DOI https://doi.org/10.51647/kelm.2022.7.57

PRZEDMIOT REALIZACJI POSTĘPOWANIA ADMINISTRACYJNEGO W ZAKRESIE ZAPEWNIENIA CYBERBEZPIECZEŃSTWA

Oleksandr Nikołajczyk
laureat Naukowego Instytutu Prawa Publicznego (Kijów, Ukraina)
ORCID ID: 0000-0002-0218-870X
onikolaichyk@gmail.com

Adnotacja. Celem artykułu jest zarysowanie i scharakteryzowanie statusu prawnego podmiotów realizujących procedury administracyjne z zakresu cyberbezpieczeństwa. W artykule, w oparciu o analizę poglądów naukowych naukowców, zaproponowano autorskie podejście do definiowania pojęcia „podmiotów realizacji procedur administracyjnych z zakresu cyberbezpieczeństwa". Podświetlony jest krąg odpowiednich tematów. Przeprowadzono analizę norm obowiązującego ustawodawstwa, na podstawie której scharakteryzowano stan prawny kluczowych podmiotów realizacji procedur administracyjnych z zakresu cyberbezpieczeństwa. Ustalono, że pod tematyką realizacji procedur administracyjnych w zakresie cyberbezpieczeństwa najwłaściwsze jest rozumienie zespołu specjalnie upoważnionych organów państwowych (reprezentowanych przez ich urzędników), które zgodnie z normami obowiązującego prawodawstwa , są umocowani i posiadają niezbędne kompetencje do wdrażania działań i środków ch do ochrony systemów i sieci informatycznych, a także koordynację działań mających na celu zapobieganie, wykrywanie i reagowanie na zagrożenia cybernetyczne.

Słowa kluczowe: cyberbezpieczeństwo, cyberprzestrzeń, procedury administracyjne, podmioty realizacji procedur administracyjnych.mających na celu stworzenie warunków niezbędny.

SUBJECTS OF PROVIDING ADMINISTRATIVE PROCEDURES IN THE FIELD OF CYBER SECURITY

Oleksandr Nikolaichyk
laureate of the Research Institute of Public Law (Kyiv, Ukraine)
ORCID ID: 0000-0002-0218-870X
onikolaichyk@gmail.com

Abstract. The purpose of the article is to outline and characterize the legal status of subjects implementing administrative procedures in the field of cyber security. In the article, based on the analysis of scientific views of scientists, the author's approach to defining the concept of "subjects of implementation of administrative procedures in the field of cyber security" is proposed. A circle of relevant subjects is highlighted. An analysis of the norms of the current legislation was carried out, on the basis of which the legal status of the key subjects of the implementation of administrative procedures in the field of cyber security was characterized. It was determined that under the subjects of the implementation of administrative procedures in the field of cyber security, it is most appropriate to understand the set of specially authorized state authorities (represented by their officials), which, in accordance with the norms of the current legislation, are empowered and have the necessary competence to implement actions and measures aimed at creation of necessary conditions for protection of information systems and networks, as well as coordination of actions to prevent, detect and respond to cyber threats.

Key words: cyber security, cyberspace, administrative procedures, subjects of implementation of administrative procedures.

СУБ'ЄКТИ РЕАЛІЗАЦІЇ АДМІНІСТРАТИВНИХ ПРОЦЕДУР У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Олександр Ніколайчик
здобувач Науково-дослідного інституту публічного права (Київ, Україна)
ORCID ID: 0000-0002-0218-870X
onikolaichyk@gmail.com

Анотація. Метою статті є виділити коло та надати характеристику правовому статусу суб'єктів реалізації адміністративних процедур у сфері забезпечення кібербезпеки. У статті, спираючись на аналіз наукових поглядів вчених, запропоновано авторський підхід щодо визначення поняття «суб'єкти реалізації адміністративних процедур у сфері забезпечення кібербезпеки». Виділено коло відповідних суб'єктів. Здійснено аналіз норм чинного законодавства, на основі чого надано характеристику правовому статусу ключових суб'єктів реалізації адміністративних процедур у сфері забезпечення кібербезпеки. Визначено, що під суб'єктами реалізації адміністративних процедур у сфері забезпечення кібербезпеки найбільш доцільно розуміти сукупність спеціально уповноважених органів державної влади (в особі їх посадових осіб), які відповідно до норм чинного законодавства наділені повноваженнями та необхідною компетенцією щодо реалізації дій та заходів, спрямованих на створення необхідних умов для захисту інформаційних систем та мереж, а також координації дій щодо запобігання, виявлення та реагування на кіберзагрози.

Ключові слова: кібербезпека, кіберпростір, адміністративні процедури, суб'єкти реалізації адміністративних процедур.

Постановка проблеми. У сучасному світі технології проникли у всі сфери життя суспільства та держави, з огляду на це кібербезпека стала невід'ємною частиною національної безпеки будь-якої розвиненої країни. Її значення зростає з кожним днем, оскільки кіберзагрози стають все більш складними та масштабними. Кіберпростір перетворився на нове поле битви, де держави, компанії та окремі особи змагаються за вплив і ресурси. Кібератаки можуть мати далекосяжні наслідки, що виходять за рамки простої крадіжки даних. Вони можуть паралізувати критичну інфраструктуру, підірвати довіру до державних інституцій, дестабілізувати суспільство і навіть вплинути на результати виборів. Варто зауважити, що забезпечення кібербезпеки передбачає реалізацію низки процедур, які носять адміністративний характер. При цьому ефективність останніх напряму залежить від того, наскільки якісно свою діяльність реалізовують спеціально уповноважені суб'єкти, кожен з яких володіє своїм, особливим правовим статусом.

Стан дослідження. На сьогоднішній день, кібербезпека є однією з актуальних теоретико-юридичних проблем сучасності дослідженню якої приділяли увагу багато науковців-правознавців. Зокрема, загальні питання її змісту та значення аналізували: О.С. Власюк, О.В. Олійник, Г.В. Форос, О.В. Харитонов та інших. Дослідженню суб'єктного складу кібербезпеки присвятили свої дослідження С.О. Гнатюк, І.В. Діордіца, О.Г. Коротченко, В.А. Ліпкан та ряд інших вчених. Втім, попри численні наукові опрацювання, все ще залишається багато практично-правових питань, зокрема присвячених переліку та характеристиці правового статусу суб'єктів реалізації адміністративних процедур у сфері забезпечення кібербезпеки.

Саме тому метою статті є виділити коло та надати характеристику правовому статусу суб'єктів реалізації адміністративних процедур у сфері забезпечення кібербезпеки.

Виклад основного матеріалу. У теорії державного управління суб'єкт – це складна система державних органів, які є носіями повноважень щодо практичного здійснення функцій управління, тобто цілеспрямованого управлінського впливу на відповідні об'єкти управління. Крім того, суб'єктом управління можуть бути: особи, організації, їх системи, які управляють підпорядкованими їм особами, організаціями та їх системами; сукупність посадових осіб, що займаються управлінською організаційною діяльністю, тобто апарат управління; органи влади, установи, підрозділи апарату управління чи посадові особи, які виробляють і ухвалюють рішення, здійснюють керуючий вплив на підпорядковані об'єкти управління (Набока, 2008: 26). Тож, суб'єкти є невід'ємним елементом реалізації адміністративних процедур в сфері забезпечення кібербезпеки. До їх переліку відноситься велика кількість представників публічної влади, правовий статус яких характеризується багатьма специфічними моментами та особливостями.

Таким чином, під суб'єктами реалізації адміністративних процедур у сфері забезпечення кібербезпеки найбільш доцільно розуміти сукупність спеціально уповноважених органів державної влади (в особі їх посадових осіб), які відповідно до норм чинного законодавства наділені повноваженнями та необхідною компетенцією щодо реалізації дій та заходів, спрямованих на створення необхідних умов для захисту інформаційних систем та мереж, а також координації дій щодо запобігання, виявлення та реагування на кіберзагрози.

Зауважимо, що чинний Закон України «Про адміністративну процедуру» не апелює визначенням «суб'єкт надання адміністративних процедур». Статус останніх трактується крізь приму поняття адміністративний орган. Згідно із Законом це орган виконавчої влади, орган влади Автономної Республіки Крим, орган місцевого самоврядування, їх посадова особа, інший суб'єкт, який відповідно до законодавства уповноважений здійснювати функції публічної адміністрації. Далі в закон вказано, що адміністративний орган розглядає і вирішує справи, віднесені до його відання законом (предметна компетенція). В адміністративному органі адміністративне провадження здійснюється та відповідний адміністративний акт приймається посадовою особою, уповноваженою відповідно до закону та/або на підставі внутрішніх розпорядчих актів адміністративного органу (є реалізатором адміністративної процедури). Документи, що підтверджують повноваження посадової особи щодо розгляду та вирішення адміністративної справи, надаються особі на її вимогу. Колегіальний адміністративний орган може уповноважити одного із своїх членів або посадову особу свого апарату (секретаріату, виконавчого органу) для проведення всіх процедурних дій. У такому разі уповноважений член колегіального адміністративного органу або посадова особа апарату (секретаріату, виконавчого органу) такого органу інформує відповідний колегіальний адміністративний орган про результати розгляду справи, після чого такий орган приймає рішення чи вчиняє дію у справі у строки, визначені законом (Про адміністративну процедур, 2022).

Закон України «Про основні засади забезпечення кібербезпеки України» вказує, що основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України (Про основні засади забезпечення кібербезпеки України, 2017). Кожен із зазначених органів державної влади має відповідний набір повноважень (прав і обов'язків) пов'язаних із здійсненням кіберзахисту за відповідним напрямом, що є сукупністю 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 функціонування комунікаційних, технологічних систем. Об'єктами кіберзахисту є: 1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону; 2) об'єкти критичної інформаційної інфраструктури; 3) комунікаційні системи, які використовуються для

задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу (Про основні засади забезпечення кібербезпеки України, 2017).

Проте, далеко не кожний суб'єкт перелічений у Законі уповноважений безпосередньо зжійснювати адміністративні процедури. Правовий статус лише окремих з них передбачає дану можливість. Зокрема, таким органом є Державна служба спеціального зв'язку та захисту інформації України. Як один з елементів національної системи кібербезпеки в Україні Служба забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, активної протидії агресії у кіберпросторі, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах; координує діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту; забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту; здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; інформує про кіберзагрози та відповідні методи захисту від них; забезпечує впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації); координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість; забезпечує функціонування Державного центру кіберзахисту та Центру активної протидії агресії у кіберпросторі, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA (Про основні засади забезпечення кібербезпеки України, 2017).

Варто наголосили, що Державна служба спеціального зв'язку та захисту інформації України реалізує різноманітні адміністративні процедури, які мають місце у галузі кібербезпеки, та має для цього в своїй структурі спеціальні підрозділи та органи: Адміністрацію, Державний центр кіберзахисту, урядову команду реагування на комп'ютерні надзвичайні події України CERT-UA тощо (Про основні засади забезпечення кібербезпеки України, 2017; Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, 2014).

Наступним суб'єктом є Національний банк України (далі – НБУ), який реалізує численні адміністративні процедури у сфері забезпечення кібербезпеки, але в сфері банківської діяльності. В царині забезпечення кібербезпеки, НБУ визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки банками, іншими особами, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторами платіжних систем та/або учасниками платіжних систем, технологічними операторами платіжних послуг, здійснює контроль за їх виконанням; створює центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту для банків, інших осіб, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг; забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки на об'єктах критичної інфраструктури в банках, інших особах, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторах платіжних систем та/або учасниках платіжних систем, технологічних операторах платіжних послуг (Про основні засади забезпечення кібербезпеки України, 2017).

Третім суб'єктом реалізації адміністративних процедур у сфері кібербезпеки є Служба безпеки України (далі – СБУ). Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», СБУ здійснює запобігання, виявлення, припинення та розкриття кримінальних правопорушень 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 (Про основні засади забезпечення кібербезпеки України, 2017).

Адміністративні процедури СБУ за напрямом забезпечення кібербезпеки пов'язано із захистом інформації, що становить державну таємницю та регульовані спеціальним законодавчим актом – Законом України «Про державну таємницю». В документі зазначено, що Служба є спеціальним уповноваженим державним органом у сфері забезпечення охорони державної таємниці. Відомство має право контролювати стан охорони державної таємниці в усіх державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, а також у зв'язку з виконанням цих повноважень одержувати безоплатно від них інформацію з питань забезпечення охорони державної таємниці. Висновки Служби безпеки України, викладені в актах офіційних перевірок за результатами контролю стану охорони державної таємниці, є обов'язковими для виконання посадовими особами підприємств, установ та організацій незалежно від їх форм власності. Крім зазначеного, СБУ надає дозволи на провадження діяльності, пов'язаної з державою таємницею та режим секретності (Про державну таємницю, 1994).

Висновки. Отже, незважаючи на широкий суб'єктний склад забезпечення кібербезпеки, який включає велику кількість різноманітних державних, правоохоронних, військових та інших органів, безпосередньо

суб'єктами реалізації саме адміністративних процедур у цій сфері можна визначити лише три публічно-правові відомства: Державну службу спеціального зв'язку та захисту інформації України, Національний банк України та Службу безпеки України. Саме вони володіють спеціальними правами та обов'язками в сфері забезпечення кібербезпеки в цілому, та з питань реалізації адміністративних процедур відповідного типу, а їх правовий статус містить ознаки адміністративних органів, що передбачені Законом України «Про адміністративну процедуру».

Література:

1. Набока Л.В. Структурно-функціональне забезпечення реалізації державно-управлінських відносин на територіальному рівні: дис… канд. юрид. наук : Харків: Харківський регіональний інститут державного управління. 2008. 252 с.
2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 №2163-VIII. Відомості Верховної Ради України. 2017. №45. Ст.403.
3. Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України: постанова Кабінету міністрів України від 23.09.2014 №411. Офіційний вісник України. 204. №73. Ст.2066.
4. Про державну таємницю: Закон України від 21.01.1994 №3855-XII. Відомості Верховної Ради України. 1994. №16. Ст.93.
5. Про адміністративну процедуру: Закон України від 17.02.2022 №2073-IX. Відомості Верховної Ради України. 2023. №15. Ст.50.

References:

1. Naboka, L.V. (2008). Strukturno-funktsionalne zabezpechennia realizatsii derzhavno-upravlinskykh vidnosyn na terytorialnomu rivni [Structural and functional support for the implementation of state-administrative relations at the territorial level]: dys… kand. yuryd. nauk : Kharkiv: Kharkivskyi rehionalnyi instytut derzhavnoho upravlinnia. 2008. 252 s. [in Ukrainian].
2. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy [On the main principles of ensuring cyber security of Ukraine: Law of Ukraine] vid 05.10.2017 №2163-VIII. Vidomosti Verkhovnoi Rady Ukrainy. 2017. №45. St.403. [in Ukrainian].
3. Pro zatverdzhennia Polozhennia pro Administratsiiu Derzhavnoi sluzhby spetsialnoho zviazku ta zakhystu informatsii Ukrainy: postanova Kabinetu ministriv Ukrainy [On the approval of the Regulation on the Administration of the State Service of Special Communication and Information Protection of Ukraine: Resolution of the Cabinet of Ministers of Ukraine] vid 23.09.2014 №411. Ofitsiinyi visnyk Ukrainy. 204. №73. St.2066. [in Ukrainian].
4. Pro derzhavnu taiemnytsiu: Zakon Ukrainy [On state secrets: Law of Ukraine] vid 21.01.1994 №3855-KhII. Vidomosti Verkhovnoi Rady Ukrainy. 1994. №16. St.93. [in Ukrainian].
5. Pro administratyvnu protseduru: Zakon Ukrainy [On administrative procedure: Law of Ukraine] vid 17.02.2022 №2073-IKh. Vidomosti Verkhovnoi Rady Ukrainy. 2023. №15. St.50. [in Ukrainian].