**НІКОЛАЙЧИК О. С.**
здобувач
*(Науково-дослідний інститут публічного права)*

**УДК 342.9**
**DOI https://doi.org/10.32842/2078-3736/2021.4.39**

# АДМІНІСТРАТИВНІ ПРОЦЕДУРИ, ПОВ'ЯЗАНІ ЗІ ЗМІСТОМ ІНФОРМАЦІЇ, ЩО ОБРОБЛЯЄТЬСЯ В КОМУНІКАЦІЙНИХ АБО В ТЕХНОЛОГІЧНИХ СИСТЕМАХ

Актуальність статті полягає в тому, що у сучасному світі, де значна частина особистої інформації зберігається та передається в цифровому вигляді, забезпечення конфіденційності та цілісності цих даних є обов'язком держави. Невиконання цього завдання може призвести до масових порушень приватності, шахрайства та інших видів злочинної діяльності, що завдасть серйозної шкоди як окремим громадянам, так і суспільству в цілому. На сьогоднішній день забезпечення кібербезпеки України відбувається за допомогою різноманітних публічно-правових інструментів. Одними з них є адміністративні процедури пов'язані із змістом інформації, що обробляється в комунікаційних або в технологічних системах. Це особливий різновид діяльності уповноважених суб'єктів, який відрізняється специфікою нормативно-правового регулювання та внутрішнім змістом. Метою статті є охарактеризувати адміністративні процедури, пов'язані із змістом інформації, що обробляється в комунікаційних або в технологічних системах. У статті, спираючись на аналіз наукових поглядів вчених та норм чинного законодавства, запропоновано авторське визначення поняття адміністративних процедур, пов'язаних із змістом інформації, що обробляється в комунікаційних або в технологічних системах. Виділено коло відповідних процедур та надано їм змістовну характеристику. Підкреслено, що основними суб'єктами реалізації цих процедур виступають Державна служба спеціального зв'язку і захисту інформації України та Національний банк України. Зроблено висновок, що адміністративні процедури пов'язані із змістом інформації, що обробляється в комунікаційних або в технологічних системах, становлять спеціальний набір форм та методів діяльності у сфері забезпечення кібербезпеки в Україні. Основними суб'єктами їх реалізації є Державна служба спеціального зв'язку і захисту інформації України та Національний банк України. Ключове призначення досліджуваних процедур полягає в організації та забезпеченні дієвого захисту інформації з обмеженим доступом, яка стосується діяльності держави та банківської системи в процесі обробки та передачі певної інформації у технологічних та телекомунікаційних системах. Зміст здійснення таких процедур включає в себе ряд оціночних, моніторингово-сканувальних, перевірочних, контрольних та експертно-дослідницьких заходів, реалізація яких дозволяє підтримувати ефективну дієздатність та безпечність роботи вищевказаних системи.

***Ключові слова:*** *адміністративні процедури, кібербезпека, кіберпростір, адміністративні процедури, комунікаційні системи, технологічні системи.*

**Nikolaichyk O. S. Administrative procedures related to the content of information processed in communication or technological systems**

Administrative procedures related to the content of information processed in communication or technological systems. The relevance of the article lies in the fact that in today's world, where a significant part of personal information is stored and transmitted in digital form, ensuring the confidentiality and integrity of this data is the responsibility of the state. Failure to accomplish this task can lead to massive privacy violations, fraud, and other types of criminal activity that will cause serious harm to both individual citizens and society as a whole. Today, Ukraine's cyber security is ensured with the help of various public legal instruments. One of them are administrative procedures related to the content of information processed in communication or technological systems. This is a special type of activity of authorized entities, which differs in the specifics of regulatory and legal regulation and internal content. The purpose of the article is to describe administrative procedures related to the content of information processed in communication or technological systems. In the article, based on the analysis of the scientific views of scientists and the norms of the current legislation, the author's definition of the concept of administrative procedures related to the content of information processed in communication or technological systems is proposed. A circle of relevant procedures was highlighted and a meaningful description was given to them. It is emphasized that the main subjects of the implementation of these procedures are the State Service for Special Communication and Information Protection of Ukraine and the National Bank of Ukraine. It was concluded that administrative procedures related to the content of information processed in communication or technological systems constitute a special set of forms and methods of activity in the field of cyber security in Ukraine. The main subjects of their implementation are the State Service for Special Communications and Information Protection of Ukraine and the National Bank of Ukraine. The key purpose of the investigated procedures is to organize and ensure effective protection of information with limited access, which concerns the activities of the state and the banking system in the process of processing and transmitting certain information in technological and telecommunication systems. The content of the implementation of such procedures includes a number of evaluation, monitoring and scanning, verification, control, and expert-research activities, the implementation of which allows maintaining the effective performance and safety of the above-mentioned system.

***Key words:*** *administrative procedures, cyber security, cyberspace, administrative procedures, communication systems, technological systems.*

**Постановка проблеми.** У сучасному світі, де значна частина особистої інформації зберігається та передається в цифровому вигляді, забезпечення конфіденційності та цілісності цих даних є обов'язком держави. Невиконання цього завдання може призвести до масових порушень приватності, шахрайства та інших видів злочинної діяльності, що завдасть серйозної шкоди як окремим громадянам, так і суспільству в цілому. На сьогоднішній день забезпечення кібербезпеки України відбувається за допомогою різноманітних публічно-правових інструментів. Одними з них є адміністративні процедури пов’язані із змістом інформації, що обробляється в комунікаційних або в технологічних системах. Це особливий різновид діяльності уповноважених суб’єктів, який відрізняється специфікою нормативно-правового регулювання та внутрішнім змістом.

**Стан дослідження**. Окремі проблемні питання, пов’язані із реалізацією адміністративних процедур у різних сферах суспільного життя, досліджувались у наукових працях: І.В. Бойко, О.Т. Зими, О.М. Соловйової, В.В. Галунька, Т.О. Коломоєць, Р.С. Мельника,

Ю.Ю. Басова та інших. Однак, незважаючи на значний теоретичний доробок, у науковій літературі фактично відсутні комплексні теоретичні опрацювання проблеми реалізації адміністративних процедур, пов'язаних зі змістом інформації, що обробляється в комунікаційних або в технологічних системах.

**Саме тому метою статті є** охарактеризувати адміністративні процедури, пов'язані із змістом інформації, що обробляється в комунікаційних або в технологічних системах.

**Виклад основного матеріалу.** В першу чергу варто зауважити, що досліджувані адміністративні процедури, пов'язані із змістом інформації, що обробляється в комунікаційних або в технологічних системах мають досить специфічний та вузький зміст, обумовлений тим фактом, що згідно до статті 2 Закону України «Про основні засади забезпечення кібербезпеки України», положення цього нормативного документу не поширюються на відносини та послуги, пов'язані із змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах [1]. Разом із цим, підзаконна нормативно-правова база показує, що відповідні адміністративні процедури не тільки існують, але й активно застосовуються в сфері кібербезпеки. На нашу думку, виникаюча в даному випадку колізія вирішується з огляду на сутність категорії «інформація».

Закон України «Про інформацію» визначає зазначений термін, як будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Згідно до розділу ІІ Закону, за змістом інформація поділяється на такі різновиди: інформація про фізичну особу; інформація довідково-енциклопедичного характеру; інформація про стан довкілля (екологічна інформація); інформація про товар (роботу, послугу); науково-технічна інформація; податкова інформація; правова інформація; статистична інформація; соціологічна інформація; критична технологічна інформація; інші види інформації. Крім того, доступ до інформації може бути обмеженим, що охоплюють такі види останньої, як конфіденційна, таємна та службова. Конфіденційною є інформація про фізичну особу, інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, а також інформація, визнана такою на підставі закону. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, якщо інше не встановлено законом. Порядок віднесення інформації до таємної або службової, а також порядок доступу до неї регулюються законами [2].

Таким чином, інформація – це дані і відомості про певний об'єкт, явища або факти дійсності, які можуть приймати, усну, письмову, електронну чи іншу форму. Зміст інформації визначає її різновид та рівень доступу до неї. Відповідно, дані та відомості конфіденційного, таємного чи службового характеру обмежені для широкого загалу та додатково охороняються законом. Разом із цим, інформація, у тому числі, обмеженого доступу, зберігається та існує на відповідних джерелах, а також передається між різноманітними суб'єктами вербально, документально та, в тому числі, за рахунок технологічних та комунікаційних систем. Нормативні вимоги щодо порядку обробки та передачі відомостей і даних прямо залежать від змісту останніх. Зокрема, вони більш суворіші у контексті руху інформації з обмеженим доступом.

Отже, адміністративні процедури у сфері кібербезпеки, пов'язані зі змістом інформації, що обробляється в комунікаційних або в технологічних системах – це окрема група впорядкованих дій, заходів та процесів, що реалізуються уповноваженими суб'єктами та спрямовані на збір, обробку, зберігання, передачу та захист інформації у відповідних інформаційно-комунікаційних та технологічних системах. Ці процедури спрямовані на забезпечення конфіденційності, цілісності та доступності даних, а також на запобігання їх несанкціонованому доступу, розкриттю, модифікації або знищенню інформації.

Більшість подібних процедур реалізується в діяльності Державної служби спеціального зв'язку та захисту інформації України. Наприклад, відповідно до Наказу Держспецзв'язку «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних систе-

мах» від 02.12.2014 №660 проводиться спеціальна процедура оцінки. Останню документом визначено, як сукупність заходів, спрямованих на виявлення загроз державним інформаційним ресурсам та запобігання несанкціонованим діям щодо інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах. Оцінка стану захищеності здійснюється з метою виявлення існуючих загроз державним інформаційним ресурсам в ІКС і є складовою частиною заходів із захисту інформації. Об'єктом оцінки стану захищеності є державні інформаційні ресурси, які обробляються в ІКС, незалежно від наявності в таких ІКС комплексної системи захисту інформації [3].

Схожою є процедура сканування інформаційних ресурсів розміщених в інтернеті на предмет вразливостей, яка проводиться згідно до Наказу Держспецзв'язку «Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті» від 15.01.2016 №20. Згідно до положень цього Наказу, сканування є однією з форм проведення оцінки стану захищеності інформації в інформаційно-комунікаційних системах і полягає у дистанційній перевірці ІКС, яка забезпечує розміщення державних інформаційних ресурсів у мережі Інтернет, на предмет виявлення в ній вразливостей, які створюють передумови до порушення конфіденційності, цілісності та доступності інформації та державних інформаційних ресурсів, що обробляються ІКС, або спостережності самої ІКС. Об'єктами сканування є ІКС, в якій обробляються розміщені в Інтернеті, її окремі елементи, програмні і програмно-апаратні засоби, що застосовані в ІКС, незалежно від наявності побудованої комплексної системи захисту інформації та/або системи управління інформаційною безпекою з підтвердженою відповідністю [4].

Адміністративні процедури, пов'язані із змістом інформації, що обробляється в комунікаційних або в технологічних системах, притаманні не тільки Держспецзв'язку, але й в діяльності Національного банку України. Зокрема, до аналізованої в статті групи відноситься процедура контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг. Загально, контроль – це функція управління. Основною метою контролю є виявлення недоліків та їх своєчасне виправлення шляхом корегування дій об'єкту контролю. Хоча контрольні заходи здійснюються шляхом різноманітних планових і позапланових перевірок, ревізій, обстежень, зазначена категорія є комплексною функцією і не зводиться лише до процесу перевірки. Контроль можна поділити на такі стадії: 1) перевірка відповідності фактично вчинюваних дій запланованим на стадії планування та виявлення недоліків; 2) оцінювання недоліків щодо можливості їх впливу на подальшу діяльність об'єкту контролю; 3) розроблення пропозицій, рекомендацій та заходів для виправлення виявлених недоліків. Контроль здійснюється на принципах підконтрольності та підзвітності одних суб'єктів щодо інших, рівності прав і законних інтересів усіх суб'єктів господарювання, об'єктивності та неупередженості здійснення контролю, наявності підстав, визначених законом, для здійснення контролю; відкритості, прозорості, плановості й системності контролю тощо [5, с.253-254].

Правовою основою контрольної діяльності здійснюваної НБУ в аспекті забезпечення кібербезпеки є Постанова Правління НБУ «Про затвердження Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг» від 16.01.2021 №4. Положення встановлює: по-перше, порядок організації та здійснення Національним банком України заходів контролю за дотриманням банками вимог законодавства, яке регулює відносини у сферах кіберзахисту, інформаційної безпеки та електронних довірчих послуг, а також нормативно-правових актів Національного банку, що здійснюється на виконання покладених на Національний банк наглядових функцій; по-друге, вимоги щодо проведення банком самооцінки стану інформаційної безпеки/кіберзахисту [6].

Національний банк здійснює контроль з метою: 1) оцінювання ефективності функціонування системи управління інформаційною безпекою банку; 2) оцінювання повноти виконання банком вимог нормативно-правових актів Національного банку з питань інформаційної безпеки, кіберзахисту; 3) оцінювання рівня управління ризиками інформаційної безпеки/

кіберризиками банком і системи внутрішнього контролю, яка функціонує на всіх організаційних рівнях, за напрямами діяльності, що перевіряються; 4) прийняття засвідчувальним центром рішення про внесення відомостей про кваліфікованого надавача електронних довірчих послуг до Довірчого списку; 5) перевірки виконання вимог нормативно-правових актів з питань надання кваліфікованих електронних довірчих послуг кваліфікованим надавачем електронних довірчих послуг, відомості про якого внесені до Довірчого списку за поданням засвідчувального центру. Національний банк здійснює контроль шляхом проведення: 1) виїзних заходів контролю у формі перевірок; 2) безвиїзних заходів контролю. Перевірка банку проводиться на підставі розпорядчого акту Національного банку про проведення планової перевірки, у якому зазначаються найменування банку, що перевіряється, підстава для проведення перевірки, дата перевірки, терміни проведення перевірки (дати початку і закінчення), склад інспекційної групи та куратор перевірки (із зазначенням прізвищ, імен, по батькові, посад та номерів службових посвідчень). Разом з цим, НБУ має право проводити позапланову перевірку з метою термінового встановлення причин, обставин, масштабу негативного впливу на життєдіяльність банку та/або банківську систему в разі отримання документально підтвердженої інформації про: 1) інциденти інформаційної безпеки/кіберінциденти, наслідком яких є реалізована загроза для безпеки інформації банку та його клієнтів; 2) інциденти інформаційної безпеки/кіберінциденти, наслідки яких можуть спричинити системний ризик у банківській системі; 3) порушення вимог законодавства у сфері електронних довірчих послуг. За результатами проведення планової або позапланової перевірки складається довідка про перевірку у двох примірниках, підписується членами інспекційної групи, куратором перевірки, керівником банку [6].

**Висновки.** Підбиваючи підсумок наукового дослідження можемо узагальнити, що адміністративні процедури пов'язані із змістом інформації, що обробляється в комунікаційних або в технологічних системах, становлять спеціальний набір форм та методів діяльності у сфері забезпечення кібербезпеки в Україні. Основними суб'єктами їх реалізації є Державна служба спеціального зв'язку і захисту інформації України та Національний банк України. Ключове призначення досліджуваних процедур полягає в організації та забезпеченні дієвого захисту інформації з обмеженим доступом, яка стосується діяльності держави та банківської системи в процесі обробки та передачі певної інформації у технологічних та телекомунікаційних системах. Зміст здійснення таких процедур включає в себе ряд оціночних, моніторингово-сканувальних, перевірочних, контрольних та експертно-дослідницьких заходів, реалізація яких дозволяє підтримувати ефективну дієздатність та безпечність роботи вищевказаних системи.

**Список використаних джерел:**

1. Про основні засади забезпечення кібербезпеки України: закон від 05.10.2017 №2163-VIII. *Відомості Верховної Ради України*. 2017. №45. Ст.403.

2. Про інформацію: закон від 02.10.1992 №2657-XII. *Відомості Верховної Ради України*. 1992. №48. Ст.650.

3. Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах: наказ від 02.12.2014 №660. *Офіційний вісник України*. 2015. №12. Ст.323.

4. Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті: наказ, порядок від 15.01.2016 №20. *Офіційний вісник України*. 2016. №17. Ст.695.

5. Курко О.М. Контроль за реалізацією адміністративно-правових форм органами прокуратури. Адміністративне право і процес. 2014. №2(8). С.253-261.

6. Про затвердження Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг: постанова, положення від 16.01.2021 №4. *Офіційний вісник України*. 2021. №11. Ст.470.