the field of national security and defense of Ukraine, it is necessary to use the capabilities of space information technologies and law enforcement agencies. However, the use of such technologies by law enforcement agencies in their activities may affect human rights. Therefore, such powers should be clearly defined by law with mandatory details of the implementation procedure. To do this, it is necessary to develop and adopt a number of normative legal acts, including program ones.

Key words: cyber security, information, information systems, state strategy, national security.

Постановка проблеми. Загрози інформаційній безпеці України, зокрема системна інформаційна війна, поширення неправдивої, видозміненої інформації, що впливає на розвиток суспільства, несформованість інформаційної концепції та стратегії поширення інформації та протидії інформаційним загрозам, недостатній рівень медіа-культури суспільства, потребують формування системи інформаційної безпеки, в якій відбуватиметься ефективна та злагоджена взаємодія суб'єктів формування та реалізації політики державної безпеки в інформаційній сфері.

Аналіз останніх досліджень і публікацій. Окремі аспекти реалізації державної політики щодо забезпечення інформаційної безпеки досліджувались у працях вітчизняних науковців Волошина О. М., Даника Ю. Г., Зайцева О. В., Новохатнія Ю. В., Попова М. О., Права Р. Ю. та інших.

Постановка завдання. Метою даної статті є дослідження повноважень правоохоронних органів при реалізації державної політики щодо забезпечення інформаційної безпеки.

Виклад основного матеріалу. В Україні активно раніше розвивалась та нині вдосконалюється правова база (ухвалено Стратегію кібербезпеки (2016 р.) [1], Доктрину інформаційної безпеки України (2016 р.) [2], Закон України «Про основні засади забезпечення кібербезпеки України» (2017 р.) [3] тощо) стосовно безпеки в інформаційній сфері. У зазначених нормативно-правових актах визначено основних суб'єктів формування та реалізації політики державної безпеки в інформаційній сфері, проте на разі не забезпечено високий рівень ефективності їх взаємодії [4, с. 1].

Кабінет Міністрів України 15.09.2021 року схвалив Стратегію інформаційної безпеки, а Указ Президента України 28.12.2021 року увів в дію рішення Ради національної безпеки і оборони України від 15.10.2021 року «Про Стратегію інформаційної безпеки» [5]. Вона є однією з низки стратегічних документів, які необхідно було розробити для реалізації Стратегії національної безпеки України і розрахована на період до 2025 року.

Метою Стратегії інформаційної безпеки є посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина [5].

Варто зауважити, що Стратегія інформаційної безпеки більшою мірою є програмним документом, що закладає підвалини для майбутньої політики держави. Відповідні документи рідко містять детальний перелік заходів, який зазвичай встановлюється планом дій. Однак, вона вказує на майбутні тренди державної політики, тому більшість застережень стосуватиметься практичних рішень, які можуть бути втілені на її виконання у майбутньому. У цьому світлі варто наголосити на потребі реального громадського обговорення проєкту плану дій, що буде розроблятися урядом, адже саме у ньому міститиметься перелік заходів, що вже безпосередньо вплинуть на регуляторне середовище [6].

Що стосується повноважень правоохоронних органів то вони в загальному вигляді визначені у Розділі «Механізми реалізації визначеної мети та завдань». Так, вказується, що Служба безпеки України у межах компетенції має моніторингові та протидійні повноваження, а розвідувальні органи України у процесі провадження розвідувальної діяльності мають сприяти реалізації та захисту національних інтересів України в інформаційній сфері за кордоном та здійснювати інші протидійні заходи [5].

Водночас Стратегія інформаційної безпеки не визначає головного органу влади, відповідального за звітування стосовно її впровадження, механізмів моніторингу ефективності впровадження Стратегії для кращого розуміння, як використовувані урядом та іншими суб'єктами інструменти досягають своїх цілей (наприклад, питання ефективності санкцій) [5].

Необхідно відмітити, що кіберпростір разом з іншими фізичними просторами визнано одним з важливих театрів воєнних дій. Набирає сили тенденція зі створення та розширення кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, що включає виведення з ладу критично важливих об'єктів інфраструктури противника шляхом руйнування інформаційних систем, які управляють такими об'єктами [7]. Тому Закон України «Про основні засади забезпечення кібербезпеки України» та Стратегія кібербезпеки України, що затверджена Указом Президента також окреслили повноваження окремих правоохоронних органів у вказаній сфері.

Тому всі вище зазначені стратегічні документи та статутні нормативно-правові акти використовувались нами при визначенні повноважень правоохоронних органів при реалізації державної політики в інформаційній безпеці. Їхній аналіз дозволив виокремити наступні групи повноважень правоохоронних органів:

1. Інформаційно-аналітичні. Наприклад, в статті 24 Закону України «Про Службу безпеки України» закріплені повноваження щодо здійснення інформаційно-аналітичної роботи в інтересах ефективного проведення органами державної влади та управління України внутрішньої й зовнішньої діяльності, вирішення проблем оборони, соціально-економічного будівництва, науково-технічного прогресу, екології та інших питань, пов'язаних із національною безпекою України. Що стосується інших правоохоронних органів, то їх інформаційно-аналітичні повноваження можна об'єднати у певні групи, серед яких такі: а) одержання інформації для виконання покладених законом завдань. Зазначена інформація може бути отримана в різний спосіб та різним шляхом: гласно-негласно, шляхом витребування, подання запитів чи під час взаємодії. Так, Національна поліція України має повноваження одержувати в установленому законодавством порядку від державних органів та органів місцевого самоврядування, підприємств, установ, організацій незалежно від форми власності та їх посадових осіб, а також громадян та їх об'єднань інформацію, документи і матеріали, необхідні для виконання покладених на неї завдань та користуватися відповідними інформаційними базами даних державних органів, державною системою урядового зв'язку та іншими технічними засобами [8]. Додамо, що Служба безпеки України має право також одержувати на письмовий запит керівника відповідного органу Служби безпеки України від міністерств, державних комітетів, інших відомств, підприємств, установ, організацій, військових частин, громадян та їх об'єднань дані і відомості, необхідні для забезпечення державної безпеки України, а також користуватись з цією метою службовою документацією і звітністю. Отримання від банків інформації, яка містить банківську таємницю, здійснюється у порядку та обсязі, що визначений Законом України «Про банки і банківську діяльність». Отримання від Центрального депозитарію цінних паперів, Національного банку України та депозитарних установ інформації, що міститься у системі депозитарного обліку цінних паперів, здійснюється в порядку та обсязі, що визначений Законом України «Про депозитарну систему України» [9]; б) створення та використання інформаційних систем та банків даних. Так, Державна прикордонна служба України має повноваження по створюванню і використанню в інтересах розвідки, контррозвідувального забезпечення охорони державного кордону України, оперативно-розшукової діяльності, участі у боротьбі з організованою злочинністю та протидії незаконній міграції інформаційних систем, у тому числі банків даних щодо осіб, які перетнули державний кордон України, осіб, які вчинили правопорушення, протидію яким віднесено до її компетенції, осіб, яким згідно із законодавством не дозволяється в'їзд в Україну або тимчасово обмежується право виїзду з України, недійсних, викрадених і втрачених документів на право виїзду за кордон та в інших випадках, передбачених законами України» [10].

2. Профілактично-запобіжні. Наприклад, правоохоронні органи розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту [3]. Так, Служба безпеки України здійснює запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, які вчиняються у кіберпросторі; … негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів [3].

3. Протидійно-реагувальні. Так, Служба безпеки України 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]. Окрім того на неї покладено обов'язок протидіяти проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуації [5].

4. Оперативно-технічні. Так, наприклад, Служба безпеки України здійснює функцію технічного регулювання у сфері спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації [9]. А Державна прикордонна служба України має повноваження з перехоплення сигналів дистанційного керування, пошкодження чи знищення безпілотних повітряних суден та/або складових частин безпілотної авіаційної системи (безпілотного авіаційного комплексу) [10].

5. Моніторингові, які проводяться з метою виявлення, фіксації, обмеження доступу та/або видалення з українського сегмента мережі Інтернет інформації, розміщення якої обмежено або заборонено законом. Так, Служба безпеки України у межах компетенції здійснює: моніторинг спеціальними методами і способами вітчизняних та іноземних засобів масової інформації та Інтернету з метою

виявлення загроз національній безпеці України в інформаційній сфері; протидію проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуації [5]. Правоохоронні органи забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління [3].

6. Правообмежуючі. Так, правоохоронні органи мають повноваження щодо обмеження участі у заходах із забезпечення інформаційної безпеки та кібербезпеки будь-яких суб'єктів господарювання, які перебувають під контролем держави, визнані Верховною Радою України державою-агресором, або держав та осіб, стосовно яких діють спеціальні економічні та інші обмежувальні заходи (санкції), прийняті на національному або міжнародному рівні внаслідок агресії щодо України, а також обмеження використання продукції, технологій та послуг таких суб'єктів для забезпечення технічного та криптографічного захисту державних інформаційних ресурсів, посилення державного контролю в цій сфері [3].

Таким чином, в Стратегії інформаційної безпеки з усіх правоохоронних органів повноваження з її реалізації визначені тільки щодо діяльності Служби безпеки України. Окремо відзначимо, що вплив безпілотних літальних апаратів і угруповань малих супутників на ринок геоінформаційних послуг в сфері безпеки і оборони з кожним роком стає все більш помітним. Масове використання дронів і малих супутників – це сучасна риса розвитку галузі. Найближчим часом джерела просторових даних забезпечуватимуть майже необмежений потік інформації будь-якого рівня детальності, а зйомка з космосу буде вестися в безперервному режимі. В області аерофотозйомки і повітряного лазерного сканування відбудеться перехід від пілотованих знімальних систем до безпілотних літальних апаратів [11, с. 20-21; 12, с. 52]. Тому опанування працівниками правоохоронних органів навичок з аналізу, а потім і щодо застосування інформації, отриманої із використання космічних та геоінформаційних технологій є не тільки важливим, а й життєво необхідним в умовах глобалізаційних інформаційних процесів. Окрім того, відповідно до вимог, на основі стандартів, доктрин і рекомендацій НАТО [13] слід нарощувати можливості системи супутникового зв'язку Збройних Сил України.

Висновки. Отже, аналіз реалізаційних повноважень правоохоронних органів інформаційної безпеки дозволяє підсумувати, що у вітчизняному законодавстві повноваження правоохоронних органів в конкретних секторах національної безпеки і оборони не конкретизуються, а лише дублюють їх статус, що визначений у статутних актах законодавства.

З метою реалізації державної політики у сфері національної безпеки і оборони України необхідно використовувати можливості космічних інформаційних технологій й правоохоронними органами. Однак використання таких технологій правоохоронними органами у своїй діяльності можуть виплинути на права людини. Тому такі повноваження мають бути чітко визначені законодавчо з обов'язковою деталізацією процедури реалізації. Для цього необхідно розробити і прийняти ряд нормативно-правових актів, в тому числі програмних.

ЛІТЕРАТУРА

1. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 р. № 96/2016 : станом на 28 серп. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text (дата звернення: 26.08.2022).
2. Про Доктрину інформаційної безпеки України : Рішення Ради нац. безпеки і оборони України від 29.12.2016 р. : станом на 28 лют. 2017 р. URL: https://zakon.rada.gov.ua/laws/show/n0016525-16#Text (дата звернення: 26.08.2022).
3. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 17 серп. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 26.08.2022).
4. Прав Р. Ю. Діяльність суб'єктів формування і реалізації політики державної безпеки в інформаційній сфері України. *Державне управління: удосконалення та розвиток*, 2018. № 9. С. 1-9 URL: http://www.dy.nayka.com.ua/pdf/9_2018/103.pdf (дата звернення: 26.08.2022).
5. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 26.08.2022).
6. Волошин О. Стратегія інформаційної безпеки – 2025: що зміниться у сфері цифрових прав. *Лабораторія цифрової безпеки* : веб-сайт. URL: https://dslua.org/publications/stratehiia-informatsiynoi-bezpeky-2025-shcho-zminytsia-u-sferi-tsyfrovykh-prav/ (дата звернення: 26.08.2022).
7. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 26.08.2022).
8. Про затвердження Положення про Національну поліцію : Постанова Каб. Міністрів України від 28.10.2015 р. № 877 : станом на 9 квіт. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/877-2015-п#Text (дата звернення: 26.08.2022).
9. Про Службу безпеки України : Закон України від 25.03.1992 р. № 2229-XII : станом на 7 трав. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text (дата звернення: 26.08.2022).
10. Про Державну прикордонну службу України : Закон України від 03.04.2003 р. № 661-IV : станом на 2 квіт. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/661-15#Text (дата звернення: 26.08.2022).
11. Даник Ю. Г. Особливості інформаційного забезпечення в сфері національної безпеки і оборони в сучасних умовах та на перспективу. *Застосування космічних та геоінформаційних систем в інтересах національної безпеки та оборони* : зб. матеріалів III Міжнар. наук.-практ. конф., 5 квіт. 2018 р. Київ : Національний університет оборони України імені Івана Черняховського, 2018. С. 19-23.
12. Зайцев О. В., Новохатній Ю. В., Попов М. О. Використання багатовимірної моделі даних для вирішення задач інтеграції новітніх ГІС в існуючі інформаційні системи військового призначення. *Застосування космічних та геоінформаційних систем в інтересах національної безпеки та оборони* : зб. матеріалів III Міжнар. наук.-практ. конф., 10 квіт. 2019 р. Київ : Національний університет оборони України імені Івана Черняховського, 2019. С. 52-53.
13. Довідник НАТО. Brussels : Office of information and press NATO, 2001. 608 с. URL: https://www.nato.int/docu/other/ukr/handbook/2001/pdf/handbook.pdf (дата звернення: 26.08.2022).