НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ПУБЛІЧНОГО ПРАВА
НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ПУБЛІЧНОГО ПРАВА

Кваліфікаційна наукова
праця на правах рукопису

НІКОЛАЙЧИК ОЛЕКСАНДР СЕРГІЙОВИЧ

УДК 342.9 (477)

ДИСЕРТАЦІЯ

АДМІНІСТРАТИВНІ ПРОЦЕДУРИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

12.00.07 – адміністративне право і процес;
фінансове право; інформаційне право

Подається на здобуття наукового ступеня кандидата юридичних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело _____О.С. Ніколайчик

Науковий керівник **Дрозд Олексій Юрійович**, доктор юридичних наук, професор

Київ – 2024

АНОТАЦІЯ

Ніколайчик О.С. Адміністративні процедури забезпечення кібербезпеки в Україні. – *Кваліфікаційна наукова праця на правах рукопису.*

Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». – Науково-дослідний інститут публічного права, Науково-дослідний інститут публічного права, Київ, 2024.

У дисертації наведено теоретичне узагальнення та нове розв'язання наукового завдання, яке полягає у тому, щоб розкрити сутність, зміст та особливості адміністративних процедур забезпечення кібербезпеки в Україні, а також спираючись на позитивний вітчизняний та зарубіжний досвід розробити пропозиції та надати рекомендації спрямовані на вдосконалення нормативно-правового регулювання здійснення відповідної діяльності.

Встановлено, що забезпечення кібербезпеки – це реалізований спеціально уповноваженими суб'єктами комплекс заходів, технологій, процесів і практик, що спрямовано на захист інформаційних систем, мереж, даних і програм від несанкціонованого доступу, використання, розкриття, зміни, руйнування або втрати. Така діяльність включає забезпечення конфіденційності, цілісності та доступності інформації, а також протидію кіберзагрозам і кібератакам з боку зловмисників у цифровому просторі.

Констатовано, що кібербезпека як об'єкт адміністративно-правового регулювання характеризується наступними особливостями: по-перше, представляє собою особливу групу правовідносин, що виникають у специфічній сфері суспільного життя; по-друге, обумовлює необхідність здійснення низки різноманітних дій та заходів спеціально уповноваженими органами державної влади, а також приватними суб'єктами; по-третє, відповідна діяльність, переважно, регулюється нормами адміністративної галузі права; по-четверте, є сферою реалізації різноманітних процедур, які носять адміністративний характер.

З’ясовано, що адміністративні процедури у сфері забезпечення кібербезпеки – це визначений законодавством України порядок дій, які реалізуються спеціально уповноваженими суб’єктами у напрямку забезпечення і захисту прав та законних інтересів фізичних та юридичних осіб, а також з метою реалізації публічних повноважень у сфері використання комунікаційних, технологічних систем, електронно-обчислювальної (комп’ютерної) техніки, програмного забезпечення та взаємодії у кіберпросторі.

Доведено, що особливостями адміністративних процедур у сфері забезпечення кібербезпеки є наступні: по-перше, особлива сфера реалізації, а також предмет з приводу якого виникають відповідні суспільні відносини; по-друге, реалізовувати відповідні процедури мають право виключно спеціально уповноважені суб’єкти, посадові особи яких володіють особливим набором професійних знань, умінь та навичок; по-третє, наявність спеціального набору нормативно-правових засад їх реалізації; по-третє, переважна більшість адміністративних процедур пов'язані з обробкою персональних даних, що вимагає дотримання вимог законодавства про захист персональних даних; по-четверте, наявність підвищеного рівня відповідальності суб’єктів, що відповідні процедури реалізовують; по-п’яте, відповідні процедури застосовуються у різних сферах забезпечення кібербезпеки, що обумовлює наявність їх різновидів.

Обґрунтовано, 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.

Зазначено, що правове регулювання реалізації адміністративних процедур у сфері забезпечення кібербезпеки – це здійснюваний за допомогою норм права регулюючий та упорядковуючий вплив на суспільні відносини, які виникають у досліджуваній сфері суспільного життя. Відповідний вплив здійснюється також за рахунок спеціальних юридичних інструментів і спрямований на забезпечення відповідності їх поведінки нормам чинного законодавства.

Аргументовано, що 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.

Встановлено, що державна таємниця є особливо важливим різновидом інформації в найбільш суспільно-значимих сферах (оборони, економіки, науки і техніки, міжнародних відносинах, галузі державної безпеки, охорони правопорядку, тощо), порядок доступу до якої обмежено законодавством України з метою недопущення її несанкціонованого розголошення, що матиме шкідливі наслідки для національної безпеки.

Акцентовано увагу на тому, що дозвіл – це надане в установленому законодавством порядку державою індивідуальне суб'єктивне право займатись відповідним видом діяльності, що має документальне підтвердження офіційного зразка. Дозвіл на провадження діяльності, пов'язаної із державною таємницею позначає право відповідного суб'єкта опрацьовувати секретну інформацію, у тому числі за допомогою комунікаційних та технологічних систем. Тобто, саме наявність дозволу

показує, чи розповсюджуються на відповідну юридичну та/або фізичну особу обов'язки та обмеження у сфері роботи із інформацією таємного характеру, а також необхідність застосування щодо його діяльності особливих заходів забезпечення кібербезпеки.

Обґрунтовано, що комунікаційні системи, які не взаємодіють з публічними мережами електронних комунікацій, є закритими або ізольованими, оскільки вони призначені для передачі інформації в межах певної організації або групи користувачів без підключення до загальнодоступних мереж, зокрема Інтернету.

Встановлено, що адміністративні процедури захисту комунікаційних систем, які не взаємодіють з публічними мережами електронних комунікацій, переважно, носять внутрішньо-системний характер та реалізуються безпосередньо користувачами відповідних систем, а також спрямовані на забезпечення безпеки інформації та запобігання несанкціонованому доступу або витоку даних в рамках ізольованих інформаційних мереж. Ці процедури є частиною загальної системи безпеки, що забезпечує належний рівень захисту від загроз як зсередини, так і ззовні організації.

Узагальнено, що політика інформаційної безпеки є ключовою адміністративною процедурою, яка забезпечує захист комунікаційних систем, що не взаємодіють з публічними мережами електронних комунікацій. Вона визначає комплекс заходів і правил, спрямованих на збереження конфіденційності, цілісності та доступності інформації в таких системах, а також на запобігання несанкціонованому доступу, порушенням роботи або втраті даних.

Встановлено, що стандарти забезпечення кібербезпеки – це набір правил, рекомендацій і вимог, що визначають методи і заходи для захисту інформаційних систем, мереж та даних від кібератак, несанкціонованого доступу, витоків даних та інших загроз кібербезпеці. Ці стандарти розроблені

для встановлення загальних практик і політик, які організації можуть використовувати для забезпечення захисту своїх цифрових активів.

Обґрунтовано, що забезпечення кібербезпеки – це безперебійний процес, який вимагає постійного оновлення та вдосконалення. Саме тому, важливим завданням законодавця, а також приватних осіб в Україні є постійне оновлення (технологічне, професійне, ресурсне, тощо) системи безпеки відповідно до нових загроз та вимог міжнародних стандартів.

Запропоновано розробити та прийняти «Концепцію розвитку системи забезпечення кібербезпеки в Україні», метою якої має бути створення та підтримка ефективного, стійкого та безпечного кіберсередовища, яке б захищало національні інтереси, сприяло сталому розвитку цифрової економіки та забезпечувало права та свободи громадян в інформаційному просторі.

Доведена необхідність доопрацювання «Стратегії кібербезпеки України», яка повинна враховувати виклики та реалії сьогодення, а також набутий досвід кібератак на кіберпростір України в останні три роки.

Підкреслено, що ефективне функціонування системи кібербезпеки України безпосередньо залежить від адекватного фінансового та матеріально-технічного забезпечення суб'єктів, що реалізують адміністративні процедури в цій сфері. Для досягнення оптимальних результатів необхідно вжити комплекс заходів, спрямованих на покращення матеріально-технічної бази та забезпечення необхідного фінансування. В даному контексті першочерговим кроком є проведення комплексного аналізу потреб суб'єктів у фінансових та матеріально-технічних ресурсах.

Ключові слова: кібербезпека, кіберпростір, об’єкт, адміністративно-правове регулювання, адміністративні процедури, суб’єкт, інформація, зміст інформації, комунікаційні системи, технологічні системи, державна таємниця, обробка інформації, стандарти, міжнародні стандарти, вдосконалення, адміністративне законодавство.

SUMMARY

Nikolaichyk O.S. Administrative Procedures for Ensuring Cybersecurity in Ukraine. – *Qualification scientific work on the rights of the manuscript.*

Thesis for obtaining a scientific degree of Candidate of Juridical Science in specialty 12.00.07 «Administrative Law and Procedure; Financial Law; Information Law». – Scientific Institute of Public Law, Scientific Institute of Public Law, Kyiv, 2024.

The thesis provides a theoretical overview and a new solution to the scientific task to reveal the essence, content and features of administrative procedures for ensuring cybersecurity in Ukraine, and, based on positive domestic and foreign experience, to develop proposals and provide recommendations aimed at improving the legal and regulatory framework for implementing the relevant activities.

It is established that cybersecurity is a set of measures, technologies, processes and practices implemented by specially authorised entities aimed at protecting information systems, networks, data and programs from unauthorised access, use, disclosure, alteration, destruction or loss. Such activities include ensuring the confidentiality, integrity and availability of information, as well as countering cyber threats and cyber-attacks by intruders in the digital space.

It is stated that cybersecurity as an object of the administrative and regulatory framework is characterised by the following features: first, it is a special group of legal relations arising in a specific sector of public life; second, it requires a number of various actions and measures to be taken by specially designated public authorities and private entities; third, the relevant activities are mainly regulated by the provisions of administrative law; fourth, it is the scope of implementing various procedures which are administrative in nature.

It is established that administrative procedures for ensuring cybersecurity are a set of actions determined by the legislation of Ukraine and implemented by specially authorised entities to ensure and protect the rights and legitimate interests of individuals and legal entities, as well as with the aim of exercising public powers in

the field of communication, technological systems, electronic computing (computer) equipment, software and interaction in cyberspace.

It is proved that the specific features of administrative procedures to ensure cybersecurity are as follows: first, a special scope of implementation, as well as the subject matter over which the relevant public relations arise; second, only specially authorised entities, officials of which have a special set of professional knowledge, skills and abilities, are entitled to implement the relevant procedures; third, there is a special set of regulatory and legal principles for their implementation; third, the vast majority of administrative procedures are related to the processing of personal data, which requires compliance with the requirements of the legislation on personal data protection; fourth, the entities implementing the relevant procedures have an increased level of responsibility; fifthly, the relevant procedures are applied in different sectors of cybersecurity, which leads to the existence of their varieties.

It is proved that the actors in the implementation of administrative procedures for ensuring cybersecurity should be understood as a set of specially designated public authorities (represented by their officials) which, in accordance with current legislation, are empowered and have the necessary competence to implement actions and measures aimed at creating the necessary conditions for the protection of information systems and networks, as well as coordinating actions to prevent, detect and respond to cyber threats.

It is noted that the legal framework for the implementation of administrative procedures for ensuring cybersecurity is a regulatory and orderly impact on social relations arising in the field of public life under study, made by means of legal provisions. The relevant impact is also exercised through special legal instruments and is aimed at ensuring that their conduct complies with the provisions of current legislation.

It is proved that administrative procedures for cybersecurity related to the content of information processed in communication or technological systems are a separate group of orderly actions, measures and processes implemented by authorised

entities and aimed at collecting, processing, storing, transmitting and protecting information in the relevant information, communication and technological systems. These procedures are aimed at ensuring the confidentiality, integrity and availability of data, as well as preventing unauthorised access, disclosure, modification or destruction of information.

It is established that state secrets are a particularly important type of information in the most socially important sectors (defence, economy, science and technology, international relations, state security, law enforcement, etc.), the procedure for access to which is restricted by Ukrainian legislation in order to prevent its unauthorised disclosure, which would have harmful consequences for national security.

The author emphasises that a permit is an individual subjective right granted by the State in accordance with the procedure established by law to engage in a relevant type of activities which has an official documentary confirmation. A permit for activities related to state secrets means the right of the relevant entity to process classified information, including through communication and technological systems. In other words, it is the existence of a permit that shows whether the relevant legal entity and/or individual is subject to obligations and restrictions in the field of processing classified information, as well as the need to apply special cybersecurity measures to its activities.

It is suggested that communication systems which do not interact with public electronic communication networks are closed or isolated, since they are designed to transmit information within a particular organisation or group of users without connecting to public networks, in particular, the Internet.

It is established that administrative procedures for the protection of communication systems that do not interact with public electronic communication networks are mainly of an intra-system nature and are implemented directly by users of the relevant systems, and are aimed at ensuring information security and preventing unauthorised access or data leakage within isolated information networks. These

procedures are part of an overall security system that ensures an adequate level of protection against threats from both inside and outside the organisation.

It can be summarised that the information security policy is a key administrative procedure that ensures the protection of communication systems that do not interact with public electronic communication networks. Вона визначає комплекс заходів і правил, спрямованих на збереження конфіденційності, цілісності та доступності інформації в таких системах, а також на запобігання несанкціонованому доступу, порушенням роботи або втраті даних.

It is established that cybersecurity standards are a set of rules, recommendations and requirements that define methods and measures to protect information systems, networks and data from cyberattacks, unauthorised access, data leaks and other cybersecurity threats. These standards are designed to establish common practices and policies that organisations can use to ensure the protection of their digital assets.

It is proved that ensuring cybersecurity is an ongoing process that requires constant updating and improvement. That is why an important task of the legislator as well as individuals in Ukraine is to constantly update (technological, professional, resource, etc.) the security system in accordance with new threats and requirements of international standards.

The author proposes to develop and adopt a ‘Concept for the Development of the Cybersecurity System in Ukraine’, which should aim to create and maintain an effective, sustainable and secure cyber environment that would protect national interests, promote the sustainable development of the digital economy and ensure the rights and freedoms of citizens in the information space.

It is proved that the ‘Cybersecurity Strategy of Ukraine’ needs to be finalised, considering the challenges and realities of today, as well as the experience of cyberattacks on Ukraine's cyberspace over the past three years.

It is emphasised that the effective functioning of Ukraine's cybersecurity system directly depends on adequate financial and logistical support of entities implementing administrative procedures in this field. To achieve optimal results, a set

of measures should be taken to improve the logistics and ensure the necessary funding. In this context, the first step is to conduct a comprehensive analysis of the financial and logistical needs of the entities.

Keywords: cybersecurity, cyberspace, object, administrative and regulatory framework, administrative procedures, actor, information, information content, communication systems, technological systems, state secret, information processing, standards, international standards, improvement, administrative legislation.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких висвітлено основні наукові результати дисертації:

1. Ніколайчик О. С. До проблеми визначення поняття кібербезпеки як об'єкта адміністративно-правового регулювання. *Юридична наука*. 2020. № 1(103). Т. 2. С. 169–172.

2. Ніколайчик О. С. Адміністративні процедури, пов'язані із захистом інформації, що становить державну таємницю, комунікаційних та технологічних систем, призначених для її оброблення. *Юридична наука*. 2020. № 3(105). Т. 2. С. 61–67.

3. Ніколайчик О. С. Адміністративні процедури, пов'язані зі змістом інформації, що обробляється в комунікаційних або в технологічних системах. *Право і суспільство.* 2021. № 6. С. 207–211.

4. Ніколайчик О. С. Суб'єкти реалізації адміністративних процедур у сфері забезпечення кібербезпеки. *KELM*. 2022. № 7 (51). С. 343–346 (Республіка Польща).

5. Ніколайчик О. С. До характеристики системи правового регулювання реалізації адміністративних процедур у сфері забезпечення кібербезпеки. *Юридичний науковий електронний журнал.* 2023. № 6. С. 850–852.

які засвідчують апробацію матеріалів дисертації:

6. Ніколайчик О. С. Види адміністративних процедур у сфері забезпечення кібербезпеки. *Актуальні проблеми взаємодії правової науки та практики її застосування*: матеріали Міжнар. наук.-практ. конф. (Київ, 16–17 берез. 2022 р.). Київ: Наук.-дослід. ін-т публіч. права, 2022. С. 118–120.

7. Ніколайчик О. С. До характеристики адміністративних процедур забезпечення кібербезпеки, які не пов'язані із проведенням заходів захисту інформації у комунікаційних, технологічних системах, обробкою та обміном інформацією в кіберпросторі. *Науково-практичні засади розвитку*

юридичної науки на сучасному етапі державотворення: матеріали Міжнар. наук.-практ. конф. (Київ, 15–16 лют. 2023 р.). Київ: Наук.-дослід. ін-т публіч. права, 2023. С. 117–121.

8. Ніколайчик О. С. Поняття адміністративних процедур у сфері забезпечення кібербезпеки. *Реформування українського законодавства: проблемні питання та шляхи їх вирішення*: матеріали Міжнар. наук.-практ. конф. (Київ, 7–8 лют. 2024 р.). Київ: Наук.-дослід. ін-т публіч. права, 2024. С. 171–173.

ЗМІСТ

ВСТУП

Обґрунтування вибору теми дослідження. Протягом останніх десятиліть цифрові технології проникли в усі сфери суспільного життя та стали невід'ємною складовою функціонування держави й суспільства. Водночас розвиток останніх спричинив появу низки ризиків, пов'язаних із захистом даних та інформації, яка міститься в інформаційному просторі. У зв'язку з цим, важливим завданням світової спільноти, зокрема українського законодавця, стало створення належного рівня забезпечення кібербезпеки, за якого інтересам держави, а також правам і свободам фізичних та юридичних осіб у кіберпросторі не буде нічого загрожувати. Особливо ця проблема загострилася в умовах повномасштабного вторгнення російської федерації, яка постійно здійснює не лише атаки на критичну інфраструктуру нашої країни, а й кібератаки. З огляду на зазначене, проблема кібербезпеки має важливе значення для забезпечення безперервності роботи безпекового сектору нашої держави, а також її критичної інфраструктури, яка охоплює енергетичні мережі, водопостачання, фінансово-економічну систему і транспорт. Кібератаки на ці системи здатні призводити до значних перебоїв у їхній роботі, що може викликати економічний хаос, порушення громадського порядку та навіть загрожувати життю громадян.

Забезпечення кібербезпеки є складною за своєю сутністю та змістом діяльністю, що передбачає реалізацію низки процедур, які переважно мають адміністративний характер. Ці процедури визначають правила і порядок реагування на кібератаки, встановлюють вимоги до захисту інформації та забезпечують узгодженість дій між різними суб'єктами у сфері кібербезпеки. Таким чином, дотримання останніх має важливе значення з точки зору забезпечення законності й ефективності реалізації діяльності щодо забезпечення кібербезпеки в Україні.

Зв'язок теми дисертації із сучасними дослідженнями. Окремі проблемні аспекти, пов'язані із забезпеченням кібербезпеки в Україні, у своїх наукових працях розглядали: О. А. Баранов, Н. Л. Березовська, І. В. Діордіца, О. В. Джафарова, О. Ю. Дрозд, Ю. В. Гаруст, Є. А. Гетьман, О. В. Задерейко, О. Ф. Кобзар, О. В. Коваленко, В. К. Колпаков, О. В. Кузьменко, В. Г. Кундеус, В. І. Курило, К. М. Куркова, Ю. П. Лісовська, Н. І. Логінова, Л. І. Луценко-Миськів, А. А. Манжула, Л. В. Набока, О. В. Олійник, Ю. В. Прокоп, Р. А. Сербин, О. О. Середа, В. І. Сіверін, Є. Ю. Соболь, Л. В. Сорока, С. М. Стежко, В. М. Столбовий, О. Г. Трофіменко, Л. С. Харченко, Р. В. Шаповал, С. І. Шевченко, Т. О. Шевченко та багато інших. Проте, попри значний теоретичний доробок, у науковій літературі недостатньо опрацьованим є питання дослідження адміністративних процедур забезпечення кібербезпеки в Україні.

Отже, наявність низки прогалин і недоліків правового та організаційного характеру, пов'язаних із реалізацією адміністративних процедур забезпечення кібербезпеки, а також відсутність комплексних наукових досліджень, присвячених вказаній проблематиці, обумовлюють актуальність і своєчасність представленої дисертаційної роботи.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження узгоджується з положеннями Стратегії інформаційної безпеки, затвердженої Указом Президента України від 28 грудня 2021 року № 685/2021; Стратегії кібербезпеки України, схваленої Указом Президента України від 26 серпня 2021 року № 447/2021; Стратегії зовнішньополітичної діяльності України, схваленої Указом Президента України від 26 серпня 2021 року № 448/2021; Цілей сталого розвитку України на період до 2030 року, затверджених Указом Президента України від 30 вересня 2019 року № 722/2019. Дисертацію виконано відповідно до плану науково-дослідної роботи Науково-дослідного інституту публічного

права «Правове забезпечення прав, свобод та законних інтересів суб'єктів публічно-правових відносин» (номер державної реєстрації 0120U105390).

Мета та завдання дослідження *Мета* дисертаційного дослідження полягає в тому, щоб на основі аналізу наукових поглядів учених, норм чинного законодавства та практики його реалізації з'ясувати сутність, зміст й особливості адміністративних процедур забезпечення кібербезпеки в Україні, а також, спираючись на позитивний вітчизняний і зарубіжний досвід, розкрити сучасні тенденції вдосконалення адміністративно-правового регулювання відповідної діяльності.

Досягнення поставленої мети зумовлює потребу у вирішенні таких *завдань*:

– схарактеризувати кібербезпеку як об'єкт адміністративно-правового регулювання;

– визначити поняття, розкрити особливості й виокремити види адміністративних процедур у сфері забезпечення кібербезпеки;

– окреслити коло суб'єктів реалізації адміністративних процедур у сфері забезпечення кібербезпеки;

– проаналізувати систему правового регулювання реалізації адміністративних процедур у сфері забезпечення кібербезпеки;

– розкрити адміністративні процедури, пов'язані зі змістом інформації, що обробляється в комунікаційних або в технологічних системах;

– схарактеризувати адміністративні процедури, пов'язані із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення;

– встановити коло адміністративних процедур захисту комунікаційних систем, які не взаємодіють з публічними мережами електронних комунікацій;

– здійснити порівняльний аналіз національних та міжнародних стандартів і практик забезпечення кібербезпеки;

– запропонувати шляхи вдосконалення правового регулювання адміністративних процедур у сфері забезпечення кібербезпеки.

Об'єктом дослідження є суспільні відносини, які виникають у процесі реалізації адміністративних процедур забезпечення кібербезпеки в Україні.

Предметом дослідження є адміністративні процедури забезпечення кібербезпеки в Україні.

Методи дисертаційного дослідження. Методологічну основу дисертаційної роботи становить сукупність загальних і спеціальних методів наукового пізнання, використання яких дало змогу комплексно підійти до виконання завдань дисертації. Так, за допомогою *логіко-семантичного* й *аналітичного* методів вдалося схарактеризувати кібербезпеку як об'єкт адміністративно-правового регулювання (підрозділ 1.1), а також визначити поняття, розкрити особливості та виокремити види адміністративних процедур у сфері забезпечення кібербезпеки (підрозділ 1.2). *Структурно-логічний* та *системно-функціональний* метод застосовано з метою окреслення кола суб'єктів реалізації адміністративних процедур у сфері забезпечення кібербезпеки (підрозділ 1.3) та узагальнення адміністративних процедур захисту комунікаційних систем, які не взаємодіють з публічними мережами електронних комунікацій (підрозділ 2.3). Метод *документального аналізу* дав змогу проаналізувати систему правового регулювання реалізації адміністративних процедур у сфері забезпечення кібербезпеки (підрозділ 1.4); розкрити адміністративні процедури, пов'язані зі змістом інформації, що обробляється в комунікаційних або в технологічних системах (підрозділ 2.1); визначити адміністративні процедури, пов'язані із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення (підрозділ 2.2). Щоб здійснити порівняльний аналіз національних та міжнародних стандартів і практик забезпечення кібербезпеки (підрозділ 3.1) було використано *порівняльно-правовий метод.* З'ясувати шляхи вдосконалення правового

регулювання адміністративних процедур у сфері забезпечення кібербезпеки (підрозділ 3.2) вдалось за допомогою методів *моделювання* та *прогнозування*.

Нормативно-правовим підґрунтям дослідження є Конституція України, міжнародні нормативно-правові акти (ратифіковані у встановленому законом порядку), а також низка законодавчих і підзаконних актів, норми яких спрямовані на регулювання адміністративних процедур забезпечення кібербезпеки в Україні.

Науково-теоретичне підґрунтя становлять праці фахівців з галузі адміністративного та інформаційного права. Крім того, було використано напрацювання фахівців з інших галузевих дисциплін, таких як теорія держави і права, теорія управління, соціологія, філософія, психологія тощо.

Інформаційну та емпіричну основу дослідження становлять періодичні видання, статистичні матеріали тощо.

Наукова новизна отриманих результатів полягає в тому, що дисертаційне дослідження є першою спробою комплексно, на монографічному рівні з'ясувати сутність та особливості адміністративних процедур забезпечення кібербезпеки в Україні в сучасних умовах, на основі чого розробити пропозиції та рекомендації, спрямовані на вдосконалення нормативно-правового регулювання відповідної діяльності. У результаті проведеного дослідження сформульовано низку нових наукових положень і висновків, основні з них такі:

вперше:

– визначено особливості адміністративних процедур у сфері забезпечення кібербезпеки, до яких віднесено такі: по-перше, особлива сфера реалізації, а також предмет, з приводу якого виникають відповідні суспільні відносини; по-друге, реалізовувати відповідні процедури мають право виключно спеціально уповноважені суб'єкти, посадові особи яких володіють набором специфічних професійних знань, умінь і навичок; по-

третє, наявність спеціального набору нормативно-правових засад їх реалізації; по-четверте, переважна більшість адміністративних процедур пов'язані з обробкою персональних даних, що вимагає дотримання вимог законодавства про захист персональних даних; по-п'яте, наявність підвищеного рівня відповідальності суб'єктів, які відповідні процедури реалізовують; по-шосте, відповідні процедури застосовуються в різних сферах забезпечення кібербезпеки, що обумовлює наявність їх різновидів;

– встановлено, що адміністративні процедури у сфері кібербезпеки, пов'язані зі змістом інформації, яку обробляють у комунікаційних або технологічних системах, становлять окрему групу впорядкованих дій, заходів і процесів, що реалізуються уповноваженими суб'єктами та спрямовані на збір, обробку, зберігання, передачу та захист інформації у відповідних інформаційно-комунікаційних і технологічних системах. Ці процедури спрямовані на забезпечення конфіденційності, цілісності та доступності даних, а також на запобігання їх несанкціонованому доступу, розкриттю, модифікації або знищенню інформації;

– окреслено адміністративні процедури захисту комунікаційних систем, які не взаємодіють з публічними мережами електронних комунікацій, до яких віднесено такі: авторизацію та аутентифікацію визначеного переліку користувачів, що мають доступ до цієї системи; здійснення внутрішнього контролю (моніторинг та аудит системи); кадрові процедури; процедури управління та реагування на інциденти; захист даних і резервне копіювання;

удосконалено:

– теоретичний підхід щодо визначення поняття «забезпечення кібербезпеки», яким запропоновано вважати реалізований спеціально уповноваженими суб'єктами комплекс заходів, технологій, процесів та практик, спрямованих на захист інформаційних систем, мереж, даних і програм від несанкціонованого доступу, використання, розкриття, зміни, руйнування або втрати. Така діяльність включає забезпечення

конфіденційності, цілісності й доступності інформації, а також протидію кіберзагрозам і кібератакам з боку зловмисників у цифровому просторі;

– твердження про те, що нормативно-правове підґрунтя реалізації адміністративних процедур у сфері кібербезпеки ґрунтується на двох групах нормативно-правових актів: 1) ті, що визначають правові, організаційні, матеріально-технічні та інші особливості процесу підтримки стану безпечного користування кіберпростором, комунікаційними та технологічними системами; 2) ті, що пояснюють зміст, значення та особливості реалізації безпосередньо адміністративних процедур у досліджуваній сфері;

– поняття суб'єктів реалізації адміністративних процедур у сфері забезпечення кібербезпеки, яким запропоновано вважати 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 і заходів, спрямованих на створення необхідних умов для захисту інформаційних систем та мереж, а також координації дій щодо запобігання, виявлення та реагування на кіберзагрози;

дістало подальшого опрацювання:

– твердження про те, що зміст адміністративних процедур, пов'язаних з інформацією, що обробляється в комунікаційних або технологічних системах, охоплює низку оцінних, моніторингово-сканувальних, перевірочних, контрольних та експертно-дослідницьких заходів, реалізація яких дозволяє забезпечувати ефективність і безпечність роботи вказаних вище систем;

– науковий підхід щодо визначення поняття стандартів забезпечення кібербезпеки, яким запропоновано вважати набір правил, рекомендацій і вимог, що визначають методи й заходи для захисту інформаційних систем, мереж та даних від кібератак, несанкціонованого доступу, витоків даних та

інших загроз кібербезпеці. Ці стандарти розроблені для встановлення загальних практик і політик, які можуть використовувати організації для забезпечення захисту своїх цифрових активів;

– обґрунтування необхідності розробки та прийняття Концепції розвитку системи забезпечення кібербезпеки в Україні, що дозволить: 1) забезпечити узгодженість і системність у правовому регулюванні адміністративних процедур у сфері кібербезпеки, усунути прогалини та суперечності в чинному законодавстві; 2) чітко визначити процедури й повноваження спеціально уповноважених суб'єктів, що спростить взаємодію між ними, забезпечить швидкість та якість прийняття управлінських рішень і зменшить бюрократичні бар'єри; 3) покращити систему правового регулювання у досліджуваній сфері, що сприятиме захисту прав суб'єктів господарювання, забезпечить прозорість та обґрунтованість рішень, які приймаються щодо них органами державної влади; 4) підвищити рівень довіри до державних органів; 5) ураховувати міжнародний досвід і стандарти у сфері кібербезпеки, що сприятиме інтеграції України в глобальний цифровий простір та поглибленню міжнародного співробітництва.

Практичне значення отриманих результатів полягає в тому, що викладені в дисертації висновки і пропозиції використовуються та можуть бути використані в:

– *науково-дослідній сфері* – як підґрунтя для проведення подальших теоретико-правових досліджень, присвячених адміністративним процедурам забезпечення кібербезпеки в Україні (акт впровадження Науково-дослідного інституту публічного права);

– *правотворчій сфері* – для розроблення нових та вдосконалення діючих законодавчих і підзаконних нормативно-правових актів, положення яких спрямовані на регулювання адміністративних процедур забезпечення кібербезпеки в Україні;

– *правозастосовній сфері* – з метою підвищення ефективності діяльності суб'єктів, які уповноважені реалізовувати адміністративні процедури у сфері забезпечення кібербезпеки в Україні;

– *освітньому процесі* – під час підготовки підручників і навчальних посібників з дисциплін «Адміністративне право»; «Інформаційне право»; «Кібербезпека» тощо.

Апробація матеріалів дисертації. Підсумки розроблення проблематики та відповідні висновки оприлюднено на міжнародних науково-практичних конференціях: «Актуальні проблеми взаємодії правової науки та практики її застосування» (м. Київ, 16–17 березня 2022 р.), «Науково-практичні засади розвитку юридичної науки на сучасному етапі державотворення» (м. Київ, 15–16 лютого 2023 р.), «Реформування українського законодавства: проблемні питання та шляхи їх вирішення» (м. Київ, 7–8 лютого 2024 р.).

Структура та обсяг дисертації. Дисертація складається зі вступу, трьох розділів, які містять дев'ять підрозділів, загальних висновків, списку використаних джерел, додатків. Загальний обсяг дисертації становить 216 сторінок. Список використаних джерел містить 193 найменування на 21 сторінці.

РОЗДІЛ 1.
ЗАГАЛЬНА ХАРАКТЕРИСТИКА АДМІНІСТРАТИВНИХ ПРОЦЕДУР ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

1.1. Кібербезпека як об’єкт адміністративно-правового регулювання

XXI століття ознаменувало стрімкий розвиток людства, який знайшов відображення у глибокій інтеграції різноманітних електронних пристроїв в поточне життя населення планети. І Україна в даному контексті не стала виключення. Особливий прорив відбувся в сфері Інтернету та похідних від нього технологій, які використовуються будь-де, починаючи від роботи банків і державних органів, закінчуючи соціальною комунікацією між людьми. На сьогодні не можна уявити життя без смартфона, який має цілодобовий доступ до всесвітньої мережі, що пропанує освітній, розважальний контент, новини, рекламу і таке інше. Однак, з розвитком інтернету та цифрових технологій в цілому з’явились нові ризики для суспільства. Зокрема, окремі особи та групи осіб почали використовувати досягнення сучасності з метою незаконного збагачення та порушення прав і законних інтересів інших представників суспільства за рахунок вчинення правопорушень, пов’язаних із незаконним використанням електронно-обчислювальних, інформаційних пристроїв та систем з метою вчинення крадіжок з кредитних карток та банківських рахунків, корпоративного шпіонажу, вчинення шахрайських дій і таке інше. Поступове зростання числа подібних негативних дій та кількості людей, що від них потерпають, отримуючи матеріальні збитки і моральну шкоду, вимагало реакції з боку держави в та її компетентних органів, що призвело до формування особливої юридичної категорії «кібербезпека», яка на сьогоднішній день виступає важливим об’єктом адміністративно-правового регулювання.

Так, перш за все, слід приділити увагу терміну «безпека». Останній найчастіше трактується як стан, при якому кому-, чому-небудь ніщо не загрожує; попередження небезпеки; умови, при яких не загрожує небезпека [96 с. 83; 84]. Водночас, в науковій літературі зміст поняття «безпека» розкривається ширше, аніж у словниковому значенні. Наприклад, його ототожнюють із суспільним порядком, який також визначається через стан, коли все здійснюється, виконується відповідно до встановлених вимог і правил [180, с. 679; 164, с.16].

У психології потребу в безпеці (бажання людини уникнути хвороб і травм, зберегти здоров'я та працездатність, уникнути посягання на її власність тощо) віднесено до первинних потреб людини. Так, згідно з розробленою А. Маслоу ієрархією потреб п'ять основних рівнів потреб становлять: 1) основні фізіологічні потреби; 2) потреба у безпеці; 3) соціальні потреби; 4) потреба у повазі та самоповазі; потреба у самореалізації та самоактуалізації. Усі ці потреби утворюють ієрархічну структуру, що як домінанта визначає поведінку людини. Фізіологічні потреби та потреба в безпеці, що мають назву потреб нижчого рівня, слугують підставою для задоволення потреб вищого порядку. Потреби ж вищого порядку не мотивують людину, поки не задоволені, хоча б частково, потреби нижчого рівня. Звідси випливає, що безпека являє собою не лише одну з основних потреб людини, але також виступає умовою її нормального розвитку, самореалізації, активної життєвої позиції, участі у житті суспільства тощо [135, с.38-39].

Як вказує Ю. Нікітін, «безпека» - це узагальнене поняття, яке існує як об'єктивне соціально-політичне явище і може застосовуватись у багатьох процесах. Воно не тільки уособлює в собі притаманні будь-якому процесу (явищу) специфічні ознаки безпеки, а й поглинає належні тільки їй загальні риси (чинники), що і дозволяє застосувати це поняття в багатьох галузях. Безпеку як узагальнене поняття слід розглядати в традиційному вимірі:

«людина – суспільство – держава» [86, с.107]. І.І. Радіонов та В.П. Тихий вважають, що безпека – це такий стан, коли людині, суспільству або державі не загрожує небезпека, характеризується багатоманітністю форм її прояву у зв'язку із чим може бути класифікована за різними критеріями на: військову, економічну, політичну, духовну, ідеологічну, фізичну, політичну, моральну, майнову, психологічну, екологічну, транспортну, виробничу, трудову, правову тощо, всесвітню або міжнародну, державну або національну, громадську або загальну, колективну або спільну, індивідуальну, особисту безпеку тощо [153, с.7-8; 135, с.38-39].

Наступного висновку з приводу вказаної проблематики дійшов у своїх працях О.С. Доценко: «Поняття безпека – це дуже ємний термін, який фіксує тривогу особи в зв'язку зі зміною звичайного існування, помітною зміною координат, у яких проходить розвиток соціальних, економічних, політичних і культурних процесів. Із безлічі сучасних теоретико-правових конструкцій визначення безпеки можна виділити те загальне, що їх об'єднує. А саме – прагнення на основі аналізу ознак передати це як стан (або положення) об'єкта, коли для нього немає небезпеки (загрози), тобто змін властивостей в гірший бік (перш за все, для життя і здоров'я людей)» [38, с.9].

Цікаве трактування поняття «безпека» надається в дисертації С.Ф. Денисюка. На думку вченого, - це збалансований, за експертною оцінкою, стан людини, соціуму, держави, природних, антропогенних систем тощо. «На сьогодні дуже часто виокремлюють безпеку людини, суспільства та держави. Ці три ціннісні об'єкти безпеки та відповідно три стани є не автономними, а займають певне положення один відносно одного. Крім того, на його думку, безпека людини – це поняття, що відображає саму суть людського життя, її ментальні, соціальні та духовні надбання. В свою чергу, безпека суспільства пов'язана з життям і відносинами людей у суспільстві», пише автор [32, с.327-328].

Таким чином, безпека є багатогранним та важливим науковим поняттям, в якому уособлюється одразу декілька аспектів, пов'язаних з фізичним захистом особи і держави від різноманітних зовнішніх загроз. Через широту своєї дефініції ця категорія має вираження практично в усіх сферах суспільного життя, зокрема: військовій, політичній, економічній, соціальній, тощо. А відтак, узагальнено можна говорити про те, що безпека – це певний динамічний стан суспільного порядку, за якого кожна людина має психологічне відчуття захищеності, а також має реальні гарантії недопущення негативного впливу на її права, свободи, інтереси, а також життя та здоров'я будь-яких негативних чинників. Сутність та зміст безпеки напряму залежить від того, в якій сфері суспільного життя воно використовується.

Так, Закон України «Про основні засади забезпечення кібербезпеки України» надає офіційне визначення вказаної категорії. В статті 1 законодавчого акту кібербезпеку визначено, як «захищеність 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» [128]. Однак, наявність офіційного нормативного визначення не є аксіомою для науковців, які будують власні формулювання категорії, подекуди, досить самостійні та відмінні від законодавчої.

Наприклад, кібербезпека активно досліджувалась серед зарубіжних науковців. Автор Оксфордського довідника з кібербезпеки П. Корніш відмітив: «Оскільки суспільства, уряди, корпорації та окремі особи стають все більш залежними від цифрового середовища, вони також стають все більш вразливими до зловживань цим середовищем. Розвинулась значна індустрія, яка надає засоби, що дозволяють зробити кіберпростір більш

безпечним, стабільним і передбачуваним. Кібербезпека займається виявленням, уникненням, управлінням і зменшенням ризиків у кіберпросторі або з кіберпростору – ризиків шкоди і збитків, які можуть виникнути в результаті чого завгодно: від індивідуальної необережності до організованої злочинності, шпигунства у сфері промислової і національної безпеки» [191]. Відомий спеціаліст та дослідник в галузі кібербезпеки Д. Ксофер трактує її, як правовий «бар'єр» (правову базу), що сприяє забезпеченню конфіденційності, цілісності та доступності державної та приватної інформації в комп'ютерних системах і мережах, захищаючи при цьому права особистості, недоторканність приватного життя, економічні інтереси та національну безпеку [190].

В статті Д. Крайгена та Р. Пєрса надано дуалістичне визначення категорії «кібербезпека». По-перше, її розтлумачено, як сферу вивчення і практики захисту систем або цифрових активів від будь-яких дій, спрямованих на нав'язування дозволу на ці системи або цифрові активи, які не узгоджуються з правами власності на об'єкт ресурсу в розумінні його власника; по-друге – захист інформації/даних, активів, послуг і систем, що становлять цінність, з метою зменшення ймовірності втрати, пошкодження, компрометації або зловживання до рівня, співмірного з їхньою цінністю [189].

Визначення поняттю «кібербезпека» надавались і в рамках вітчизняних наукових аналізів та розробок. Наприклад, О.А. Баранов пише: «Кібербезпека – це деякий стан систем, за якого нейтралізуються загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах. Крім того, завдяки включенню до переліку об'єктів, на які можуть діяти якісь загрози з кіберпростору, послуг інформаційних систем це визначення терміну дозволяє мати на увазі наявність якихось загроз функціональності систем більш високого порядку, до яких в якості складових елементів входять інформаційні системи. Це положення має важливий

методологічний зміст у розумінні місця і ролі проблеми кібербезпеки в контексті інших видів безпеки» [7, с.55; 10, с.37]. В.С. Цимбалюк вважає, що кібербезпека – це стан захищеності передбачених законодавством норм і параметрів інформаційної процесії та відносин, що забезпечує необхідні умови існування держави, людини та суспільства як суб'єктних процесів і відносин [167, с.78–79; 151].

Л.С. Харченко, В.А. Ліпкан, О.В. Логінов описують кібербезпеку як складову національної безпеки, процес управління загрозами та небезпеками (результат управління загрозами та небезпеками) державними і недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України [165, с.46]. В наукових роботах І.В. Діордіца кібербезпека розглядається, як сукупність узгоджених за завданнями елементів кібернетичної безпеки, які комплектуються та розгортаються за єдиним замислом і планом у кібернетичному просторі з метою забезпечення кібернетичної безпеки інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем [37].

О.В. Олійник, О.В. Соснін, Л.Є. Шиманський наголошують: «Кібербезпеку створюють через призму загроз як комплекс системних упереджувальних заходів із наданням гарантій захисту життєво важливих інтересів особистості, суспільству і державі від негативних інформаційних впливів в економіці, внутрішній і зовнішній політиці, в науково-технологічній, соціокультурній і оборонній сферах, системі державного управління, самостійного і незалежного розвитку всіх елементів національного інформаційного простору та забезпечення інформаційного суверенітету країни, захисту від маніпулювання інформацією і дезінформацією та впливів на свідомість, підсвідомість і психіку як індивіда, так і суспільства в цілому, спроможність держави нейтралізувати чи послабити дію внутрішніх і зовнішніх інформаційних загроз» [100, с.540–541; 71, с.9-11].

Г.В. Форос одночасно пропонує широке та вузьке визначення поняття «кібербезпека». На його погляд, у широкому сексі, кібербезпека – це сукупність вольових суспільних відносин, що складаються в процесі свідомого і добровільного дотримання громадянами встановлених в нормах права та в інших нормах неюридичного характеру правил поведінки в кіберпросторі, і тим самим забезпечуються злагоджене, стійке, спільне життя людей в умовах розвинутого суспільства. При розгляді кібербезпеки у вузькому значенні необхідно говорити, перш за все про захищеність 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. Кібербезпека являє собою реалізацію заходів професійно підготовленими фахівцями щодо захисту та страхування дій, засобів, технологій, критично важливих об’єктів інфраструктури суспільства та держави від цифрових атак, які використовуються у кіберпросторі. Кібербезпека передбачає збереження та постійне вдосконалення властивостей безпеки, спрямованих проти відповідних кіберзагроз [162, с.132].

Дослідження наукових джерел показує відсутність одноманітного сприйняття серед науковців змісту кібербезпеки, яка характеризується як сукупність суспільних відносин, комплекс технічних заходів захисту інформації, стан, система елементів і таке інше. Законодавче визначення більш лаконічне, але воно звужує сутність досліджуваної категорії окреслюючи її чіткі рамки – кіберпростір, що відповідно до Закону є середовищем (віртуальним простором), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з’єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет

та/або інших глобальних мереж передачі даних [128]. Підхід законодавця відповідає міжнародним стандартам, адже згідно до Конвенції Організації Об'єднаних Націй про кіберзлочинність від 23.11.2001, діяння, що складають зміст останньої об'єднує аспект їх вчинення в рамках комп'ютерних систем і мереж за допомогою комп'ютерної техніки, об'єктом чого є комп'ютерні дані [59]. Поряд із цим, визначення представлене в Законі України від 05.10.2017 №2163-VIII нехтує правовою стороною явища кібербезпеки, яке передбачає не тільки відповідні механізми захисту інтересів особи та держави, але й виникнення суспільно-правових відносин регламентованих нормами права. Крім того, помилково розглядати вказане явище тільки у царині кіберпростору, адже тут також має місце функціонування багатьох суміжних механізмів та дій пов'язаних із використанням комунікаційних, технологічних систем, електронно-обчислювальної (комп'ютерної) техніки, програмного забезпечення тощо.

Таким чином, проведений аналіз дає змогу говорити про те, що кібербезпеку найбільш доцільно тлумачити у широкому та вузькому розумінні. Так, відповідно до широкого підходу, кібербезпека – це сукупність врегульованих нормами законодавства суспільно-правових відносин, які виникають з приводу забезпечення дотримання всіма суб'єктами нормативно-правових вимог і стандартів у сфері використання комунікаційних та технологічних систем, а також електронно-обчислювальної (комп'ютерної) техніки, програмного забезпечення у кіберпросторі, порушення якого є підставою для їх притягнення до юридичної відповідальності. У вузькому значенні кібербезпека – це стан суспільно-правового порядку, за якого повністю відсутні та/або мінімізовані, а також своєчасно виявляються, попереджаються і припиняються негативні чинники та протиправні дії, які порушують права та інтереси людини, громадянина, суспільства і держави при використанні комунікаційних, технологічних систем, електронно-обчислювальної (комп'ютерної) техніки,

програмного забезпечення та взаємодії в кіберпросторі, що забезпечує сталий розвиток інформаційного суспільства, культури використання комп'ютерної техніки та цифрових комунікацій.

З огляду на зазначене вище, цілком справедливим буде говорити про те, що забезпечення кібербезпеки - це реалізований спеціально уповноваженими суб'єктами комплекс заходів, технологій, процесів і практик, що спрямовано на захист інформаційних систем, мереж, даних і програм від несанкціонованого доступу, використання, розкриття, зміни, руйнування або втрати. Така діяльність включає забезпечення конфіденційності, цілісності та доступності інформації, а також протидію кіберзагрозам і кібератакам з боку зловмисників у цифровому просторі.

Наведене авторське визначення висвітлює ключові особливості явища кібербезпеки, на які варто звернути більш детальну увагу. Так, існує широкий спектр явищ, які відповідають змісту негативних чинників і протиправних дій, які порушують належний стан кібербезпеки. Першими з них варто відмітити найбільш тяжкі – кіберзлочини – (комп'ютерні злочини) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [128]. Представлене в Законі поняття – це юридичне узагальнення, яке відсилає нас до положень Кримінального кодексу України (далі – ККУ), відповідно до якого кіберзлочин є кримінальним правопорушенням – передбачене ККУ суспільно небезпечне винне діяння (дія або бездіяльність), вчинене суб'єктом кримінального правопорушення. Кримінальні правопорушення поділяються на кримінальні проступки і злочини. Так, проступком є передбачене ККУ діяння (дія чи бездіяльність), за вчинення якого передбачене основне покарання у виді штрафу в розмірі не більше трьох тисяч неоподатковуваних мінімумів доходів громадян або інше покарання, не пов'язане з позбавленням волі. В свою чергу, злочини

поділяються на нетяжкі, тяжкі та особливо тяжкі. Нетяжким злочином є передбачене Кодексом діяння (дія чи бездіяльність), за вчинення якого передбачене основне покарання у виді штрафу в розмірі не більше десяти тисяч неоподатковуваних мінімумів доходів громадян або позбавлення волі на строк не більше п’яти років. Тяжким злочином є передбачене ККУ діяння (дія чи бездіяльність), за вчинення якого передбачене основне покарання у виді штрафу в розмірі не більше двадцяти п’яти тисяч неоподатковуваних мінімумів доходів громадян або позбавлення волі на строк не більше десяти років. Особливо тяжким злочином виступає діяння (дія чи бездіяльність), за вчинення якого передбачене основне покарання у виді штрафу в розмірі понад двадцять п’ять тисяч неоподатковуваних мінімумів доходів громадян, позбавлення волі на строк понад десять років або довічного позбавлення волі [65].

Таким чином, кіберзлочин є різновидом кримінального правопорушення, відповідальність за який встановлена ККУ. Умовно їх можна поділити на дві групи: звичайні різновиди кримінальних правопорушень вчинених в кіберпросторі або пов’язані із ним, а також злочини в сфері використання електронно-обчислювальних машин. В першому випадку ми говоримо про різноманітні злочинні дії проти громадян та їх власності, які здійснюються із використанням можливостей кіберпростору та інформаційних технологій: викрадення реквізитів платіжних карток (фішинг, вішинг, шиммінг, скимінг); незаконні фінансові операції з використанням платіжних карток або їх реквізитів, які не ініційовані або не підтверджені її власником (кардінг); заволодіння коштами через фіктивні інтернет-магазини, інтернет-аукціони, сайти та інші засоби телекомунікації (онлайн–шахрайство); порушення авторського права і суміжних прав шляхом незаконного розповсюдження програмних продуктів через комп'ютерні мережі (піратство) тощо [68].

Другу групу складають кваліфіковані кримінальні правопорушення, передбачені спеціальним Розділом XVI ККУ «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», зокрема: «1) несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж; 2) створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут; 3) несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації; 4) перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку» тощо [65].

Водночас, окрім кіберзлочинів, досліджуваний стан суспільно-правового порядку порушують такі негативні явища, як кібершпигунство, кібертероризм, кіберрозвідка (шпигунські, терорестичні та розвідницькі дії, вчинювані в кіберпросторі або за його допомогою), а також кібератаки та інші інциденти кібербезпеки. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», кібератака – це «спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання

несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту» [128]. В свою чергу, інцидент кібербезпеки визначається, як подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів [128].

Другу особину кібербезпеки визначає її специфічний об'єкт. Слово «об'єкт» має латинське походження і застосовуються в значенні існуючого поза свідомістю предмета або явища, на які спрямована певна діяльність суб'єкта [44, с.318]. Виходячи з цього об'єктом безпеки виступають матеріальні або нематеріальні явища дійсності, що захищаються в межах стану суспільно-правового порядку відповідного різновиду. В кожному окремому випадку даний параметр буде відрізнятись, наприклад: а) об'єктом екологічної безпеки у процесі діяльності залізничного транспорту виступають рухомі (пересувні) транспортні засоби та стаціонарні об'єкти матеріально-технічного обслуговування; б) об'єктом безпеки інформаційних відносин у галузі реклами є рекламна інформація і рекламна діяльність в інформаційному просторі України, котра повинна здійснюватися на засадах непорушності прав та свобод людини і громадянина (право на достовірну інформацію); духовних, морально-етичних, культурних, історичних, інтелектуальних та матеріальних цінностей суспільства; конституційного

ладу, суверенітету, територіальної цілісності і недоторканості держави; в) об’єктом економічної безпеки вчені визначаються все те, на що спрямовані дії із забезпечення стану (бухгалтерська інформація, комерційна таємниця, інформаційні ресурси, майно організації та засоби виробництва) і таке інше [4, с.7; 152, с.118; 35, с.46]

В свою чергу, об’єкти кібербезпеки унікальні та визначені частиною 1 статті 4 Закону України «Про основні засади забезпечення кібербезпеки України», а саме: «1) конституційні права і свободи людини і громадянина; 2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища; 3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність; 4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави; 5) об’єкти критичної інфраструктури» [128].

Особлива важливість перелічених чинників, які становлять об’єкт кібербезпеки, зумовлюють наступну специфіку даного явища пов’язану із організаційною системою його суб’єктів. Їх перелік в більшій частині складають представники публічної влади нашої держави: органи державної влади та місцевого самоврядування. Згідно до статті 5 Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 №2163-VIII Координація діяльності у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України. Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України (далі – РНБО) здійснює координацію та контроль за діяльністю суб’єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України. Кабінет Міністрів України (далі – КМУ) забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у

кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (крім об'єктів критичної інфраструктури у банківській системі України та на ринках небанківських фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг). Суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є: 1) міністерства та інші центральні органи виконавчої влади; 2) місцеві державні адміністрації; 3) органи місцевого самоврядування; 4) правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; 5) Збройні Сили України, інші військові формування, утворені відповідно до закону; 6) Національний банк України; 7) підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури; 8) суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом [128].

Таким чином, проведений аналіз дає змогу констатувати, що кібербезпека як об'єкт адміністративно-правового регулювання характеризується наступними особливостями: по-перше, представляє собою особливу групу правовідносин, що виникають у специфічній сфері суспільного життя; по-друге, обумовлює необхідність здійснення низки різноманітних дій та заходів спеціально уповноваженими органами державної влади, а також приватними суб'єктами; по-третє, відповідна діяльність, переважно, регулюється нормами адміністративної галузі права;

по-четверте, є сферою реалізації різноманітних процедур, які носять адміністративний характер.

1.2. Поняття, особливості та види адміністративних процедур у сфері забезпечення кібербезпеки

Робота всього публічного апарату пронизана численними регламентами і порядками, з огляду на які органи державної влади та їх посадові особи вирішують поставлені перед ними завдання. Законодавство України забезпечує послідовність і цілеспрямованість функціонування цих суб'єктів: по-перше, з метою задоволення вимог законності, а, по-друге – ефективності надання населенню публічних послуг в різноманітних секторах суспільних відносин. Наприклад, державна реєстрація актів цивільного стану передбачає складання актів цивільного стану щодо офіційного визнання і підтвердження державою фактів народження фізичної особи та її походження, шлюбу, розірвання шлюбу, зміни імені, смерті [112]. Наведене є прикладом однієї з багатьох адміністративних процедур, здійснюваних уповноваженими органами державної влади та місцевого самоврядування для сприяння реалізації прав і законних інтересів громадян. Такий різновид діяльності зустрічається в усіх сферах публічних відносин у тому числі за напрямом забезпечення кібербезпеки, де вони мають свій порядок та особливості.

Так, слово «процедура» розуміється у трьох ключових значеннях: офіційно встановлений чи узвичаєний порядок здійснення, виконання або оформлення чого-небудь; ряд яких-небудь дій, хід виконання чого-небудь; лікувальний захід призначений лікарем тощо [146, с. 343]. Окремі науковці, наприклад, М.М. Касьяненко, М.В. Гринюк, П.В. Цимбал та Л.В. Трофімова дійшли висновку, що процедура – це логічно завершений набір операцій, які

виконуються у визначеній технологією послідовності [52, с.59; 156, с.88]. За Т.О. Тополянською процедура – це встановлена модель, план, що забезпечує системність розвитку явища у певному процесі [154]. Н.В. Дикань і І.І. Борисенко пишуть: «Процедура — це запрограмоване рішення, вона характеризує дії, які слід вживати в конкретній ситуації» [34, с.38]. О.О. Середа визначає сутність категорії наступним чином: «Процедура потрібна для втілення в життя, реалізації на практиці встановлених правил, порядків, інструкцій. Процедура – це, передусім, відповідна практика, це фактичні дії, поєднані певною метою. Процедурою можна назвати й послідовність, яка складається з багатьох «кроків», і менш складну, менш насичену різноманітними діями операцію, яка може складатися лише з одної дії (наприклад, купівля квитка в касі кінотеатру). У будь-якому випадку процедура – це практика, яка підкріплює теорію, утворюється та регулюється теорією» [141, с.11]. Тож, у загальному розумінні процедура – це послідовність якихось дій, процесів, операцій, що становлять собою комплексну діяльність спрямовану на досягнення конкретизованого, чітко визначеного результату.

Правова наука в цілому апелює терміном «процедура» в тому ж ключі, але наділяє його галузевими особливостями. Як пише М.Д. Гнатюк: правова процедура є складовою частиною матеріального права. На відміну від процесів вона регламентується матеріально-правовими нормами, сприяє реалізації матеріального регулятивного правовідношення [22, с.127]. О.П. Євсєєв зазначає: «Юридична процедура може бути визначена як нормативно або індивідуально встановлений порядок послідовно вчинюваних уповноваженими суб'єктами права узгоджених юридичних дій, спрямованих на досягнення спільного для них правового результату. Під порядком, у свою чергу, слід розуміти належну, виражену в нормах позитивного права (інколи різної юридичної сили) модель поведінки, що передбачає те, які дії і в якій послідовності повинен виконати суб'єкт права,

щоб досягти тих цілей, для реалізації яких ця процедура створена» [43, с.104]. «Правова (юридична) процедура – це система правових відносин, що складаються в певній послідовності, направлених на досягнення правового результату, який може виражатися у формуванні юридичних норм, утворень або припиненні певних правовідносин (головних для процедури), запобігання правопорушенням, також в інших, правових наслідках», - доводить Р.С. Алімов [2, с.20].

В своєму дисертаційному дослідження К.В. Николина зробила висновок про те, що юридична процедура – це елемент соціальних процедур, який реалізується у сфері права, а також складається із системи послідовних дій відповідних суб'єктів. До ознак юридичної процедури вчена віднесла наступні: а) являє собою особливий різновид правовідносин, що мають процедурний характер та визначають особливості юридичної практичної діяльності; б) має цілісний характер, оскільки складається із певної послідовності дій суб'єктів юридичної процедури, в результаті чого досягається певний юридично значимий результат; в) виникає на підставі норм права, тобто має офіційний правовий характер; г) порядок здійснення юридичної процедури регламентується відповідними процедурними нормами права; має власну націленість, що полягає у зміні правової дійсності; ґ) має інтелектуальний та вольовий характер, оскільки залежить від свідомості та волевиявлення суб'єкта юридичної процедури; визначає послідовність дій суб'єктів юридичної процедури; д) результатом здійснення юридичної процедури є реалізація прав, свобод, законних інтересів суб'єкта права або виконання юридичних обов'язків; є) виявляється у юридичній діяльності; являє собою сукупність послідовних актів поведінки, кожний з яких викликає відповідні локальні наслідки, що впливає на зміст та результативність всієї юридичної процедури [85, с.4-5].

Таким чином, проведене наукове дослідження дає змогу констатувати, що з правової точки зору процедура – це регламентований нормами права

прядок вчинення уповноваженими суб'єктами юридично значимих дій з метою задоволення законних інтересів суспільства і держави. Здійснення правової процедури в обов'язковому порядку передбачає отримання якогось кінцевого, формально-вираженого правового результату у вигляді зміни, припинення або появи нових правовідносин.

Адміністративні процедури походять від класичних правових, але мають власну мету. Довгий час їх поняття існувало виключно у теоретико-правовому розрізі, але ситуація змінилась у 2023 році, коли Верховною Радою України було прийнято Закон України «Про адміністративну процедуру». Закон регулює відносини органів виконавчої влади, органів влади Автономної Республіки Крим, органів місцевого самоврядування, їх посадових осіб, інших суб'єктів, які відповідно до закону уповноважені здійснювати функції публічної адміністрації, з фізичними та юридичними особами щодо розгляду і вирішення адміністративних справ шляхом прийняття та виконання адміністративних актів. Відповідно до його положень, адміністративна процедура – це визначений законом порядок розгляду та вирішення справи – справа, що стосується публічно-правових відносин щодо забезпечення реалізації права, свободи чи законного інтересу особи та/або виконання нею визначених законом обов'язків, захисту її права, свободи чи законного інтересу, розгляд якої здійснюється адміністративним органом [111].

Водночас, відсутність протягом довгого часу офіційного тлумачення адміністративних процедур зумовило появу численних наукових концепцій щодо розкриття змісту категорії. Наприклад, А. Селіванов доводить: адміністративна процедура – це порядок застосування норм матеріального права [138, с.35; 156, с.89]. І.Б. Пробко вважає, що адміністративна процедура – це форма адміністративного процесу, встановлена законом, нормативно-правовими актами органу виконавчої влади, певна складова порядку (алгоритму) управлінської діяльності [133, с.9]. Н.Р. Нижник вказує,

що у науковій праці «Правове регулювання державно-управлінських відносин» відзначає, що процедури, як і будь-яке об'єктивне правове явище, має нормативний і фактичний вияв. Вчений робить такий висновок: «З одного боку, вони є сукупністю загальноприйнятих і специфічних дій, які визначають послідовність здійснення різних дій і взаємодій між учасниками державно-управлінських відносин чи оформлення будь-яких справ, спрямованих на досягнення певного завершального результату. З іншого боку, процедури повинні виступати орієнтиром для дій. Критеріями наявності процедурної упорядкованості діяльності є: чітку цільова спрямованість, зорієнтованість на конкретний об'єкт управління, тривалість у часі, послідовність здійснення процедурних дій та їх документальна фіксація» [83; 31, с.84].

Р.В. Ігонін та М.В. Вікторчук виділили наступні особливості адміністративних процедур: 1) адміністративні процедури застосовуються в публічній сфері; 2) адміністративні процедури застосовуються при здійсненні правозастосовної діяльності; 3) адміністративні процедури охоплюють управлінську діяльність позитивної спрямованості, тобто діяльність, спрямовану на створення умов для ефективної реалізації прав і законних інтересів громадян та організацій; 4) адміністративні процедури спрямовані на упорядкування діяльності уповноважених органів виконавчої влади; 5) для адміністративних процедур характерний особливий суб'єктний склад (однією зі сторін в адміністративній процедурі завжди виступає державний орган або посадова особа, наділені державно-владними повноваженнями); 6) адміністративні процедури закріплюються адміністративно-процесуальними нормами, які, своєю чергою, регулюють застосування матеріальних норм адміністративного та інших галузей права (фінансового, господарського, трудового та інше) і при цьому регламентують діяльність уповноважених органів і посадових осіб [51, с.182–190; 98, с.31-32].

Натомість, І.В. Бойко, О.Т. Зима, О.М. Соловйова займають позицію, відповідно до якої адміністративна процедура – це структурований, нормативно закріплений порядок прийняття адміністративних актів або укладення адміністративно-правових договорів, спрямований на вирішення конкретних справ у сфері публічного управління. Ознаками адміністративної процедури є такі: 1) має правовий характер, оскільки принципи та правила, що визначають адміністративну процедуру, містяться в приписах нормативно-правових актів; 2) вміщує норми, що регламентують як діяльність суб'єкта публічного адміністрування, так і поведінку приватних осіб; 3) спрямована на прийняття адміністративного акта суб'єктом владних управлінських повноважень; 4) застосовується для вирішення конкретної адміністративної справи; 5) має основним призначенням забезпечення ефективної реалізації прав приватних осіб і унеможливлення їх порушення; 6) тягне за собою настання зовнішніх наслідків, тобто застосування процедурних правил породжує права й обов'язки осіб, які знаходяться поза системою публічного адміністрування; 7) має, як правило, безспірний характер, тобто завдяки адміністративній процедурі вирішуються позитивні управлінські справи [13, с.7-8].

Наступним висновків дійшов О.В. Пабат в процесі аналізу і розкриття змісту адміністративних процедур: «Розкриваючи сутність такого поняття, як адміністративна процедура вчений зазначає, що вона є сукупністю процесуальних норм, які регулюють процедуру, порядок діяльності державного апарату, апарату органів місцевого самоврядування, об'єднань громадян, окремої організації, установи, підприємства (незалежно від форм власності) і відповідають на запитання «як, яким чином робити?». Тобто закріплюють процесуальні форми, способи і методи здійснення службової діяльності. Однією з суттєвих ознак, властивих адміністративним процедурам, є те, що такі процедури стосуються тільки тих відносин, де одним з учасників є представник публічної адміністрації. Тобто йдеться про

розгляд та вирішення адміністративним органом або його посадовою особою справ, які стосуються конкретних приватних осіб, що є другою стороною в цих відносинах. Адміністративна процедура є загальною моделлю провадження, встановлює єдиний порядок розгляду й вирішення адміністративними органами та їхніми посадовими особами індивідуальних адміністративних справ і складається з таких елементів: початок процедури або сповіщення сторін процесу; збирання та надання всієї значущої інформації сторонам; слухання (як формальне, так і неформальне), рідше – адміністративний суд; вирішення справи» [102, с.74].

Підсумовуючи викладене можна відмітити, що на сьогоднішній день склались дві відносно самостійні концепції щодо тлумачення змісту та призначення адміністративних процедур. Відповідно до однієї з позицій ця категорія охоплює всю публічно-управлінську діяльність органів державної влади і місцевого самоврядування із реалізації покладених на них законодавством повноважень, вирішення адміністративних справ щодо забезпечення реалізації прав, свобод і законних інтересів фізичних та юридичних осіб, а також внутрішньої організації своєї діяльності. В даному випадку поняття «адміністративна процедура» ототожнюється із адміністративною діяльністю державних і муніципальних органів. Друга концепція відповідає законодавчому трактуванню та характеризує адміністративну процедуру, як регламентований законодавством України порядок дій спеціально уповноважених суб’єктів з приводу забезпечення реалізації та захисту прав, свобод і законних інтересів фізичних та юридичних, кінцевим етапом якого є прийняття адміністративного акту.

Таким чином, адміністративні процедури у сфері забезпечення кібербезпеки – це визначений законодавством України порядок дій, які реалізуються спеціально уповноваженими суб’єктами у напрямку забезпечення і захисту прав та законних інтересів фізичних та юридичних осіб, а також реалізації публічних повноважень у сфері використання

комунікаційних, технологічних систем, електронно-обчислювальної (комп'ютерної) техніки, програмного забезпечення та взаємодії у кіберпросторі.

Для повноти дослідження проблеми адміністративних процедур у сфері кібербезпеки варто здійснити їх класифікацію. Відмітимо, що Закон України «Про адміністративну процедуру» не висвітлює в своїх нормах різновиди зазначеної категорії, на відміну від наукових джерел. Наприклад, С.Т. Гончарук до найпоширеніших адміністративних процедур відносить такі основні види: 1) у справах за зверненнями громадян; 2) у справах про адміністративні правопорушення; 3) заохочувальні; 4) дозвільно-реєстраційні; 5) контрольно-наглядові; 6) установчі; 7) щодо підготовки та прийняття управлінських актів; 8) щодо застосування заходів адміністративного припинення; 9) з питань діловодства та документообігу; 10) з питань кадрової роботи; 11) щодо організації внутрішньо-апаратної діяльності; 12) щодо індивідуальних звернень юридичних осіб з питань управлінського характеру та інші [26, с.87–88].

Г.В. Фоміч адміністративні процедури у публічній службі, з огляду на їх багатоаспектність та різноманітність, класифікував на: 1) організаційні адміністративні процедури: а) процедури вступу на публічну службу, які, у свою чергу, включають процедури: конкурсу, зарахування на посаду, призначення на посаду, виборів на посаду, обрання на посаду; б) процедури оцінювання діяльності публічних службовців: процедури щорічної оцінки й атестаційної процедури; в) процедури щодо просування по публічній службі: процедури стажування, процедури кадрового резерву, процедури присвоєння рангу, чину, звання; г) заохочувальні адміністративні процедури; 2) юрисдикційні адміністративні процедури: а) процедури службового розслідування щодо публічних службовців; б) процедура притягнення до дисциплінарної відповідальності загального характеру; в) процедура

притягнення до дисциплінарної відповідальності спеціального характеру [161, с.18; 77, с.67].

В свою чергу С.В. Братель виділяє юрисдикційні та неюрисдикційні адміністративні процедури. Юрисдикційні визначають порядок діяльності юрисдикційних органів. Ними передбачено регулювання порядку взаємовідносин сторін у конфлікті та притаманна ознака змагальності сторін. Неюрисдикційні процедури характеризуються відсутністю санкцій при правовому регулюванні, відсутністю спору. Вони відображають встановлений порядок діяльності органів публічного адміністрування. Також С.В. Братель виділяє серед неюрисдикційних процедур нормотворчі, правозастосовні, реєстраційні, атестаційні, контрольно-наглядові процедури [26, с.87-88; 77, с.67].

М.В. Вербіцька та О.Б. Росоляк поділяють адміністративні процедури у сфері господарської діяльності залежно від їх мети на: 1) процедури організаційного характеру (процедури реєстраційного, дозвільного типу тощо); 2) процедури контролюючої природи, наприклад, здійснення перевірки контролюючим органом господарюючого суб'єкта; 3) адміністративні процедури регулятивного типу, що мають відношення до правотворчої діяльності публічно-адміністраційних суб'єктів стосовно винесення управлінських рішень індивідуального або колективного характеру, що відносяться до діяльності господарюючих суб'єктів – процедура публічних закупівель [17, с.153].

Х.П. Ярмакі акцентує увагу на тому, що адміністративні процедури, що здійснюються органами публічного управління у взаємовідносинах з фізичними та юридичними особами, можна розділити на сім видів: 1) щодо надання прав; 2) пов'язані із забезпеченням виконання фізичними та юридичними особами своїх обов'язків; 3) ліцензійно-дозвільні; 4) реєстраційні; 5) з прийняття несприятливих актів для фізичних та юридичних осіб; 6) контрольно-наглядові; 7) процедури державного

заохочення. Вчений резюмує: «Більшість із зазначених видів адміністративних процедур, крім процедур з прийняття несприятливих актів для фізичних та юридичних осіб, контрольно-наглядових та процедур державного заохочення, реалізуються в процесі реалізації адміністративних процедур» [184, с.267].

Тож, адміністративні процедури можуть бути класифіковані вкрай по-різному. Їх типізація прямо залежить від сфери публічного управління та компетенції окремо взятих уповноважених суб'єктів. Зокрема, в галузі забезпечення кібербезпеки складно використати будь-який із запропонованих вище підходів, адже Закон України «Про основні засади забезпечення кібербезпеки України» практично не освітлює в своїх положеннях дане питання. Згідно до його статей в зазначеній сфері можливе проведення заходів 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. В частині 2 цієї ж статті зазначається, що функціонування національної системи кібербезпеки забезпечується шляхом: 1) формування конкурентного середовища у сфері електронних комунікацій, надання послуг із захисту інформації та кіберзахисту; 2) проведення навчань щодо дій у разі надзвичайних ситуацій та інцидентів у кіберпросторі; 3) функціонування системи аудиту інформаційної безпеки, запровадження кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту; 4) державно-приватної взаємодії у запобіганні кіберзагрозам об'єктам критичної інфраструктури, реагуванні на кібератаки та кіберінциденти, усуненні їх наслідків, зокрема в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період. Закон передбачає державно-приватну взаємодію у сфері кібербезпеки між суб'єктами національної системи

кібербезпеки та приватними фізичними і юридичними особами, що включає в себе надання консультативної та практичної допомоги з питань реагування на кібератаки [128].

Отже, документ показує формат адміністративного забезпечення сфери кібербезпеки, але не конкретизує, що саме з переліченого є процедурою та в якому порядку вона надається. Вирішення даного питання можна знайти в підзаконній нормативно-правовій документації. Згідно до неї види адміністративних процедур логічно розподіляти основуючись на змісті об'єкту з приводу якого вони проводяться. Наприклад, першою групою є процедури, здійснення яких безпосередньо не пов'язано із проведенням заходів захисту інформації у комунікаційних, технологічних системах, обробкою та обміном інформацією в кіберпросторі тощо. Вони носять суто організаційний характер та спрямовані на упорядкування управлінських зв'язків, державного регулювання кібербезпеки в цілому.

Прикладом такої процедури є ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації та технічного захисту інформації. Законом України «Про ліцензування видів господарської діяльності» визначається, що ліцензування – це засіб державного регулювання провадження видів господарської діяльності, спрямований на забезпечення безпеки та захисту економічних і соціальних інтересів держави, суспільства, прав та законних інтересів, життя і здоров'я людини, екологічної безпеки та охорони навколишнього природного середовища [125].

В аспекті забезпечення кібербезпеки, ліцензування здійснюється з метою виконання положень Постанови КМУ «Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України» від 16.11.2016 №821. Документ передбачає проведення

адміністративної процедури із перевірки відповідності суб’єкта господарювання визначеним ліцензійним умовам, які встановлюють вичерпний перелік документів, що додаються до заяви про одержання ліцензії, кадрові, організаційні та технологічні вимоги, обов’язкові для виконання під час провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації [33].

З ліцензуванням пов’язано іншу важливу організаційну-управлінську адміністративну процедуру – здійснення державного нагляду (контролю) у сфері додержання вимог законодавства з надання послуг у галузі технічного захисту інформації та криптографічного захисту інформації. Відповідно до Закону України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності», – це «діяльність уповноважених законом центральних органів виконавчої влади, їх територіальних органів, державних колегіальних органів, органів виконавчої влади Автономної Республіки Крим, місцевих державних адміністрацій, органів місцевого самоврядування в межах повноважень, передбачених законом, щодо виявлення та запобігання порушенням вимог законодавства суб'єктами господарювання та забезпечення інтересів суспільства, зокрема належної якості продукції, робіт та послуг, допустимого рівня небезпеки для населення, навколишнього природного середовища» [127].

Інший приклад адміністративної процедури організаційно-управлінського забезпечення сектору кібербезпеки регламентовано Наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України «Про затвердження Порядку координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, електронних

комунікаційних та інформаційно-комунікаційних системах» від 10.06.2008 №94, який визначає механізм координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань, пов'язаних із запобіганням вчиненню порушень безпеки інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах (далі – ІКС), виявленням та усуненням наслідків інших несанкціонованих дій щодо державних інформаційних ресурсів в ІКС. Метою цього Порядку є організація координації діяльності з питань запобігання вчиненню порушень безпеки інформації в ІКС, виявлення та усунення наслідків інших несанкціонованих дій щодо державних інформаційних ресурсів в ІКС, а також впровадження єдиної процедури надання суб'єктами координації інформації про вчинення та/або спроби вчинення несанкціонованих дій щодо державних інформаційних ресурсів в ІКС [120]. В свою чергу, Наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України «Про затвердження Вимог до аудиторів інформаційної безпеки на об’єктах критичної інфраструктури та порядку їх атестації (переатестації)» від 30.04.224 №228 встановлено особливості адміністративної процедури розгляду та перевірки на відповідність вимогам нормативних документів заявників з метою отримання ними права проводити незалежні аудити інформаційної безпеки на об’єктах критичної інфраструктури [115].

Наступну групу становлять адміністративні процедури, пов’язані із змістом інформації, що обробляється в комунікаційних або в технологічних системах. Наприклад, Наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 16.05.2007 №93 затверджено Положення про державну експертизу у сфері технічного захисту інформації [117]. Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України «Про затвердження Порядку

сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті» від 15.01.2016 №20, визначає порядок процедури проведення оцінки стану захищеності інформації в інформаційно-комунікаційних системах, що 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 [122]. В рамках аналізу цієї ж групи можна для прикладу навести Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» від 02.12.2014 №660, котрий визначає правові та організаційні засади проведення оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах державних органів, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України, підприємств, установ і організацій незалежно від форм власності [121].

На наш погляд, третю групу адміністративних процедур у сфері забезпечення кібербезпеки складають ті, що пов'язані з захистом інформації, що становить державну таємницю, комунікаційних та технологічних систем, призначених для її оброблення. Це спеціальний вид процедурної діяльності, специфіка якого пов'язана зі статтею 2 Закону України «Про основні засади забезпечення кібербезпеки України». Згідно до неї, положення законодавчого акту не поширюються на діяльність, пов'язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення [128].

В даному випадку варто зауважити: діяльність пов’язана із захистом інформації, що становить державну таємницю охоплюється змістом кібербезпеки та є її органічною частино. Водночас, особливе значення подібної інформації передбачає регулювання процесу її обробки та забезпечення безпеки спеціальними нормативно-правовими документами, які встановлюють більш суворі правила, вимоги та процедурні порядки. За допомогою цього конструкція кібербезпеки такої інформації передбачає особливу правову модель та спеціальні технічні рішення. У зв’язку із цим адміністративні процедури в даному аспекті регламентовані, у першу чергу, Законом України «Про державну таємницю» від та підзаконними документами прийнятими на виконання Закону [114].

Тож, проведений у даному підрозділі дисертаційного дослідження аналіз дає змогу дійти до висновку, що особливостями адміністративних процедур у сфері забезпечення кібербезпеки є наступні: по-перше, особлива сфера реалізації, а також предмет з приводу якого виникають відповідні суспільні відносини; по-друге, реалізовувати відповідні процедури мають право виключно спеціально уповноважені суб’єкти, посадові особи яких володіють особливим набором професійних знань, умінь та навичок; по-третє, наявність спеціального набору нормативно-правових засад їх реалізації; по-третє, переважна більшість адміністративних процедур пов'язані з обробкою персональних даних, що вимагає дотримання вимог законодавства про захист персональних даних; по-четверте, наявність підвищеного рівня відповідальності суб’єктів, що відповідні процедури реалізовують; по-п’яте, відповідні процедури застосовуються у різних сферах забезпечення кібербезпеки, що обумовлює наявність їх різновидів.

На нашу думку, адміністративні процедури у сфері забезпечення кібербезпеки слід поділити на наступні групи: 1) адміністративні процедури пов’язані із організаційно-управлінським забезпеченням кібербезпеки; 2) адміністративні процедури, пов’язані із змістом інформації, що

обробляється в комунікаційних або в технологічних системах; 3) адміністративні процедури, пов’язані із захистом інформації, що становить державну таємницю, комунікаційних та технологічних систем, призначених для її оброблення; 4) адміністративні процедури захисту комунікаційних систем, які не взаємодіють з публічними мережами електронних комунікацій.

1.3. Суб’єкти реалізації адміністративних процедур у сфері забезпечення кібербезпеки

Невід’ємним елементом реалізації адміністративних процедур у сфері забезпечення кібербезпеки постає суб’єктний склад. Етимологічно слово «суб’єкт» має такі значення: 1) істота, здатна до пізнання навколишнього світу, об'єктивної дійсності й до цілеспрямованої діяльності; 2) особа, група осіб, організація і таке інше, яким належить активна роль у певному процесі, акті; 3) особа чи організація як носій певних прав та обов'язків; 4) людина як носій певних фізичних і психічних якостей; людина як об'єкт дослідження; 5) людина, особа; 6) логічний предмет, предмет думки; 7) підмет речення і таке інше [15, с.1408-1409; 61, с.173].

У філософському розумінні суб’єкт (від латинського «subject» – лежачий в основі) – поняття, що вживалося вже Арістотелем, а також у середньовіччі, у понятті субстанції (щось незмінне у протилежності станам та властивостям, що змінюється). Тільки із XVII століття воно починає використовуватися у сучасному розумінні, тобто як позначення психолого-теоретико-пізнавального Я, протиставлюваного, чомусь іншому не-Я, предмету [136, с.116].

За визначенням С.О. Сергеєва, суб’єкт – це індивід. Саме він наділений відчуттям, сприйняттям, емоціями, здатністю оперувати образами та найзагальнішими абстракціями; він діє у процесі практики як реальна

матеріальна сила, що змінює матеріальні системи. Але суб'єкт – це не тільки індивід, це і колектив, і соціальна група, клас, суспільство в цілому [140, с.106]. В роботі М.Й. Штангерта наведено думку, що суб'єкт – це людина, люди на найвищому для кожного з них рівні активності, цілісності, автономності та інше; творець власної історії, свого життєвого шляху; той, хто здійснює діяльність, спілкування, поведінку, споглядання й інші види специфічно людської активності: творчої, моральної, вільної та іншої. Тобто, це якісно визначений спосіб самоорганізації, саморегуляції, узгодження зовнішніх і внутрішніх умов активності, центр координації всіх психічних процесів, станів, властивостей, здібностей, можливостей (і обмежень) особистості співвідносно з об'єктивними і суб'єктивними (мети, домагання, завдань) умовами діяльності тощо [175, с.22-23]. Цікаву думку пропонує І.М. Берназюк відповідно до якої: суб'єкт – це представник певної категорії осіб (фізичних чи юридичних), як уособлення стійкої сукупності соціально важливих рис, що характеризують цю категорію в системі суспільних відносин. Такий суб'єкт є носієм рис, що визначаються особливостями: національними, етнічними, професійними, віковими, територіальними тощо [9, с.166]. Отже, суб'єкт – це той, хто приймає участь у чомусь, виконує якусь діяльність, є частиною якоїсь спільноти, наприклад: суб'єкт поліцейської діяльності, суб'єкт соціальної групи і таке інше.

Ґрунтовної оцінки і визначення поняття суб'єкту набуло в галузі управління. Так, А.О. Собакарь пише, що суб'єкт управління – це той, хто управляє або керує. Суб'єкт управління може бути як індивідуальним, так і колективним (колегіальним). Але незалежно від того він чинить вплив на суспільні формування, що діють у різних сферах суспільного життя, тобто вплив на об'єкт управління. Метою такого впливу є спрямування об'єкта по шляху певного розвитку, надання йому стану впорядкованості, якісного визначення, відповідності певним вимогам чи ознакам [147, с.78]. І.Б. Тацишин наголошує на тому, що суб'єктом управління є певна фізична

або юридична особа, наділена певними управлінськими функціями щодо предмета управління [152, с.137].

О.М. Бандурка та С.М. Яровий зауважують: суб'єкт управління – це органічна складова системи управління, наділена владними повноваженнями приймати управлінські рішення, здійснювати вольовий, інтелектуальний і моральний вплив на об'єкт системи управління. Він є структурно окресленою спільністю людей з органами управління, які формуються ними, та керівним складом (на персональному рівні), наділеним управлінськими функціями, який здійснює управлінську діяльність [6, с.11; 186, с.140]. За М.К. Якимчуком суб'єкт управління – це той учасник процесу управління, який за своїм функціональним призначенням покликаний практично здійснювати цілеспрямований упорядковуючий вплив на відповідний об'єкт (об'єкти). Найчастіше як суб'єкт управління виступають відповідні організації й органи, тобто колективи людей, уповноважені на здійснення управлінського впливу в заданих параметрах [183, с.96-98].

У державному управлінні, згідно до тлумачення Л.В. Набоки, «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 [81, с.26].

В правовій науці переважає дуалістичний підхід до тлумачення категорії «суб'єкт», який вживають у значенні «суб'єкт права» або «суб'єкт правовідносин». Як зауважує Ю.А. Нікіфоров, різниця між поняттям суб'єкт права і суб'єкт правовідносин полягає у тому, що: 1) будучи суб'єктом права,

індивід чи будь-які колективні утворення не можуть бути одночасно суб'єктом усіх можливих правовідносин; 2) щойно народжені, малолітні діти та деякі інші суб'єкти права не можуть бути суб'єктами більшості правовідносин. Категорія суб'єкт права набагато ширше від суб'єкта правовідносин. Суб'єкт права – це загальне, а суб'єкт правовідносин – конкретне. Будь-який суб'єкт правовідношення є одночасно і суб'єктом права, але не кожний суб'єкт права є суб'єктом правовідношення. Під суб'єктами права слід розуміти таких учасників суспільних відносин, які на підставі чинного законодавства визнаються носіями суб'єктивних прав і відповідних обов'язків [87, с.33]. В.В. Шуба обґрунтовує позицію про те, що суб'єкт права – це носій передбачених правовими нормами суб'єктивних прав та обов'язків, що має потенційну можливість участі у правовідносинах, тоді як суб'єкт правовідносин – це реальний учасник правовідносин. У конкретному випадку суб'єкт права може і не бути учасником правовідносин. Таким чином, вчений доходить висновку, що поняття «суб'єкт права» є більш широким за змістом, ніж поняття «суб'єкт правовідносин» [176, с.82]. «Суб'єкти права виступають як особи, що мають правосуб'єктність. Іншими словами, це громадяни, організації, громадські об'єднання, які можуть бути носіями юридичних прав та обов'язків, а відтак, брати участь у правовідносинах. У конкретному випадку суб'єкт права може і не бути учасником правовідносин. Суб'єкт права має потенційну можливість вступати у правовідносини, для чого він наділяється об'єктивним правом відповідною правосуб'єктністю», - пише Л.І. Миськів [78, с.111].

Варто відзначити, що суб'єкт, як реалізатор адміністративної процедур не знайшов належного опрацювання у науковій спільноті. Натомість, Законом України «Про адміністративну процедуру» надається визначення органам та особам, які виконують завдання процедурної діяльності. Згідно до пункту 1 частини 1 статті 2 Закону, адміністративний орган – 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). 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. 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 [111].

Отже, суб'єкт в праві – це фізична або юридична особа, наділена правами та обов'язками, а також здатністю реалізовувати покладені на неї правомочності та законні інтереси з метою чого взаємодіє з іншими суб'єктами права, вступаючи у суспільно-правові відносини. Суб'єкт може набувати нових прав та обов'язків, розширювати свій правовий статус виходячи із специфіки відносин в які він вступає. Наприклад, кожен громадянина, відповідно до Конституції України, володіє базовим набором юридичних можливостей. Водночас, коли він вступає на служби в державні органи на нього покладаються додаткові, спеціальні обов'язки та надаються особливі права, не доступні учасника інших суспільно-правових відносин.

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.

Тож, реалізація адміністративних процедур в цілому доступне обмеженому коло учасників публічно-правових відносин, які мають право реалізувати даний тип діяльності, зокрема, в сфері забезпечення кібербезпеки. Ураховуючи вказане, а також наукові концепції та положення Закону України «Про адміністративну процедуру» можемо зробити наступний висновок з приводу досліджуваної в даному розділі дисертація проблеми. Суб'єкти реалізації адміністративних процедур у сфері забезпечення кібербезпеки – це сукупність спеціально уповноважених органів державної влади та їх посадових осіб, наділених особливими правами та обов'язками в сфері реалізації відповідних різновидів адміністративних процедур в секторі кібербезпеки України.

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 [128].

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 [128].

Проте, далеко не кожний суб’єкт перелічений у вказаному вище Законі уповноважений безпосередньо надавати адміністративні процедури. Правовий статус лише окремих з них передбачає дану можливість. Зокрема, таким є Державна служба спеціального зв’язку та захисту інформації України, яка згідно до Закону України є державним органом, який призначений для забезпечення функціонування і розвитку державної системи урядового зв’язку, Національної системи конфіденційного зв’язку, формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, поштового зв’язку спеціального призначення, урядового фельд’єгерського зв’язку, активної протидії агресії у кіберпросторі, а також інших завдань відповідно до закону [113]. 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 [128].

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. Наприклад, відповідно до Постанови КМУ «Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України» від 03.09.2014 №411 адміністрація є центральним органом виконавчої влади із спеціальним статусом, діяльність якого спрямовується і координується Кабінетом Міністрів України через Віце-прем'єр-міністра України з інновацій, розвитку освіти, науки та технологій - Міністра цифрової трансформації і який забезпечує формування та реалізує державну політику у сферах організації спеціального зв'язку, захисту інформації, кіберзахисту, активної протидії агресії у кіберпросторі. В аспекті покладених на Адміністрацію завдань, даний орган: «1) установлює порядок створення та допуску до експлуатації, допускає до експлуатації засоби криптографічного захисту службової інформації та інформації, що становить державну таємницю, засоби, комплекси та системи спеціального зв'язку, визначає криптографічні алгоритми для застосування у засобах криптографічного захисту інформації;

2) здійснює повноваження органу ліцензування у сфері криптографічного і технічного захисту інформації; 3) порушує в установленому порядку питання про: а) припинення обробки інформації на об'єктах інформаційної діяльності або проведення інформаційної діяльності з використанням інформаційно-комунікаційних систем в державних органах, органах місцевого самоврядування, військових формуваннях, утворених відповідно до закону, на підприємствах, в установах і організаціях незалежно від форми власності, що проводиться з порушенням вимог законодавства у сфері захисту інформації, вимога щодо захисту якої встановлена законом, криптографічного та/або технічного захисту інформації; б) зупинення дії або скасування спеціальних дозволів на провадження діяльності, пов'язаної з державною таємницею, у разі виявлення порушень у сфері криптографічного і технічного захисту інформації і таке інше» [116].

Іншим структурним елементом відомства є Державний центр кіберзахисту Держспецзв'язку, який є державною установою, яка входить до загальної структури Служби та має своїм завдання: «1) впровадження організаційно-технічної моделі кібербезпеки як складової національної системи кібербезпеки; 2) забезпечення створення та функціонування основних складових системи захищеного доступу державних органів до мережі Інтернет; 3) забезпечення створення та функціонування системи антивірусного захисту національних інформаційних ресурсів; 4) аудит інформаційної безпеки та стану кіберзахисту об'єктів критичної інформаційної інфраструктури; 5) забезпечення створення та функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту; 6) забезпечення створення та функціонування системи взаємодії команд реагування на комп'ютерні надзвичайні події; 7) у взаємодії з іншими суб'єктами забезпечення кібербезпеки, розробка сценаріїв реагування на кіберзагрози, заходів щодо протидії таким загрозам, програм та методик проведення кібернавчань;

8) створення та забезпечення функціонування Національного центру резервування державних інформаційних ресурсів» [101].

В свою чергу, завданнями урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA: «1) накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів; 2) надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів; 3) організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту; 4) підготовка та розміщення на своєму офіційному веб-сайті рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз; 5) взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки; 6) взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки «FIRST» із сплатою щорічних членських внесків; 7) взаємодія з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору; 8) опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту; 9) сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам» [128].

Наступним суб'єктом виступає Національний банк України (далі – НБУ), який реалізує численні адміністративні процедури в сфері забезпечення кібербезпеки, але в сфері банківської діяльності. Закон України

«Про Національний банк України» закріплює, що НБУ є центральним банком України, особливим центральним органом державного управління, юридичний статус, завдання, функції, повноваження і принципи організації якого визначаються Конституцією України, законами України. Відповідно до Конституції України основною функцією Національного банку є забезпечення стабільності грошової одиниці України. У межах своїх повноважень він сприяє фінансовій стабільності, в тому числі стабільності банківської системи. Відповідно до статті 7 Закону НБУ виконує наступні функції, зокрема: «1) монопольно здійснює емісію національної валюти України та організує готівковий грошовий обіг; 2) встановлює для банків правила проведення банківських операцій, бухгалтерського обліку і звітності, захисту інформації, коштів та майна; 3) організовує створення та методологічно забезпечує систему грошово-кредитної та фінансової статистики, статистики платіжного балансу, міжнародної інвестиційної позиції, зовнішнього боргу, статистичної інформації фінансових установ, державне регулювання та нагляд за діяльністю яких здійснює Національний банк; 4) здійснює погодження статутів банків і змін до них, ліцензування банківської діяльності та операцій у передбачених законом випадках, веде Державний реєстр банків, створює та веде Кредитний реєстр Національного банку України тощо» [126].

Натомість 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 [128]. Конкретним прикладом процедурної діяльності НБУ є здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг відповідно до Постанови Правління НБУ від 16.01.2021 №4 [119].

Третім суб'єктом реалізації адміністративних процедур у сфері кібербезпеки є Служба безпеки України (далі – СБУ). Згідно до Закону України «Про Службу безпеки України» це державний орган спеціального призначення з правоохоронними функціями, який забезпечує державну безпеку України. СБУ підпорядкована Президенту України. На орган покладається захист державного суверенітету, конституційного ладу, територіальної цілісності, науково-технічного і оборонного потенціалу України, законних інтересів держави та прав громадян від розвідувально-підривної діяльності іноземних спеціальних служб, посягань з боку окремих організацій, груп та осіб, а також забезпечення охорони державної таємниці. До завдань Служби безпеки України також входить попередження, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, тероризму та інших протиправних дій, які безпосередньо створюють загрозу життєво важливим інтересам України. Діяльність Служби безпеки України здійснюється на основі дотримання прав і свобод людини. Органи і співробітники Служби безпеки України повинні

поважати гідність людини і виявляти до неї гуманне ставлення, не допускати розголошення відомостей про особисте життя людини. У виняткових випадках з метою припинення та розкриття державних злочинів окремі права та свободи особи можуть бути тимчасово обмежені у порядку і межах, визначених Конституцією та законами України [132].

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 [128].

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 [114].

Отже, незважаючи на широкий суб'єктний склад забезпечення кібербезпеки, який включає велику кількість різноманітних державних, правоохоронних, військових та інших органів, суб'єктами реалізації 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 у сфері забезпечення кібербезпеки в цілому, та з питань реалізації адміністративних процедур відповідного типу, зокрема, а їх правовий статус відповідає ознакам адміністративних органів, передбачених Законом України «Про адміністративну процедуру».

1.4. Правове регулювання реалізації адміністративних процедур у сфері забезпечення кібербезпеки

Адміністративні процедури в сфері кібербезпеки в силу своєї правової природи та глибокої сутності, мають багато спільного із адміністративними процедурами в інших сферах публічно-правових відносин. Разом із цим, їм притаманний і ряд специфічних, досить важливих рис обумовлених змістом правового регулювання даної категорії. Термін «регулювання» походить від латинського слова «regulo», що має значення «улаштовую, упорядковую». Сучасні тлумачні словники визначають дане слово таким чином: 1) направляти розвиток, рух чого-небудь з метою упорядкувати, систематизувати; 2) зрівнювати (хід, рух), розміряти, встановлювати в

порядку; 3) налагоджувати, створювати умови для нормальної діяльності, функціонування чого-небудь; [144, с.543; 16]. В економічному словнику регулювання (від англійської «regulation») визначається, як функція менеджменту щодо вивчення змін та факторів зовнішнього середовища, що мають вплив на якість управлінського рішення та ефективність функціонування системи менеджменту фірми, вжиттю заходів із доведення (удосконаленню) параметрів «входу» системи або процесів в ній до нових потреб «виходу» (споживачів) [25]. Отже, згідно до словникових положень, регулювання – це приведення чогось до відповідного порядку, систематизуючий вплив на певні об'єкти, діяльність із забезпечення структури і таке інше.

В межах науки управління регулювання, за поглядом І.О. Щебликіна та Д.В. Грибанова – це вид управлінської діяльності, спрямований на усунення відхилень, збоїв, недоліків тощо в керованій системі шляхом розроблення і впровадження керуючою системою відповідних заходів. Регулювання покликане усунути всі недоліки, відхилення, збої, виявлені у процесі контролювання. При цьому регулювальні заходи можуть застосовуватись на всіх попередніх етапах технології менеджменту (планування, організування, мотивування). Для цього вдаються до коригуючих дій, що базуються на виборі таких рішень: усунення відхилень; перегляд стандартів і критеріїв; усунення відхилень з переглядом стандартів і відхилень [177; 18, с.56]. Т.Г. Андрусяк вимічає: регулювання в сфері державного управління, визначається як функціональне призначення останнього і відповідні способи й технології забезпечення здійснення владної волі держави. Найважливішими серед них є: 1) встановлення загальноприйнятних умов нормальної упорядкованості суспільних відносин, загальних правил суспільної життєдіяльності; 2) актуалізація панування загальної волі, що виражається державою, у дійсній і поточній державно-управлінський діяльності, єдності державних органів у рамках єдиної публічно-правової особи, форм і методів

його планомірної діяльності; 3) вироблення арсеналу засобів державного управління [3]. Державне регулювання безпосередньо розглянуто Т. Кравцовою, як окрема галузь державного управління, яка являє собою цілеспрямовану організуючу діяльність органів державної влади, що реалізується за допомогою специфічних, притаманних лише їй правових форм і методів, які держава може застосовувати лише у сфері підприємництва [64, с.4; 27, с.68];

В юридичній царині поняття «регулювання» у структурі словосполучення «правове регулювання» відрізняється великим теоретичним навантаженням та складає одну з головних проблем правової науки. Це також відповідний вплив, але особливого типу, порядку організації та значення. В енциклопедичних джерелах, зокрема, Юридичній енциклопедії Ю.С. Шемшученка правове регулювання охарактеризовано, як один з основних засобів державного впливу на суспільні відносини з метою їх упорядкування в інтересах людини, суспільства і держави. Воно є різновидом соціального регулювання. Предмет правового регулювання – правові, політичні, економічні та інші суспільні відносини, впорядкувавши яких неможливе без використання норм права. Правове регулювання в Україні забезпечується системою державних органів законодавчої, виконавчої і судової гілок влади, прокуратурою та іншими контролюючими органами [179, с.40-41]. Автори Популярної юридичної енциклопедії розглядають категорію, як здійснюваний державою за допомогою всіх юридичних засобів владний вплив на суспільні відносини з метою їх упорядкування, закріплення, охорони й розвитку, а також вплив на поведінку та свідомість громадян шляхом проголошення їх прав та обов’язків, встановлення певних дозволів та заборон, затвердження певних правових актів тощо [108, с.369]. В Словнику юридичних термінів В.П. Марчука правове регулювання тлумачиться, як форма впливу на суспільні відносини, що здійснюються за

допомогою правових засобів [73, с.72]. Науковці у своїй більшості підтримують позицію викладену в довідниках.

Наприклад, на думку А.Т. Комзюка, правове регулювання – це специфічний вплив, який здійснюється правом як особливим нормативним інституційним регулятором. При цьому правове регулювання має цілеспрямований, організаційний, результативний характер і здійснюється за допомогою цілісної системи засобів, що реально виражають саму матерію права як нормативного інституту утворення – регулятора [58, с.47; 173, с.1055]. На думку І.П. Петрової та Д.Г. Мулявки, правове регулювання слід розуміти як різнобічний вплив на суспільні відносини всіх правових явищ, у тому числі правових ідей, принципів правового життя суспільства, які не втілені в юридичні форми (закони, нормативно-правові акти тощо) [103, с.10; 174, с.61]. А.М. Куліш правове регулювання розкриває, як здійснюваний в інтересах суспільства за допомогою норм права, вплив на поведінку учасників суспільних відносин з метою встановлення й упорядкування останніх [67, с.62].

С.В. Бобровник доводить, що правове регулювання – це особливий різновид соціального регулювання, яке: має визначений предмет, тобто сферу відносин, які усвідомлюються суб'єктами і мають для них і суспільства важливе значення; здійснюється нормативно закріпленими способами, які характеризують як активне право, так і пасивне право суб'єкта (дозволи), пасивний обов'язок вчиняти правомірні дії в інтересах уповноваженої сторони (зобов'язання); забезпечується певними методами, що координують дії учасників суспільних відносин, характеризуючи їх рівне становище у сфері права, або визначають їх субординаційну підлеглість у процесі використання прав і вдосконалення обов'язків, підкреслюючи цим наявність в одного із суб'єктів владних повноважень; стосується діяльності визначених суб'єктів, якими можуть бути фізичні, посадові, юридичні особи, органи держави та держава в цілому; визначає межі державно-правового втручання у

суспільні відносини, має цілеспрямований, організаційний та упорядкований характер; здійснюється за допомогою системи правових засобів, які в сукупності визначаються як механізм правового регулювання [12; 148, с.31]. О.Ф. Скакун, пише про те, що термін «правове регулювання» описує не тільки здійснюване державою за допомогою права і сукупності правових засобів упорядкування суспільних відносин, але й їх юридичне закріплення, охорона і розвиток, та підкреслює, що правовий вплив з усією його багатоманітністю здійснюється на суспільне життя, на свідомість та поведінку людей за допомогою правових і неправових засобів [143, с.488; 30, с.20].

І.М. Шопіна наголошує на поліаспектності розуміння правового регулювання, а саме: 1) в інституційному аспекті правове регулювання – це процес, наслідками якого є здійснення цілеспрямованого правового впливу держави на суспільні відносини; 2) у діяльнісному аспекті правове регулювання – це діяльність держави, її органів і посадових осіб, а також уповноважених на те громадських організацій щодо встановлення обов'язкових для виконання юридичних норм (правил) поведінки суб'єктів права їх реалізації в конкретних відносинах та застосування державного примусу до правопорушників з метою досягнення стабільного правопорядку в суспільстві; 3) у нормативно-юридичному аспекті правове регулювання – це здійснюване за допомогою спеціальних юридичних засобів упорядкування суспільних відносин, що включає їх юридичне закріплення, охорону, контроль за їх стабільністю та відновлення у випадку порушення тощо [173, с.1059].

Отже, категорія «правове регулювання» визначає призначення права, як ключового та єдиного регулятора суспільно-правових відносин. В ньому консолідується інформація про порядок практичної дії всієї юридичної системи із упорядкування поведінки суб'єктів відповідних соціальних зв'язків. Зміст правового регулювання становить система нормативно-

правових актів, що закріплюють в собі загальнообов’язкові правила та вимоги, вихідні засади (принципи) дії права на відповідні відносини (предмет регулювання), а також інші легальні інструменти.

Таким чином, правове регулювання реалізації адміністративних процедур у сфері забезпечення кібербезпеки - це здійснюваний за допомогою норм права регулюючий та упорядковуючий вплив на суспільні відносини, які виникають у досліджуваній сфері суспільного життя. Відповідний вплив здійснюється також за рахунок спеціальних юридичних інструментів і спрямований на забезпечення відповідності їх поведінки нормам чинного законодавства.

З огляду на зазначене вище, розглядати нормативно-правові акти у досліджуваній сфері найбільш доцільно в залежності від їх юридичної сили. В даному контексті, перш за все, слід приділити увагу Основному Закону нашої держави. Відмітимо, що прямих згадок про «кібербезпеку» в Конституції України немає. Це пояснюється тим, що Конституція є фундаментальним законом держави і зазвичай містить загальні принципи організації державної влади та прав і свобод людини. Однак, Конституція України містить ряд положень, які опосередковано пов'язані з забезпеченням кібербезпеки: 1) Стаття 32: Гарантує право на недоторканність приватного життя, особисту та сімейну таємницю. Це положення є основою для захисту персональних даних громадян у цифровому середовищі; 2) Стаття 34: Забезпечує свободу думки і слова, а також право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб. Це положення визначає правові рамки для використання інформаційних технологій; Стаття 106: Визначає, що захист державної таємниці здійснюється відповідно до закону. Це положення стосується захисту інформації, яка має стратегічне значення для держави. Таким чином, хоча Конституція України не містить прямої згадки про кібербезпеку, вона створює загально-правову основу для забезпечення цього виду безпеки.

Далі в розрізі представленої проблематики слід вказати міжнародні нормативно-правові акти. Зокрема, Конвенція Ради Європи про кіберзлочинність від 23.11.2001, відома як Будапештська конвенція, є єдиним юридично обов'язковим міжнародним документом з цього питання; у ній зазначено, що це перша міжнародна угода щодо злочинів, вчинених через Інтернет та інші комп'ютерні мережі, яка стосується зокрема порушень авторських прав, пов'язаного з комп'ютерами шахрайства, дитячої порнографії та порушень мережевої безпеки. Вона також стосується протиправних діянь виражених у формі зламу комп'ютерних мереж та перехоплення даних. Будапештська конвенція служить настановою для будь-якої країни, що розробляє всеохоплююче національне законодавство проти кіберзлочинів, та основою для міжнародного співробітництва між державами-учасницями цієї угоди [172; 59].

Конвенція стала підґрунтям для прийняття на території нашої держави цільового Закону України «Про основні засади забезпечення кібербезпеки України». Це головний акт зазначеної сфери, який визначає 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 [128].

До інших нормативних джерел правового регулювання реалізації адміністративних процедур у сфері кібербезпеки відносяться законодавчі акти, якими регламентовано повноваження та функції органів державної влади, що виступають суб'єктами забезпечення кібербезпеки: Державної служби спеціального зв'язку і захисту інформації України, Служби безпеки України, Національного банку України, Національної поліції України і таке інше. На основі цих законів створено об'ємну підзаконну базу, де знаходять

уточнення відповідні процедурні та інші типи діяльності органів державної влади.

Разом з цим, в контексті досліджуваної проблеми існує окрема правова засада – Закон України «Про адміністративну процедуру», у фокусі якого на відміну від інших юридичних документів знаходяться питання безпосередньо процедурної діяльності. Закон регулює відносини органів виконавчої влади, органів влади Автономної Республіки Крим, органів місцевого самоврядування, їх посадових осіб, інших суб'єктів, які відповідно до закону уповноважені здійснювати функції публічної адміністрації, з фізичними та юридичними особами щодо розгляду і вирішення адміністративних справ у дусі визначеної Конституцією України демократичної та правової держави та з метою забезпечення права і закону, а також зобов'язання держави забезпечувати і захищати права, свободи чи законні інтереси людини і громадянина [111; 60].

З огляду на вищевказане, нормативно-правове підґрунтя реалізації адміністративних процедур у сфері кібербезпеки основується на двох групах нормативно-правових актів: 1) ті, що визначають правові, організаційні, матеріально-технічні та інші особливості процесу підтримки стану безпечного користування кіберпростором, комунікаційними та технологічними системами; 2) ті, що пояснюють зміст, значення та особливості реалізації безпосередньо адміністративних процедур у досліджуваній сфері.

Подібна структура нормативно-правових актів дозволяє вірно упорядковувати суспільно-правові відносини відмежовуючи зв'язки з приводу чинення процедурної діяльності від інших, схожих за змістом, наприклад, відносин кримінального процесуального порядку, які також передбачають різнопланову, широку та систематизовану діяльність публічно-правових організацій. Окрім того, наявність спеціального законодавства дає підстави диференціювати суб'єктів забезпечення кібербезпеки на тих, хто

має повноваження адміністративного органу в розумінні Закону України «Про адміністративну процедуру» та усіх інших.

Зауважений дуалізм також проявляється і в принципах правового регулювання. В юридичній літературі загальновизнано, що принципи права – це основні, вихідні положення, які визначають загальну спрямованість права. Принципи права не тільки визначають зміст конкретних правових норм, а й, будучи їх складовими, безпосередньо регулюють суспільні відносини. Це стрижень усієї правової матерії. Вони виступають орієнтирами для формування права, відображають його сутність і реально існуючі зв'язки у правовій системі, пов'язані із засобами, механізмами правового регулювання [23, с.88; 14; 29, с.31].

Відповідно до визначеного, принципи правового регулювання реалізації адміністративних процедур в сфері забезпечення кібербезпеки – це основоположні, вихідні засади, які виражають ідею та соціальне призначення права згідно до чого спрямовується правове регулювання суспільних відносин в царині надання органами публічної влади адміністративних процедур забезпечення кібербезпеки.

Так, адміністративно-процедурна діяльність передусім основується на принципах, які визначають гуманістичну ідею державної влади та особливості регламенту відносин пов'язаних із кібербезпекою в цілому. За статтею 3 Конституції України людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю. Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Держава відповідає перед людиною за свою діяльність. Утвердження і забезпечення прав і свобод людини є головним обов'язком держави [60].

Згідно до Закону України «Про основні засади забезпечення кібербезпеки України» прийняття суб'єктами владних повноважень рішень на виконання норм законодавства про кібербезпеку здійснюються з

додержанням принципів: «1) мінімально необхідного регулювання, згідно з яким рішення (заходи) суб'єктів владних повноважень повинні бути необхідними і мінімально достатніми для досягнення мети і завдань, визначених законодавством; 2) об'єктивності та правової визначеності, максимально можливого застосування національного та міжнародного права щодо повноважень і обов'язків державних органів, підприємств, установ, організацій, громадян у сфері кібербезпеки; 3) забезпечення захисту прав користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій, та/або послуг із захисту інформації, кіберзахисту, у тому числі прав щодо невтручання у приватне життя і захисту персональних даних; 4) прозорості, згідно з яким рішення (заходи) суб'єктів владних повноважень мають бути належним чином обґрунтовані та повідомлені суб'єктам, яких вони стосуються, до набрання ними чинності (їх застосування); 5) збалансованості вимог та відповідальності, згідно з яким має бути забезпечено баланс між встановленням відповідальності за невиконання вимог кібербезпеки та кіберзахисту, а також за запровадження надмірних вимог та обмежень; 6) недискримінації, згідно з яким рішення, дії та бездіяльність суб'єктів владних повноважень не можуть призводити до юридичного або фактичного обсягу прав та обов'язків особи, який є: а) відмінним від обсягу прав та обов'язків інших осіб у подібних ситуаціях, якщо тільки така відмінність не є необхідною та мінімально достатньою для задоволення загальносуспільного інтересу; б) таким, як і обсяг прав та обов'язків інших осіб у неподібних ситуаціях, якщо така однаковість не є необхідною та мінімально достатньою для задоволення загальносуспільного інтересу; 7) еквівалентності вимог до забезпечення кібербезпеки об'єктів критичної інфраструктури, згідно з яким застосування правових норм повинно бути якомога більш рівнозначним щодо кіберзахисту комунікаційних та технологічних систем об'єктів критичної інфраструктури,

що належать до одного сектору економіки та/або які здійснюють аналогічні функції» [128].

Поряд із цим, при виконанні своїх повноважень суб'єкти забезпечення кібербезпеки, що володіють правом надавати адміністративні процедури, мають враховувати принципи здійснення останніх, до яких відноситься: «1) верховенство права, у тому числі законності та юридичної визначеності; 2) рівність перед законом; 3) обґрунтованість; 4) безсторонність (неупередженість) адміністративного органу; 5) добросовісність і розсудливість; 6) пропорційність; 7) відкритість; 8) своєчасність і розумний строк; 9) ефективність; 10) презумпція правомірності дій та вимог особи; 11) офіційність; 12) гарантування права особи на участь в адміністративному провадженні; 13) гарантування ефективних засобів правового захисту. Зокрема, згідно із окремими з цих принципів, адміністративний орган забезпечує належність та повноту з'ясування обставин справи, безпосередньо досліджує докази та інші матеріали справи» [111]. Під час здійснення адміністративного провадження обов'язково враховуються всі обставини, що мають значення для вирішення справи. Адміністративний орган забезпечує однакове ставлення до всіх учасників адміністративного провадження. Не допускається неправомірна заінтересованість в результатах розгляду та вирішення справи. Крім того, особа має право бути заслуханою адміністративним органом, надавши пояснення та/або заперечення у визначеній законом формі до прийняття адміністративного акта, який може негативно вплинути на право, свободу чи законний інтерес особи. Адміністративний орган зобов'язаний здійснювати інформування та консультування учасників адміністративного провадження з питань, що стосуються адміністративного провадження, а також щодо змісту їхніх прав та обов'язків [111].

Специфічних ознак також набуває предмет правового регулювання реалізації адміністративних процедур в сфері забезпечення кібербезпеки.

Зауважимо, слово «предмет» означає: 1) будь-яке конкретне матеріальне явище, що сприймається органами чуття; 2) логічне поняття, що становить зміст думки, пізнання; 3) те, на що спрямована пізнавальна, творча, практична діяльність кого-, чого-небудь; 4) коло знань, що становить окрему дисципліну викладання [145]. Філософія під предметом розглядає: 1) певну частину, сторону, той чи інший конкретний аспект об'єкта, що досліджується відповідною наукою; 2) коло найсуттєвіших питань, які вивчає наука; 3) єдність об'єкта, умов і засобів пізнання реальності [21; 79, с.93] Як зазначає О.М. Ярошенко, предмет – це категорія, яка визначає певну цілісність, виокремлену зі світу різноманітних об'єктів у процесі людської діяльності й пізнання. Предмет, пов'язаний з виявленням певних особливостей об'єкта, дозволяє відмежовувати галузі права [187187, с.92].

В свою чергу, предмет правового регулювання, за визначенням С.І. Запари – це група (вид) суспільних відносин, виділена на підставі певних ознак, які залежать від діяльності, поведінки і від самих учасників суспільних відносин [46, с.33]. В дисертаційному дослідженні В.М. Фесюніна визначається, що предмет правового регулювання – це все розмаїття суспільних відносин, які змінюються відповідно до конкретно-історичних умов, що регулює право. Своєї черги, безпосереднім предметом правового регулювання є вольова поведінка учасників суспільних відносин, через яку тільки і можна здійснювати відповідний вплив [160, с.54]. В тлумаченні В.В. Галунько, В.І. Курило та С.О. Короєда, предмет правового регулювання – це та сфера, на яку поширюється право, матеріальний критерій розподілу права на структурні елементи: інститути, галузі, підгалузі. Категорія відповідає на питання: що регулюється правом [1, с.9]. Влучну думку запропонувала Ю.Ю. Івчук, наголосивши: предмет правового регулювання – це те, на що впливає право. Кожна галузь об'єднує такі правові норми, які регулюють особливий, якісно визначений вид суспільних відносин, що об'єктивно вимагає специфічної правової регламентації. Таким чином,

головним фактором, що обумовлює відмінність однієї галузі права від іншої, є своєрідність суспільних відносин, які регулюються цими галузями права [50, с.34].

Таким чином, предмет правового регулювання – це сукупність суспільно-правових відносин регламентованих та упорядкованих відповідними юридичними засобами та інструментами які виникають між суб'єктами права. Відмінністю предмета правового регулювання реалізації адміністративних процедур у сфері забезпечення кібербезпеки є незвичайність останнього. Його складають суспільно-правові відносини особливого порядку виникнення, між окремими суб'єктами державної влади та фізичними і юридичними особами, які охоплюються наступне коло питань: 1) реагування уповноважених публічних органів на порушення встановленого порядку роботи із комунікаційними, технологічними системами, використання електронно-обчислювальної (комп'ютерної) техніки, програмного забезпечення та взаємодії в кіберпросторі; 2) забезпечення надійності, правильності, безпечності використання всіма фізичними та юридичними особами комунікаційних, технологічних систем, комп'ютерних мереж, кіберпростору; 3) здійснення державного регулювання та контролю процесів, пов'язаних із використанням фізичними та юридичними особами кіберпростору, а також порядку обробки інформації в комунікаційних, технологічних системах нормативним вимогам та стандартам безпеки; 4) реалізації прав громадян, інших фізичних та юридичних осіб на безпечне і безперешкодне користування кіберпростором, обмін та обробку інформації в технологічних, комунікаційних системах, за допомогою електронно-обчислювальної техніки (комп'ютерів).

Остання особливість уособлена в правових інструментах, які застосовуються для правового регулювання реалізації адміністративних процедур в сфері кібербезпеки. Зокрема, чинним законодавством

передбачено спеціальну форму реалізації процедурної діяльності у вигляді адміністративного акту.

Адміністративний акт є об'єктивованим вираженням правової форми діяльності суб'єктів державного управління; адміністративно-правові акти управління є основною юридичною формою перетворення у життя завдань та функцій виконавчої влади. До найбільш значних якісних ознак адміністративного акту, що визначають його юридичну природу відносяться: по-перше, він має державно-владний характер і є обов'язковим для адресата та має правове походження. Адміністративний акт це – перш за все юридично-владне волевиявлення відповідного суб'єкта виконавчої влади. У ньому знаходить свій вираз владна природа управлінської діяльності держави. По-друге, виконання адміністративно-правового акту забезпечується владою державного примусу. Юридична сила акту державного управління, як акту, що створений волею людей, означає, що він має державно-владний характер, забезпечується примусовою владою держави. Правовий характер адміністративно-правового акту є рисою, яка властива всім актам державних органів. Особливість правового характеру адміністративного акту органу виконавчої влади полягає в тому, що він містить державно-владне юридичне рішення управлінських питань [75, с.117]

Відповідно до Закону України «Про адміністративну процедуру» адміністративний акт – це рішення або юридично значуща дія індивідуального характеру, прийняте (вчинена) адміністративним органом для вирішення конкретної справи та спрямоване (спрямована) на набуття, зміну, припинення чи реалізацію прав та/або обов'язків окремої особи (осіб) [111].

Отже, адміністративний акт стандартизує реалізацію адміністративних процедур у сфері забезпечення кібербезпеки, адже за допомогою встановлення обов'язковості даної форми законодавець показує, яким має бути результат процедурної діяльності. Крім того, обов'язковість прийняття

кінцевого документу виступає своєрідною гарантією реалізації мети і завдань підтримки належного рівня кібербезпеки. Видання адміністративного акту – це логічне завершення адміністративної процедури із гарантованим, законним рішенням щодо прав, свобод та інтересів відповідних фізичних та юридичних осіб.

У підсумку слід вказати, що правове регулювання реалізації адміністративних процедур у сфері забезпечення кібербезпеки ґрунтується на дуалізмі нормативної основи та принципів. Механізм юридичного впливу комбінує в собі юридичні документи та вихідні засади, що відносяться і до сектору кібербезпеки, і до галузі реалізації адміністративних процедур. В сукупності вони забезпечують регламент специфічного предмету суспільно-правових відносин, які охоплюють питання державного регулювання і забезпечення безпеки використання юридичними та фізичними особами кіберпростору, технологічних, комунікаційних систем. За рахунок спеціальних інструментів правового регулювання досягається гарантованість конкретизованого юридичного результату провадження таких процедур.

Таким чином, проведене наукове дослідження дає змогу констатувати, що на сьогоднішній день система правового регулювання реалізації адміністративних процедур у сфері забезпечення кібербезпеки складається із ряду нормативно-правових актів різної юридичної сили, кожен із яких регулює певний напрямок досліджуваного питання. При цьому слід зауважити, що незважаючи на значну увагу збоку законодавця та урегульованість досліджуваного питання, у зазначеній сфері залишається чимала кількість проблем. Зокрема: по-перше, невизначеним є перелік адміністративних процедур, які реалізуються у відповідній сфері суспільного життя; по-друге, коло та правовий статус суб’єктів, які здійснюють відповідну діяльність є досить розмитим; по-третє, законодавцем недостатньо розробленим є питання впровадження міжнародних стандартів у цій сфері.

Висновки до розділу 1

Аргументовано, що у найбільш загальному розумінні безпека – це певний динамічний стан суспільного порядку, за якого кожна людина має психологічне відчуття захищеності, а також має реальні гарантії недопущення негативного впливу на її права, свободи, інтереси, а також життя та здоров'я будь-яких негативних чинників.

Зроблено висновок про те, що кібербезпеку найбільш доцільно тлумачити у широкому та вузькому розумінні. Так, відповідно до широкого підходу, кібербезпека – це сукупність врегульованих нормами законодавства суспільно-правових відносин, які виникають з приводу забезпечення дотримання всіма суб'єктами нормативно-правових вимог і стандартів у сфері використання комунікаційних та технологічних систем, а також електронно-обчислювальної (комп'ютерної) техніки, програмного забезпечення у кіберпросторі, порушення якого є підставою для їх притягнення до юридичної відповідальності. У вузькому значенні кібербезпека – це стан суспільно-правового порядку, за якого повністю відсутні та/або мінімізовані, а також своєчасно виявляються, попереджаються і припиняються негативні чинники та протиправні дії, які порушують права та інтереси людини, громадянина, суспільства і держави при використанні комунікаційних, технологічних систем, електронно-обчислювальної (комп'ютерної) техніки, програмного забезпечення та взаємодії в кіберпросторі, що забезпечує сталий розвиток інформаційного суспільства, культури використання комп'ютерної техніки та цифрових комунікацій.

Встановлено, що забезпечення кібербезпеки - це реалізований спеціально уповноваженими суб'єктами комплекс заходів, технологій, процесів і практик, що спрямовано на захист інформаційних систем, мереж, даних і програм від несанкціонованого доступу, використання, розкриття,

зміни, руйнування або втрати. Така діяльність включає забезпечення конфіденційності, цілісності та доступності інформації, а також протидію кіберзагрозам і кібератакам з боку зловмисників у цифровому просторі.

Констатовано, що кібербезпека як об'єкт адміністративно-правового регулювання характеризується наступними особливостями: по-перше, представляє собою особливу групу правовідносин, що виникають у специфічній сфері суспільного життя; по-друге, обумовлює необхідність здійснення низки різноманітних дій та заходів спеціально уповноваженими органами державної влади, а також приватними суб'єктами; по-третє, відповідна діяльність, переважно, регулюється нормами адміністративної галузі права; по-четверте, є сферою реалізації різноманітних процедур, які носять адміністративний характер.

Відмічено, що з правової точки зору процедура – це регламентований нормами права прядок вчинення уповноваженими суб'єктами юридично значимих дій з метою задоволення законних інтересів суспільства і держави. Здійснення правової процедури в обов'язковому порядку передбачає отримання якогось кінцевого, формально-вираженого правового результату у вигляді зміни, припинення або появи нових правовідносин.

Наголошено, що на сьогоднішній день склались дві відносно самостійні концепції щодо тлумачення змісту та призначення адміністративних процедур. Відповідно до першого підходу, ця категорія охоплює всю публічно-управлінську діяльність органів державної влади і місцевого самоврядування із реалізації покладених на них законодавством повноважень, а також вирішення адміністративних справ щодо забезпечення реалізації прав, свобод і законних інтересів фізичних та юридичних осіб, а також внутрішньої організації їхньої діяльності. В даному випадку поняття «адміністративна процедура» ототожнюється із адміністративною діяльністю державних і муніципальних органів. Друга концепція відповідає законодавчому трактуванню та характеризує адміністративну процедуру, як

регламентований законодавством України порядок дій спеціально уповноважених суб'єктів з приводу забезпечення реалізації та захисту прав, свобод і законних інтересів фізичних та юридичних, кінцевим етапом якого є прийняття адміністративного акту.

З'ясовано, що адміністративні процедури у сфері забезпечення кібербезпеки – це визначений законодавством України порядок дій, які реалізуються спеціально уповноваженими суб'єктами у напрямку забезпечення і захисту прав та законних інтересів фізичних та юридичних осіб, а також з метою реалізації публічних повноважень у сфері використання комунікаційних, технологічних систем, електронно-обчислювальної (комп'ютерної) техніки, програмного забезпечення та взаємодії у кіберпросторі.

Доведено, що особливостями адміністративних процедур у сфері забезпечення кібербезпеки є наступні: по-перше, особлива сфера реалізації, а також предмет з приводу якого виникають відповідні суспільні відносини; по-друге, реалізовувати відповідні процедури мають право виключно спеціально уповноважені суб'єкти, посадові особи яких володіють особливим набором професійних знань, умінь та навичок; по-третє, наявність спеціального набору нормативно-правових засад їх реалізації; по-третє, переважна більшість адміністративних процедур пов'язані з обробкою персональних даних, що вимагає дотримання вимог законодавства про захист персональних даних; по-четверте, наявність підвищеного рівня відповідальності суб'єктів, що відповідні процедури реалізовують; по-п'яте, відповідні процедури застосовуються у різних сферах забезпечення кібербезпеки, що обумовлює наявність їх різновидів.

Аргументовано, що адміністративні процедури у сфері забезпечення кібербезпеки слід поділити на наступні групи: 1) адміністративні процедури пов'язані із організаційно-управлінським забезпеченням кібербезпеки; 2) адміністративні процедури, пов'язані із змістом інформації, що

обробляється в комунікаційних або в технологічних системах; 3) адміністративні процедури, пов’язані із захистом інформації, що становить державну таємницю, комунікаційних та технологічних систем, призначених для її оброблення; 4) адміністративні процедури захисту комунікаційних систем, які не взаємодіють з публічними мережами електронних комунікацій.

Обґрунтовано, 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.

Підкреслено, що незважаючи на широкий суб’єктний склад забезпечення кібербезпеки, який включає велику кількість різноманітних державних, правоохоронних, військових та інших органів, суб’єктами реалізації 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 у сфері забезпечення кібербезпеки в цілому, та з питань реалізації адміністративних процедур відповідного типу, зокрема, а їх правовий статус відповідає ознакам адміністративних органів, передбачених Законом України «Про адміністративну процедуру».

Зазначено, що правове регулювання реалізації адміністративних процедур у сфері забезпечення кібербезпеки - це здійснюваний за допомогою норм права регулюючий та упорядковуючий вплив на суспільні відносини, які виникають у досліджуваній сфері суспільного життя. Відповідний вплив здійснюється також за рахунок спеціальних юридичних інструментів і

спрямований на забезпечення відповідності їх поведінки нормам чинного законодавства.

Наголошено, що нормативно-правове підґрунтя реалізації адміністративних процедур у сфері кібербезпеки основується на двох групах нормативно-правових актів: 1) ті, що визначають правові, організаційні, матеріально-технічні та інші особливості процесу підтримки стану безпечного користування кіберпростором, комунікаційними та технологічними системами; 2) ті, що пояснюють зміст, значення та особливості реалізації безпосередньо адміністративних процедур у досліджуваній сфері.

Відмічається, що адміністративний акт стандартизує реалізацію адміністративних процедур у сфері забезпечення кібербезпеки, адже за допомогою встановлення обов'язковості даної форми законодавець показує, яким має бути результат процедурної діяльності. Крім того, обов'язковість прийняття кінцевого документу виступає своєрідною гарантією реалізації мети і завдань підтримки належного рівня кібербезпеки. Видання адміністративного акту – це логічне завершення адміністративної процедури із гарантованим, законним рішенням щодо прав, свобод та інтересів відповідних фізичних та юридичних осіб.

Констатовано, що на сьогоднішній день система правового регулювання реалізації адміністративних процедур у сфері забезпечення кібербезпеки складається із ряду нормативно-правових актів різної юридичної сили, кожен із яких регулює певний напрямок досліджуваного питання. При цьому слід зауважити, що незважаючи на значну увагу збоку законодавця та урегульованість досліджуваного питання, у зазначеній сфері залишається чимала кількість проблем. Зокрема: по-перше, невизначеним є перелік адміністративних процедур, які реалізуються у відповідній сфері суспільного життя; по-друге, коло та правовий статус суб'єктів, які здійснюють відповідну діяльність є досить розмитим; по-третє, законодавцем недостатньо розробленим є питання впровадження міжнародних стандартів у цій сфері.

РОЗДІЛ 2.
ПОРЯДОК ЗДІЙСНЕННЯ ОКРЕМИХ АДМІНІСТРАТИВНИХ ПРОЦЕДУР У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

2.1. Адміністративні процедури, пов'язані із змістом інформації, що обробляється в комунікаційних або в технологічних системах

Одну з груп адміністративних процедур в сфері забезпечення кібербезпеки на території України становлять ті, що пов'язані із змістом інформації, що обробляється в комунікаційних або в технологічних системах. Вона об'єднує в собі діяльність різних органів влади та їх посадових осіб. Водночас, дані процедури мають досить специфічний та вузький зміст, обумовлений тим фактом, що згідно до статті 2 Закону України «Про основні засади забезпечення кібербезпеки України», положення закону не поширюються на відносини та послуги, пов'язані із змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах [128]. 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».

Слово «інформація» походить від латинського «informatio» (роз'яснення, виклад, поінформованість) та означає сукупність даних, знань, відомостей тощо [56, с.35]. З погляду теорії семіотики інформація – це міра ліквідації невизначеності знання одержувача повідомлення про стан об'єкта чи яку-не- будь подію. Для визначення інформації використовують два основних підходи: атрибутивний і функціональний. Атрибутивний підхід розглядає інформацію як об'єктивну властивість усіх матеріальних об'єктів, функціональний же стверджує, що інформація є умовою і результатом

активної діяльності і можлива тільки на соціальному рівні. Крім того, інформація розглядається як усі відомості, знання, повідомлення, що допомагають у вирішенні того чи іншого завдання. Інформація як окрема наукова категорія з погляду технічних фахівців становить набір будь-яких даних, а на думку гуманітаріїв, – це певні відомості [2828, с.69; 105, с.78].

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 Закон 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. До інформації з обмеженим доступом не можуть бути віднесені такі відомості: «1) про стан довкілля, якість харчових продуктів і предметів побуту; 2) про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей; 3) про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про

соціально-демографічні показники, стан правопорядку, освіти і культури населення; 4) про факти порушення прав і свобод людини, включаючи інформацію, що міститься в архівних документах колишніх радянських органів державної безпеки, пов’язаних з політичними репресіями, Голодомором 1932-1933 років в Україні та іншими злочинами, вчиненими особами, які брали участь або сприяли реалізації російської імперської політики, представниками комуністичного та/або націонал-соціалістичного (нацистського) тоталітарних режимів; 5) про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб; 5-1) щодо діяльності державних та комунальних унітарних підприємств, господарських товариств, у статутному капіталі яких більше 50 відсотків акцій (часток) належать державі або територіальній громаді, а також господарських товариств, 50 і більше відсотків акцій (часток) яких належать господарському товариству, частка держави або територіальної громади в якому становить 100 відсотків, що підлягають обов’язковому оприлюдненню відповідно до закону; 6) інші відомості, доступ до яких не може бути обмежено відповідно до законів та міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України» [124].

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 системах» 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 (далі – КСЗІ) [121].

Оцінка стану захищеності в державних органах, органах місцевого самоврядування, військових формуваннях, на підприємствах, в установах і організаціях незалежно від форм власності проводиться згідно з річним

планом, який затверджується наказом Адміністрації Держспецзв'язку, або позапланово. Планова оцінка стану захищеності проводиться в державних органах, військових формуваннях, на підприємствах, в установах і організаціях незалежно від форм власності не частіше ніж один раз на п'ять років. Позапланова оцінка стану захищеності проводиться в державних органах, органах місцевого самоврядування, військових формуваннях, на підприємствах, в установах і організаціях незалежно від форм власності за їх безпосередніми зверненнями та рішенням Голови Держспецзв'язку або його заступника за напрямом діяльності згідно з розподілом функціональних обов'язків. За результатами оцінки стану захищеності складається акт, де викладаються результати роботи комісії та рекомендації стосовно підвищення рівня захищеності державних інформаційних ресурсів, який затверджується Головою Держспецзв'язку або його заступником за напрямом діяльності згідно з розподілом функціональних обов'язків [121].

Порядок проведення даної адміністративної процедури передбачає покладення на суб’єктів її здійснення, а також суб’єктів які оцінюються додаткових обов’язків, що визначають специфіку зазначеного різновиду діяльності. Так, згідно до Наказу з метою здійснення оцінки стану захищеності: «1) Держспецзв'язку: створює комісію з оцінки стану захищеності; здійснює планування проведення оцінки стану захищеності в державних органах, органах місцевого самоврядування, військових формуваннях, на підприємствах, в установах і організаціях незалежно від форм власності; розробляє загальну програму та методику оцінки стану захищеності в державних органах, органах місцевого самоврядування, військових формуваннях, на підприємствах, в установах і організаціях незалежно від форм власності, а також окремі програми та методики оцінки захищеності залежно від виду ІКС та режиму доступу до інформації, що в ній обробляється; визначає перелік документів, що стосуються функціонування ІКС та підлягають аналізу під час проведення оцінки стану захищеності;

визначає та оприлюднює на офіційному веб-сайті Держспецзв'язку у мережі Інтернет перелік спеціалізованого програмного забезпечення та програмно-апаратних засобів, які використовуються для проведення оцінки захищеності; 2) державні органи, органи місцевого самоврядування, військові формування, підприємства, установи і організації незалежно від форм власності, в яких здійснюється оцінка стану захищеності: надають комісії всі необхідні документи, що стосуються функціонування ІКС; надають комісії доступ до ІКС; повідомляють Держспецзв'язку про стан виконання рекомендацій, зазначених в Акті» [121].

Схожою до попередньої 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 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 [122].

Сканування проводиться Державним центром кіберзахисту Державної служби спеціального зв’язку та захисту інформації України: «1) за письмовим зверненням державного органу, органу місцевого самоврядування, військового формування, підприємства, установи і

організації державної форми власності; 2) в автоматичному режимі відповідно до переліку об’єктів сканування, який формується у рамках планування проведення оцінки стану захищеності в державних органах, органах місцевого самоврядування, військових формуваннях, на підприємствах, в установах і організаціях незалежно від форм власності» [122]. Посадовим особам ДЦКЗ Держспецзв’язку, що безпосередньо проводять сканування, забороняється розголошувати його результати третім сторонам, а також використовувати виявлені вразливості для проведення дій, що можуть призвести до порушення штатного режиму функціонування ІКС, що сканується, порушення цілісності, конфіденційності та доступності інформації та розміщених в інтернеті, а також для отримання доступу до персональних даних, що можуть оброблятися в ІКС [122].

За результатами сканування за письмовим зверненням посадові особи Держспецзв’язку, що безпосередньо здійснювали процедуру, складають акт за нормативно встановленою формою. В свою чергу, за результатами проведення автоматизованого дистанційного сканування ДЦКЗ Держспецзв’язку інформує: розпорядників розміщених в Інтернеті – якщо під час автоматизованого дистанційного сканування виявлено вразливості та недоліки у налаштуванні ІКС, в якій обробляються державні інформаційні ресурси [122122].

Наступною адміністративною процедурою, яку реалізовує Держспецзв’язку, виступає державна експертиза у сфері технічного захисту інформації. За своєю сутністю це особлива процедурна діяльність, яка суттєво відрізняється від оцінки та сканування. Зауважимо, поняття «експертиза» походить від французького слова «expertise» (досвідчений, випробуваний) та означає вивчення, перевірку, аналітичне дослідження, кількісну або якісну оцінку висококваліфікованим фахівцем, установою, організацією певного питання, явища, процесу, предмету тощо, які вимагають спеціальних знань у відповідній сфері суспільної діяльності. За

гносеологічною природою експертиза – це різновид практичного пізнання конкретних фактів, явищ з використанням положень науки, наукових засобів і методів за науково розробленою і апробованою практикою методикою. В основі експертизи як виду дослідження лежать як відомі (вихідні) емпіричні дані, так і наукові факти, функції яких полягають у встановленні предмета експертизи, виявленні видів зв'язків між емпіричними даними, визначенні можливості існування шуканого факту тощо [70, с.11].

Проблематика експертної діяльності має досить тривалу історію. Перш за все, експертна робота пов'язана із технічними та прикладними науками, де на практичному рівні відбувається процес отримання нових знань про людину і особливості її біологічного розвитку; природу і техніку, завдяки проведенню так званих медичних, технічних, екологічних експертиз. Практична експертна діяльність, особливо наукова експертна діяльність, входить до складу засобів обґрунтування гіпотез та апробації результатів наукового пізнання. У сучасній практиці експертна діяльність знаходить своє відображення в окремому специфічному інституті, що наділений рядом специфічних ознак, основними серед яких є незалежність, неупередженість, самостійність, професійність та забезпеченість висококваліфікованим кадровим потенціалом. Експертна діяльність отримує міждисциплінарний статус, оскільки застосовується не лише в прикладних технічних науках, а й в гуманітарній сфері (соціології, політології, економіці тощо). В юридичному значенні експертна діяльність безпосередньо пов'язується з інститутами криміналістики, кримінального й цивільного процесів та судочинства. Наукові дослідження експертної діяльності в сфері криміналістики і судочинства мають тривалу історію становлення й розвитку та пов'язані з такими поняттями, як дактилоскопічна експертиза, експертиза документів, судово-медична експертиза, наукова та науково-технічна експертиза тощо [181, с.333; 24; 54; 36, с.170-171].

Отже, експертиза – це складна, багаторівнева діяльність осіб, які володіють спеціальними знаннями у відповідній галузі, яка передбачає комплексне дослідження якогось об'єкту, його внутрішньої специфіки згідно до поставлених експертних завдань. Так, інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю сертифікатом або позитивним експертним висновоком за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації [49].

Згідно до Наказу Держспецзв'язку «Про затвердження Положення про державну експертизу у сфері технічного захисту інформації» від 16.05.2007 №93 така експертиза проводиться з метою дослідження, перевірки, аналізу та оцінки об'єктів експертизи щодо їх відповідності вимогам нормативних документів з технічного захисту інформації та можливості їх використання для забезпечення технічного захисту інформації. Об'єктами експертизи є: «1) комплексні системи захисту інформації (далі – КСЗІ) які є невід'ємною складовою інформаційної, електронної комунікаційної або інформаційно-комунікаційної системи; 2) апаратні, апаратно-програмні і програмні засоби, які реалізують функції ТЗІ та/або оцінки стану захисту інформації; 3) організаційно-технічне рішення для впровадження типової компоненти КСЗІ в ІКС – задокументоване уніфіковане рішення для багаторазового розгортання складових КСЗІ в ІКС, самодостатнє для вирішення певного завдання, що містить проєктні рішення програмно-технічного комплексу, організаційно-технічні рішення щодо регламенту функціонування типової компоненти ІКС та опис (алгоритм) процедури впровадження (розгортання) компоненти КСЗІ в ІКС (далі - ОТР КСЗІ)» [117]. Суб'єктами експертизи є: «юридичні та фізичні особи - власники (розпорядники) інформаційних,

електронних комунікаційних, інформаційно-комунікаційних систем; апаратних, апаратно-програмних і програмних засобів, які реалізують функції ТЗІ; Адміністрація Держспецзв'язку; територіальні органи Адміністрації Держспецзв'язку; навчальні заклади, науково-дослідні, науково-виробничі установи, підприємства, установи та організації, які проводять експертизу; державні органи, які проводять експертизу в сфері свого управління; фізичні особи, які на постійній або професійній основі здійснюють діяльність, пов'язану з наданням експертних послуг» [117].

З метою організації та проведення експертиз, координації заходів і прийняття рішень щодо проведення експертиз в Адміністрації Держспецзв'язку створюється експертна рада з питань державної експертизи в сфері технічного захисту інформації. За результатами експертного дослідження складається спеціальний, експертний висновок, котрий повинен містити: загальні відомості щодо об'єкта експертизи (тип, місце розташування, власник); загальну характеристику об'єкта експертизи (призначення, функції, можливості щодо вирішення певних завдань захисту інформації); перелік нормативних документів з ТЗІ, на відповідність вимогам яких проводиться оцінка об'єкта експертизи; назви програми та методики, згідно з якими проводилася оцінка об'єкта експертизи, ким розроблені та затверджені, реєстраційний номер та дату затвердження; перелік документів і специфікацій програмних та технічних засобів ТЗІ; перелік засобів ТЗІ (із зазначенням їх типів, заводських номерів, року випуску) – у разі проведення експертизи засобів ТЗІ; результати робіт щодо кожного пункту програми проведення експертизи об'єкта; розгорнутий висновок щодо відповідності об'єкта експертизи вимогам нормативних документів із ТЗІ; сферу використання (вимоги до умов експлуатації) об'єкта експертизи; строк дії експертного висновку; особливі думки експертів, зафіксовані в протоколах виконання робіт [117].

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 підрозділі 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» [69, 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». 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 [119].

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» [119]. 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)» [119].

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 [119].

Підбиваючи підсумок представленого підрозділу дисертаційного 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 виступає 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.

2.2. Адміністративні процедури, пов'язані із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення

Найбільш специфічним та особливим різновидом адміністративних процедур в сфері кібербезпеки є ті, що пов'язані із захистом державної таємниці, а також комунікаційних, технологічних систем, призначених для її оброблення. Унікальні ознаки такої діяльності формуються завдяки відмінному правовому статусу та спеціальних вимог щодо організації захисту зазначеної інформації, порівняно із іншими передбаченими законодавством типами відомостей і даних. Закон України «Про державну таємницю» встановлює: «державна таємниця або секретна інформація – це вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому законодавством, державною таємницею і підлягають охороні державою» [114].

Зміст державної таємниці неодноразово ставав предметом наукових досліджень, які також варто взяти до уваги. Так, в розумінні В.Ф. Пузирного державна таємниця – непросте і досить суперечливе соціально-правове явище. «Під державною таємницею, на наш погляд, треба розуміти інформацію, яка в установленому порядку віднесена до державної таємниці та захищається державою відповідно до нормативно-правових актів. Державна таємниця є самостійним правовим інститутом суверенної демократичної держави, який визначає коло відомостей, поширення яких може заподіяти шкоду зовнішній безпеці України. Інститут державної таємниці є основною складовою системи інформаційної безпеки, що є частиною системи національної безпеки держави», - пише автор [134, с.40-41].

А.М. Благодарний наголошує, що державна таємниця – це найважливіші для України відомості в різних сферах життєдіяльності. Витік такої інформації ставить під загрозу інтереси України у сфері зовнішньополітичної, економічної, науково-технічної, оперативно-розшукової та інших видів діяльності. Тому охорона державної таємниці була й залишається складовою частиною загальної системи забезпечення національної безпеки України. При порушенні законодавства про державну таємницю суспільна шкідливість полягає у створенні можливості потрапляння відомостей, що становлять державну таємницю, у розпорядження іноземної розвідки або інших організацій і осіб, які можуть використати їх на шкоду державі, суспільству чи окремим громадянам [11, с.13-14].

Наступну наукову позицію з приводу змісту державної таємниці наводить О.Г. Семенюк: сукупність відомостей, засекречування яких продиктоване суспільною необхідністю безпечних умов існування особи, суспільства та держави [139, с.42-43]. Визначаючи родову належність поняття «державна таємниця» В.І. Олійник виокремив наступні ознаки категорії: 1) цей вид таємниці включає відомості (інформацію) у певних сферах життя держави, що закріплені нормативно; 2) ці відомості мають відповідний гриф секретності, суворо регламентований порядок засекречування й розсекречування, процедури допуску до роботи з ними, закріплені на законодавчому рівні; 3) відомості можуть бути відомі або довірені тільки особам, які мають допуск до них, на яких поширюється обов'язок зберігати ці відомості в таємниці; 4) недоторканність відомостей забезпечується державним захистом і встановленою юридичною відповідальністю; 5) незаконне отримання й поширення цих відомостей може заподіяти шкоду передусім національним інтересам [99]. Схожий науковий підхід наводить О. Шамсутдінов, який до ознак державної таємниці відносить: 1) обмеженість доступу до державної таємниці як виду таємної

інформації, тобто відомості, що становлять таку таємницю, підлягають засекречуванню (обмеженню їх поширення і доступу до їх матеріальних носіїв); 2) значущість, важливість такого роду відомостей у певний проміжок часу для інтересів держави, тобто в разі розголошення державної таємниці національній безпеці України може бути завдана суттєва шкода (матеріальний критерій); 3) чітке визначення сфер, у яких може існувати державна таємниця, а саме: оборона, економіка, наука і техніка, зовнішні відносини, державна безпека й охорона правопорядку; 4) передбачуваність відомостей, що становлять державну таємницю, законом, тобто встановлення переліку таких відомостей у спеціальному правовому акті – Зводі, на підставі та в межах якого створюються розгорнуті переліки відомостей, що становлять державну таємницю (формальний критерій); 5) охорона такої секретної інформації державою, тобто встановлення на підставі чинного законодавства єдиного порядку забезпечення охорони зазначеної інформації державноправовими засобами [170, с.22-23; 134, с.39].

З огляду на зазначене вище, що державна таємниця є особливо важливим різновидом інформації в найбільш суспільно-значимих сферах (оборони, економіки, науки і техніки, міжнародних відносинах, галузі державної безпеки, охорони правопорядку, тощо), порядок доступу до якої обмежено законодавством України з метою недопущення її несанкціонованого розголошення, що матиме шкідливі наслідки для національної безпеки. Тож, головними ознаками державної таємниці є: 1) її становлять не всі відомості, а лише ті, що прямо віднесені до даної категорії інформації в установленому законом порядку; 2) спеціальний захист державної таємниці передбачає особливий порядок надання уповноваженим суб’єктам доступу до відомостей і даних, які становлять зміст цієї категорії; 3) обробка, передача та збереження відомостей і даних, що становлять державну таємницю, у тому числі в комунікаційних та технологічних

системах, відбувається із дотриманням спеціальних правил та використанням заходів захисту.

Таким чином, адміністративні процедури, пов’язані із захистом інформації, що становить державну таємницю, а також комунікаційних та технологічних систем призначених для її оброблення – це системна та систематизована діяльність спеціально уповноважених органів державної влади, яка спрямована на вчинення особливого роду дій та заходів спрямованих на організацію дієвого захисту та підтримки високого рівня безпеки при обробці та використанні інформації, що становить державну таємницю у відповідних системах, з метою запобігання та попередження її несанкціонованого витоку, що може нанеси шкоду національним інтересам та безпеці.

Першим прикладом подібних адміністративних процедур є процес віднесення інформації до державної таємниці. Дана процедура цікава тим, що результат її здійснення – це фактичне створення секретної інформації, а також встановлення можливості користуватись нею у тому числі за допомогою комунікаційних, технологічних систем. Так, Закон України «Про державну таємницю» визначає, що віднесення інформації до державної таємниці – це процедура прийняття рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з установленням ступеня їх секретності шляхом обґрунтування та визначення можливої шкоди національній безпеці України у разі розголошення цих відомостей, включенням цієї інформації до Зводу відомостей, що становлять державну таємницю, та з опублікуванням цього Зводу, змін до нього. До державної таємниці можуть бути віднесений чіткий перелік даних, наприклад, про: зміст стратегічних і оперативних планів та інших документів бойового управління, підготовку та проведення військових операцій, стратегічне та мобілізаційне розгортання військ, а також про інші найважливіші показники, які характеризують організацію, чисельність, дислокацію, бойову і

мобілізаційну готовність, бойову та іншу військову підготовку, озброєння та матеріально-технічне забезпечення Збройних Сил України та інших військових формувань; винаходи, дослідження і розробку нових зразків озброєння в інтересах забезпечення національної безпеки і оборони та про результати таких досліджень і розробок; особовий склад Сил спеціальних операцій Збройних Сил України, а також осіб, які співпрацюють або раніше співпрацювали на конфіденційній основі із Силами спеціальних операцій Збройних Сил України, фінансування та матеріально-технічне забезпечення руху опору, засоби, зміст, плани, організацію, завдання, форми, методи і результати ведення руху опору, оперативний резерв та мережу осередків руху опору; зміст секретної інформації, що отримується від іноземної держави чи міжнародної організації; системи та засоби криптографічного захисту секретної інформації, їх розроблення, виробництво, технологію виготовлення та використання; аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися і загрожують безпеці громадян, а також інші дані та відомості передбачені статтею 8 Закону [114].

Рішення про віднесення інформації до державної таємниці приймається спеціальним державним експертом з питань таємниць, що є посадовою особою, уповноваженою здійснювати відповідно до вимог законодавства віднесення інформації до державної таємниці у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, зміни ступеня секретності цієї інформації та її розсекречування [114]. Перелік посадових осіб, які виконують функції державного експерта з питань таємниць затверджено Указом Президента України від 19.05.2020 №190/2020 [129].

Віднесення інформації до державної таємниці здійснюється мотивованим рішенням державного експерта з питань таємниць за його власною ініціативою, за зверненням керівників відповідних державних

органів, органів місцевого самоврядування, підприємств, установ, організацій чи громадян. «Державний експерт з питань таємниць відносить інформацію до державної таємниці з питань, прийняття рішень з яких належить до його компетенції згідно з посадою. У разі, якщо прийняття рішення про віднесення інформації до державної таємниці належить до компетенції кількох державних експертів з питань таємниць, воно за ініціативою державних експертів або за пропозицією Служби безпеки України приймається колегіально та ухвалюється простою більшістю голосів. При цьому кожен експерт має право викласти свою думку. Інформація вважається державною таємницею з часу опублікування Зводу відомостей, що становлять державну таємницю, до якого включена ця інформація, чи зміни до нього у порядку, встановленому законодавством. Інформація відноситься до державної таємниці з урахуванням таких принципів: дотримання балансу інтересів національної безпеки, демократичних принципів відкритості та прозорості; вільного обігу інформації; презумпції публічності інформації до її віднесення в установленому законодавством порядку до державної таємниці. У разі невідповідності інформації вимогам, встановленим законодавством, забороняється віднесення її до державної таємниці. Засекречуванню підлягає інформація, а не документ. Якщо документ містить державну таємницю, для ознайомлення надається інформація, доступ до якої не обмежений» [114].

Наступною адміністративною процедурою пов’язаною із захистом інформації, що становить державну таємницю, комунікаційних та технологічних систем, призначених для її оброблення є надання дозволу на провадження діяльності пов’язаною із секретними відомостями та даними. Взагалі, пише В.М. Бевзенко, дозвіл – це закріплена нормою права допустима можливість здійснення суб’єктами правовідносин певних дій або допустима можливість утримуватися від їх вчинення; це межі допустимої законом поведінки таких суб’єктів [8, с.176]. «Дозвіл – це надання особі права на свої

власні активні дії (роби, як вважаєш за потрібне). Прикладом здійснення правового регулювання за допомогою цього способу може бути будь-яка правова норма, що надає суб'єкту право на одержання тих чи інших благ. Дозвіл превалює в основному в галузях, які належать до приватного права», - наголошує О.С. Гальченко [19, с.114].

С.М. Шило в своїх наукових працях проводить узагальнення наукових підходів до тлумачення категорії «дозвіл» та наголошує, що під даним поняттям варто розуміти офіційний документ установленої форми, виданий уповноваженим суб'єктом (органом державної влади, посадовою особою) на підставі, у межах повноважень та у спосіб і в порядку, що регламентовані чинним законодавством України, який дає право на певний вид діяльності або окрему діяльність з використанням чітко визначених предметів, речовин або матеріалів [171, с.307].

В.І. Сіверин виділяє в своїх наукових працях визначення категорії «дозвільна система», під якою вчений розуміє засновану на відповідних нормах або правилах сукупність правових відносин, які складаються з приводу здійснення суб'єктами публічної адміністрації дозвільної діяльності. Автор зазначає, що дозвільними відносинами названі суспільні відносини у сфері організації дозвільної діяльності та надання дозвільних послуг, а також контролю такої діяльності та законності надання дозвільних послуг, урегульовані нормами різних галузей права, забезпечувані державним примусом вольові відносини, які виражаються у конкретному зв'язку між суб'єктом надання дозвільних послуг з приводу організації та контролю такої діяльності, а також між суб'єктами публічної адміністрації, які надають дозвільні послуги та відповідними суб'єктами, які мають бажання їх отримати [142, с.41; 166]. О.В. Запотоцька пропонує під дозволом у широкому значенні розуміти законодавчо надане право власника дозволу діяти на власний розсуд у межах предмета дозволу та реалізовувати свої права й обов'язки у відповідному напрямку. На її погляд, дозвільна діяльність

– це законодавчо регламентована діяльність уповноваженого суб'єкта публічної адміністрації та їх посадових осіб, яка направлена на надання законодавчої можливості суб'єкту-заявнику отримати право вчинення певних дій і бути учасником правовідносин, які визначені предметом дозволу. Елементами дозвільної системи, на її думку, є такі: 1) суб'єкт владних повноважень, який законом уповноважений здійснювати дозвільну діяльність і відповідно видавати дозвіл; 2) суб'єкт-заявник, тобто особа, яка звернулася до вповноваженого органу з метою отримання дозволу; 3) предмет дозволу; 4) об’єкт дозволу; 5) правовідносини, що виникають між суб’єктом владних повноважень і суб’єктом-заявником; 6) правозастосовний акт, який визначає порядок та сферу реалізації дозволу [47, с.111-112].

Узагальнюючи наведені визначення можна вказати, що дозвіл – це надане в установленому законодавством порядку державою індивідуальне суб’єктивне право займатись відповідним видом діяльності, що має документальне підтвердження офіційного зразка. Дозвіл на провадження діяльності, пов’язаної із державною таємницею позначає право відповідного суб’єкта опрацьовувати секретну інформацію, у тому числі за допомогою комунікаційних та технологічних систем. Тобто, саме наявність дозволу показує, чи розповсюджуються на відповідну юридичну та/або фізичну особу обов’язки та обмеження у сфері роботи із інформацією таємного характеру, а також необхідність застосування щодо його діяльності особливих заходів забезпечення кібербезпеки.

Адміністративна процедура надання дозволу на провадження діяльності, пов’язаної з державною таємницею регламентована статтею 20 Закон України «Про державну таємницю». Згідно до положень останньої, «державні органи, органи місцевого самоврядування, підприємства, установи, організації мають право провадити діяльність, пов'язану з державною таємницею, після надання їм Службою безпеки України спеціального дозволу на провадження діяльності, пов'язаної з державною

таємницею. Надання дозволу здійснюється на підставі заявок державних органів, органів місцевого самоврядування, підприємств, установ і організацій та результатів спеціальної експертизи щодо наявності умов для провадження діяльності, пов'язаної з державною таємницею. З метою визначення наявності умов для провадження діяльності, пов'язаної з державною таємницею, Служба безпеки України може створювати спеціальні експертні комісії, до складу яких включати фахівців державних органів, органів місцевого самоврядування, підприємств, установ і організацій за погодженням з їх керівниками. Результати спеціальної експертизи щодо наявності умов для провадження діяльності, пов'язаної з державною таємницею, оформляються відповідним актом» [114]. Дозвіл на провадження діяльності, пов'язаної з державною таємницею, надається державним органам, органам місцевого самоврядування, підприємствам, установам, організаціям за результатами спеціальної експертизи за умови, що вони: «а) відповідно до компетенції, державних завдань, програм, замовлень, договорів (контрактів) беруть участь у діяльності, пов'язаній з державною таємницею; б) мають приміщення для проведення робіт, пов'язаних з державною таємницею, сховища для зберігання засекречених документів та інших матеріальних носіїв секретної інформації, що відповідають вимогам щодо забезпечення секретності зазначених робіт, виключають можливість доступу до них сторонніх осіб, гарантують збереження носіїв секретної інформації; в) додержуються передбачених законодавством вимог режиму секретності робіт та інших заходів, пов'язаних з використанням секретної інформації, порядку допуску осіб до державної таємниці, прийому іноземних громадян, а також порядку здійснення технічного та криптографічного захисту секретної інформації; г) мають режимно-секретний орган» [114].

Термін дії дозволу на провадження діяльності, пов'язаної з державною таємницею, встановлюється Службою безпеки України і не може перевищувати 5 років. Його тривалість залежить від обсягу робіт

(діяльності), що здійснюються державним органом, органом місцевого самоврядування, підприємством, установою, організацією, ступеня секретності та обсягу пов'язаних з цими роботами (діяльністю) відомостей, що становлять державну таємницю, а також категорії режиму секретності. Дозвіл на провадження діяльності, пов'язаної з державною таємницею, може бути скасований або його дія може бути зупинена Службою безпеки України на підставі акта проведеної нею перевірки, висновки якого містять дані про недодержання державним органом, органом місцевого самоврядування, підприємством, установою, організацією умов, передбачених цією статтею. У разі виникнення кризової ситуації, що загрожує національній безпеці України, оголошення рішення про проведення мобілізації та (або) введення правового режиму воєнного стану надання спеціального дозволу на провадження діяльності, пов’язаної з державною таємницею, органам військового управління, військовим частинам, установам і організаціям Збройних Сил України, інших військових формувань, правоохоронних органів спеціального призначення, Державної спеціальної служби транспорту, Державної служби спеціального зв’язку та захисту інформації України, що відмобілізовуються, доукомплектовуються, заново формуються, здійснюється у десятиденний термін [114].

Наступною варто розібрати процедуру контролю за забезпечення охорони державної таємниці, яка провадиться СБУ згідно до законодавства України та передбачає перевірку, у тому числі, комунікаційних та технологічних джерел оброки секретної інформації. Наприклад, Законом України «Про Служби безпеки України» закріплено, що «Центральне управління Служби безпеки України відповідає за стан державної безпеки, координує і контролює діяльність інших органів Служби безпеки України. До його складу входять апарат Голови Служби безпеки України та функціональні підрозділи: контррозвідки, військової контррозвідки, контррозвідувального захисту інтересів держави у сфері інформаційної

безпеки, захисту національної державності, інформаційно-аналітичний, оперативно-технічний, оперативного документування, слідчий, зв'язку, по роботі з особовим складом, адміністративно-господарський, фінансовий, військово-медичний та інші згідно з організаційною структурою Служби безпеки України. У межах своєї компетенції Центральне управління Служби безпеки України вносить Президенту України пропозиції про видання актів з питань збереження державної таємниці, обов'язкових для виконання органами державного управління, підприємствами, установами, організаціями і громадянами» [132].

Далі в тексті Закону визначено, що СБУ відповідно до своїх основних завдань, зокрема, зобов’язана брати участь у розробці і здійсненні відповідно до Закону України «Про державну таємницю» та інших актів законодавства заходів щодо забезпечення охорони державної таємниці та здійснення контролю за додержанням порядку обліку, зберігання і використання документів та інших матеріальних носіїв, що містять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, сприяти у порядку, передбаченому законодавством, підприємствам, установам, організаціям та підприємцям у збереженні комерційної таємниці, розголошення якої може завдати шкоди життєво важливим інтересам України. В цей же час СБУ надано право подавати органам державної влади, органам місцевого самоврядування, підприємствам, установам, організаціям усіх форм власності обов'язкові для розгляду пропозиції з питань національної безпеки, у тому числі із забезпечення охорони державної таємниці [132].

Безпосередньо сутність контрольної процедури за забезпеченням охорони державної таємниці встановлено Розділом V Закону України «Про державну таємницю», де вказано наступне: керівники державних органів, органів місцевого самоврядування, підприємств, установ і організацій зобов'язані здійснювати постійний контроль за забезпеченням охорони

державної таємниці. Державні органи, органи місцевого самоврядування, підприємства, установи і організації, що розміщують замовлення у підрядників, зобов'язані контролювати стан охорони державної таємниці, яка була передана підрядникам у зв'язку з виконанням замовлення. Державні органи, яким рішенням державного експерта з питань таємниць було надано право вирішувати питання про доступ державних органів, органів місцевого самоврядування, підприємств, установ, організацій до конкретної секретної інформації, зобов'язані контролювати стан охорони державної таємниці в усіх державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, які виконують роботи, пов'язані з відповідною державною таємницею, або зберігають матеріальні носії зазначеної секретної інформації. Контролює їх діяльність із захисту державної таємниці, у тому числі в процесі обробки секторної інформації за допомогою комунікаційних, технологічних систем Служба безпеки України [114].

Останньою варто розглянути адміністративну процедуру погодження СБУ щодо створення, реорганізації чи ліквідації режимна-секретних органів. Останні створюються на правах окремих структурних підрозділів в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, що провадять діяльність, пов'язану з державною таємницею, з метою розроблення та здійснення заходів щодо забезпечення режиму секретності, постійного контролю за їх додержанням. До складу режимно-секретного органу входять підрозділи режиму, секретного діловодства та інші підрозділи, що безпосередньо забезпечують охорону державної таємниці, залежно від специфіки діяльності державного органу, органу місцевого самоврядування, підприємства, установи та організації. Основними завданнями РСО є: а) недопущення необґрунтованого допуску та доступу осіб до секретної інформації; б) своєчасне розроблення та реалізація разом з іншими структурними підрозділами державних органів, органів

місцевого самоврядування, підприємств, установ і організацій заходів, що забезпечують охорону державної таємниці; в) запобігання розголошенню секретної інформації, випадкам втрат матеріальних носіїв цієї інформації, заволодінню секретною інформацією іноземними державами, іноземними юридичними особами, іноземцями, особами без громадянства та громадянами України, яким не надано допуску та доступу до неї; г) виявлення та закриття каналів просочення секретної інформації в процесі діяльності державних органів, органів місцевого самоврядування, підприємства, установи, організації; д) забезпечення запровадження заходів режиму секретності під час виконання всіх видів робіт, пов'язаних з державною таємницею, та під час здійснення зовнішніх відносин; е) організація та ведення секретного діловодства; є) здійснення контролю за станом режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях та на підпорядкованих їм об'єктах. РСО мають право: а) вимагати від усіх працівників державного органу, органу місцевого самоврядування, підприємства, установи та організації, а також відряджених неухильного виконання вимог законодавства щодо забезпечення охорони державної таємниці; б) брати участь у розгляді проектів штатних розписів державного органу, органу місцевого самоврядування, підприємства, установи та організації та підвідомчих їм установ, підприємств у частині, що стосується РСО, вносити пропозиції щодо структури та чисельності працівників цих органів; в) брати участь у проведенні атестації працівників, що виконують роботи, пов'язані з державною таємницею, а також у розгляді пропозицій щодо виплати в установленому нормативними актами порядку компенсації за роботу в умовах режимних обмежень тощо [114].

Крім зазначеного, в своїй роботі РСО перевіряють стан дотримання вимог Постанов КМУ «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-

комунікаційних системах» від 29.03.2006 №373 та «Про затвердження Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 16.02.1998 №180дск [123; 118].

Таким чином, адміністративні процедури, пов'язані із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення, становлять важливу та специфічну групу процедур в сфері забезпечення кібербезпеки. Проведене в підрозділі дослідження показує, що вони, передусім, пов'язані із інформацією особливого порядку та суспільної значимості, розголошення якої може мати негативні наслідки для національної безпеки. Адміністративні процедури в даній галузі є органічною складовою загального механізму забезпечення державної таємниці в Україні. Такими процедурами, як вбачається, є наступні: процедура віднесення інформації до державної таємниці; надання дозволу на провадження діяльності пов'язаною із секретними відомостями та даними; контроль за забезпеченням охорони державної таємниці; процедури погодження СБУ щодо створення, реорганізації чи ліквідації режимно-секретних органів.

2.3. Адміністративні процедури захисту комунікаційних систем, які не взаємодіють з публічними мережами електронних комунікацій

Окрему увагу в розрізі піднятої у дисертаційній роботі проблематики слід приділити адміністративним процедурам захисту комунікаційних систем, які не взаємодіють з публічними мережами електронних комунікацій. При цьому варто зауважити, що на відповідні системи не поширюється дія Закону України «Про основні засади забезпечення кібербезпеки України»,

однак при цьому вони відіграють важливу роль у загальній системі забезпечення кібербезпеки держави.

Комунікаційні системи, які не взаємодіють з публічними мережами електронних комунікацій, є закритими або ізольованими, оскільки вони призначені для передачі інформації в межах певної організації або групи користувачів без підключення до загальнодоступних мереж, зокрема Інтернету. Ці системи розроблені для забезпечення високого рівня безпеки, конфіденційності та надійності передачі даних, що робить їх особливо цінними в умовах, де необхідно захистити інформацію від несанкціонованого доступу, витоків або кібератак. Відсутність взаємодії з зовнішнім світом робить ці системи стійкими до більшості зовнішніх загроз, але в той же час вимагає високого рівня внутрішнього контролю та управління для запобігання внутрішнім загрозам або помилкам.

Комунікаційні системи, які не взаємодіють з публічними мережами, часто використовуються в секторах, де захист даних і конфіденційність є критично важливими. Наприклад, у військових і розвідувальних структурах такі системи застосовуються для обміну секретною або «чутливою» інформацією, що не повинна потрапити до ворожих рук. В урядових органах ці системи використовуються для забезпечення безпеки державної інформації і передачі даних, що мають значення для національної безпеки. У корпоративному середовищі, особливо в галузях із високими вимогами до конфіденційності, таких як фінансові послуги, фармацевтика або інфраструктурні компанії, закриті комунікаційні системи забезпечують захист інтелектуальної власності, комерційної таємниці та іншої конфіденційної інформації.

З технічної точки зору, такі системи можуть базуватися на різних технологіях, включаючи приватні локальні мережі (LAN), внутрішні телефонні системи, захищені цифрові радіомережі або закриті оптоволоконні лінії зв'язку. Вони можуть включати власні сервери, шифрувальні пристрої, і

спеціалізоване програмне забезпечення для захисту даних. Крім того, такі системи часто обладнані засобами фізичного захисту, такими як контроль доступу до приміщень, в яких розташована комунікаційна інфраструктура.

Однією із важливих особливостей таких систем є необхідність забезпечення їхньої стійкості до внутрішніх загроз і помилок. Це вимагає суворого контролю за доступом користувачів, а також регулярних перевірок і моніторингу систем для виявлення потенційних слабких місць або спроб несанкціонованого доступу. Адміністратори таких систем повинні мати високу кваліфікацію і доступ до засобів, що дозволяють швидко реагувати на будь-які інциденти, що можуть виникнути.

А відтак, адміністративні процедури захисту комунікаційних систем, які не взаємодіють з публічними мережами електронних комунікацій, переважно, носять внутрішньо-системний характер та реалізуються безпосередньо користувачами відповідних систем, а також спрямовані на забезпечення безпеки інформації та запобігання несанкціонованому доступу або витоку даних. Ці процедури є частиною загальної системи безпеки, що забезпечує належний рівень захисту від загроз як зсередини, так і ззовні організації.

Так, серед вказаних вище адміністративних процедур, перш за все, слід виділити формування політики інформаційної безпеки певного суб’єкта. Відповідно до сучасних політологічних уявлень політика – це діяльність, спрямована на загальну організацію суспільства, узгодження інтересів окремих громадян і соціальних груп шляхом застосування влади як відносин панування (підкорення) [107, с.165]. З огляду на зазначене вище, цілком справедливим буде говорити про те, що взагалі, політика представляє собою сукупність принципів, норм, правил та стратегій, спрямованих на досягнення певних цілей і керування діяльністю в конкретній сфері суспільного життя або в межах певної організації, тощо. Тож, політика визначає загальні підходи до вирішення проблем, управління ресурсами, прийняття рішень та

забезпечення контролю за їх виконанням. Вона може стосуватися різних аспектів суспільного життя, включаючи економічні, соціальні, правові та інші сфери.

Таким чином, політика інформаційної безпеки — це сукупність правил, принципів та настанов, які визначають стратегії та підходи певного суб'єкта до захисту своїх інформаційних ресурсів від несанкціонованого доступу, розголошення, модифікації, знищення або інших форм втручання. А відтак, дана політика формалізує вимоги до захисту інформаційних активів і визначає порядок управління ризиками, пов'язаними із інформаційною та кібербезпекою.

Значення політики інформаційної безпеки в розрізі представленої проблематики полягає у наступному: по-перше, вона спрямована на формування комплексного підходу в рамках певного суб'єкта щодо захисту інформаційних активів (що включають дані, інформаційні системи, мережі та апаратні засоби); по-друге, допомагає виявляти, оцінювати та управляти ризиками, пов'язаними із інформаційною безпекою, що знижує ймовірність інцидентів і збитків; по-третє, формує необхідний рівень довіри у учасників відповідних правовідносин; по-третє, дозволяє певному суб'єкту організувати свою діяльність так, щоб відповідати законодавству про кібербезпеку; по-п'яте, сприяє формуванню культури інформаційної безпеки в організації, підвищуючи обізнаність і залучення співробітників до забезпечення безпеки інформаційних ресурсів.

Тож, вказане вище дає змогу виділити наступні характерні властивості політики інформаційної безпеки: 1) охоплює всі аспекти інформаційної безпеки, включаючи технічні, організаційні та процедурні заходи; 2) спрямована на забезпечення відповідності суб'єкта міжнародним та державним стандартам у галузі кібербезпеки; 3) повинна узгоджуватись із загальними цілями функціонування певного суб'єкта (незалежно від галузевої належності, форми власності; тощо); 4) встановлює, хто в

організації несе відповідальність за виконання конкретних завдань із забезпечення інформаційної безпеки; 5) відповідна політика має бути достатньо гнучкою, щоб враховувати зміни в бізнес-середовищі, нові загрози та технологічні досягнення.

Розглядаючи приклади політики інформаційної безпеки, варто вказати, що у сфері банківської діяльності вона описує та регламентує функціонування цієї системи відповідно до вимог: 1) стандарту України з питань інформаційної безпеки ДСТУ ISO/IEC 27001:2015 “Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги”; 2) стандарту України з питань інформаційної безпеки ДСТУ ISO/IEC 27002:2015 “Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки”; 3) постанови Правління Національного банку України №95 від 28.09.2017 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України»; 4) методичних рекомендацій щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів; Національного банку України, визначених листом Національного банку України від 01.03.2011 N 24-112/365; 5) інших законодавчих та нормативно-правових актів України, а також внутрішніх нормативних документів Банку, а також міжнародних та внутрідержавних платіжних систем та систем переказу коштів [106].

Таким чином, політика інформаційної безпеки є ключовою адміністративною процедурою, яка забезпечує захист комунікаційних систем, що не взаємодіють з публічними мережами електронних комунікацій. Вона визначає комплекс заходів і правил, спрямованих на збереження конфіденційності, цілісності та доступності інформації в таких системах, а також на запобігання несанкціонованому доступу, порушенням роботи або втраті даних. Окрім того, значення цієї процедури полягає у тому, що такі системи, зазвичай, використовуються для зберігання та обробки критично

важливої інформації, яка не повинна потрапити до рук третіх осіб. Відсутність взаємодії з публічними мережами значно знижує ризик зовнішніх атак, однак не виключає внутрішніх загроз. Тому чітко визначена політика інформаційної безпеки забезпечує надійний захист від внутрішніх ризиків і гарантує стабільність функціонування комунікаційних систем.

Наступною важливою процедурою є контроль та управління доступом, що передбачає авторизацію та аутентифікацію визначеного переліку користувачів, що мають доступ до даної системи. Система контролю та управління доступом (СКУД) є важливим елементом безпеки в сучасному світі. Вона дозволяє контролювати доступ до об’єктів, приміщень та ресурсів, забезпечуючи безпеку приміщень і конфіденційність інформації. У цій статті розглянемо, чому потрібна система контролю доступу, її переваги та функції. Традиційні системи контролю доступу базуються на фізичних ключах, замках та пропускних системах. Однак, ці системи мають свої обмеження, такі як втрата ключів, вразливість до копіювання ключів та високі витрати на заміну. IP-системи контролю доступу використовують сучасні технології, такі як картки доступу, біометричні дані, системи розпізнавання обличчя та інші електронні методи. Вони надають більшу гнучкість, безпеку та зручність управління доступом, а також забезпечують легкий адміністративний контроль [82]. Сучасні системи контролю доступу можуть керувати описаними вище правами доступу як у режимі онлайн, так і оффлайн. Оффлайнові системи складаються з цифрових циліндрів і розсувних систем для дверей, на відміну від онлайн-системи, авторизації зберігаються на картці-пропуску. Перевагами електронної системи контролю доступу є: «не потрібно вносити жодних змін до системи загалом, якщо ідентифікаційний носій загублений; допускається негайне припинення дії втраченого транспондера або ідентифікаційної картки; постійний перегляд усіх особистих прав на доступ; можна визначити численні профілі доступу; зміни в правах на доступ можуть бути внесені будь-коли; захист майна та

даних за допомогою управління доступом: персонал та відвідувачі мають індивідуально визначені права доступу до певних зон у визначений час; спрацювання тривоги в разі маніпуляцій або спроби несанкціонованих дій; більше жодних «забутих» дверей; управління доступом може включати запис часу» [40].

Отже, управління доступом забезпечує не лише захист даних від несанкціонованого доступу, але й гарантує підтримку цілісності, конфіденційності та доступності інформації. Це критичний елемент загальної стратегії захисту інформаційних ресурсів, який сприяє підвищенню рівня безпеки комунікаційних систем і захисту від потенційних загроз. Сутність управління доступом полягає в контролі та регулюванні того, хто і на яких умовах може отримати доступ до певних ресурсів, даних, або систем. Це включає процеси аутентифікації, авторизації, ідентифікації користувачів та моніторингу їхньої діяльності.

Так, аутентифікація - це процедура перевірки та підтвердження особи користувача перед наданням доступу до певної системи, додатку або ресурсу. Її мета полягає в тому, щоб переконатися, що людина, яка намагається отримати доступ, дійсно є тим, за кого вона себе видає. Це забезпечує безпеку, запобігає несанкціонованому доступу та захищає конфіденційні дані від несанкціонованого використання. Процес автентифікації починається з того, що користувач надає системі унікальну інформацію, яка ідентифікує його, наприклад, логін і пароль. Після введення цих даних система перевіряє їх наявність у базі даних. Якщо введені дані відповідають даним у системі, користувач вважається успішно аутентифікованим і отримує доступ. У разі помилки, користувачеві може бути відмовлено в доступі [157]. В свою чергу «авторизація — це спосіб захисту. Вона визначає права користувачів таким чином, що вони будуть неоднакові: хтось може увійти в акаунт/надіслати повідомлення/користуватися пристроєм, хтось може редагувати вміст, а хтось — ні. Для того, щоб визначити, хто має той чи інший привілей,

проводиться аутентифікація — користувач визначається як такий, що має право на певні дії. В широкому сенсі авторизація — це, наприклад, ключ від номера, що надають після поселення в готелі. В інтернеті — це процес перевірки користувача і надання йому певних прав. Якщо розглядати, що таке авторизація з точки зору процесу, то: система отримує запит на здійснення певних дій; аутентифікує користувача як такого, що має чи не має на них право; задовольняє чи відхиляє запит (пропускає в поштову скриньку, робочий акаунт, банківський застосунок тощо)» [182].

Що ж стосується ідентифікації, то вона представляє собою процес визначення особи або об'єкта, що дозволяє системі або організації підтвердити, хто або що намагається отримати доступ до певного ресурсу чи системи. У контексті інформаційної безпеки, ідентифікація є першою фазою контролю доступу і відіграє ключову роль у захисті даних і ресурсів. Сутність ідентифікації полягає в тому, щоб асоціювати суб'єкта (наприклад, користувача) із унікальним ідентифікатором, таким як ім'я користувача, номер посвідчення особи, біометричний відбиток або інший унікальний атрибут. Цей ідентифікатор має бути достатньо унікальним, щоб розрізняти різних користувачів або об'єкти в системі. Ідентифікація є лише першим кроком у процесі управління доступом. Таким чином, ідентифікація має велике значення для забезпечення безпеки систем, оскільки вона дозволяє ефективно контролювати доступ до даних і ресурсів, запобігаючи несанкціонованому доступу та зловживанню правами доступу. Вона є основою для побудови довірчих відносин у цифровому середовищі і сприяє забезпеченню конфіденційності, цілісності та доступності інформації.

Таким чином, проведений аналіз дає змогу констатувати, що управління доступом виконує кілька ключових функцій:

- по-перше, дозволяє надавати доступ лише тим користувачам, які мають відповідні повноваження, що знижує ризик несанкціонованого доступу до критичної інформації;

- по-друге, чітко визначені правила доступу допомагають запобігти потенційним загрозам, таким як внутрішні атаки або витік даних, забезпечуючи той факт, що тільки уповноважені особи можуть здійснювати певні дії в системі;
- по-третє, управління доступом дозволяє вести детальний облік того, хто, коли і яким чином отримав доступ до інформаційних ресурсів. Це сприяє виявленню підозрілої активності та своєчасному реагуванню на інциденти безпеки;
- по-четверте, гнучкість у налаштуванні прав доступу. Так, різні рівні доступу можуть бути налаштовані для різних груп користувачів або індивідуально, що дозволяє адаптувати систему безпеки до конкретних потреб організації.

Наступними процедурами є здійснення внутрішнього контролю (моніторинг та аудит системи). На переконання Ю.С. Шемшученка, який зазначає, що внутрішній контроль – це фактично самоконтроль, який здійснюється всередині самої публічної адміністрації стосовно окремих органів, підрозділів, персоналу. Він проводиться вищестоящими інституціями щодо нижчестоящих або спеціально виділеними для цих цілей посадовцями, органами чи підрозділами. Цей контроль спрямований безпосередньо на охорону від порушень норм права підконтрольними суб'єктами і опосередковано — на захист суб'єктивних прав і охоронюваних законом інтересів конкретних осіб [39, с.578]. Досить цікавою є позиція Л.П. Кулаковської, яка зазначає, що внутрішній є засобом зворотного зв'язку між об'єктом управління й органом управління, інформуючи про дійсний стан об'єкта і фактичне виконання управлінських рішень. Внутрішній контроль - це процес, який забезпечує відповідність функціонування конкретного об'єкта прийнятим управлінським рішенням і спрямований на успішне досягнення поставленої мети. Основною його метою є об'єктивне вивчення фактичного стану справ відповідного суб'єкта, виявлення та

попередження тих факторів і умов, які негативно впливають на виконання прийнятих рішень і досягнення поставленої мети, та доведення цієї інформації до органу управління [66]. Для того щоб система внутрішнього контролю виправдала очікування власників та керівництва підприємства від її створення, вона має забезпечувати виконання ряду вимог: «до бухгалтерської звітності повинна включатися лише та інформація, яка була правильно задокументована, класифікована, оцінена та відображена в обліку; бухгалтерська звітність повинна містити об'єктивну інформацію в цілому по підприємству; забезпечувати своєчасність виявлення всіх відхилень планових показників від фактичних, проведення їх аналізу та притягнення винних осіб до відповідальності; фінансові ресурси підприємства не привласнювалися чи неефективно використовувалися; внутрішня звітність передається уповноваженим особам оперативно для прийняття ними управлінських рішень» [137].

Отже, поняття внутрішнього контролю охоплює комплекс організаційних, технічних і адміністративних заходів, спрямованих на забезпечення безпеки, цілісності і доступності інформації та ресурсів, що обробляються в таких системах. Внутрішній контроль включає в себе регулярні перевірки, моніторинг, управління доступом, управління ризиками та оцінку відповідності політикам і стандартам безпеки.

Значення внутрішнього контролю в розрізі представленої у роботі проблематики полягає у наступному:

1) захист від внутрішніх загроз, адже навіть у відокремлених системах, що не мають прямого доступу до публічних мереж, можуть існувати ризики несанкціонованого доступу або зловживання збоку персоналу. Внутрішній контроль забезпечує виявлення і запобігання таким загрозам через моніторинг доступу, ведення журналів подій та регулярні перевірки;

2) це гарантія цілісності та доступності даних. Внутрішній контроль допомагає забезпечити, щоб інформація в системах залишалася точною і

доступною тільки для уповноважених осіб. Це досягається через контроль за змінами, аудит даних і перевірку на відповідність стандартам безпеки;

3) управління ризиками. Внутрішній контроль дозволяє проактивно управляти ризиками, що можуть виникнути навіть у системах, ізольованих від публічних мереж. Оцінка і управління ризиками допомагають виявити потенційні проблеми і вжити заходів для їх усунення до того, як вони стануть критичними;

4) забезпечує відповідність нормативним вимогам і стандартам безпеки, що включає дотримання внутрішніх політик, законодавчих актів і галузевих стандартів;

5) регулярні перевірки і аудит в рамках внутрішнього контролю допомагають виявити недоліки в існуючих процесах і процедурах, що дозволяє вдосконалювати їх і підвищувати загальну ефективність системи.

Загалом, внутрішній контроль є критично важливим для забезпечення безпеки і ефективності комунікаційних систем, навіть якщо вони не взаємодіють з публічними мережами. Він створює механізми захисту і моніторингу, які допомагають забезпечити конфіденційність, цілісність і доступність інформації, а також підтримують загальну надійність і стійкість систем.

Далі в розрізі представленої проблематики слід вказати «кадрові процедури». Загалом, пише В.Ю. Кікінчук, кадрові процедури розглядаються як складова кадрової політики (кадрової роботи, управління кадрами, тощо). Відповідно до цього, слід зазначити, що в теорії управління відсутнє чітке визначення самого поняття кадрової процедури, яке досить часто використовується під час тлумачення спеціалізованих кадрових понять. Так, у комплексі операцій та процедур, направлених на реалізацію кадрової функції, деякі науковці вбачають сутність роботи з кадрами, а кадрова робота ними визначається як комплекс операцій і процедур зі складання та обробки кадрової документації, направлених на реалізацію кадрових функцій та

закріплених за спеціальними апаратами [управління, відділи кадрів, тощо) [53]. В.В. Сокуренко зазначає, що кадрові процедури – це закономірна реалізація певних заходів, які, зокрема, передбачені нормативно-правовими актами. Така діяльність спрямована на формування стабільного висококваліфікованого персоналу в органах поліції, тобто його підбір, підготовку та розстановку, а також забезпечення професійного й особистого розвитку [158].

Проаналізувавши різні наукові підходи, К.Г. Гарбузюк дійшов до наступних висновків з приводу сутності кадрових процедур в органах Національної поліції, а саме: «1) зміст кадрових процедур як взагалі, так і в сфері поліцейської діяльності неправильно розглядати з якоїсь одної позиції, так як він існує одразу у двох вимірах – управлінському та правовому. Дійсно, механізми реалізації кадрових процедур мають здебільшого адміністративно- або трудо-управлінську природу, так як стосуються внутрішнього «життя» органів Національної поліції, але при цьому, кожна процедура регламентована правом та здійснюється уповноваженими на її проведення суб'єктами, через що має юридичний результат у вигляді породження нових правовідносин, або зміни чи припинення інших; 2) будь-яка кадрова процедура в діяльності органів Національної поліції – це завжди цілісний комплекс регламентованих нормами права заходів, об'єднаних спільною метою та направлених на виконання окремих завдань кадрового забезпечення поліцейських; 3) кадрові процедури не одноманітні між собою. Так, кадрове забезпечення Національної поліції – це широке явище, реалізація якого відбувається в контексті проведення великого кола різних процедур, кожна з яких має особливий механізм здійснення та викликає відповідний юридичний результат; 4) кадрові процедури забезпечують послідовність кадрового забезпечення в органах та підрозділах Національної поліції, формують систему роботи з кадрами та підвищуються її цільову орієнтованість; окрім того, кадрові процедури цілком можна вважати

інструментом підтримки законності кадрового забезпечення, адже кожна з них являє собою окремий кластер кадрової роботи, що реалізується відповідно до чітко встановленої законодавчої моделі [20].

Таким чином, кадрові процедури — це сукупність дій і заходів, які організація здійснює для управління своїм персоналом з метою забезпечення ефективного функціонування комунікаційних систем, які не взаємодіють з публічними мережами електронних комунікацій. Вони включають процеси відбору, найму, адаптації, атестації, навчання, підвищення кваліфікації, просування, звільнення працівників, а також інші процедури, пов'язані з управлінням трудовими ресурсами, з метою забезпечення ефективної роботи та розвитку організації.

Тож, кадрові процедури в контексті забезпечення ефективного функціонування комунікаційних систем, які не взаємодіють з публічними мережами електронних комунікацій включають в себе:

1) суворий відбір та перевірку персоналу. Так, відбір персоналу включає ретельну перевірку всіх кандидатів, що мають працювати із захищеними системами. Це передбачає вивчення біографії та минулого досвіду роботи, аналіз кваліфікацій і перевірку рекомендацій. Крім того, важливим аспектом є перевірка надійності та доброчесності кандидатів, що може включати аналіз фінансового стану, можливі конфлікти інтересів, а також проведення психологічних тестів для оцінки рівня стресостійкості та здатності дотримуватися правил конфіденційності.

2) навчання та підвищення кваліфікації**.** Після відбору працівників проводиться регулярне навчання з питань інформаційної безпеки та захисту комунікаційних систем. Це включає навчання методам захисту даних, практикам безпечного використання обладнання, а також розумінню процедур реагування на інциденти. Працівники отримують знання про можливі загрози та способи їхнього виявлення й запобігання, що допомагає

мінімізувати ризик людських помилок, які можуть призвести до компрометації систем;

3) розмежування доступу та повноважень. До прикладу, організація встановлює чіткі правила щодо доступу до захищених комунікаційних систем, керуючись принципом мінімальних привілеїв. Це означає, що кожному працівнику надається лише той рівень доступу, який необхідний для виконання його конкретних службових обов'язків. Таке обмеження допомагає зменшити ризики несанкціонованого доступу до критичної інформації та зловживання службовим становищем;

4) регулярні перевірки та атестації**.** Працівники регулярно проходять перевірки на знання процедур безпеки та свою здатність діяти відповідно до них у випадку надзвичайних ситуацій. Ці перевірки можуть включати тестування на знання політик безпеки, а також практичні вправи для перевірки готовності до реагування на потенційні інциденти безпеки;

5) контроль за дотриманням правил безпеки. В даному контексті проводиться постійний моніторинг діяльності персоналу для виявлення можливих порушень або незвичних дій, які можуть свідчити про потенційні загрози безпеці. Це може включати автоматизований контроль за доступом до даних, а також документальна фіксація дій користувачів у системі. У випадку виявлення порушень негайно вживаються заходи для їх усунення та запобігання подібним інцидентам у майбутньому;

6) процедури звільнення. Слід зазначити, що коли працівник залишає організацію, важливо здійснити ретельні заходи для захисту інформації. Це включає негайне відкликання всіх прав доступу до захищених систем, повернення обладнання та документів, що можуть містити конфіденційну інформацію, а також проведення інструктажу щодо збереження професійної таємниці після звільнення. Такий підхід мінімізує ризик втрати даних і запобігає можливим зловживанням після звільнення працівника.

Далі в розрізі представленої проблематики слід звернути увагу на процедури управління та реагування на інциденти (зокрема, кіберінциденти). «Кіберінцидент - це масштабна подія або серія подій, які суттєво впливають на активи організації та вимагають від організації реагування з метою запобігання або обмеження впливу на організацію. Предмет події - це перший крок у процесі аналізу, за допомогою якого організація визнає, що відбувається кіберінцидент. У процесі сортування організація визначає, як класифікувати подію або серію подій, як її оцінити і чи досягає поріг, за яким подія вважається кіберінцидентом, що підлягає декларуванню. Поріг, за яким подія вважається кіберінцидентом що стався, відбувається або є неминучим і вимагає реагування, є унікальним для кожної організації і залежить від таких факторів, як організаційна структура, вимоги місії, а також закони та нормативні акти. Наприклад, технічний збій, час усунення якого перевищує допустимий час відновлення критично важливої послуги, може бути порогом для оголошення кіберінциденту» [109].

Існує кілька підходів до реагування на інциденти, і багато організацій покладаються на організацію зі стандартів безпеки, яка керує їхнім підходом. SysAdmin Audit Network Security (SANS) – це приватна організація, яка пропонує система шести кроків реагування шестикрокову систему реагування, наведену нижче. Багато організацій також застосовують систему відновлення після інцидентів Національного інституту стандартизації та технологій (NIST): «1) підготовка. Перш ніж інцидент станеться, важливо зменшити вразливості й визначити політику та процедури безпеки. На етапі підготовки організації проводять оцінку ризиків, щоб визначити свої слабкі місця й установити пріоритетність активів. Цей етап включає розробку й вдосконалення процедур безпеки, визначення ролей та обов’язків, а також оновлення систем для зменшення ризиків. Більшість організацій регулярно повертаються до цього етапу та вдосконалюють політику, процедури й системи відповідно до накопиченого досвіду або змін у технологіях;

2) ідентифікація загроз. За один день команда безпеки може отримати тисячі сповіщень, які вказують на підозрілу активність. Деякі з них є помилковими або не досягають рівня інциденту. Після виявлення інциденту команда вивчає характер порушення та документує результати, зокрема, джерело порушення, тип атаки й цілі зловмисника. На цьому етапі команда також має інформувати зацікавлені сторони й повідомляти про подальші кроки; 3) локалізація загрози. Наступним пріоритетом є якнайшвидша локалізація загрози. Що довше зловмисники мають доступ до системи, то більшої шкоди вони можуть завдати. Команда безпеки працює над тим, щоб швидко ізолювати програми або системи, які зазнали атаки, від решти мереж. Це допомагає запобігти доступу зловмисників до інших частин бізнесу; 3) усунення загрози. Після завершення локалізації команда видаляє зловмисника та будь-які зловмисні програми з уражених систем і ресурсів. Це може передбачати виведення систем в офлайн. Команда також продовжує інформувати зацікавлені сторони про прогрес; 4) відновлення. Відновлення після інциденту може зайняти кілька годин. Коли загроза зникає, команда відновлює системи й дані з резервних копій і контролює уражені області, щоб переконатися, що зловмисник не повернеться; 5) зворотний зв'язок і доопрацювання. Коли інцидент вирішено, команда аналізує те, що сталося, і визначає, як удосконалити процес. Навчання на цьому етапі допомагає команді посилити захист організації [178].

Варто зауважити, що кожен план реагування на інциденти індивідуальний і охоплює специфіку та можливості конкретної компанії, але є деякі основні правила, яких необхідно дотримуватись. По-перше, план має бути добре продуманим, а не лише написаним відповідно до внутрішніх чи нормативних вимог. По-друге, він має бути добре відомий людям, які братимуть участь у його реалізації. По-третє, це має бути здійснено. В Інтернеті можна знайти багато хороших планів реагування на інциденти, вони легко доступні, але їх необхідно адаптувати до ваших власних

можливостей. По-четверте, кожен план слід протестувати, а потім доопрацювати. Відрепетований план знижує час відгуку, ймовірність помилок та рівень стресу для всіх учасників. По-п'яте, і це найголовніше, кожен план реагування на інциденти необхідно регулярно оновлювати [159].

Таким чином, реагування на кіберінциденти в контексті захисту комунікаційних систем, які не взаємодіють з публічними мережами електронних комунікацій, має свої особливості, оскільки такі системи є ізольованими і мають обмежений доступ ззовні. Основна увага зосереджується на внутрішніх загрозах, таких як помилки співробітників, інсайдерські атаки або несанкціонований фізичний доступ до обладнання. Важливим аспектом є постійний моніторинг і контроль за діями користувачів усередині системи, щоб оперативно виявляти будь-які підозрілі дії, що можуть призвести до кіберінциденту. Реагування на такі інциденти вимагає наявності чітких протоколів і процедур, які визначають подальші кроки для локалізації та нейтралізації загрози, мінімізації збитків та швидкого відновлення нормального функціонування систем. Крім того, враховуючи обмежену взаємодію з зовнішніми мережами, особлива увага приділяється фізичній безпеці та контролю доступу до місць розташування обладнання, а також використанню захищених каналів для передачі даних та оновлень. Таким чином, реагування на кіберінциденти в таких системах орієнтоване на запобігання внутрішнім загрозам і забезпечення постійної готовності до швидкої і ефективної реакції на будь-які інциденти безпеки.

І останніми процедурами, яким ми приділимо увагу, є захист даних і резервне копіювання. Так, захист даних - це заходи та протоколи, що забезпечують конфіденційність, цілісність та доступність даних. Він передбачає захист даних від несанкціонованого доступу, крадіжки, пошкодження та втрати. Захист даних поширюється на будь-яку інформацію, що зберігається в електронному вигляді, наприклад, персональні дані, фінансові записи та ділові документи. Захист даних має вирішальне

значення, оскільки він гарантує, що ваша конфіденційна інформація залишається безпечною та конфіденційною. Персональні дані, такі як інформація про кредитні картки та медичні записи, можуть бути використані кіберзлочинцями для крадіжки особистих даних, шахрайства та інших незаконних дій. Компанії також повинні захищати свої дані, щоб уникнути репутаційних втрат, фінансових збитків та юридичних наслідків [48]. В свою чергу резервне копіювання (резервування) – копіювання даних з метою подальшого швидкого їх відновлення. До найбільш поширених технологій, які використовуються для резервного копіювання, відносяться: «1. Архівація системи у повному обсязі з копіюванням на який-небудь надійний зовнішній носій і розміщенням його далеко від основної системи (цей метод вимагає багато часу і незручний в процесі відновлення). 2. Снепшоти файлових систем. 3. Використовуються лише для запобігання випадкового вилучення файлів, але якраз в цьому випадку дуже корисні і ефективні. 3. Повні копії файлових систем або дисків. Для захисту від відмови жорстких дисків цей спосіб дещо поступається RAID; для відновлення випадково вилучених файлів може бути порівнянний за зручністю зі снепшотами, залежно від ситуації. 4. RAID (англ. Redundant Array of Independent Disks) – технологія віртуалізації даних, за якою об'єднуються кілька дисків в логічний елемент для надійності зберігання даних та підвищення продуктивності накопичувачів. Мінімізуються або виключаються зовсім простої в разі відмови жорстких дисків. Хоч середня частота таких відмов збільшується (оскільки кількість дисків більша), але ліквідовувати їх наслідки стає простіше. 5. Перевірка «відбитків файлів» (fingerprints). Використання цього методу допомагає з'ясовувати, коли потрібно звертатися до резервних копій. Особливо це важливо для «оффлайнових» резервних копій» [163].

Таким чином, саме зазначені вище адміністративні процедури відображають найбільш важливі аспекти захисту комунікаційних систем, які не взаємодіють з публічними мережами електронних комунікацій. Однак, як

суттєвий недолік слід відзначити законодавчу неврегульованість відповідних процедур. А відтак, дана прогалина потребує усунення.

Висновки до розділу 2

Відмічено, що 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.

Аргументовано, що 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.

Узагальнено, 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 виступає 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.

Встановлено, що державна таємниця є особливо важливим різновидом інформації в найбільш суспільно-значимих сферах (оборони, економіки, науки і техніки, міжнародних відносинах, галузі державної безпеки, охорони правопорядку, тощо), порядок доступу до якої обмежено законодавством України з метою недопущення її несанкціонованого розголошення, що матиме шкідливі наслідки для національної безпеки. Тож, головними ознаками державної таємниці є: 1) її становлять не всі відомості, а лише ті, що прямо віднесені до даної категорії інформації в установленому законом порядку; 2) спеціальний захист державної таємниці передбачає особливий порядок надання уповноваженим суб'єктам доступу до відомостей і даних, які становлять зміст цієї категорії; 3) обробка, передача та збереження відомостей і даних, що становлять державну таємницю, у тому числі в комунікаційних та технологічних системах, відбувається із дотриманням спеціальних правил та використанням заходів захисту.

З'ясовано, що адміністративні процедури, пов'язані із захистом інформації, що становить державну таємницю, а також комунікаційних та технологічних систем призначених для її оброблення – це системна та

систематизована діяльність спеціально уповноважених органів державної влади, яка спрямована на вчинення особливого роду дій та заходів спрямованих на організацію дієвого захисту та підтримки високого рівня безпеки при обробці та використанні інформації, що становить державну таємницю у відповідних системах, з метою запобігання та попередження її несанкціонованого витоку, що може нанеси шкоду національним інтересам та безпеці.

Акцентовано увагу на тому, що дозвіл – це надане в установленому законодавством порядку державою індивідуальне суб'єктивне право займатись відповідним видом діяльності, що має документальне підтвердження офіційного зразка. Дозвіл на провадження діяльності, пов'язаної із державною таємницею позначає право відповідного суб'єкта опрацьовувати секретну інформацію, у тому числі за допомогою комунікаційних та технологічних систем. Тобто, саме наявність дозволу показує, чи розповсюджуються на відповідну юридичну та/або фізичну особу обов'язки та обмеження у сфері роботи із інформацією таємного характеру, а також необхідність застосування щодо його діяльності особливих заходів забезпечення кібербезпеки.

Підкреслено, що адміністративні процедури, пов'язані із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення, становлять важливу та специфічну групу процедур в сфері забезпечення кібербезпеки. Проведене в підрозділі дослідження показує, що вони, передусім, пов'язані із інформацією особливого порядку та суспільної значимості, розголошення якої може мати негативні наслідки для національної безпеки. Адміністративні процедури в даній галузі є органічною складовою загального механізму забезпечення державної таємниці в Україні. Такими процедурами, як вбачається, є наступні: процедура віднесення інформації до державної таємниці; надання дозволу на провадження діяльності пов'язаною із секретними відомостями та

даними; контроль за забезпеченням охорони державної таємниці; процедури погодження СБУ щодо створення, реорганізації чи ліквідації режимно-секретних органів.

Обґрунтовано, що комунікаційні системи, які не взаємодіють з публічними мережами електронних комунікацій, є закритими або ізольованими, оскільки вони призначені для передачі інформації в межах певної організації або групи користувачів без підключення до загальнодоступних мереж, зокрема Інтернету. Ці системи розроблені для забезпечення високого рівня безпеки, конфіденційності та надійності передачі даних, що робить їх особливо цінними в умовах, де необхідно захистити інформацію від несанкціонованого доступу, витоків або кібератак. Відсутність взаємодії з зовнішнім світом робить ці системи стійкими до більшості зовнішніх загроз, але в той же час вимагає високого рівня внутрішнього контролю та управління для запобігання внутрішнім загрозам або помилкам. Комунікаційні системи, які не взаємодіють з публічними мережами, часто використовуються в секторах, де захист даних і конфіденційність є критично важливими. Наприклад, у військових і розвідувальних структурах, такі системи застосовуються для обміну секретною або «чутливою» інформацією, що не повинна потрапити до ворожих рук. В урядових органах ці системи використовуються для забезпечення безпеки державної інформації і передачі даних, що мають значення для національної безпеки. У корпоративному середовищі, особливо в галузях із високими вимогами до конфіденційності, таких як фінансові послуги, фармацевтика або інфраструктурні компанії, закриті комунікаційні системи забезпечують захист інтелектуальної власності, комерційної таємниці та іншої конфіденційної інформації.

Встановлено, що адміністративні процедури захисту комунікаційних систем, які не взаємодіють з публічними мережами електронних комунікацій, переважно, носять внутрішньо-системний характер та реалізуються

безпосередньо користувачами відповідних систем, а також спрямовані на забезпечення безпеки інформації та запобігання несанкціонованому доступу або витоку даних в рамках ізольованих інформаційних мереж. Ці процедури є частиною загальної системи безпеки, що забезпечує належний рівень захисту від загроз як зсередини, так і ззовні організації.

Відмічено, що політика інформаційної безпеки — це сукупність правил, принципів та настанов, які визначають стратегії та підходи певного суб'єкта до захисту своїх інформаційних ресурсів від несанкціонованого доступу, розголошення, модифікації, знищення або інших форм втручання. А відтак, дана політика формалізує вимоги до захисту інформаційних активів і визначає порядок управління ризиками, пов'язаними із інформаційною та кібербезпекою. Значення політики інформаційної безпеки в розрізі представленої проблематики полягає у наступному: по-перше, вона спрямована на формування комплексного підходу в рамках певного суб'єкта щодо захисту інформаційних активів (що включають дані, інформаційні системи, мережі та апаратні засоби); по-друге, допомагає виявляти, оцінювати та управляти ризиками, пов'язаними із інформаційною безпекою, що знижує ймовірність інцидентів і збитків; по-третє, формує необхідний рівень довіри у учасників відповідних правовідносин; по-третє, дозволяє певному суб'єкту організувати свою діяльність так, щоб відповідати законодавству про кібербезпеку; по-п'яте, сприяє формуванню культури інформаційної безпеки в організації, підвищуючи обізнаність і залучення співробітників до забезпечення безпеки інформаційних ресурсів.

Виділено наступні характерні властивості політики інформаційної безпеки: 1) охоплює всі аспекти інформаційної безпеки, включаючи технічні, організаційні та процедурні заходи; 2) спрямована на забезпечення відповідності суб'єкта міжнародним та державним стандартам у галузі кібербезпеки; 3) повинна узгоджуватись із загальними цілями функціонування певного суб'єкта (незалежно від галузевої належності,

форми власності; тощо); 4) встановлює, хто в організації несе відповідальність за виконання конкретних завдань із забезпечення інформаційної безпеки; 5) відповідна політика має бути достатньо гнучкою, щоб враховувати зміни в бізнес-середовищі, нові загрози та технологічні досягнення.

Узагальнено, що політика інформаційної безпеки є ключовою адміністративною процедурою, яка забезпечує захист комунікаційних систем, що не взаємодіють з публічними мережами електронних комунікацій. Вона визначає комплекс заходів і правил, спрямованих на збереження конфіденційності, цілісності та доступності інформації в таких системах, а також на запобігання несанкціонованому доступу, порушенням роботи або втраті даних. Окрім того, значення цієї процедури полягає у тому, що такі системи, зазвичай, використовуються для зберігання та обробки критично важливої інформації, яка не повинна потрапити до рук третіх осіб. Відсутність взаємодії з публічними мережами значно знижує ризик зовнішніх атак, однак не виключає внутрішніх загроз. Тому чітко визначена політика інформаційної безпеки забезпечує надійний захист від внутрішніх ризиків і гарантує стабільність функціонування комунікаційних систем.

Констатовано, що управління доступом забезпечує не лише захист даних від несанкціонованого доступу, але й гарантує підтримку цілісності, конфіденційності та доступності інформації. Це критичний елемент загальної стратегії захисту інформаційних ресурсів, який сприяє підвищенню рівня безпеки комунікаційних систем і захисту від потенційних загроз. Сутність управління доступом полягає в контролі та регулюванні того, хто і на яких умовах може отримати доступ до певних ресурсів, даних, або систем. Це включає процеси аутентифікації, авторизації, ідентифікації користувачів та моніторингу їхньої діяльності. Зазначено, що управління доступом виконує кілька ключових функцій: по-перше, дозволяє надавати доступ лише тим користувачам, які мають відповідні повноваження, що знижує ризик

несанкціонованого доступу до критичної інформації; по-друге, чітко визначені правила доступу допомагають запобігти потенційним загрозам, таким як внутрішні атаки або витік даних, забезпечуючи той факт, що тільки уповноважені особи можуть здійснювати певні дії в системі; по-третє, управління доступом дозволяє вести детальний облік того, хто, коли і яким чином отримав доступ до інформаційних ресурсів. Це сприяє виявленню підозрілої активності та своєчасному реагуванню на інциденти безпеки; по-четверте, гнучкість у налаштуванні прав доступу. Так, різні рівні доступу можуть бути налаштовані для різних груп користувачів або індивідуально, що дозволяє адаптувати систему безпеки до конкретних потреб організації.

Наголошено, що поняття внутрішнього контролю охоплює комплекс організаційних, технічних і адміністративних заходів, спрямованих на забезпечення безпеки, цілісності і доступності інформації та ресурсів, що обробляються в таких системах. Внутрішній контроль включає в себе регулярні перевірки, моніторинг, управління доступом, управління ризиками та оцінку відповідності політикам і стандартам безпеки. Значення внутрішнього контролю в розрізі представленої у роботі проблематики полягає у наступному: 1) захист від внутрішніх загроз, адже навіть у відокремлених системах, що не мають прямого доступу до публічних мереж, можуть існувати ризики несанкціонованого доступу або зловживання збоку персоналу. Внутрішній контроль забезпечує виявлення і запобігання таким загрозам через моніторинг доступу, ведення журналів подій та регулярні перевірки; 2) це гарантія цілісності та доступності даних. Внутрішній контроль допомагає забезпечити, щоб інформація в системах залишалася точною і доступною тільки для уповноважених осіб. Це досягається через контроль за змінами, аудит даних і перевірку на відповідність стандартам безпеки; 3) управління ризиками. Внутрішній контроль дозволяє проактивно управляти ризиками, що можуть виникнути навіть у системах, ізольованих від публічних мереж. Оцінка і управління ризиками допомагають виявити

потенційні проблеми і вжити заходів для їх усунення до того, як вони стануть критичними; 4) забезпечує відповідність нормативним вимогам і стандартам безпеки, що включає дотримання внутрішніх політик, законодавчих актів і галузевих стандартів; 5) регулярні перевірки і аудит в рамках внутрішнього контролю допомагають виявити недоліки в існуючих процесах і процедурах, що дозволяє вдосконалювати їх і підвищувати загальну ефективність системи.

Аргументовано, що кадрові процедури — це сукупність дій і заходів, які організація здійснює для управління своїм персоналом з метою забезпечення ефективного функціонування комунікаційних систем, які не взаємодіють з публічними мережами електронних комунікацій. Вони включають процеси відбору, найму, адаптації, атестації, навчання, підвищення кваліфікації, просування, звільнення працівників, а також інші процедури, пов'язані з управлінням трудовими ресурсами, з метою забезпечення ефективної роботи та розвитку організації.

Узагальнено, що кадрові процедури в контексті забезпечення ефективного функціонування комунікаційних систем, які не взаємодіють з публічними мережами електронних комунікацій включають в себе: 1) суворий відбір та перевірку персоналу. Так, відбір персоналу включає ретельну перевірку всіх кандидатів, що мають працювати із захищеними системами. Це передбачає вивчення біографії та минулого досвіду роботи, аналіз кваліфікацій і перевірку рекомендацій. Крім того, важливим аспектом є перевірка надійності та доброчесності кандидатів, що може включати аналіз фінансового стану, можливі конфлікти інтересів, а також проведення психологічних тестів для оцінки рівня стресостійкості та здатності дотримуватися правил конфіденційності; 2) навчання та підвищення кваліфікації. Після відбору працівників проводиться регулярне навчання з питань інформаційної безпеки та захисту комунікаційних систем. Це включає навчання методам захисту даних, практикам безпечного використання

обладнання, а також розумінню процедур реагування на інциденти. Працівники отримують знання про можливі загрози та способи їхнього виявлення й запобігання, що допомагає мінімізувати ризик людських помилок, які можуть призвести до компрометації систем; 3) розмежування доступу та повноважень. До прикладу, організація встановлює чіткі правила щодо доступу до захищених комунікаційних систем, керуючись принципом мінімальних привілеїв. Це означає, що кожному працівнику надається лише той рівень доступу, який необхідний для виконання його конкретних службових обов'язків. Таке обмеження допомагає зменшити ризики несанкціонованого доступу до критичної інформації та зловживання службовим становищем; 4) регулярні перевірки та атестації. Працівники регулярно проходять перевірки на знання процедур безпеки та свою здатність діяти відповідно до них у випадку надзвичайних ситуацій. Ці перевірки можуть включати тестування на знання політик безпеки, а також практичні вправи для перевірки готовності до реагування на потенційні інциденти безпеки; 5) контроль за дотриманням правил безпеки. В даному контексті проводиться постійний моніторинг діяльності персоналу для виявлення можливих порушень або незвичних дій, які можуть свідчити про потенційні загрози безпеці. Це може включати автоматизований контроль за доступом до даних, а також документальна фіксація дій користувачів у системі. У випадку виявлення порушень негайно вживаються заходи для їх усунення та запобігання подібним інцидентам у майбутньому; 6) процедури звільнення. Слід зазначити, що коли працівник залишає організацію, важливо здійснити ретельні заходи для захисту інформації. Це включає негайне відкликання всіх прав доступу до захищених систем, повернення обладнання та документів, що можуть містити конфіденційну інформацію, а також проведення інструктажу щодо збереження професійної таємниці після звільнення. Такий підхід мінімізує ризик втрати даних і запобігає можливим зловживанням після звільнення працівника.

Обґрунтовано, що реагування на кіберінциденти в контексті захисту комунікаційних систем, які не взаємодіють з публічними мережами електронних комунікацій, має свої особливості, оскільки такі системи є ізольованими і мають обмежений доступ ззовні. Основна увага зосереджується на внутрішніх загрозах, таких як помилки співробітників, інсайдерські атаки або несанкціонований фізичний доступ до обладнання. Важливим аспектом є постійний моніторинг і контроль за діями користувачів усередині системи, щоб оперативно виявляти будь-які підозрілі дії, що можуть призвести до кіберінциденту. Реагування на такі інциденти вимагає наявності чітких протоколів і процедур, які визначають подальші кроки для локалізації та нейтралізації загрози, мінімізації збитків та швидкого відновлення нормального функціонування систем. Крім того, враховуючи обмежену взаємодію з зовнішніми мережами, особлива увага приділяється фізичній безпеці та контролю доступу до місць розташування обладнання, а також використанню захищених каналів для передачі даних та оновлень. Таким чином, реагування на кіберінциденти в таких системах орієнтоване на запобігання внутрішнім загрозам і забезпечення постійної готовності до швидкої і ефективної реакції на будь-які інциденти безпеки.

РОЗДІЛ 3.
СУЧАСНІ ТЕНДЕНЦІЇ УДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ЗДІЙСНЕННЯ ОКРЕМИХ АДМІНІСТРАТИВНИХ ПРОЦЕДУР ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

3.1. Порівняльний аналіз національних та міжнародних стандартів і практик забезпечення кібербезпеки

Оптимальне забезпечення кібербезпеки передбачає поєднання національних та міжнародних стандартів, а також застосування найкращих світових практик у цій сфері. Організації повинні регулярно оцінювати свої системи захисту інформації та адаптувати їх до нових загроз. А відтак, цілком справедливим буде говорити про те, що міжнародне співробітництво в галузі кібербезпеки є ключовим фактором для боротьби з кіберзлочинністю. В даному контексті варто відзначити, що Законом України «Про основні засади забезпечення кібербезпеки України» закріплено, що функціонування національної системи кібербезпеки забезпечується шляхом: «вироблення і оперативної адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО; створення нормативно-правової та термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу та НАТО; встановлення обов’язкових вимог інформаційної безпеки об’єктів критичної інформаційної інфраструктури, у тому числі під час їх створення, введення в експлуатацію, експлуатації та модернізації з урахуванням міжнародних стандартів та специфіки галузі, до якої належать відповідні об’єкти

критичної інформаційної інфраструктури; формування конкурентного середовища у сфері електронних комунікацій, надання послуг із захисту інформації та кіберзахисту; функціонування системи аудиту інформаційної безпеки, запровадження кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту»; тощо [128]. Тож, зазначене вище дає змогу зробити висновок про те, що забезпечення кібербезпеки є фактично неможливим без дотримання національних та міжнародних стандартів у цій сфері.

Взагалі, поняття «стандарт» належить до категорії особливого роду. В.В. Яременко та О.М. Сліпушко вказують, що відповідно до однієї з дефініцій, вказують наведених у тлумачних словниках англійської мови, стандарт (англ. standard) – це ознаки певного явища, встановлені компетентним органом, звичаєм або загальною згодою як модель чи практика. У філології "стандарт" тлумачиться як загальноприйнятий взірець, типова форма, норма, шаблон чого-небудь; те, що позбавлене індивідуальних особливостей [97, с.372; 168]. Загальними ознаками, які характеризують поняття «стандарт», вказує В.В. Жернаков, є наступні: 1) нормативне закріплення стандарту; 2) встановлення певного рівня вимог або гарантій залежно від сфери застосування даного стандарту; 3) еталонний характер, тобто стандарт є орієнтиром для зіставлення з ним інших подібних об'єктів [80, с.19].

Автори юридичної енциклопедії під вказаним поняттям розуміють міжнародно-правові норми і принципи, які закріплюють правила поведінки суб'єктів міжнародно-державного співробітництва. Стандарти встановлюють певні мінімальні вимоги, яких повинні дотримуватися всі держави. Міжнародні стандарти містяться в міжнародних договорах, інших джерелах міжнародного права та в міжнародних документах, не наділених обов'язковою юридичною силою, що приймаються окремими міжнародними організаціями [179, с.615].

Досить розгорнутою э позиція О.М. Петроє, Л.І. Даниленко, Н.Б. Ларіної, які тлумачать стандарт як нормативний документ, розроблений, як правило, за відсутності протиріч із суттєвих питань у більшості заінтересованих сторін і затверджений відповідним органом, в якому викладено для загального і багаторазового використання правила, вимоги, загальні принципи, характеристики щодо різних видів діяльності або їх результатів для досягнення оптимального ступеня впорядкування у певній галузі [104, с.13]. Окрім того, вказані вище науковці наголошують, що в практичному плані, стандарт, як правило, означає письмовий документ: стандарт – це документ, розроблений на основі консенсусу та затверджений уповноваженим органом, що встановлює призначені для загального і багаторазового використання правила, інструкції або характеристики, які стосуються діяльності чи її результатів, включаючи продукцію, процеси або послуги, дотримання яких є необов'язковим. Це документ, який встановлює вимоги для конкретного товару, матеріалу, компонента системи або служби, або докладно описує конкретний метод або процедуру. Стандарт може містити вимоги до термінології, позначок, пакування, маркування чи етикетування, які застосовуються до певної продукції, процесу чи послуги. Стандартом може бути і норма, і зразок, і еталон, і модель, що приймається за вихідну точку для співставлення з ним інших подібних явищ; стандарт – це й документ, що встановлює єдині норми, правила, загальні принципи, характеристики та вимоги для загального і багаторазового застосування [104, с.14].

Отже, взагалі, стандарт — це нормативний документ, який встановлює загальні вимоги, правила, норми або характеристики для певного продукту, процесу, послуги або системи. Стандарти розробляються на основі узагальненого досвіду та знань і служать для забезпечення якості, безпеки, взаємозамінності та відповідності законодавчим вимогам. Вони можуть бути

національними, міжнародними або галузевими і застосовуються як основа для сертифікації та оцінки відповідності.

Що ж стосується представленої у роботі проблематики, то стандарти забезпечення кібербезпеки — це набір правил, рекомендацій і вимог, що визначають методи і заходи для захисту інформаційних систем, мереж та даних від кібератак, несанкціонованого доступу, витоків даних та інших загроз кібербезпеці. Ці стандарти розроблені для встановлення загальних практик і політик, які організації можуть використовувати для забезпечення захисту своїх цифрових активів.

Варто відзначити, що з огляду на глобальність категорії кібербезпеки, то слід відзначити наявність національних та міжнародних стандартів у цій сфері. Так, в першу чергу, безумовно, слід виділити міжнародні стандарти, запроваджені Міжнародною організацією зі стандартизації (ISO). Це глобальний орган, який розробляє та публікує міжнародні стандарти для забезпечення якості, безпеки та ефективності в різних секторах. Заснована в 1947 році, ISO має багату історію просування стандартизації для сприяння міжнародній торгівлі та зміцненню співпраці між країнами. Його основна мета — сприяти узгодженості та досконалості продуктів, послуг і систем, зміцнювати довіру та дозволяти підприємствам працювати на рівних умовах. Використовуючи стандарти ISO, організації можуть оптимізувати процеси, зменшити витрати та досягти більшої задоволеності клієнтів [193].

ISO відіграє вирішальну роль у кібербезпеці, забезпечуючи структурований підхід до управління ризиками, дотримання нормативних вимог і впровадження надійних систем управління інформаційною безпекою. Дотримання стандартів ISO гарантує, що організації створюють надійну основу для своїх протоколів кібербезпеки. Завдяки інтеграції ISO 27001 компанії можуть систематично виявляти, оцінювати та зменшувати ризики, які можуть поставити під загрозу безпеку їхніх даних. Впровадження ISO 9001 дозволяє їм оптимізувати процеси, підвищити операційну ефективність

і зосередитися на управлінні якістю [193]. Інтеграція стандартів ISO сприяє культурі постійного вдосконалення в організації. За допомогою регулярних аудитів і оцінок компанії можуть виявити прогалини в своїх заходах кібербезпеки та вжити активних заходів для усунення вразливих місць. Цей проактивний підхід не тільки покращує захист даних, але й створює довіру зацікавлених сторін і клієнтів.

Варто зауважити, що ISO допомагає організаціям захищатися від кібератак, сприяючи впровадженню найкращих практик, запроваджуючи надійні засоби контролю та підвищуючи стійкість до нових загроз. Впровадження стандартів ISO не тільки допомагає зміцнити захист, але й прививає культуру постійного вдосконалення в організації. Дотримуючись цих вказівок, компанії можуть завчасно виявляти вразливості та усувати їх до того, як зловмисники використають їх. А відтак, стандарти ISO надають організаціям основу для встановлення чітких процесів реагування на інциденти та відновлення, гарантуючи, що навіть у разі кібератаки вони зможуть швидко пом’якшити вплив і відновити нормальну роботу.

Стандарти ISO для кібербезпеки, включають ISO 27001, ISO 27002 і ISO 27005. Так, ISO 27001 — це міжнародно визнаний стандарт, який визначає вимоги до створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою (СУІБ). Одним із ключових аспектів ISO 27001 є його сильна увага до системи управління інформаційною безпекою (ISMS), яка діє як системний підхід до управління конфіденційною інформацією компанії. У цьому стандарті описано різні способи контролю, яких організації повинні дотримуватися, щоб забезпечити безпеку своїх інформаційних активів. Процедури сертифікації ISO 27001 передбачають ретельний аудит, який проводять акредитовані органи сертифікації для оцінки відповідності СУІБ організації вимогам стандарту. Ці органи сертифікації відіграють вирішальну роль у підтвердженні

відповідності організацій необхідним критеріям, викладеним у стандарті ISO 27001 [193].

ISO 27002 забезпечує комплексну структуру для управління інформаційною безпекою, що охоплює такі аспекти, як контроль доступу, використання технологій, відповідність нормативним вимогам і найкращі практики захисту організаційних даних. Він є важливим інструментом для організацій, які прагнуть встановити надійні заходи безпеки для захисту конфіденційної інформації. Стандарт заглиблюється в принципи контролю доступу, які диктують, хто може отримати доступ до даних, гарантуючи доступ лише авторизованому персоналу. У ньому викладено технологічні рекомендації щодо безпечної обробки даних, протоколів шифрування та заходів безпеки мережі. ISO 27002 встановлює суворі вимоги щодо відповідності галузевим нормам і найкращим міжнародним практикам, сприяючи розвитку культури захисту даних і зниження ризиків.

ISO 27005 зосереджується на управлінні ризиками в інформаційній безпеці, надаючи вказівки щодо оцінки ризиків, виявлення вразливостей, аналізу загроз і дотримання стандартів безпеки. Суть ISO 27005 полягає в сприянні проактивного підходу до ідентифікації, оцінки та визначення пріоритетів ризиків для забезпечення конфіденційності, цілісності та доступності інформаційних активів. Оцінка ризику є основою стандарту. Він допомагає організаціям зрозуміти потенційні вразливості, загрози та їхні потенційні наслідки, сприяючи таким чином прийняттю обґрунтованих рішень і розподілу ресурсів. Наголошуючи на важливості безперервного моніторингу та управління вразливими місцями, ISO 27005 допомагає організаціям швидко й ефективно усувати недоліки, зменшуючи ймовірність інцидентів безпеки та порушень [193].

Таким чином, у наш час, коли технології проникають у кожну сферу життя, питання захисту інформації набуває особливої актуальності. Кіберзагрози стають все більш витонченими та складними, тому захист

даних від несанкціонованого доступу, зміни або знищення є одним із найважливіших завдань для будь-якої організації. Саме для забезпечення високого рівня кібербезпеки та створення єдиного підходу до захисту інформації були розроблені міжнародні стандарти. Ці документи встановлюють загальноприйняті правила та рекомендації, які допомагають організаціям створити надійні системи захисту інформації. Їх значення полягає у наступному: по-перше, вони забезпечують спільну мову для обговорення питань кібербезпеки на глобальному рівні. Це дозволяє фахівцям з різних країн ефективно співпрацювати та обмінюватися досвідом; по-друге, стандарти пропонують системний підхід до управління інформаційною безпекою, що допомагає організаціям виявити та усунути вразливі місця у своїх системах; по-третє, дотримання міжнародних стандартів підвищує довіру клієнтів, партнерів та інвесторів до організації, оскільки свідчить про серйозний підхід до питань безпеки. І, нарешті, стандарти допомагають спростити процес сертифікації, оскільки багато систем сертифікації інформаційної безпеки базуються на міжнародних стандартах.

В Україні серед державних стандартів слід виділити «Стандарт України з питань інформаційної безпеки ДСТУ ISO/IEC 27001:2015». Цей стандарт створений для визначення вимог для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та постійного вдосконалення системи управління інформаційною безпекою (СУІБ). Прийняття системи управління інформаційною безпекою є стратегічним рішенням для організації. На проектування та впровадження системи управління інформаційною безпекою організації впливають потреби та цілі організації, вимоги щодо безпеки, застосовувані організаційні процеси, розмір і структура організації. Очікують, що всі ці чинники змінюються з часом. Система управління інформаційною безпекою забезпечує збереження конфіденційності, цілісності й доступності інформації за допомогою

запровадження процесу управління ризиками та надає впевненості зацікавленим сторонам, що ризиками належним чином управляють. Важливо, щоб система управління інформаційною безпекою була частиною та інтегрувалася в процеси організації та загальну структуру управління, щоб інформаційну безпеку розглядали в процесах розроблення, інформаційних системах і заходах безпеки. Очікують, що впровадження системи управління інформаційною безпекою буде масштабованим відповідно до потреб організації. Цей стандарт може бути використано зацікавленими внутрішніми та зовнішніми сторонами для оцінки можливості організації відповідати власним вимогам щодо інформаційної безпеки. Послідовність, з якою вимоги надано в цьому стандарті, не відображає їх важливості чи послідовності, з якою їх має бути впроваджено. Перелік пунктів понумеровано лише для цілей забезпечення посилань [76].

Таким чином, з огляду на зазначене вище, вказаний вище стандарт - це національна версія міжнародного стандарту ISO/IEC 27001:2013, яка встановлює вимоги до створення, впровадження, функціонування, моніторингу, перегляду, підтримки та вдосконалення системи управління інформаційною безпекою (СУІБ) в організаціях. Цей стандарт є основним документом, який допомагає організаціям захищати свої інформаційні активи від різних загроз, включаючи несанкціонований доступ, витік даних, кібератаки та інші ризики інформаційної безпеки. ДСТУ ISO/IEC 27001:2015 надає організаціям структурований підхід до забезпечення інформаційної безпеки, допомагаючи їм: 1) визначити, які саме загрози можуть вплинути на інформаційну безпеку організації; 2) впровадити необхідні заходи для захисту інформації від різних типів загроз (наприклад, кібератак, втрати даних, несанкціонованого доступу); 3) зменшити ризики, пов’язані з перебоями в роботі інформаційних систем; 4) підвищити довіру клієнтів; 5) забезпечити дотримання вимог українського законодавства в галузі захисту інформації. Основними принципами досліджуваного стандарту є:

а) системний підхід, відповідно до якого СІБ повинна бути інтегрованою частиною загальної системи управління організації; б) СІБ повинна постійно вдосконалюватися через планування, виконання, перевірку та коригування; в) принцип безперервного вдосконалення. Слід також відмітити, що ДСТУ ISO/IEC 27001:2015 охоплює широкий спектр аспектів інформаційної безпеки, включаючи: 1) розробку та впровадження політик і процедур в області інформаційної безпеки; 2) визначення відповідальності, повноважень та ресурсів для забезпечення інформаційної безпеки; 3) захист інформації від несанкціонованого доступу; 4) захист інформаційних активів від фізичних загроз; 5) розробку процедур виявлення, реагування та розслідування інцидентів інформаційної безпеки, а також плану відновлення після кіберінцидентів.

Наступним національним стандартом є ДСТУ ISO/IEC 27002:2015, який є національною версією міжнародного стандарту ISO/IEC 27002:2013 і містить керівні принципи щодо управління інформаційною безпекою. Цей стандарт призначений для забезпечення організацій різних типів та розмірів практичними рекомендаціями щодо захисту інформаційних активів. Стандарт базується на кращих світових практиках у сфері інформаційної безпеки і служить доповненням до ДСТУ ISO/IEC 27001:2015, допомагаючи деталізувати та впроваджувати заходи контролю, необхідні для управління ризиками у галузі інформаційної безпеки.

Основна мета зазначеного вище стандарту полягає у забезпеченні належного захисту інформаційних активів, таких як дані, інформаційні системи, процеси, мережі та сервіси, від усіх видів загроз. Стандарт включає набір практичних рекомендацій та заходів контролю, які допомагають організаціям захищати конфіденційність, цілісність та доступність інформації. Ці заходи контролю охоплюють широкий спектр аспектів інформаційної безпеки, таких як управління доступом, безпека персоналу, фізична і екологічна безпека, управління комунікаціями та операціями,

криптографічний захист, забезпечення безперервності бізнесу та інші. Стандарт також підкреслює важливість систематичного підходу до управління інформаційною безпекою, пропонуючи рекомендації щодо аналізу ризиків, вибору та реалізації відповідних заходів контролю, а також моніторингу та оцінки ефективності цих заходів. Водночас, ДСТУ ISO/IEC 27002:2015 наголошує на важливості культури інформаційної безпеки, підтримці високого рівня обізнаності серед працівників організації та їхньої відповідальності за забезпечення безпеки інформаційних активів.

Варто зауважити, що впровадження стандартів ISO для кібербезпеки включає визначення критичних інформаційних активів, оцінку ризиків, визначення засобів контролю безпеки, забезпечення відповідності нормативним вимогам і встановлення процедур для постійного вдосконалення. Ідентифікація активів є початковим кроком у процесі впровадження ISO, де компанії повинні точно визначити інформаційні активи, важливі для їх діяльності та безпеки. Це включає такі дані, як конфіденційна інформація про клієнтів, інтелектуальна власність і фінансові записи. Оцінка ризиків передбачає ретельний аналіз потенційних загроз і вразливостей, які можуть поставити під загрозу ці активи. Проводячи комплексну оцінку ризиків, організації можуть визначати пріоритети своїх зусиль у сфері безпеки та ефективно розподіляти ресурси. Далі визначаються заходи безпеки для пом’якшення виявлених ризиків. Це передбачає вибір і впровадження таких заходів, як брандмауери, протоколи шифрування, засоби контролю доступу та системи моніторингу для захисту від потенційних кіберзагроз.

Окрім стандартів ISO слід також вказати:

- контроль організації обслуговування (SOC) типу 2 — це основа кібербезпеки на основі довіри та стандарт аудиту, розроблений Американським інститутом сертифікованих бухгалтерів (AICPA), щоб допомогти перевірити, чи постачальники та партнери безпечно керують

даними клієнтів. SOC2 визначає понад 60 вимог відповідності та розширені процеси аудиту для систем і засобів контролю сторонніх розробників. Аудит може тривати рік. У цей момент видається звіт, який засвідчує стан кібербезпеки постачальників. Завдяки своїй комплексності SOC2 є однією з найжорсткіших систем безпеки для впровадження, а особливо для організацій у фінансовому чи банківському секторі, які стикаються з вищими стандартами відповідності, ніж в інших секторах. Тим не менш, це важлива структура безпеки, яка повинна бути центральною для будь-якої сторонньої програми управління ризиками;

- стандарт захисту критичної інфраструктури (NERC CIP), створений для пом'якшення зростання кількості атак на критично важливу інфраструктуру США та зростання ризику для третіх сторін. Він являє собою набір стандартів кібербезпеки, розроблених для того, щоб допомогти працівникам комунального та енергетичного секторів зменшити кібер ризику та забезпечення надійності масових електричних систем. Отже, система безпеки NERC-CIP вимагає від постраждалих організацій виявляти та пом'якшувати кіберризики збоку третіх сторін. NERC-SIP передбачає низку засобів контролю, включаючи класифікацію систем і критичних активів, навчання персоналу, реагування на інциденти та планування, плани відновлення критичних кіберактивів, оцінку вразливості тощо;

- загальний регламент захисту даних (GDPR), який був прийнятий у 2016 році з метою посилення процедур і практик захисту даних для громадян Європейського Союзу (ЄС). GDPR впливає на всі організації, засновані в ЄС, або будь-який бізнес, який збирає та зберігає особисті дані громадян ЄС, включно з компаніями США. Структура безпеки включає 99 статей, які стосуються обов'язків компанії щодо відповідності, включаючи права споживача на доступ до даних, політику та процедури захисту даних, вимоги сповіщення про порушення даних (компанії повинні повідомити свій

національний регулятор протягом 72 годин після виявлення порушення) тощо.

В рамках представленої проблематики варто відзначити, що Україна запровадила ряд стандартів, пов'язаних із забезпеченням кібербезпеки. Разом із тим, адаптація національних та міжнародних стандартів має свою специфіку:

1) охоплення та адаптивність. В даному контексті слід відзначити, що міжнародні стандарти, зазвичай, більш загальні та адаптивні, щоб задовольнити потреби широкого кола організацій по всьому світу, зокрема в Україні, адже вони надають рамки, які можна адаптувати відповідно до специфічних потреб організації. Національні стандарти, навпаки, часто розробляються та адаптуються з урахуванням конкретних загроз і регуляторних вимог, що робить їх більш конкретними щодо певної галузі або типу організації, правової культури, тощо;

2) особливі регуляторні вимоги. Зокрема, національні стандарти включають вимоги, необхідні для відповідності місцевому законодавству та нормативним актам, адже міжнародні стандарти, як правило, більш універсальні і можуть використовуватися як основа для відповідності різним регуляторним вимогам у різних країнах;

3) застосування та сертифікація. Міжнародні стандарти, такі як ISO/IEC 27001, широко застосовуються для сертифікації в різних країнах і часто є основою для підвищення глобальної довіри та визнання. Національні стандарти можуть мати обмежену географічну застосовність і можуть використовуватися, в основному, в межах однієї країни або регіону;

4) методологія та підхід до ризиків. Міжнародні стандарти, зазвичай, надають структурований підхід до управління ризиками з акцентом на ідентифікацію, оцінку та управління ризиками інформаційної безпеки. Національні стандарти можуть включати додаткові заходи або вимоги, що відображають місцеві загрози.

5) національні стандарти є більш гнучкими для адаптації до вітчизняних реалій, тоді як міжнародні – більш структуровані та формалізовані.

Окрему увагу у розрізі представленої проблематики слід звернути на зарубіжний досвід забезпечення кібербезпеки, адже як відзначалось раніше, в різних країнах відповідні стандарти працюють по-різному. В даному контексті особливу увагу слід приділити досвіду Сполучених Штатів Америки. Лідерство в кіберпросторі, цифровій економіці та нових цифрових технологіях є ключовим для розвитку США, викладеного в Стратегії національної безпеки (NSB) від жовтня 2022 року щодо «вільного, відкритого, безпечного та процвітаючого світу». Вказана вище Стратегія передбачає: 1) перерозподіл відповідальності за захист кіберпростору на уряд і організації приватного сектору, які є найбільш спроможними та мають найкращі позиції для зменшення ризиків; 2) переналаштування стимулів для сприяння довгостроковим інвестиціям у кібербезпеку за допомогою дипломатії, партнерства та обміну інформацією. Ця стратегія буде доповнена майбутньою цифровою політикою Агентства США з міжнародного розвитку (USAID). Щоб просувати NSS і NCS, Державний департамент, співпрацюючи з іншими федеральними агентствами, Уряд розробив стратегію міжнародної політики в кіберпросторі та цифрових технологій, зосереджену на побудові широкої цифрової солідарності за трьома керівними принципами та чотирма напрямами дій, які мають бути пріоритетними протягом наступних трьох до п'ять років. Такими принципами є наступні:

- по-перше, Державний департамент дотримуватиметься позитивного бачення кіберпростору та цифрових технологій, зосередженого на забезпеченні переваг технологій і заснованого на міжнародних зобов’язаннях і міжнародному праві, включаючи міжнародне право. Сполучені Штати мають намір працювати з союзниками та партнерами над майбутнім, у якому люди в усьому світі безпечно користуватимуться

цифровими технологіями для пошуку, отримання та передачі інформації та ідей в Інтернеті, беручи участь у вільних, відкритих та поінформованих суспільствах;

- по-друге, Державний департамент інтегрує кібербезпеку, сталий розвиток і технологічні інновації. Кібербезпека, безпека даних і кіберстійкість є передумовами та факторами економічного зростання та здорового громадянського простору, де громадяни можуть реалізувати свої права;

- по-третє, Державний департамент запроваджує комплексний політичний підхід, який використовує відповідні інструменти дипломатії та міжнародної державної майстерності в усій цифровій екосистемі. Ця екосистема включає, але не обмежується цим, апаратне забезпечення, програмне забезпечення, протоколи, технічні стандарти, постачальників, операторів, користувачів і ланцюги поставок, що охоплюють телекомунікаційні мережі, підводні кабелі, хмарні обчислення, центри обробки даних та супутникову мережеву інфраструктуру, операційні технології, програми, веб- платформ і споживчих технологій, а також Інтернету речей (IoT), штучного інтелекту (AI) та інших критичних і нових технологій [192].

Забезпечення кібербезпеки в США відзначається комплексним підходом, що поєднує як урядові, так і приватні ініціативи для захисту національних інтересів у кіберпросторі. Особливості цієї системи кібербезпеки базуються на високому рівні міжвідомчої координації, тісній співпраці з приватним сектором, впровадженні стандартів та практик кібербезпеки, а також на постійному вдосконаленні політики безпеки і технологій.

Однією із ключових особливостей кібербезпеки в США є акцент на захисті критичної інфраструктури, до якої входять енергетичний сектор, фінансові установи, охорона здоров'я, транспортні мережі та комунікаційні

системи. Американський уряд визначає критичну інфраструктуру як об'єкти, виведення з ладу яких може суттєво вплинути на національну безпеку, економіку та суспільство. Для захисту цих об'єктів уряд активно співпрацює з приватним сектором, адже більшість критичних інфраструктур в США перебуває у приватній власності. Така співпраця передбачає обмін інформацією про загрози, спільну розробку стандартів та рекомендацій з кібербезпеки, а також проведення спільних навчань і тренувань.

Ще однією важливою особливістю є розробка та впровадження стандартів кібербезпеки. Національний інститут стандартів і технологій США (NIST) розробив Cybersecurity Framework (CSF), який став ключовим інструментом для управління кіберризиками в організаціях як державного, так і приватного сектору. Цей фреймворк був розроблений у тісній співпраці з представниками бізнесу, академічних установ і експертів з кібербезпеки, що дозволило врахувати широкий спектр потреб і загроз.

Демонструючи свою постійну прихильність до підтримки кібербезпеки, США оголосили, що надають ще $8 млн. на кібербезпеку від Державного департаменту, у додаток до $10 млн., які були виділені у 2017 році. Частина цього фінансування буде спрямована на підтримку нового проекту з кібербезпеки Агентства США з міжнародного розвитку, за яким планується інвестувати загалом до $38 млн. протягом чотирьох років у розбудову потенціалу кібербезпеки України шляхом підтримки правової та регуляторної реформи, розвитку робочої сили у галузі інформаційних технологій, залучення приватного сектору. Очікується, що фінансування буде спрямовано на практичну реалізацію таких проектів: посилення кібербезпеки критичної інфраструктури; розробка та реалізація оновленої кіберстратегії; підвищення рівня кіберзахисту, реагування на інциденти, засоби обміну інформацією; підвищення обізнаності щодо кібербезпеки для всіх зацікавлених сторін; підготовка кадрів із надійного захисту систем промислового управління і цифрової криміналістики. Ці проекти

доповнюють американо-українське співробітництво з інших питань кібербезпеки [149].

Важливо відзначити, що в США існує сильний акцент на правовому та регуляторному забезпеченні кібербезпеки. Закони, такі як Закон про модернізацію кібербезпеки уряду (Federal Information Security Modernization Act, FISMA) та Закон про обмін інформацією про кібербезпеку (Cybersecurity Information Sharing Act, CISA), надають юридичні рамки для організацій, що займаються кібербезпекою, і сприяють обміну інформацією про загрози між урядом і приватним сектором. Ці закони також зобов'язують федеральні агентства дотримуватися стандартів і правил кібербезпеки, регулярно перевіряти свої інформаційні системи на предмет вразливостей і повідомляти про будь-які інциденти кібербезпеки. Не можна також не відмітити, що особливої уваги в США надають і підготовці кадрів у сфері кібербезпеки. На національному рівні реалізуються численні освітні програми та ініціативи, спрямовані на підвищення кваліфікації та компетентності фахівців з кібербезпеки. Університети та інші навчальні заклади співпрацюють з урядовими установами та компаніями для розробки навчальних програм, що відповідають сучасним викликам кібербезпеки. Ці зусилля підкріплюються інвестиціями в дослідження та розвиток нових технологій для захисту кіберпростору.

Ще одна країна, досвіду якої ми хотіли б приділити увагу, - Великобританія. Загальний регламент захисту даних Великобританії (GDPR) вимагає, щоб персональні дані оброблялися безпечно з використанням відповідних технічних та організаційних заходів. Регламент не вимагає певного набору заходів кібербезпеки, а радше очікує від особи «відповідних» дій. GDPR зосереджується на чіткій підзвітності щодо захисту даних, покладаючи пряму відповідальність на компанії за доведення того, що вони дотримуються принципів регламенту, а не бездіяльний підхід Закону про захист даних. Це означає, що компаніям потрібно буде взяти на себе

обов’язкові дії, такі як навчання персоналу, внутрішні аудити даних і ведення детальної документації, якщо вони хочуть уникнути порушення правил GDPR. Про порушення необхідно повідомляти відповідні органи протягом 72 годин після інциденту [188].

Закон про захист даних 2018 року містить вказівки та найкращі практики щодо обробки даних. Кожен, хто відповідає за використання персональних даних, повинен дотримуватися суворих правил, які називаються «принципами захисту даних». Вони повинні переконатися, що інформація: використовується справедливо, законно та прозоро; використовується для певних, явних цілей; використовується таким чином, що є адекватним, відповідним і обмеженим лише тим, що необхідно; точні та, де необхідно, оновлюються; зберігається не довше, ніж це необхідно; обробляються у спосіб, який забезпечує належну безпеку, включаючи захист від незаконної або неавторизованої обробки, доступу, втрати, знищення або пошкодження [188].

Директива NIS спрямована на підвищення рівня загальної безпеки та стійкості мережевих та інформаційних систем у всьому ЄС. Це стосується компаній і організацій, визначених як оператори основних послуг (OES), зовнішніх постачальників IT і керованих послуг (MSP), постачальників основних послуг, таких як енергетичні, транспортні, медичні та водопровідні компанії, а також постачальників важливих цифрових послуг, таких як хмарні обчислення і пошукові системи в Інтернеті. Регуляторні обов’язки виконуються компетентними органами (CA). Критерії для ідентифікації OES і перелік CA у Великобританії можна знайти в Регламенті NIS. NCSC розробив деякі ресурси, які організації, на які поширюються правила NIS, ймовірно, знайдуть корисними. Це: набір принципів кібербезпеки та стійкості для забезпечення основних послуг; збірка допоміжних вказівок; кібернетична система оцінки (CAF), що включає показники належної практики. У сукупності ці ресурси відомі як колекція NCSC CAF, і їх можна

знайти на веб-сайті. Використання колекції CAF поширюється за межі організацій, призначених як OES згідно з правилами NIS. З цієї причини термінологія колекції CAF має на меті узагальнити та розширити термінологію, яка використовується в правилах NIS.

Велика Британія, як одна з провідних цифрових економік світу, приділяє значну увагу забезпеченню кібербезпеки. Її підхід до цього питання має ряд характерних особливостей, які відрізняють його від інших країн. Однією із ключових особливостей британської моделі кібербезпеки є тісна співпраця між державними органами та приватним сектором. Компанії з різних галузей, особливо з IT-сектору, активно залучаються до розробки та впровадження заходів кібербезпеки, обмінюються інформацією про загрози та розробляють спільні стратегії захисту. Такий підхід дозволяє оперативно реагувати на нові загрози та ефективно використовувати ресурси.

Великобританія має розвинену систему забезпечення кібербезпеки, яка включає в себе низку державних органів та приватних компаній, що працюють спільно для захисту цифрового простору країни. До таких інституцій відносяться: 1) Національний центр кібербезпеки (NCSC) - це урядовий орган, відповідальний за координацію та підтримку кібербезпеки у Великій Британії. NCSC надає практичні поради та інструменти для захисту від кібератак, проводить дослідження та розробляє політику в галузі кібербезпеки; 2) Центр урядового зв'язку (GCHQ). Цей орган займається розвідкою сигналів і кібербезпекою. GCHQ відіграє важливу роль у захисті критичної національної інфраструктури та боротьбі з кіберзагрозами; 3) Національне агентство з боротьби зі злочинністю (NCA), яке відповідає за розслідування кіберзлочинів та притягнення злочинців до відповідальності.

Британська система кібербезпеки також характеризується фокусом на інноваціях. Країна активно підтримує розвиток технологій в галузі кібербезпеки, що дозволяє їй бути лідером в цій сфері. В Британії функціонують численні дослідницькі центри та стартапи, які розробляють

нові рішення для захисту від кіберзагроз. Цей інноваційний підхід допомагає Британії залишатися на крок попереду своїх конкурентів. З огляду на зазначене вище, цілком справедливим буде говорити про те, що ще однією особливістю британської моделі є розподілена відповідальність між різними державними органами та приватними компаніями. Такий підхід дозволяє більш ефективно використовувати ресурси і уникати надмірної централізації. Однак, з іншого боку, він може призводити до розпорошення зусиль і ускладнювати координацію дій.

Важливим аспектом британської кібербезпеки є міжнародне співробітництво. Британія активно співпрацює з іншими країнами в галузі кібербезпеки. Вона бере участь у розробці міжнародних стандартів і угод, а також надає допомогу іншим країнам у підвищенні їхнього рівня кіберзахисту. Розвинена індустрія кібербезпеки є ще одним фактором, який сприяє високому рівню кібербезпеки у Великій Британії. Країна має потужну індустрію кібербезпеки, яка пропонує широкий спектр продуктів і послуг. Це створює конкуренцію на ринку і сприяє зниженню вартості рішень для забезпечення кібербезпеки.

Таким чином, британська модель кібербезпеки є однією з найрозвиненіших у світі. Вона характеризується тісною співпрацею держави та приватного сектору, фокусом на інноваціях, розподіленою відповідальністю, сильною кіберрозвідкою та активним міжнародним співробітництвом. Однак, як і будь-яка система, вона має свої недоліки і вимагає постійного вдосконалення. Досвід Британії може бути корисним для інших країн, які прагнуть підвищити рівень своєї кібербезпеки.

Підбиваючи підсумок представленого підрозділу дисертаційного дослідження слід узагальнити, що забезпечення кібербезпеки – це безперебійний процес, який вимагає постійного оновлення та вдосконалення. Саме тому, важливим завданням законодавця, а також приватних осіб в Україні є постійне оновлення (технологічне, професійне, ресурсне, тощо)

системи безпеки відповідно до нових загроз та вимог міжнародних стандартів. З огляду на зазначене вище, розробка національних та запровадження міжнародних стандартів кібербезпеки в Україні є необхідним кроком для забезпечення безпеки держави та її громадян. Це дозволить підвищити стійкість критичної інфраструктури, захистити персональні дані та сприяти розвитку цифрової економіки.

3.2. Шляхи вдосконалення правового регулювання адміністративних процедур у сфері забезпечення кібербезпеки

Вирішення проблем, пов'язаних із реалізацією адміністративних процедур у сфері забезпечення кібербезпеки вимагає комплексного покращення системи правового регулювання суспільних відносин, які виникають у досліджуваній сфері суспільного життя. Недоліки відповідного забезпечення, як вбачається, обумовлені:

1) історичними та політичними чинниками, зокрема: а) тривалий період перебування в складі СРСР призвів до того, що багато систем і мереж були побудовані за застарілими стандартами, що робить їх більш вразливими до сучасних кібератак; б) політичні потрясіння та конфлікти, які переживала Україна, відволікали ресурси і увагу від питань кібербезпеки; в) розташування України на стику інтересів різних геополітичних гравців робить її привабливою мішенню для кібератак; 2) технічними факторами: а) застаріле обладнання та програмне забезпечення, яке важко захистити від сучасних кібератак; б) бюджетні обмеження, що ускладнюють фінансування заходів із забезпечення кібербезпеки; в) дефіцит кваліфікованих кадрів; г) відсутність єдиної державної системи кібербезпеки, що ускладнює координацію зусиль із захисту від кібератак; 3) соціальними факторами, які обумовлені низьким рівнем кібергігієни, а також відсутність достатньої

обізнаності населення про кіберзагрози; 4) економічними чинниками. Так, впровадження сучасних систем захисту вимагає значних фінансових інвестицій, що є недоступним для багатьох організацій. Окрім того, бюджетні кошти, які виділяються на кібербезпеку, часто конкурують з іншими пріоритетними напрямками розвитку держави; 5) війною в Україні, що спричинила: а) масовані кібератаки збоку російської федерації на критичну інфраструктуру, що призводить до значних збитків, а також перешкоджає нормальному функціонуванню всього державного апарату; б) дестабілізацію роботи не тільки державного, але й приватного сектору, що значно шкодить фінансовому та економічному розвитку держави; в) відтік кваліфікованих кадрів у галузі кібербезпеки.

Як бачимо, проблема забезпечення кібербезпеки, а також реалізації адміністративних процедур у цій сфері, має комплексних характер, та обумовлена не тільки повномасштабною військової агресією збоку російської федерації, але й іншими факторами. З огляду на зазначене вище, вказана проблематика неодноразово потрапляла у поле зору не тільки законодавця, а й цілої низки вітчизняних науковців.

В даному контексті в першу чергу слід відмітити два стратегічних нормативних документа: «Стратегія інформаційної безпеки» та «Стратегія кібербезпеки України». Так, 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. Досягнення мети здійснюватиметься шляхом ужиття заходів щодо стримування та протидії загрозам інформаційній безпеці України та нейтралізації інформаційної агресії, у тому числі спеціальних інформаційних операцій держави-агресора, спрямованих на підрив державного суверенітету,

територіальної цілісності України, забезпечення інформаційної стійкості суспільства та держави, створення ефективної системи взаємодії між органами державної влади, органами місцевого самоврядування та суспільством, а також розвиток міжнародної співпраці у сфері інформаційної безпеки на засадах партнерства та взаємної підтримки» [131]. «Очікуваними результатами реалізації Стратегії є: захищений інформаційний простір України; ефективне функціонування системи стратегічних комунікацій; здійснення ефективної протидії поширенню незаконного контенту; забезпечення сталого процесу інформаційної реінтеграції громадян України, які проживають на тимчасово окупованих територіях України, та поширення українського телерадіомовлення на територіях України, прилеглих до тимчасово окупованих територій; суттєве підвищення рівня медіакультури та медіаграмотності населення; дотримання конституційних прав особи на вільне вираження своїх поглядів і переконань, захист приватного життя; забезпечення захисту прав журналістів; формування української громадянської ідентичності [131]. У даному нормативно-правовому акті йдеться про те, що питання, пов'язані із кібербезпекою, визначаються Стратегією кібербезпеки України, затвердженою Указом Президента України від 26 серпня 2021 року № 447.

А відтак, наступним документом, якому приділимо увагу, - це Стратегія кібербезпеки України. У Стратегії зазначається, що «забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. Реалізація зазначеного пріоритету буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі. XXI століття знаменується активним формуванням шостого технологічного укладу та ризиками, з якими стикається цивілізація внаслідок упровадження новітніх технологій. Питома вага кіберзагроз зростає і ця тенденція в міру розвитку інформаційних технологій та їх конвергенції з технологіями штучного

інтелекту в найближче десятиліття посилюватиметься. Зростання такого впливу на функціонування структур управління як національних, так і транснаціональних формує нову безпекову ситуацію. Між світовими центрами сили відбувається поділ сфер впливу у кіберпросторі, посилюється їх прагнення за рахунок такого поділу забезпечити реалізацію власних геополітичних інтересів» [130].

У вказаному нормативному документі зазначається, що «Україна прагне створити максимально відкритий, вільний, стабільний і безпечний кіберпростір в інтересах забезпечення прав і свобод людини, соціального, політичного і економічного розвитку держави. Для подальшої розбудови національної системи кібербезпеки на засадах стримування, кіберстійкості, взаємодії необхідним є: посилення спроможності національної системи кібербезпеки для унеможливлення збройної агресії проти України у кіберпросторі або з його використанням, нейтралізації розвідувально-підривної діяльності, мінімізації загроз кіберзлочинності та кібертероризму (стримування); набуття здатності швидко адаптуватися до внутрішніх і зовнішніх загроз у кіберпросторі, підтримувати та відновлювати стале функціонування національної інформаційної інфраструктури, насамперед об'єктів критичної інформаційної інфраструктури (кіберстійкість); забезпечення розвитку комунікації, координації та партнерства між суб'єктами забезпечення кібербезпеки на національному рівні, розвиток стратегічних відносин у сфері кібербезпеки із ключовими іноземними партнерами, передусім з Європейським Союзом, Сполученими Штатами Америки та іншими державами - членами НАТО, співробітництво у цій сфері з іншими державами та міжнародними організаціями на основі національних інтересів України (взаємодія). Україна, крім основних суб'єктів національної системи кібербезпеки, залучить до вирішення завдань у цій сфері більш широке коло учасників, у тому числі суб'єктів господарювання, громадські об'єднання та окремих громадян України» [130].

Пріоритетами забезпечення кібербезпеки України є: убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства; захист прав, свобод і законних інтересів громадян України у кіберпросторі; європейська і євроатлантична інтеграція у сфері кібербезпеки. Формування нової якості національної системи кібербезпеки потребує чіткого та зрозумілого визначення стратегічних цілей, що мають бути досягнуті протягом періоду реалізації цієї Стратегії [130]. Стратегія є основою для обґрунтування розподілу необхідних для забезпечення кібербезпеки матеріальних, кадрових та інших ресурсів. Фінансування заходів з реалізації Стратегії здійснюватиметься в межах видатків, передбачених Державним бюджетом України та з інших джерел, не заборонених законодавством. У порядку координації Національний координаційний центр кібербезпеки під час підготовки матеріалів до засідань Ради національної безпеки і оборони України щодо проекту Закону України про Державний бюджет України та пропозицій до Бюджетної декларації по статтях, пов'язаних із забезпеченням національної безпеки і оборони України, аналізує пропозиції суб'єктів забезпечення кібербезпеки України щодо фінансування заходів з кібербезпеки, передбачених положеннями Стратегії кібербезпеки України, та надає відповідні пропозиції. Згідно із законодавством державні органи, підприємства, установи та організації передбачатимуть у своїх планах фінансові витрати на кібербезпеку. У рамках державно-приватного партнерства, міжнародної технічної допомоги залучатимуться інвестиції, які спрямовуватимуться на розбудову національної системи кібербезпеки [130].

«Ефективність реалізації Стратегії буде визначатися через постійний моніторинг її виконання та спиратися на чітку систему індикаторів стану кібербезпеки, які буде розроблено протягом першого року реалізації Стратегії. Індикатори мають визначати прогрес, якого досягли суб'єкти забезпечення кібербезпеки в реалізації Стратегії з таких питань, як: виконання стратегічних завдань у межах цілей, визначених Стратегією (за

кожним завданням); досягнення стратегічних цілей, визначених Стратегією (за кожною ціллю); рівень впливу заходів, що здійснюються в межах Стратегії, на національну систему кібербезпеки та цифрову трансформацію держави» [130]. «Упровадження індикаторів стану кібербезпеки забезпечить покращення процесу моніторингу виконання Стратегії у реальному часі з використанням сучасних веб-ресурсів (онлайн-платформ), прозорість вжитих заходів для суспільства і держави. Посилення впливу національної системи кібербезпеки на суспільний розвиток буде визначатися за такими критеріями: рівень довіри населення до держави щодо безпечності кіберпростору; формування безпечного інформаційного суспільства, в якому до заходів кібербезпеки, крім державних інституцій, залучені приватні суб'єкти та громадяни; рівень захищеності національних інтересів у сфері кібербезпеки (як приклад, рівень впливу на розвиток ситуації, пов'язаної з агресією Російської Федерації проти України)» [130].

Тож, зазначені вище нормативні документи, безумовно, позитивним чином вплинули на розвиток системи забезпечення кібербезпеки в Україні. Однак сьогодні, в умовах повномасштабного вторгнення збоку російської федерації, велика кількість положень «Стратегії кібербезпеки України» не тільки втратили свою актуальність, а й потребують комплексного перегляду та адаптації до сучасних реалій.

З огляду на зазначене вище, першочерговим кроком у напрямку вдосконалення правового регулювання адміністративних процедур у сфері забезпечення кібербезпеки має бути розробка кардинально нової, адаптованої до сучасних викликів та загроз «Концепції розвитку системи забезпечення кібербезпеки в Україні». Чому саме концепція? Відповідно до «Енциклопедичного словника з державного управління», «концепція – це спосіб тлумачення та розуміння процесів або явищ; система аргументів, що підтверджують певне положення, сукупність ідей щодо конкретного предмету дослідження, доктрина, теоретичний напрямок або підхід, головна

ідея. Вона також виступає формою ключового ідейного задуму під час розробки державної політики або офіційно затвердженого документа. Як основний ідейний задум, зазначає дослідниця, концепція визначає стратегію дій для реалізації реформ, програм або планів дій, здебільшого на національному рівні. У цьому контексті концепція слугує фундаментом для ухвалення рішень і вирішення конкретних завдань. Як документ, концепція розробляється державними установами для визначення основних принципів (напрямів, пріоритетів) реалізації державної політики у відповідній сфері, включаючи заходи для вирішення конкретних проблем» [41, с.342]. Ключовими компонентами концепції мають бути: «розробка теоретико-методологічних основ; адекватність відображення назрілих потреб розвитку суспільства; визначення основних пріоритетів та орієнтирів, першочергових і невідкладних завдань; чітка постановка найближчих та перспективних цілей; визначення кола суб'єктів і об'єктів; удосконалення законотворчого процесу, підвищення його якості, соціальної та наукової обґрунтованості; своєчасне та повноцінне правове забезпечення здійснюваних реформ; посилення гарантій прав особи; формування єдиного політико-правового простору, усунення колізій в нормативно-правових актах; удосконалення форм і методів реалізації правової політики, вироблення пропозицій і рекомендацій щодо їх оптимізації, підвищення ефективності; послідовна демократизація всієї політико-правової сфери суспільства, припинення конфронтації між різними гілками влади» [45].

Таким чином, у найбільш загальному розумінні концепція – це система поглядів, ідей або принципів, які об’єднуються в єдину цілісну картину, що пояснює певне явище, процес або ідею. Це своєрідний каркас, на якому будується розуміння, тлумачення і подальше дослідження будь-якого об’єкта чи процесу. Як нормативно-правовий акт, концепція – це особливого роду підзаконний нормативно-правовий акт, положення якого визначають основні

напрями, принципи, цілі та завдання державної політики у певній сфері суспільного життя.

Тож, прийняття «Концепції розвитку системи забезпечення кібербезпеки в Україні» має важливе значення, оскільки вона дозволить: 1) забезпечити узгодженість та системність у правовому регулюванні адміністративних процедур у сфері кібербезпеки, усунути прогалини та суперечності в чинному законодавстві; 2) чітко визначити процедури та повноваження спеціально уповноважених суб'єктів, що спростить взаємодію між ними, забезпечить швидкість та якість прийняття управлінських рішень та зменшить бюрократичні бар'єри; 3) покращити систему правового регулювання у досліджуваній сфері, що сприятиме захисту прав суб'єктів господарювання, забезпечить прозорість та обґрунтованість рішень, які приймаються щодо них органами державної влади; 4) підвищити рівень довіри до державних органів; 5) враховувати міжнародний досвід та стандарти у сфері кібербезпеки, що сприятиме інтеграції України в глобальний цифровий простір та поглибленню міжнародного співробітництва.

Таким чином, метою «Концепції розвитку системи забезпечення кібербезпеки в Україні» має бути створення та підтримка ефективного, стійкого та безпечного кіберсередовища, яке б захищало національні інтереси, сприяло сталому розвитку цифрової економіки та забезпечувало права та свободи громадян в інформаційному просторі. З огляду на окреслену мету, завданнями, які має містити дана Концепція, мають бути: 1) розробка ефективної системи управління кібербезпекою на державному рівні; 2) забезпечення взаємодії та координації суб'єктів забезпечення кібербезпеки (які включають як державний, так і приватний сектори); 3) визначення чітких адміністративних процедур забезпечення кібербезпеки та реагування на кіберінциденти; 4) розробка та впровадження заходів щодо підвищення стійкості органів державної влади та організацій різних форм

власності до кібератак; 5) розробка та впровадження сучасних технологій захисту інформації; 6) підвищення рівня обізнаності громадян щодо кібербезпеки; 7) підготовка висококваліфікованих фахівців у галузі кібербезпеки, а також створення умов для їх постійного навчання та підвищення кваліфікації; 8) стимулювання розвитку наукових досліджень у сфері кібербезпеки; 9) забезпечення активної участі у міжнародних ініціативах з кібербезпеки, що має включати обмін досвідом та технологіями; 10) комплексне вдосконалення чинного законодавства, гармонізація національних та міжнародних стандартів у цій сфері; 11) створення національної системи інформування про кіберінциденти.

Відповідно до зазначеної вище Концепції має бути прийнято стратегічний нормативно-правовий акт: «Стратегію кібербезпеки України в умовах воєнного стану». Стратегія, відповідно до Енциклопедичного словника з державного управління, являє собою виважений підхід до розв’язання критично важливих і складних (стратегічних) проблем; модель програмування діяльності для досягнення встановлених цілей. Стратегія обов’язково визначає пріоритети (першочергові для реалізації напрями, цілі, проблеми), які дають корисну основу для розподілу обмежених ресурсів [41, с.679]. На переконання В.Я. Малиновського, стратегія - це детальний всеохоплюючий комплексний план, що розробляється на перспективу з метою реалізації місії (основного призначення) організації та цілей, що її конкретизують. Стратегія розробляється та формулюється вищим керівництвом, роль якого полягає не лише в ініціюванні такого процесу, а й у реалізації плану із залученням усіх ланок управління та оцінці результатів стратегічного планування. Стратегія нерозривно пов'язана з політикою як засобом її реалізації. Якщо стратегія визначає курс на розподіл обмежених ресурсів для досягнення визначених цілей, то політика визначає загальні орієнтири для дій та прийняття рішень, які сприяють здійсненню поставлених цілей [72, с.238-239]. Отже, стратегія – це загальний план дій,

спрямований на досягнення довгострокових цілей. Це своєрідна «дорожня карта», яка визначає напрямок руху, ресурси, необхідні для досягнення мети, а також способи подолання можливих перешкод.

Стратегія кібербезпеки України в умовах воєнного стану має бути комплексним документом, який визначає пріоритетні напрямки та заходи для забезпечення стійкості критичної інфраструктури, захисту інформаційних систем держави та суспільства від кібератак, а також сприяння ефективній взаємодії всіх суб'єктів забезпечення кібербезпеки. Вона передбачає як технічні заходи (створення резервних систем, підвищення рівня захисту інформації), так і організаційні (розвиток кадрів, міжнародне співробітництво). Головна мета – зберегти стабільність функціонування держави та суспільства в умовах збройного конфлікту, де кіберпростір став одним із основних полів бою. Ключовими аспектами такої стратегії мають бути: 1) Комплексний підхід, що включає поєднання технічних, організаційних та правових заходів; 2) орієнтація на майбутнє, постійна адаптація до нових загроз та технологій; 3) міжвідомча координація, що включає співпрацю всіх зацікавлених органів державної влади та приватного сектору; 4) обмін досвідом та технологіями з партнерами. Основними завдання зазначеної вище Стратегії є: захист критичної інфраструктури; захист державних інформаційних систем; захист персональних даних громадян; протидія дезінформації; підвищення кібергігієни населення.

Окрім зазначених вище кроків, має бути доопрацьовано «Стратегію кібербезпеки України», яка повинна враховувати виклики та реалії сьогодення, а також набутий досвід кібератак на кіберпростір України в останні три роки. В даному контексті вбачається необхідним: а) забезпечити консолідацію зусиль усіх державних органів, приватного сектору та міжнародних партнерів для оперативного виявлення, аналізу та нейтралізації кіберзагроз; б) розробити план впровадження штучного інтелекту та машинного навчання для швидкого аналізу великих обсягів даних та

виявлення аномалій; в) визначити критично важливі об'єкти інфраструктури та розробити індивідуальні плани їх захисту; г) забезпечити регулярне оновлення програмного забезпечення та операційних систем для усунення вразливостей; ґ) створити умови для навчання населення критично оцінювати інформацію та розпізнавати фейки; тощо.

Як зазначалось раніше, низка проблем, пов’язаних із забезпеченням кібербезпеки, досліджувалась рядом науковців. Так, О. Трофименко, Ю. Прокоп, Н. Логінова та О. Задерейко дійшли до висновку, що «проблема ефективного забезпечення кібербезпеки потребує комплексного вирішення і вимагає скоординованих дій на національному, регіональному та міжнародному рівнях для запобігання, підготовки, реагування та відновлення інцидентів з боку органів влади, приватного сектора і громадянського суспільства. З огляду на сучасні суспільно-політичні та інформаційні виклики визначення політичних, науково-технічних, організаційних та просвітницьких напрямів конструювання ефективної системи кіберзахисту у рамках комплексної протидії кіберзагрозам сприятиме формуванню ефективного механізму протидії загрозам у кібернетичній сфері, випереджальному реагування на динамічні зміни, що відбуваються у кіберпросторі, розробленню та впровадження ефективних засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватись як засіб стримування військових конфліктів та загроз у кіберпросторі» [155]. Окрім того, згадані вище автори зазначають, що «серед першочергових завдань, які стоять перед державними інститутами України в рамках забезпечення інформаційного та цифрового суверенітетів, є: здійснення автоматичного моніторингу свого інформаційного простору; впровадження законодавства про відповідальність за контент; впровадження законодавства, яке регулює фільтрацію інтернет-контенту; недопущення використання новітніх інформаційних технологій для поширення соціально шкідливих ідей і закликів (расизму, шовінізму, радикального націоналізму);

правовий захист національної культури і мови від впливу домінуючих в інформаційному плані країн; знаходження соціально прийнятного балансу між свободою слова і поширенням інформації та невід'ємним правом держави забезпечувати незалежну політику; захист від культурної експансії зарубіжних інтернет-ресурсів; перехід державних установ на використання програмного та технічного забезпечення власної розробки і виробництва» [155].

О. Косиця, досліджуючи актуальні питання вдосконалення законодавства у сфері протидії кіберзлочинності, дійшла до наступних висновків: по-перше, в національне правове поле вкрай необхідним є введення та визначення таких понять, кіберпростір, кібертероризм, кіберекстремизм, кібервійни, кіберзлочин, кіберзлочинність, та комплексно - які правопорушення є кіберзлочинами; по-друге, не дивлячись на те, що необхідний комплекс організаційно-правових і технічних заходів протидії кіберзлочинності ще буде створений, його розробка має відбуватися з активним запозиченням досвіду високороз-винених країн, ІТ-спеціалістів, аналітичних і статистичних даних підрозділів із боротьби з тероризмом та екстремізмом в органах безпеки, підрозділів Національної поліції з протидії, виявлення та розслідування правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку на основі міжнародного співробітництва спеціальних підрозділів компетентних органів; по-третє, виконання рішення РНБО (п. 6.): «Національній поліції України разом зі Службою безпеки України вжити невідкладних заходів щодо забезпечення повного та об'єктивного розслідування кібератак на інформаційно-телекомунікаційні системи фінансового сектору держави» можливо за умови вдосконалення взаємодії міжнаціональною поліцією України та Службою безпеки України, а саме нормативного врегулювання порядку спільного використання цілодобової контактної мережі для надання невідкладної допомоги під час

розслідування кіберзлочинів; по-четверте, у системі органів Національної поліції раціональним і неминучим є створення організованої системи взаємодії та координації з метою надання допомоги під час розслідування злочинів, учинених у мережі Інтернет або через комп'ютерну систему чи інформаційно-телекомунікаційну мережу [63].

О.В. Коваленко у своєму науковому дослідженні вказує, що з метою удосконалення державного механізму моніторингу загроз кібербезпеці доцільно розробити та упровадити в державно-управлінську практику паспорти загроз кібербезпеці, до складу яких мають входити такі розділи: загальна характеристика загрози кібербезпеці; характеристика можливого розвитку загрози кібербезпеці; діяльність суб'єктів забезпечення кібербезпеки щодо реагування на загрози. Окрім того, автор зазначає, що з метою удосконалення механізму державного реагування на виявлені загрози кібербезпеці варто розробити та упровадити в практику державного управління технологію державного реагування на загрози кібербезпеці, до складу яких входять такі структурні елементи: цілісна теоретична концепція, яка відображає закономірності функціонування об'єкту кібербезпеки; об'єкт кібербезпеки і предмет державно-управлінського впливу; алгоритм державно-управлінського впливу на об'єкт кібербезпеки; технологічні способи і засоби державно-управлінського впливу на об'єкт кібербезпеки; елемент контролю результату застосування цієї технології [55].

Найбільш перспективними напрямами розвитку національної системи кіберзахисту, на думку О. Бакалінської та О. Бакалінського, є: вдосконалення правової основи кіберзахисту об'єктів критичної інфраструктури; впровадження системи незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури; створення галузевих центрів реагування на кіберінциденти; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки; розвиток системи підготовки кадрів у сфері кібербезпеки; підвищення цифрової грамотності (правил кібергігієни)

громадян та культури безпекового поводження в кіберпросторі, впровадження систем інформаційного комплаєнсу та, насамперед, створення довірчих відносин між державою та суспільством, для якого держава повинна грати сервісну роль [5].

В.М. Столбовий та Д.П. Кисленко зазначають, що реалізація заходів із підвищення кібербезпеки на державному та корпоративному рівнях у контексті цифровізації суспільства є однією з найактуальніших проблем, що безпосередньо впливає на стабільну роботу критичної інфраструктури, безпечне функціонування державних органів і забезпечення належної суспільної діяльності. З огляду на постійне зростання кількості кібератак і шкідливих дій у кіберпросторі, розуміння та ефективне управління кіберризиками стають необхідними для забезпечення безпеки держав, бізнесу та громадян. Це вимагає системного підходу, активної співпраці й постійного вдосконалення стратегій та заходів із кібербезпеки. Основні підходи до підвищення кібербезпеки включають аутсорсинг, аналіз і моніторинг технологій кібератак, технічні інновації, реалізацію державних стратегій кібербезпеки та співпрацю з міжнародними інституціями. Удосконалення існуючих підходів до розробки стратегій кібербезпеки на державному та корпоративному рівнях вимагає врахування перспективних напрямів, які потрібно використовувати при формуванні політики кібербезпеки. Подальший розвиток сфери кібербезпеки на цих рівнях передбачає вдосконалення законодавства, політик та стратегій, спрямованих на забезпечення безпеки в цифровому середовищі. Крім того, необхідно налагодити співпрацю між державними органами, корпоративним сектором, науково-дослідними установами та громадянським суспільством для ефективної протидії кіберзагрозам. У майбутньому шлях до стійкого функціонування суспільства в умовах цифровізації лежить у консолідації зусиль усіх зацікавлених сторін, залученні експертів та впровадженні новітніх технологій кібербезпеки [150].

Отже, науковці досить по-різному підходять до вирішення проблем, пов’язаних із забезпеченням кібербезпеки. Однак при цьому, жоден підхід не можна визнати комплексним. Окрім того, вчені фактично поза своєю увагою залишили питання правового регулювання адміністративних процедур у сфері забезпечення кібербезпеки.

Таким чином, проведений вище аналіз наукових поглядів вчених та норм чинного законодавства, дає змогу сформулювати власний підхід щодо напрямів вдосконалення правового регулювання адміністративних процедур у сфері забезпечення кібербезпеки. Зокрема, в даному контексті необхідно в Законі України «Про основні засади забезпечення кібербезпеки України» необхідно: а) уточнити теоретичну частину Закону, зокрема визначити поняття «адміністративні процедури забезпечення кібербезпеки»; б) встановити коло адміністративних процедур, а також розкрити їх зміст; в) визначити сфери застосування цих адміністративних процедур; г) окреслити коло суб’єктів реалізації відповідних процедур, а також визначити їх правовий статус.

Окрім того, необхідно вдосконалити організаційно-управлінські аспекти, які забезпечують реалізацію адміністративних процедур у досліджуваній сфері суспільного життя. В даному контексті необхідно:

- покращити систему кадрового забезпечення суб’єктів, що уповноважені реалізовувати діяльність у досліджуваній сфері. В Енциклопедії державного управління зазначається, що кадрове забезпечення – це здійснювана в процесі управління діяльність, змістом якої є забезпечення органів, установ, їх підрозділів необхідним контингентом осіб, які відповідають певним вимогам, інформацією про них, а також впровадження науково-обґрунтованих методів добору, розстановки, професійного навчання, підготовки та перепідготовки кадрів, стимулювання їхньої роботи, правового регулювання трудової діяльності та надання правового захисту працевлаштованим [42]. Н.В. Прижиналінська визначає

кадрове забезпечення - це комплекс заходів, спрямованих на пошук, оцінку і установлення заздалегідь передбачених трудових відносин, як для розвитку кар'єри на самому підприємстві, так і для залучення нових працівників як тимчасових, так і постійних співробітників. Цей процес включає в себе керування підприємством, планування, організацію персоналу, аналіз відносин з управління, забезпечення умов праці та розвиток кадрового потенціалу. З точки зору керування персоналом кадрове забезпечення може суттєво впливати на досягнення цілей підприємства, якщо всі елементи взаємодії з персоналом (набір, відбір, адаптація, розвиток кар'єри, оцінка результатів праці, сучасні методи мотивації і організації праці) об'єднані в єдину програму, що є невід'ємною частиною кадрової стратегії підприємства. У контексті формування кадрового резерву підприємства важливою є підготовка інноваційно налаштованих кадрів - кваліфікованих співробітників, які мають здатність до творчої праці, професійного розвитку та освоєння науково-інформаційних технологій. Це можливо завдяки розвитку системи безперервної освіти та навчання протягом життя [110]. Таким чином, кадрове забезпечення – це ключовий чинник, від якого напряму залежить якість та ефективність реалізації адміністративних процедур забезпечення кібербезпеки. Зазначене пояснюється тим, що лише висококваліфіковані фахівці здатні належним чином виконувати покладені на них обов’язки, а також швидко адаптуватись до змін кіберсфери, яка активно розвивається. Тож, з метою удосконалення кадрового забезпечення суб’єктів реалізації адміністративних процедур у сфері кібербезпеки першочерговим кроком має бути створення чіткої системи вимог до кваліфікації фахівців, які працюють у сфері кібербезпеки. Ці вимоги мають враховувати як загальні знання в галузі інформаційних технологій, так і специфічні компетенції, необхідні для виконання конкретних функцій. Окрім того, важливим елементом є розробка та впровадження ефективних програм навчання та підвищення кваліфікації. Ці програми мають бути орієнтовані на постійне

оновлення знань фахівців з урахуванням нових загроз та технологій. І останній аспект, якому слід приділити увагу, - створення системи мотивації працівників, яка б стимулювала їх професійний розвиток та підвищувала зацікавленість у роботі в сфері кібербезпеки;

- переглянути фінансове та матеріально-технічне забезпечення галузі кібербезпеки. Так, фінансове забезпечення представляє собою процес планування, мобілізації, розподілу та використання фінансових ресурсів для досягнення стратегічних цілей організації, підприємства або держави. Воно включає в себе формування джерел фінансування, управління бюджетом, контроль за витратами та забезпечення ефективного використання коштів для підтримки стабільного функціонування і розвитку в умовах ринкової економіки. В свою чергу матеріально-технічне забезпечення - це сукупність суспільних відносин, урегульованих нормативними актами або договорами по забезпеченню матеріально-технічними ресурсами, необхідними для своєчасного та безперебійного здійснення адміністративного судочинства, а також виконання завдань які стоять перед ним. відповідно до норм чинного законодавства [62, с.56]. Отже, ефективне функціонування системи кібербезпеки України безпосередньо залежить від адекватного фінансового та матеріально-технічного забезпечення суб'єктів, що реалізують адміністративні процедури в цій сфері. Для досягнення оптимальних результатів необхідно вжити комплекс заходів, спрямованих на покращення матеріально-технічної бази та забезпечення необхідного фінансування. В даному контексті першочерговим кроком є проведення комплексного аналізу потреб суб'єктів у фінансових та матеріально-технічних ресурсах. Такий аналіз дозволить визначити пріоритетні напрямки фінансування та сформувати чіткий перелік необхідного обладнання, програмного забезпечення та інших матеріальних ресурсів. Важливим аспектом є розробка та впровадження механізмів сталого фінансування заходів із забезпечення кібербезпеки. Це може бути досягнуто шляхом: 1) збільшення бюджетних

асигнувань; 2) залучення коштів міжнародних донорів; 3) створення спеціальних фондів для фінансування наукових досліджень, розробки нових технологій та підготовки фахівців у галузі кібербезпеки; 4) впровадження механізмів співфінансування, зокрема необхідним є залучення коштів приватного сектору для фінансування спільних проектів у сфері кібербезпеки. Окрім того, переконані, що для ефективного використання фінансових ресурсів необхідно впровадити систему прозорого та ефективного управління бюджетними коштами. Це передбачає розробку чітких критеріїв оцінки ефективності використання коштів, проведення регулярних аудиторських перевірок та забезпечення відкритості інформації про витрачання бюджетних коштів;

- вдосконалити науково-методичне забезпечення досліджуваної сфери суспільного життя. Науково-методичне забезпечення – це створення умов для запровадження досягнень науки та техніки в практику, що включає в себе апробацію, уточнення умов і порядку застосування, розробку методичних рекомендацій чи інструкцій, підготовку користувачів тощо [74, с.22]. Отже, ефективне функціонування системи кібербезпеки України безпосередньо залежить від наявності сучасних науково-методичних розробок та їх впровадження у практичну діяльність. Для досягнення оптимальних результатів необхідно здійснювати комплекс заходів, спрямованих на удосконалення науково-методичного забезпечення суб'єктів, що реалізують адміністративні процедури в цій сфері. Так, першочерговим завданням є створення єдиної національної системи науково-методичного забезпечення у досліджуваній галузі. Така система повинна об’єднати зусилля наукових установ, закладів вищої освіти, державних органів та приватного сектору для розробки та впровадження нових наукових знань та методик. Окрім того, ключовим елементом є стимулювання наукових досліджень у галузі кібербезпеки. Необхідно забезпечити фінансування наукових проектів, спрямованих на розробку нових технологій захисту

інформації, аналіз кіберзагроз та розробку ефективних методів протидії їм. Важливим є також створення умов для проведення наукових конференцій, семінарів та інших заходів, спрямованих на обмін досвідом та ідеями між науковцями та практиками. Тож, для забезпечення практичної значущості наукових досліджень необхідно тісно інтегрувати науку та практику.

Таким чином, проведений аналіз дає змогу дійти до висновку, що запровадження вказаних вище кроків дозволить якісно покращити організаційні та правові аспекти реалізації адміністративних процедур у сфері забезпечення кібербезпеки.

Висновки до розділу 3

Встановлено, що стандарти забезпечення кібербезпеки — це набір правил, рекомендацій і вимог, що визначають методи і заходи для захисту інформаційних систем, мереж та даних від кібератак, несанкціонованого доступу, витоків даних та інших загроз кібербезпеці. Ці стандарти розроблені для встановлення загальних практик і політик, які організації можуть використовувати для забезпечення захисту своїх цифрових активів.

Відмічено, що у наш час, коли технології проникають у кожну сферу життя, питання захисту інформації набуває особливої актуальності. Кіберзагрози стають все більш витонченими та складними, тому захист даних від несанкціонованого доступу, зміни або знищення є одним із найважливіших завдань для будь-якої організації. Саме для забезпечення високого рівня кібербезпеки та створення єдиного підходу до захисту інформації були розроблені міжнародні стандарти. Ці документи встановлюють загальноприйняті правила та рекомендації, які допомагають організаціям створити надійні системи захисту інформації. Їх значення полягає у наступному: по-перше, вони забезпечують спільну мову для

обговорення питань кібербезпеки на глобальному рівні. Це дозволяє фахівцям з різних країн ефективно співпрацювати та обмінюватися досвідом; по-друге, стандарти пропонують системний підхід до управління інформаційною безпекою, що допомагає організаціям виявити та усунути вразливі місця у своїх системах; по-третє, дотримання міжнародних стандартів підвищує довіру клієнтів, партнерів та інвесторів до організації, оскільки свідчить про серйозний підхід до питань безпеки. І, нарешті, стандарти допомагають спростити процес сертифікації, оскільки багато систем сертифікації інформаційної безпеки базуються на міжнародних стандартах.

Зауважено, що впровадження стандартів ISO для кібербезпеки включає визначення критичних інформаційних активів, оцінку ризиків, визначення засобів контролю безпеки, забезпечення відповідності нормативним вимогам і встановлення процедур для постійного вдосконалення. Ідентифікація активів є початковим кроком у процесі впровадження ISO, де компанії повинні точно визначити інформаційні активи, важливі для їх діяльності та безпеки. Це включає такі дані, як конфіденційна інформація про клієнтів, інтелектуальна власність і фінансові записи. Оцінка ризиків передбачає ретельний аналіз потенційних загроз і вразливостей, які можуть поставити під загрозу ці активи. Проводячи комплексну оцінку ризиків, організації можуть визначати пріоритети своїх зусиль у сфері безпеки та ефективно розподіляти ресурси. Далі визначаються заходи безпеки для пом’якшення виявлених ризиків. Це передбачає вибір і впровадження таких заходів, як брандмауери, протоколи шифрування, засоби контролю доступу та системи моніторингу для захисту від потенційних кіберзагроз.

Узагальнено, що Україна запровадила ряд стандартів, пов’язаних із забезпеченням кібербезпеки. Разом із тим, адаптація національних та міжнародних стандартів у досліджуваній сфері має свою специфіку:

1) охоплення та адаптивність. Так, міжнародні стандарти, зазвичай, більш загальні та адаптивні, щоб задовольнити потреби широкого кола організацій по всьому світу, адже вони надають рамки, які можна адаптувати відповідно до специфічних потреб організації. Національні стандарти, навпаки, часто розробляються та адаптуються з урахуванням конкретних загроз і регуляторних вимог, що робить їх більш конкретними щодо певної галузі або типу організації, правової культури, тощо;

2) особливі регуляторні вимогу. У даному випадку національні стандарти включають вимоги, необхідні для відповідності місцевому законодавству та нормативним актам, адже міжнародні стандарти, як правило, більш універсальні і можуть використовуватися як основа для відповідності різним регуляторним вимогам у різних країнах;

3) застосування та сертифікація. Міжнародні стандарти, такі як ISO/IEC 27001, широко застосовуються для сертифікації в різних країнах і часто є основою для підвищення глобальної довіри та визнання. Національні стандарти ж мають обмежену географічну застосовність і можуть використовуватися, в основному, в межах однієї країни або регіону;

4) методологія та підхід до ризиків. Міжнародні стандарти, зазвичай, надають структурований підхід до управління ризиками з акцентом на ідентифікацію, оцінку та управління ризиками інформаційної безпеки. Національні стандарти можуть включати додаткові заходи або вимоги, що відображають місцеві загрози.

5) національні стандарти є більш гнучкими для адаптації до вітчизняних реалій, тоді як міжнародні – більш структуровані та формалізовані.

Обґрунтовано, що забезпечення кібербезпеки – це безперебійний процес, який вимагає постійного оновлення та вдосконалення. Саме тому, важливим завданням законодавця, а також приватних осіб в Україні є постійне оновлення (технологічне, професійне, ресурсне, тощо) системи

безпеки відповідно до нових загроз та вимог міжнародних стандартів. З огляду на зазначене вище, розробка національних та запровадження міжнародних стандартів кібербезпеки в Україні є необхідним кроком для забезпечення безпеки держави та її громадян. Це дозволить підвищити стійкість критичної інфраструктури, захистити персональні дані та сприяти розвитку цифрової економіки.

Акцентовано увагу на тому, що недоліки правового регулювання реалізації адміністративних процедур у сфері забезпечення кібербезпеки обумовлені: 1) історичними та політичними чинниками, зокрема: а) тривалий період перебування в складі СРСР призвів до того, що багато систем і мереж були побудовані за застарілими стандартами, що робить їх більш вразливими до сучасних кібератак; б) політичні потрясіння та конфлікти, які переживала Україна, відволікали ресурси і увагу від питань кібербезпеки; в) розташування України на стику інтересів різних геополітичних гравців робить її привабливою мішенню для кібератак; 2) технічними факторами: а) застаріле обладнання та програмне забезпечення, яке важко захистити від сучасних кібератак; б) бюджетні обмеження, що ускладнюють фінансування заходів із забезпечення кібербезпеки; в) дефіцит кваліфікованих кадрів; г) відсутність єдиної державної системи кібербезпеки, що ускладнює координацію зусиль із захисту від кібератак; 3) соціальними факторами, які обумовлені низьким рівнем кібергігієни, а також відсутність достатньої обізнаності населення про кіберзагрози; 4) економічними чинниками. Так, впровадження сучасних систем захисту вимагає значних фінансових інвестицій, що є недоступним для багатьох організацій. Окрім того, бюджетні кошти, які виділяються на кібербезпеку, часто конкурують з іншими пріоритетними напрямками розвитку держави; 5) війною в Україні, що спричинила: а) масовані кібератаки збоку російської федерації на критичну інфраструктуру, що призводить до значних збитків, а також перешкоджає нормальному функціонуванню всього державного апарату;

б) дестабілізацію роботи не тільки державного, але й приватного сектору, що значно шкодить фінансовому та економічному розвитку держави; в) відтік кваліфікованих кадрів у галузі кібербезпеки.

Зазначено, що у найбільш загальному розумінні концепція – це система поглядів, ідей або принципів, які об'єднуються в єдину цілісну картину, що пояснює певне явище, процес або ідею. Це своєрідний каркас, на якому будується розуміння, тлумачення і подальше дослідження будь-якого об'єкта чи процесу. Як нормативно-правовий акт, концепція – це особливого роду підзаконний нормативно-правовий акт, положення якого визначають основні напрями, принципи, цілі та завдання державної політики у певній сфері суспільного життя.

Аргументовано «Концепції розвитку системи забезпечення кібербезпеки в Україні» має важливе значення, оскільки вона дозволить: 1) забезпечити узгодженість та системність у правовому регулюванні адміністративних процедур у сфері кібербезпеки, усунути прогалини та суперечності в чинному законодавстві; 2) чітко визначити процедури та повноваження спеціально уповноважених суб'єктів, що спростить взаємодію між ними, пришвидшать швидкість та якість прийняття управлінських рішень та зменшать бюрократичні бар'єри; 3) покращити систему правового регулювання у досліджуваній сфері, що сприятиме захисту прав суб'єктів господарювання, забезпечить прозорість та обґрунтованість рішень, які приймаються щодо них органами державної влади; 4) підвищити рівень довіри до державних органів; 5) враховувати міжнародний досвід та стандарти у сфері кібербезпеки, що сприятиме інтеграції України в глобальний цифровий простір та поглибленню міжнародного співробітництва.

Встановлено, що метою «Концепції розвитку системи забезпечення кібербезпеки в Україні» має бути створення та підтримка ефективного, стійкого та безпечного кіберсередовища, яке б захищало національні

інтереси, сприяло сталому розвитку цифрової економіки та забезпечувало права та свободи громадян в інформаційному просторі. З огляду на окреслену мету, завданнями, які має містити дана Концепція, мають бути: 1) розробка ефективної системи управління кібербезпекою на державному рівні; 2) забезпечення взаємодії та координації суб'єктів забезпечення кібербезпеки (які включають як державний, так і приватний сектори); 3) визначення чітких адміністративних процедур забезпечення кібербезпеки та реагування на кіберінциденти; 4) розробка та впровадження заходів щодо підвищення стійкості органів державної влади та організацій різних форм власності до кібератак; 5) розробка та впровадження сучасних технологій захисту інформації; 6) підвищення рівня обізнаності громадян щодо кібербезпеки; 7) підготовка висококваліфікованих фахівців у галузі кібербезпеки, а також створення умов для їх постійного навчання та підвищення кваліфікації; 8) стимулювання розвитку наукових досліджень у сфері кібербезпеки; 9) забезпечення активної участі у міжнародних ініціативах з кібербезпеки, що має включати обмін досвідом та технологіями; 10) комплексне вдосконалення чинного законодавства, гармонізація національних та міжнародних стандартів у цій сфері; 11) створення національної системи інформування про кіберінциденти.

Обґрунтовано, що Стратегія кібербезпеки України в умовах воєнного стану має бути комплексним документом, який визначає пріоритетні напрямки та заходи для забезпечення стійкості критичної інфраструктури, захисту інформаційних систем держави та суспільства від кібератак, а також сприяння ефективній взаємодії всіх суб'єктів забезпечення кібербезпеки. Вона передбачає як технічні заходи (створення резервних систем, підвищення рівня захисту інформації), так і організаційні (розвиток кадрів, міжнародне співробітництво). Головна мета – зберегти стабільність функціонування держави та суспільства в умовах збройного конфлікту, де кіберпростір став одним із основних полів бою. Ключовими аспектами такої

стратегії мають бути: 1) Комплексний підхід, що включає поєднання технічних, організаційних та правових заходів; 2) орієнтація на майбутнє, постійна адаптація до нових загроз та технологій; 3) міжвідомча координація, що включає співпрацю всіх зацікавлених органів державної влади та приватного сектору; 4) обмін досвідом та технологіями з партнерами. Основними завдання зазначеної вище Стратегії є: захист критичної інфраструктури; захист державних інформаційних систем; захист персональних даних громадян; протидія дезінформації; підвищення кібергігієни населення.

Доведена необхідність доопрацювання «Стратегії кібербезпеки України», яка повинна враховувати виклики та реалії сьогодення, а також набутий досвід кібератак на кіберпростір України в останні три роки. В даному контексті вбачається необхідним: а) забезпечити консолідацію зусиль усіх державних органів, приватного сектору та міжнародних партнерів для оперативного виявлення, аналізу та нейтралізації кіберзагроз; б) розробити план впровадження штучного інтелекту та машинного навчання для швидкого аналізу великих обсягів даних та виявлення аномалій; в) визначити критично важливі об'єкти інфраструктури та розробити індивідуальні плани їх захисту; г) забезпечити регулярне оновлення програмного забезпечення та операційних систем для усунення вразливостей; ґ) створити умови для навчання населення критично оцінювати інформацію та розпізнавати фейки; тощо.

З метою вдосконалення правового регулювання адміністративних процедур у сфері забезпечення кібербезпеки обґрунтовано, що в Законі України «Про основні засади забезпечення кібербезпеки України» необхідно: а) уточнити теоретичну частину Закону, зокрема визначити поняття «адміністративні процедури забезпечення кібербезпеки»; б) встановити коло адміністративних процедур, а також розкрити їх зміст; в) визначити сфери

застосування цих адміністративних процедур; г) окреслити коло суб’єктів реалізації відповідних процедур, а також визначити їх правовий статус.

Доведено, що кадрове забезпечення – це ключовий чинник, від якого напряму залежить якість та ефективність реалізації адміністративних процедур забезпечення кібербезпеки. Зазначене пояснюється тим, що лише висококваліфіковані фахівці здатні належним чином виконувати покладені на них обов’язки, а також швидко адаптуватись до змін кіберсфери, яка активно розвивається. Тож, з метою удосконалення кадрового забезпечення суб’єктів реалізації адміністративних процедур у сфері кібербезпеки першочерговим кроком має бути створення чіткої системи вимог до кваліфікації фахівців, які працюють у сфері кібербезпеки. Ці вимоги мають враховувати як загальні знання в галузі інформаційних технологій, так і специфічні компетенції, необхідні для виконання конкретних функцій. Окрім того, важливим елементом є розробка та впровадження ефективних програм навчання та підвищення кваліфікації. Ці програми мають бути орієнтовані на постійне оновлення знань фахівців з урахуванням нових загроз та технологій. І останній аспект, якому слід приділити увагу, - створення системи мотивації працівників, яка б стимулювала їх професійний розвиток та підвищувала зацікавленість у роботі в сфері кібербезпеки;

Підкреслено, що ефективне функціонування системи кібербезпеки України безпосередньо залежить від адекватного фінансового та матеріально-технічного забезпечення суб'єктів, що реалізують адміністративні процедури в цій сфері. Для досягнення оптимальних результатів необхідно вжити комплекс заходів, спрямованих на покращення матеріально-технічної бази та забезпечення необхідного фінансування. В даному контексті першочерговим кроком є проведення комплексного аналізу потреб суб'єктів у фінансових та матеріально-технічних ресурсах. Такий аналіз дозволить визначити пріоритетні напрямки фінансування та сформувати чіткий перелік необхідного обладнання, програмного

забезпечення та інших матеріальних ресурсів. Важливим аспектом є розробка та впровадження механізмів сталого фінансування заходів із забезпечення кібербезпеки. Це може бути досягнуто шляхом: 1) збільшення бюджетних асигнувань; 2) залучення коштів міжнародних донорів; 3) створення спеціальних фондів для фінансування наукових досліджень, розробки нових технологій та підготовки фахівців у галузі кібербезпеки; 4) впровадження механізмів співфінансування, зокрема необхідним є залучення коштів приватного сектору для фінансування спільних проектів у сфері кібербезпеки. Окрім того, переконані, що для ефективного використання фінансових ресурсів необхідно впровадити систему прозорого та ефективного управління бюджетними коштами. Це передбачає розробку чітких критеріїв оцінки ефективності використання коштів, проведення регулярних аудиторських перевірок та забезпечення відкритості інформації про витрачання бюджетних коштів;

Констатовано, що належне функціонування системи кібербезпеки України безпосередньо залежить від наявності сучасних науково-методичних розробок та їх впровадження у практичну діяльність. Для досягнення оптимальних результатів необхідно здійснювати комплекс заходів, спрямованих на удосконалення науково-методичного забезпечення суб'єктів, що реалізують адміністративні процедури в цій сфері. Так, першочерговим завданням є створення єдиної національної системи науково-методичного забезпечення у досліджуваній галузі. Така система повинна об’єднати зусилля наукових установ, закладів вищої освіти, державних органів та приватного сектору для розробки та впровадження нових наукових знань та методик. Окрім того, ключовим елементом є стимулювання наукових досліджень у галузі кібербезпеки. Необхідно забезпечити фінансування наукових проектів, спрямованих на розробку нових технологій захисту інформації, аналіз кіберзагроз та розробку ефективних методів протидії їм. Важливим є також створення умов для проведення наукових конференцій,

семінарів та інших заходів, спрямованих на обмін досвідом та ідеями між науковцями та практиками. Тож, для забезпечення практичної значущості наукових досліджень необхідно тісно інтегрувати науку та практику.

ВИСНОВКИ

У дисертації наведено теоретичне узагальнення та нове вирішення наукового завдання, яке полягало в тому, щоб розкрити сутність, зміст та особливості адміністративних процедур забезпечення кібербезпеки в Україні, а також, спираючись на позитивний вітчизняний і зарубіжний досвід, розробити пропозиції та рекомендації, спрямовані на вдосконалення нормативно-правового регулювання суспільних відносин, що виникають у досліджуваній сфері суспільного життя. У результаті дослідження сформульовано низку нових наукових висновків, основні з них такі:

1. Констатовано, що кібербезпека як об’єкт адміністративно-правового регулювання означена такими особливостями: по-перше, становить особливу групу правовідносин, що виникають у специфічній сфері суспільного життя; по-друге, обумовлює необхідність здійснення низки різноманітних дій та заходів спеціально уповноваженими органами державної влади, а також приватними суб’єктами; по-третє, відповідна діяльність переважно регулюється нормами адміністративної галузі права; по-четверте, є сферою реалізації різноманітних процедур, які мають адміністративний характер.

2. Поняттям «адміністративні процедури у сфері забезпечення кібербезпеки» запропоновано вважати визначений законодавством України порядок дій, які реалізуються спеціально уповноваженими суб’єктами в напрямі забезпечення та захисту прав і законних інтересів фізичних та юридичних осіб, а також з метою реалізації публічних повноважень у сфері використання комунікаційних, технологічних систем, електронно-обчислювальної (комп’ютерної) техніки, програмного забезпечення та взаємодії в кіберпросторі.

Доведено, що особливостями адміністративних процедур у сфері забезпечення кібербезпеки є такі: по-перше, особлива сфера реалізації, а

також предмет, з приводу якого виникають відповідні суспільні відносини; по-друге, реалізовувати відповідні процедури мають право виключно спеціально уповноважені суб'єкти, посадові особи яких володіють набором специфічних професійних знань, умінь і навичок; по-третє, наявність спеціального набору нормативно-правових засад їх реалізації; по-четверте, переважна більшість адміністративних процедур пов'язані з обробкою персональних даних, що вимагає дотримання вимог законодавства про захист персональних даних; по-п'яте, наявність підвищеного рівня відповідальності суб'єктів, які відповідні процедури реалізовують; по-шосте, відповідні процедури застосовуються в різних сферах забезпечення кібербезпеки, що обумовлює наявність їх різновидів.

Адміністративні процедури у сфері забезпечення кібербезпеки запропоновано поділити на такі групи: 1) адміністративні процедури, пов'язані з організаційно-управлінським забезпеченням кібербезпеки; 2) адміністративні процедури, пов'язані зі змістом інформації, що обробляється в комунікаційних або технологічних системах; 3) адміністративні процедури, пов'язані із захистом інформації, що становить державну таємницю, комунікаційних і технологічних систем, призначених для її оброблення; 4) адміністративні процедури захисту комунікаційних систем, які не взаємодіють з публічними мережами електронних комунікацій.

3. Зауважено, що попри широкий суб'єктний склад забезпечення кібербезпеки, який охоплює значну кількість різноманітних державних, правоохоронних, військових та інших органів, основними суб'єктами реалізації адміністративних процедур у цій сфері є три публічно-правові відомства: Державна служба спеціального зв'язку та захисту інформації України, Національний банк України та Служба безпеки України. Саме вони наділені спеціальними правами та обов'язками у сфері забезпечення кібербезпеки, зокрема з питань реалізації адміністративних процедур

відповідного типу, а їх правовий статус відповідає ознакам адміністративних органів, передбачених Законом України «Про адміністративну процедуру».

4. Обґрунтовано положення про те, що на сьогодні система правового регулювання реалізації адміністративних процедур у сфері забезпечення кібербезпеки складається з низки нормативно-правових актів різної юридичної сили, кожен з яких регулює певний напрям досліджуваного питання. Зауважено, що попри значну увагу з боку законодавця та врегульованість досліджуваного питання, у зазначеній сфері залишається чимала кількість проблем, зокрема: по-перше, невизначеним є перелік адміністративних процедур, які реалізуються у відповідній сфері суспільного життя; по-друге, коло та правовий статус суб'єктів, які здійснюють відповідну діяльність, є досить розмитими; по-третє, законодавцем недостатньо розроблено питання впровадження міжнародних стандартів у цій сфері.

5. Аргументовано, що адміністративні процедури у сфері кібербезпеки пов'язані зі змістом інформації, що обробляється в комунікаційних або технологічних системах. Це – окрема група впорядкованих дій, заходів і процесів, що реалізуються уповноваженими суб'єктами та спрямовані на збір, обробку, зберігання, передачу й захист інформації у відповідних інформаційно-комунікаційних і технологічних системах. Зазначені процедури спрямовані на забезпечення конфіденційності, цілісності та доступності даних, а також на запобігання їх несанкціонованому доступу, розкриттю, модифікації або знищенню інформації. Наголошено, що основними суб'єктами реалізації цих процедур є Державна служба спеціального зв'язку і захисту інформації України та Національний банк України. До відповідних процедур зараховано такі: оцінка стану захищеності суб'єкта; сканування інформаційних ресурсів, розміщених у мережі Інтернет; експертиза; контрольні процедури.

6. Адміністративними процедурами, пов’язаними із захистом інформації, що становить державну таємницю, а також комунікаційних і технологічних систем, призначених для її оброблення, запропоновано вважати системну та систематизовану діяльність спеціально уповноважених органів державної влади, яка передбачає вчинення дій і заходів, спрямованих на організацію ефективного захисту та підтримки високого рівня безпеки під час оброблення та використання інформації, що становить державну таємницю у відповідних системах з метою запобігання та попередження її несанкціонованого витоку, що може завдати шкоди національним інтересам і безпеці. Серед відповідних процедур виокремлено: віднесення інформації до державної таємниці; надання дозволу на провадження діяльності, пов’язаної із секретними відомостями й даними; контроль за забезпеченням охорони державної таємниці; процедури погодження СБУ щодо створення, реорганізації чи ліквідації режимно-секретних органів.

7. Встановлено, що адміністративні процедури захисту комунікаційних систем, які не взаємодіють з публічними мережами електронних комунікацій, переважно мають внутрішньосистемний характер і реалізуються безпосередньо користувачами відповідних систем, а також спрямовані на забезпечення безпеки інформації та запобігання несанкціонованому доступу або витоку даних. Ці процедури є частиною загальної системи безпеки, що забезпечує належний рівень захисту від загроз як зсередини, так і ззовні організації. До вказаних процедур зараховано: формування політики безпеки; контроль та управління доступом; авторизація та аутентифікація визначеного переліку користувачів, що мають доступ до цієї системи; здійснення внутрішнього контролю (моніторинг та аудит системи); кадрові процедури; процедури управління та реагування на інциденти; захист даних і резервне копіювання.

8. З’ясовано, що Україна запровадила низку стандартів, пов’язаних із забезпеченням кібербезпеки. Водночас адаптація національних і міжнародних стандартів у досліджуваній сфері має певну специфіку, а саме:

1) охоплення та адаптивність. Так, міжнародні стандарти зазвичай є більш загальними й адаптивними, щоб задовольнити потреби широкого кола організацій по всьому світу, адже вони надають межі, які можна адаптувати відповідно до специфічних потреб організації. Національні стандарти, навпаки, часто розробляються та адаптуються з урахуванням конкретних загроз і регуляторних вимог, що робить їх більш конкретними щодо певної галузі або типу організації, правової культури тощо;

2) особливі регуляторні вимоги. У цьому контексті національні стандарти включають вимоги, необхідні для відповідності національному законодавству та нормативним актам, адже міжнародні стандарти зазвичай є більш універсальними й можуть використовуватися як основа для відповідності регуляторним вимогам у різних країнах;

3) застосування та сертифікація. Міжнародні стандарти, такі як ISO/IEC 27001, широко застосовуються для сертифікації в різних країнах і часто є основою для підвищення глобальної довіри та визнання. Натомість національні стандарти мають обмежену географічну застосовність і можуть використовуватися переважно в межах однієї країни або регіону;

4) методологія та підхід до ризиків. Міжнародні стандарти зазвичай надають структурований підхід до управління ризиками з акцентом на ідентифікацію, оцінку та управління ризиками інформаційної безпеки. Національні стандарти можуть включати додаткові заходи або вимоги, що відображають місцеві загрози.

5) національні стандарти є більш гнучкими для адаптації до вітчизняних реалій, тоді як міжнародні – більш структуровані та формалізовані.

9. Доведено, що шляхи вдосконалення правового регулювання адміністративних процедур у сфері забезпечення кібербезпеки слід поділити на дві великі групи:

1) нормативно-правовий напрям, у межах якого необхідно: а) розробити та прийняти Концепцію розвитку системи забезпечення кібербезпеки в Україні; б) привести у відповідність до вказаної Концепції Стратегію кібербезпеки України, яка буде адаптована до сучасних умов, викликів і набутого досвіду ведення війни (зокрема кібервійни) проти російської федерації; в) прийняти Стратегію кібербезпеки України в умовах воєнного стану; г) внести зміни до Закону України «Про основні засади забезпечення кібербезпеки України», а саме: уточнити теоретичну частину Закону, зокрема визначити поняття «адміністративні процедури забезпечення кібербезпеки»; встановити коло адміністративних процедур, а також розкрити їх зміст; визначити сфери застосування цих адміністративних процедур; окреслити коло суб'єктів реалізації відповідних процедур, а також їх правовий статус;

2) організаційно-управлінський напрям, у межах якого варто: а) покращити систему кадрового забезпечення суб'єктів, що уповноважені реалізовувати діяльність у досліджуваній сфері; б) переглянути фінансове та матеріально-технічне забезпечення галузі кібербезпеки; в) удосконалити науково-методичне забезпечення досліджуваної сфери суспільного життя.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Адміністративне право України : навч. посіб. / [В. В. Галунько, В. І. Курило, С. О. Короєд, О. Ю. Дрозд, І. В. Гиренко, О. М. Єщук, І. М. Риженко, А. А. Іванищук, Р. Д. Саунін, І. М. Ямкова] ; за ред. проф. В. В. Галунька. Херсон : Грінь Д. С., 2015. Т. 1. Загальне адміністративне право. 272 с.

2. Алімов Р. С. Процедури в адміністративному праві України: теорія і практика : дис. … канд. юрид. наук : 12.00.07. Донецьк, 2002. 164 с.

3. Андрусяк Т. Г. Теорія держави і права / Фонд сприяння розвитку укр. правової думки та пропаганди державницьких традицій "Право для України". Львів,1997. 200 с.

4. Антонюк У. В. Правове забезпечення екологічної безпеки у діяльності залізничного транспорту : автореф. дис. … канд. юрид. наук : 12.00.06. Київ, 2009. 21 с.

5. Бакалінська О, Бакалинський О. Правове забезпечення кібербезпеки в Україні. *Підприємництво, господарство і право*. 2019. № 9. С. 100–108.

6. Бандурка О. М. Управління в органах внутрішніх справ України : підручник. Харків : Університет внутрішніх справ, 1998. 480 с.

7. Баранов О. А. Про тлумачення та визначення поняття «кібербезпека». *Правова інформатика*. 2014. № 2 (42). С. 54–62.

8. Бевзенко В. М. Суб’єкти владних повноважень в адміністративному судочинстві України : дис. … д-ра юрид. наук : 12.00.07. Харків, 2010. 463 с.

9. Беназюк І. М. Конституційно-правові основи опозиційної діяльності в Україні : дис. … канд. юрид. наук : 12.00.02. Київ, 2010. 187 с.

10. Березовська Н. Л. Кібербезпека як об’єкт кримінально-правової охорони. *Кібербезпека в Україні: правові та організаційні питання* :

матеріали Всеукр. наук.-практ. конф. (м. Одеса, 21 жовт. 2016 р.) / ОДУВС. Одеса, 2016. С. 37–40.

11. Благодарний А. М. Адміністративна відповідальність за порушення законодавства про державну таємницю : дис. … канд. юрид. наук : 12.00.07. Київ, 2006. 200 с.

12. Бобровник С. В. Колізійні норми як засіб удосконалення сучасного законодавства. *Парламентаризм в Україні: теорія та практика* : матеріали міжнар. наук.-практ. конф., присвячена 10-й річниці з дня проголошення незалежності України та 5-й річниці з дня прийняття Конституції України. Київ, 2001. С. 497–498.

13. Бойко І. В., Зима О. О., Соловйова О. М. Адміністративна процедура : конспект лекцій / за заг. ред. І. В. Бойко. Харків : Право, 2017. 132 с.

14. Васильченко О. П. Джерела конституційного права України системно-функціональний аналіз) : дис. … канд. юрид. наук : 12.00.02. Київ, 2007. 248 с.

15. Великий тлумачний словник сучасної української мови (з дод. і допов.) / [уклад. і голов. ред. В. Т. Бусел]. Київ ; Ірпінь : Перун, 2005. 1728 с.

16. Великий тлумачний словник сучасної української мови / [уклад. і голов. ред. В. Т. Бусел]. Київ ; Ірпінь : Перун, 2001. 1440 с.

17. Вербіцька М. В., Росоляк О. Б. Адміністративні процедури у сфері господарської діяльності. *Порівняльно-аналітичне право*. 2017. №. 3. С. 151–153.

18. Галунько В. В. Адміністративно-правові основи організації та діяльності державної служби охорони при Міністерстві внутрішніх справ України : дис. … канд. юрид. наук : 12.00.07. Київ, 2003. 207 с.

19. Гальченко О. С. Удосконалення правового регулювання оплати праці в умовах ринкової економіки : дис. … канд. юрид. наук : 12.00.05. Луганськ, 2010. 188 с.

20. Гарбузюк К. Г. До проблеми визначення поняття та видів кадрових процедур в органах Національної поліції. *Юридична наука*. 2020. № 9 (111). С. 122–127. URL: https://journal-nam.com.ua/index.php/journal/article/view/506/479.

21. Гнатюк Л. В. Введення у філософію справжнього : наук. вид. Київ : Київське братство, 1997. 326 с.

22. Гнатюк М. Д. Правозастосування та його місце в процесі реалізації права : дис. … канд. юрид. наук : 12.00.01. Київ, 2007. 211 с.

23. Головін А. П. Адміністративно-правове регулювання діяльності міліції громадської безпеки : дис. … канд. юрид. наук : 12.00.07. Київ, 2004. 209 с.

24. Головченко Л. Н. Оцінка висновків криміналістичної експертизи : дис. ... канд. юрид. наук : 12.00.09. Київ, 1995. 216 с.

25. Гончаров С. М., Кушнір Н. Б. Тлумачний словник економіста / за ред. проф. С. М. Гончарова. Київ : Центр учбової літератури, 2009. 264 с.

26. Гончарук С. Т. Основи адміністративного права України : навч. посіб. Київ : Аванпост-Прим, 2004. 200 с.

27. Гулєвська Г. Ю. Організаційно-правові аспекти державного регулювання нотаріальної діяльності в Україні : дис. … канд. юрид. наук : 12.00.07. Запоріжжя, 2004. 205 с.

28. Даніл'ян В. О. Глобальне інформаційне суспільство: культура і людина. *Філософські обрії* : наук.-теорет. часопис. 2005. Вип. 14. С. 67–78.

29. Демків Р. Я. Закон в системі нормативно-правового регулювання діяльності міліції : дис. … канд. юрид. наук : 12.00.01. Київ, 2007. 218 с.

30. Демків Р. Я. Правове регулювання як юридичне явище: окремі аспекти розуміння. *Науковий вісник Ужгородського національного університету*. Серія : Право. 2015. Вип. 34 (1). С. 19–23.

31. Денисюк Д. С. Адміністративно-правові засади дозвільно діяльності ДАІ МВС України : дис. … канд. юрид. наук : 12.00.07. Харків, 2010. 192 с.

32. Денисюк С. Ф. Громадський контроль за правоохоронною діяльністю в Україні: адміністративно-правові засади : дис. … д-ра. юрид. наук : 12.00.07. Київ, 2010. 393 с.

33. Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України : постанова Кабінету Міністрів України від 16 лист. 2016 р. № 821. *Офіційний вісник України.* 2016. № 93. Ст. 3033.

34. Дикань Н. В., Борисенко І. І. Менеджмент : навч. посіб. Київ : Знання, 2008. 389 с.

35. Дикий А. П. Організація бухгалтерського обліку як інструмент забезпечення економічної безпеки підприємств : дис. … канд. екон. наук : 08.00.09. Житомир, 2009. 279 с.

36. Дідич Т. О. Нормопроектування: теоретико-правовий аспект : дис. … канд. юрид. наук : 12.00.01. Київ, 2006. 215 с.

37. Діордіца І. В. Поняття та зміст національної системи кібербезпеки. *Національний юридичний журнал: теорія і практика*. 2016. DECEMBRIE. С. 37–42.

38. Доценко О. С. Організація управління міліцією громадської безпеки в сучасних умовах : автореф. дис. … канд. юрид. наук : 12.00.07. Ірпінь, 2003. 21 с.

39. Екологічне право України : Академічний курс : підручник / за заг. ред. Ю. С. Шемшученко. Київ : Юридична думка, 2005. 848 с.

40. Електронне управління доступом — гнучке та безпечне. *GEZE* : [сайт]. URL: https://www.geze.ua/uk/cikavi-novini/temi/upravlinnja-dostupom

41. Енциклопедичний словник з державного управління / [уклад. : Ю. П. Сурмін, В. Д. Бакуменко, А. М. Михненко та ін.] ; за ред. Ю. В. Ковбасюка, В. П. Трощинського, Ю. П. Сурміна. Київ : НАДУ, 2010. 820 с.

42. Енциклопедія державного управління : у 8 т. / [наук.-ред. кол. : С. М. Серьогін, В. М. Сороко та ін.]. Київ : НАДУ, 2011. Т. 6. Державна служба. 524 с.

43. Євсєєв О. П. Процедури в конституційному праві України : дис. … канд. юрид. наук : 12.00.02. Харків, 2008. 220 с.

44. Єрмоленко В. М. Аграрні майнові правовідносини приватних сільськогосподарських підприємств в Україні : дис. … д-ра юрид. наук : 12.00.06. Київ, 2007. 380 с.

45. Железняк Н. А. Правові та організаційні форми діяльності Міністерства юстиції України у здійсненні державної правової політики (теоретичні та практичні питання) : дис. ... канд. юрид. наук : 12.00.07. Київ, 2004. 258 с.

46. Запара С. І. Удосконалення процедури вирішення колективних трудових спорів (конфліктів) примирними органам в Україні : дис. … канд. юрид. наук : 12.00.05. Київ, 2005. 198 с.

47. Запотоцька О. В. Поняття та зміст дозволу як засобу публічного адміністрування у сфері безпечності та якості харчових продуктів. *Науковий вісник Міжнародного гуманітарного університету.* Серія : Юриспруденція. 2017. № 30, т. 1. С. 111–113.

48. Захист ваших даних: що потрібно знати про захист даних. *ITEЗ* : [сайт]. URL: https://itez.com.ua/data-protection.html.

49. Захист інформації. *Державна служба спеціального зв'язку та захисту інформації України* : [сайт]. URL: https://cip.gov.ua/ua/statics/zakhist-informaciyi.

50. Івчук Ю. Ю. Теоретичні підходи до системи трудового права України в умовах ринкової економіки : дис. … канд. юрид. наук : 12.00.05. Луганськ, 2004. 175 с.

51. Ігонін Р. В., Вікторчук М. В. Поняття та особливості адміністративних процедур. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2019. Вип. 2. С. 182–190.

52. Касьяненко М. М., Гринюк М. В., Цимбал П. В. Організація роботи та управління органами державної податкової служби України : навч. посіб. Ірпінь : Академія ДПС України, 2001. 229 с.

53. Кікінчук В. Ю. Класифікація кадрових процедур в Національній поліції України. *Правові механізми забезпечення та захисту прав і свобод людини і громадянина, інтересів суспільства та держави* : тези доп. учасників наук.-практ. конф. (Харків, 14 черв. 2019 р.) / Наук.-дослід. ін-т публ. політики і соц. наук. Харків, 2019. С. 79–82. URL: https://library.pp-ss.pro/index.php/ndippsn_20190614/article/view/kikinchuk/pdf.

54. Коба В. Я. Оцінка достовірності висновків експерта під час судово-медичної діагностики повішення : дис. ... канд. мед. наук : 14.00.24. Київ, 1994. 135 с.

55. Коваленко О. В. Концептуальні засади розвитку національної системи кібербезпеки України на сучасному етапі державного будівництва. *Державне управління: удосконалення та розвиток*. 2020. № 6. URL: http://www.dy.nayka.com.ua/pdf/6_2020/104.pdf.

56. Козьяков І. Методологічні аспекти предметизації прокурорського нагляду. *Вісник Національної академії Прокуратури України*. 2009. № 4. С. 31–37.

57. Колпаков В. К., Кузьменко О. В. Адміністративне право України : підручник. Київ : Юрінком Інтер. 2003. 544 с.

58. Комзюк А. Т. Заходи адміністративного примусу в правоохоронній діяльності міліції: поняття, види та організаційно-правові

питання реалізації : монографія / за заг. ред. О. М. Бандурки. Харків : Нац. ун-т внутр. справ, 2002. 336 с.

59. Конвенція про кіберзлочинність : підписана 23 лист. 2001 р. *Офіційний вісник України*. 2007. № 65. Ст. 2535.

60. Конституція України : Закон України від 28 черв. 1996 р. № 254к/96-ВР. *Офіційний вісник України*. 2010. № 72/1. Ст. 2598.

61. Коржанський М. Й. Кримінальне право України. Загальна частина : курс лекцій. Київ : Наукова думка, 1996. 334 с.

62. Корнієнко Г. С. Правове регулювання матеріально-технічного забезпечення сільськогосподарських товаровиробників в умовах реформування АПК : дис. ... канд. юрид. наук : 12.00.06. Київ, 2003. 190 с.

63. Косиця О. Актуальні питання вдосконалення законодавства у сфері протидії кіберзлочинності. *Національний юридичний журнал : теорія і практика.* 2017. № 2. С. 81–84. URL: http://jurnaluljuridic.in.ua/archive/2017/2/19.pdf.

64. Кравцова Т. Правова природа державного регулювання підприємницької діяльності. *Підприємництво, господарство і право*. 2003. № 8. С. 3–6.

65. Кримінальний кодекс України : прийнятий 05 квіт. 2001 р. № 2341-III. *Відомості Верховної Ради України*. 2001. № 25. Ст. 131.

66. Кулаковська Л. П., Піча Ю. В. Організація і методика аудиту : навч. посіб. [2-ге вид.]. Київ : Каравела, 2005. 560 с.

67. Куліш А. М. Організаційно-правове забезпечення статусу працівників податкової міліції України : дис. … канд. юрид. наук : 12.00.07. Харків, 2003. 177 с.

68. Кундеус В. Г. Поняття та види кіберзлочинів. *Держава і злочинність. Нові виклики в епоху постмодерну* : зб. тез доп. наук.-практ. конф., присвяч. пам’яті віце-президента Кримінологічної асоціації України, професора, О. М. Литвака (м. Харків, 23 квіт. 2020 р.) / МВС України ;

Харків. нац. ун-т внутр. справ ; Кримінол. асоц. України. Харків, 2019. С. 44–45.

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

70. Легких К. В. Загальнонаукові та процесуальні питання проведення судової правової експертизи в судочинстві України : автореф. дис. … канд. юрид. наук : 12.00.09. Київ, 2009. 22 с.

71. Лісовська Ю. П. Кібербезпека: ризики та заходи : навч. посіб. Київ : Кондор, 2019. 272 с.

72. Малиновський В. Я. Державне управління : навч. посіб. [2-ге, допов. та перероб.]. Київ : Атіка, 2003. 576 с.

73. Марчук В. П. Словничок юридичних термінів : навч. посіб. Київ : МАУП, 2003. 128 с.

74. Матвієнко В. В. Криміналістичне забезпечення методики розслідування злочинів : дис. … канд. юрид. наук : 12.00.09. Київ, 2009. 248 с.

75. Мельник Ю. В. Правове регулювання діяльності місцевих органів виконавчої влади : дис. … канд. юрид. наук : 12.00.07. Київ, 2006. 185 с.

76. Методи захисту системи управління інформаційною безпекою / Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT) : ДСТУ ISO/IEC 27001:2015: офіц. вид. Київ : УкрНДНЦ, 2016. 28 с. URL: https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf.

77. Миколаєць А. П. Види адміністративних процедур у сфері взаємодії держави та громадськості. *Актуальні проблеми вітчизняної юриспруденції*. 2022. № 4. С. 65–70.

78. Миськів Л. І. Адміністративно-правові засади діяльності вищих навальних закладів МВС України з питань морально-правового виховання курсантів : дис. … канд. юрид. наук : 12.00.07. Харків, 2008. 203 с.

79. Митрофанов І. І. Що ж регулюється кримінальним правом? *Наше право*. 2016. № 1. С. 92–98.

80. Міжнародні соціальні стандарти : навч. посіб. / [авт.-сост. : А. М. Юшко, Н. М. Швець] ; за заг. ред. В. В. Жернакова. Харків : Нац. ун-т "Юрид. акад. України ім. Ярослава Мудрого", 2013. 121 с.

81. Набока Л. В. Структурно-функціональне забезпечення реалізації державно-управлінських відносин на територіальному рівні : дис. … канд. наук з держ. упр. : 25.00.01 Харків, 2008. 252 с.

82. Навіщо потрібна система контролю та управління доступом (СКУД)? *Vamark* : [сайт]. URL: https://vamark.ua/blog/navishho-potribna-systema-kontrolyu-ta-upravlinnya-dostupom-skud/.

83. Нижник Н. Р. Правовое регулирование государственно-управленческих отношений : автореф. дис. … д-ра юрид. наук : 12.00.02. Киев, 1992. 39 с.

84. Нижник Н. Р. Ситник Г. П. Білоус В. Т. Національна безпека України (методологічні аспекти, стан і тенденції розвитку) : навч. посіб. / за заг. ред. П. В. Мельника, Н. Р. Нижник. Київ : Преса України, 2000. 304 с.

85. Николина К. В. Юридична процедура: поняття, ознаки, види, місце в системі правових категорій : автореф. дис. … канд. юрид. наук : 12.00.01. Київ, 2011. 19 с.

86. Нікітін Ю. Конституціоналізм і національна безпека в контексті соціального виміру. *Вісник Академії правових наук України*. 2006. № 3 (46). С. 103–112.

87. Нікіфоров В. Ю. Захист профспілками соціально-трудових прав працівників в умовах ринкової економіки (теоретично-правовий аспект) : дис. … канд. юрид. наук : 12.00.05. Харків, 2004. 187 с.

88. Ніколайчик О. С. Адміністративні процедури, пов'язані зі змістом інформації, що обробляється в комунікаційних або в технологічних системах. *Право і суспільство*. 2021. № 6. С. 207–211.

89. Ніколайчик О. С. Адміністративні процедури, пов’язані із захистом інформації, що становить державну таємницю, комунікаційних та технологічних систем, призначених для її оброблення. *Юридична наука*. 2020. № 3(105). Т. 2. С. 61–67.

90. Ніколайчик О. С. Види адміністративних процедур у сфері забезпечення кібербезпеки. *Актуальні проблеми взаємодії правової науки та практики її застосування* : матеріали міжнар. наук.-практ. конф. (м. Київ, 16–17 берез. 2022 р.) / Наук.-дослід. ін-т публ. права. Київ, 2022. С. 118–120.

91. Ніколайчик О. С. До проблеми визначення поняття кібербезпеки як об’єкта адміністративно-правового регулювання. *Юридична наука*. 2020. № 1(103). Т. 2. С. 169–172.

92. Ніколайчик О. С. До характеристики адміністративних процедур забезпечення кібербезпеки, які не пов’язані із проведенням заходів захисту інформації у комунікаційних, технологічних системах, обробкою та обміном інформацією в кіберпросторі. *Науково-практичні засади розвитку юридичної науки на сучасному етапі державотворення* : матеріали міжнар. наук.-практ. конф. (м. Київ, 15–16 лют. 2023 р. / Наук.-дослід. ін-т публ. права. Київ, 2023. С. 117–121.

93. Ніколайчик О. С. До характеристики системи правового регулювання реалізації адміністративних процедур у сфері забезпечення кібербезпеки. *Юридичний науковий електронний журнал.* 2023. № 6. С. 850–852.

94. Ніколайчик О. С. Поняття адміністративних процедур у сфері забезпечення кібербезпеки. *Реформування українського законодавства: проблемні питання та шляхи їх вирішення* : матеріали міжнар. наук.-практ. конф. (м. Київ, 07–08 лют. 2024 р.) / Наук.-дослід. ін-т публ. права. Київ, 2024. С. 171–173.

95. Ніколайчик О. С. Суб’єкти реалізації адміністративних процедур у сфері забезпечення кібербезпеки. *KELM.* 2022. № 7 (51). С. 343–346.

96. Новий словник української мови : в 3 т. / [уклад. В. В. Яременко, О. М. Сліпушко]. 2-ге вид., виправл. Київ : АКОНІТ, 2001. Т. 1. А–К. 926 с.

97. Новий тлумачний словник української мови : у 4 т. / [уклад. В. В. Яременко, О. М. Сліпушко]. Київ : АКОНІТ, 1998. Т. 4. 941 с.

98. Оксінь В. Сутність адміністративних процедур вирішення питань місцевого значення в Україні. *Вісник АПСВТ*. 2020. № 3–4. С. 26–34.

99. Олійник В. І. Визначення родової належності поняття «державна таємниця». *Право і суспільство*. 2015. № 5 (2). С. 143–148.

100. Олійник О. В. Кібербезпека України: доктрина адміністративно-правового регулювання : дис. ... д-ра юрид. наук : 12.00.07. Київ, 2013. 451 с.

101. Основні завдання Державного центру кіберзахисту Держспецзв'язку. *Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України* : [сайт]. URL: https://scpc.gov.ua/uk/main-functions-and-tasks.

102. Пабат О. В. Роль адміністративної процедури в профілактиці злочинів у сфері службової діяльності. *Право і безпека*. 2008. № 7'2. С. 73–77.

103. Петрова І. П., Мулявка Д. Г. Нормативно-правове регулювання організації і діяльності міліції України : монографія. Ірпінь : Нац. акад. ДПС України, 2005. 176 с.

104. Петроє О. М., Даниленко Л. І., Ларіна Н. Б. Впровадження європейських стандартів суспільного розвитку в Україні : навч.-метод. матеріали. Київ : НАДУ, 2015. 92 с.

105. Політанський В. С. Поняття інформаційного суспільства: теоретико-правовий підхід. *Вісник Національної академії правових наук України.* 2017. № 1 (88). С. 77–86.

106. Політика інформаційної безпеки АТ «ЮНЕКС БАНК» (версія 4.0). *ЮНЕКС БАНК* : [сайт]. URL:

https://unexbank.ua/storage/uploads/7b4ffcf4-59f0-4538-a2e5-a62cce02887a/2024_Polityka_inform_bezpeky.pdf.

107. Політологія : навч. посіб. для вузів / [упоряд. та ред. М. Сазонова]. Харків : Фоліо, 1998. 735 с.

108. Популярна юридична енциклопедія / [В. К. Гіжевський, В. В. Головченко, В. С. Ковальський (кер.) та ін.]. Київ : Юрінком Інтер, 2002. 528 с.

109. Посібник з додаткових ресурсів CRR. 23 с. URL: chrome-extension://mhjfbmdgcfjbbpaeojofohoefgiehjai/index.html.

110. Прижиналінська Н. В. Формування кадрового потенціалу аграрного сектора регіону. *Вісник аграрної науки Причорномор'я*. Спеціальний випуск. 2007. № 3 (42). С. 43–48.

111. Про адміністративну процедуру : Закон України від 17 лют. 2022 р. № 2073-IX. *Відомості Верховної Ради України*. 2023. № 15. Ст. 50.

112. Про державну реєстрацію актів цивільного стану : Закон України від 01 лип. 2010 р. № 2398-VI. *Відомості Верховної Ради України*. 2010. № 38. Ст. 509.

113. Про державну службу спеціального зв’язку та захисту інформації України : Закон України від 23 лют. 2006 р. № 3475-IV. *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text.

114. Про державну таємницю : Закон України від 21 січ. 1994 р. № 3855-XII. *Відомості Верховної Ради України*. 1994. № 16. Ст. 93.

115. Про затвердження Вимог до аудиторів інформаційної безпеки на об'єктах критичної інфраструктури та порядку їх атестації (переатестації) : наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 30 квіт. 2024 № 228. *Офіційний вісник України*. 2024. № 57. Ст. 3413.

116. Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України : постанова

Кабінету Міністрів України від 23 верес. 2014 р. № 411. *Офіційний вісник України.* 2014. № 73. Ст. 2066.

117. Про затвердження Положення про державну експертизу у сфері технічного захисту інформації : наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16 трав. 2007 р. № 93. *Офіційний вісник України*. 2007. № 52. Ст.2153.

118. Про затвердження Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : постанова Кабінету Міністрів України від 16 лют. 1998 р. № 180. *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/laws/card/180-98-п.

119. Про затвердження Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг : постанова Правління Національного банку України від 16 січ. 2021 р. № 4. *Офіційний вісник України*. 2021. № 11. Ст. 470.

120. Про затвердження Порядку координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах : наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 10 черв. 2008 р. № 94. *Офіційний вісник України*. 2008. № 52. Ст. 1753.

121. Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах : наказ Адміністрації Державної

служби спеціального зв'язку та захисту інформації України від 02 груд. 2014 р. № 660. *Офіційний вісник України*. 2015. № 12. Ст. 323.

122. Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті : наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 15 січ. 2016 р. № 20. *Офіційний вісник України*. 2016. № 17. Ст. 695.

123. Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах : постанова Кабінету Міністрів України від 29 берез. 2006 р. № 373. *Офіційний вісник України*. 2006. № 13. Ст. 878.

124. Про інформацію : Закон України від 02 жовт. 1992 р. № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650.

125. Про ліцензування видів господарської діяльності : Закон України від 02 берез. 2015 р. № 222-VIII. *Відомості Верховної Ради України*. 2015. № 23. Ст. 1234.

126. Про Національний банк України : Закон України від 20 трав. 1999 р. № 679-XIV. *Відомості Верховної Ради України*. 1999. № 29. Ст. 238.

127. Про основні засади державного нагляду (контролю) у сфері господарської діяльності : Закон України від 05 квіт. 2007 р. № 877-V. *Відомості Верховної Ради України*. 2007. № 29. Ст. 389.

128. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017 р. № 2163-VIII. *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/2163-19/conv#Text.

129. Про Перелік посадових осіб, на яких покладається виконання функцій державного експерта з питань таємниць : указ Президента України від 19 трав. 2020 р. № 190/2020. *Офіційний вісник Президента України*. 2020. № 12. Ст. 606.

130. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" : указ Президента України від 26 серп. 2021 р. № 447/2021. *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/447/2021/conv#Text.

131. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки" : указ Президента України від 28 груд. 2021 р. № 685/2021. *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/685/2021/conv#Text.

132. Про Службу безпеки України : Закон України від 25 берез. 1992 р. № 2229-XII. *Відомості Верховної Ради України*. 1992 № 27. Ст. 382.

133. Пробко І. Б. Провадження у справах про порушення законодавства з фінансових питань : автореф. дис. … канд. юрид. наук : 12.00.07. Львів, 2009. 19 с.

134. Пузирний В. Ф. Державна таємниця: поняття та сутність. *Актуальні проблеми юридичної науки та практики*. 2020. № 1 (6). С. 37–41.

135. Радіонов І. І. Кримінальна відповідальність за бандитизм : дис. … канд. юрид. наук : 12.00.08. Харків, 2003. 205 с.

136. Робак В. А. Кримінальна відповідальність за створення не передбачених законом воєнізованих або збройних формувань : дис. … канд. юрид. наук : 12.00.08. Харків, 2008. 259 с.

137. Савченко Р. О., Савченко Н. М., Дем’янюк І. В. Внутрішній контроль: проблеми та перспективи. *Ефективна економіка*. 2019. № 9. URL: http://www.economy.nayka.com.ua/?op=1&z=7288. DOI: 10.32702/2307-2105-2019.9.51.

138. Селіванов А. Адміністрування податків: нові проблеми в адміністративному та фінансовому праві України. *Право України*. 2002. № 2. С. 34–38.

139. Семенюк О. Г. Теоретико-правовий аналіз поняття державної таємниці. *Інформація і право*. 2016. № 3 (18). С. 35–44.

140. Сергеєв С. О. Правове регулювання фіскальних правовідносин в Україні : дис. … канд. юрид. наук : 12.00.07. Харків, 2007. 185 с.

141. Середа О. О. Правова процедура: теоретико-правові засади та практичні виміри : автореф. дис. … канд. юрид. наук : 12.00.01. Київ, 2008. 16 с.

142. Сіверін В. І. Адміністративно-правові засади надання дозвільних послуг суб'єктами публічної адміністрації : дис. ... канд. юрид. наук : 12.00.07. Харків, 2010. 193 с.

143. Скакун О. Ф. Теорія держави і права : підручник. Харків : Консум, 2001. 656 с.

144. Словник синонімів української мови : в 2 т. / [А. А. Бурячок, Г. М. Гнатюк, С. І. Головощук та ін.]. Київ : Наукова думка, 2000. Т. 2. 954 с.

145. Словник української мови : в 11 т. / [редкол.: І. К. Білодід (голова) та ін.] ; АН Української РСР ; Ін-т мовознав. ім. О. О. Потебні. Київ : Наук. думка, 1976. Т. 7. Поїхати – Приробляти. 723 с.

146. Словник української мови : в 11 т. / [редкол.: І. К. Білодід (голова) та ін.] ; АН Української РСР ; Ін-т мовознав. ім. О. О. Потебні. Київ : Наук. думка, 1977. Т. 8. Природа – Ряхтливий. 927 с.

147. Собакарь А. О. Організаційно-правові основи утворення і функціонування спеціальних економічних зон в Україні : дис. … канд. юрид. наук : 12.00.07. Донецьк, 2002. 216 с.

148. Соловйов В. М. Поняття і сутність правового регулювання державного управління України. *Університетські наукові записки*. 2007. № 3 (23). С. 27–33.

149. Стежко С. М., Шевченко Т. О. Сучасний досвід США у сфері забезпечення кібербезпеки. *Інформація і право*. 2021. № 2. С. 139–144.

150. Столбовий В. М., Кисленко Д. П. Заходи підвищення кібербезпеки на державному та корпоративному рівнях в умовах диджиталізації суспільства. *Наукові записки Львівського університету*

бізнесу та права. Серія : Економічна. Серія : Юридична. 2023. Вип. 37. С. 175–183. URL: http://eprints.zu.edu.ua/38236/1/Стаття_Іваненко.pdf.

151. Стратегії розвитку України : теорія і практика / за ред. О. С. Власюка. Київ : НІСД, 2002. 864 с.

152. Тацишин І. Б. Адміністративно-правове забезпечення інформаційних відносин в галузі реклами : дис. … канд. юрид. наук : 12.00.07. Львів, 2009. 198 с.

153. Тихий В. П. Кримінальна відповідальність за порушення правил безпеки поводження із загально-небезпечними предметами. Київ : УМК ВО, 1989. 97 с.

154. Тополянська Т. О. Конституційно-процесуальні основи реалізації права законодавчої ініціативи : автореф. дис. … канд. юрид. наук : 12.00.02. Київ, 2009. 22 с.

155. Трофіменко О. Г., Прокоп Ю. В., Логінова Н. І., Задерейко О. В. Кібербезпека України: аналіз сучасного стану. *Захист інформації*. 2019. Т. 21, № 3. С. 150–157.

156. Трофімова Л. В. Організаційно-правове забезпечення діяльності юридичних підрозділів органів Державної податкової служби України : дис. … канд. юрид. наук : 12.00.07. Ірпінь, 2003. 203 с.

157. У чому різниця між процесами аутентифікації та авторизації. *Навчальний центр FoxmindEd* : [сайт]. URL: https://foxminded.ua/riznytsia-mizh-avtentyfikatsiieiu-ta-avtoryzatsiieiu/.

158. Управління органами Національної поліції України : підручник / за заг. ред. д-ра юрид. наук, доц. В. В. Сокуренка ; МВС України ; Харків. нац. ун-т внутр. справ. Харків : ХНУВС, 2017. 580 с.

159. Управління реагуванням на інциденти: як забезпечити безперервність бізнесу під час кіберінцидентів? *Span.eu* : [сайт]. URL: https://www.span.eu/ua/інсайти/реагування-на-інциденти/.

160. Фесюнін В. М. Організаційно-правові засади взаємодії органів державної податкової служби з населенням : дис. … канд. юрид. наук : 12.00.07. Харків, 2007. 187 с.

161. Фоміч Г. В. Адміністративні процедури у публічній службі України : автореф. дис. ... канд. юрид. наук : 12.00.07. Одеса, 2010. 20 с.

162. Форос Г. В., Жогов В. С. Особливості трактування поняття «кібербезпека» в сучасній юридичній науці. *Правова держава*. 2019. № 33. С. 128–134.

163. Франчук В. М. Резервне копіювання даних. *Науковий часопис НПУ імені М. П. Драгоманова.* Серія 2 : Комп'ютерно-орієнтовані системи навчання 2018. № 20 (27). С. 61–66. DOI: https://doi.org/10.31392/NPU-nc.series2.2018.20(27).10. URL: https://vfranchuk.fi.npu.edu.ua/images/files/statty/88.pdf.

164. Харитонов О. В. Дозвільна система в Україні : дис. … канд. юрид. наук : 12.00.07. Харків, 2004. 197 с.

165. Харченко Л. С., Ліпкан В. А., Логінов О. В. Кібербезпека України : глосарій / за заг. ред. Р. А. Калюжного. Київ : Текст, 2004. 136 с.

166. Хатнюк Ю. А. Поняття та особливості дозвільного провадження. *Науковий вісник Ужгородського Національного університету.* Серія : Право. 2018. Т. 2, Вип. 48. С. 20–23.

167. Цимбалюк В. С. Інформаційне право (основи теорії і практики) : монографія. Київ : Освіта України, 2010. 388 с.

168. Чорнописька В. Правові стандарти як міжнародно-правова категорія: теоретичні основи. *Вісник Національного університету "Львівська політехніка"*. Серія : Юридичні науки. 2022. Т. 9, № 4. С. 88–95.

169. Шала Л. В. Концепція приватної власності у римському праві та її рецепція у праві України : дис. ... канд. юрид. наук : 12.00.01. Львів, 2010. 207 с.

170. Шамсутдінов О. Відповідальність за розголошення державної таємниці за новим кримінальним законодавством України. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні* : наук.-техн. зб. 2001. Вип. 2. С. 21–25.

171. Шило С. М. Дозвільна система як особливий вид діяльності органів публічної адміністрації. *Науковий вісник Ужгородського Національного університету*. Серія : Право. 2023. Вип. 75, ч. 1. С. 305–310.

172. Шипілов Ю. Правова база української кібербезпеки: загальний огляд і аналіз. Міжнародна фундація виборчих систем, 2021. 40 с.

173. Шопіна І. М. Щодо концептуальних підходів до визначення поняття правового регулювання. *Форум права*. 2011. № 2. С. 1055–1061.

174. Шоптенко С. С. Особливості правового регулювання адміністративно-правового статусу судової міліції в Україні. *Право і безпека*. 2010. № 1 (33). С. 60–65.

175. Штангерт М. Й. Філософські проблеми правового виховання молоді (на прикладі закладів освіти МВС України) : дис. … д-ра. юрид. наук : 12.00.12. Львів, 2006. 240 с.

176. Шуба В. В. Адміністративно-правові відносини в діяльності органів Прокуратури України: загальнотеоретичні аспекти : дис. … канд. юрид. наук : 12.00.07. Дніпро, 2006. 200 с.

177. Щебликіна І. О., Грибова Д. В. Основи менеджменту : навч. посіб. Мелітополь : ММД, 2015. 479 с.

178. Що таке реагування на інциденти?_*Microsoft* : [сайт]. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-incident-response#:~:text=Реагування%20на%20інциденти%20–%20це%20дії,або%20збоїв%20у%20заходах%20безпеки.

179. Юридична енциклопедія : в 6 т. / [редкол.: Ю. С. Шемшученко (гол. редкол.) та ін.]. Київ : Укр. енцикл., 2003. Т. 5. П – С. 736 с.

180. Юридична енциклопедія : в 6 т. / [редкол.: Ю. С. Шемшученко (гол. редкол.) та ін.]. Київ : Укр. енцикл., 1998. Т. 1. А – Г. 720 с.

181. Юридична енциклопедія : в 6 т. / [редкол.: Ю. С. Шемшученко (гол. редкол.) та ін.]. Київ : Укр. енцикл., 1999. Т. 2. Д – Й. 744 с.

182. Як верифікувати користувача на сайті: дзвінки, SMS, електронна пошта. *CityHost.ua* : [сайт]. URL: https://cityhost.ua/uk/blog/yak-verifikuvati-koristuvacha-na-sayti-dzvinki-sms-elektronna-poshta.html.

183. Якимчук М. К. Організаційно-правові основи управління в органах прокуратури України : дис. … канд. юрид. наук : 12.00.07. Чернівці, 2002. 212 с.

184. Ярмакі Х. П. Адміністративна процедура як складова частина адміністративного процесу. *Науковий вісник публічного та приватного права*. 2019. Вип. 3, т. 1. С. 262–268.

185. Ярмакі Х. П. Адміністративно-наглядова діяльність міліції в Україні : монографія. Одеса : Юрид. літ., 2006. 336 с.

186. Яровий С. М. Організаційно-правове забезпечення виховної роботи в закладах освіти МВС України : дис. … канд. юрид. наук : 12.00.07. Харків, 2003. 204 с.

187. Ярошенко О. М. До питання про предмет права соціального забезпечення. *Вісник Національної академії правових наук України*. 2017. № 3 (90). С. 90–98.

188. Cyber security regulations and directors duties in the UK. URL: https://www.ncsc.gov.uk/collection/board-toolkit/cyber-security-regulation-and-directors-duties-in-the-uk#section_1.

189. Dan Craigen, Nadia Diakun-Thibault, Randy Purse Defining Cybersecurity. Technology Innovation Management Review. 2014. URL: https://timreview.ca/article/835.

190. Jeff Kosseff. Defining Cybersecurity Law. *IOWA LAW REVIEW*. 2018. Vol. 103:985. C. 985–1031.

191. Paul Cornish. The Oxford Handbook of Cyber Security. 2021. 890 p.

192. United States International Cyberspace & Digital Policy Strategy. URL: https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/.

193. What is the ISO for cyber security? URL: https://www.dataguard.co.uk/blog/what-is-the-iso-for-cyber-security/.

ДОДАТКИ

Додаток А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких висвітлено основні наукові результати дисертації:

1. Ніколайчик О. С. До проблеми визначення поняття кібербезпеки як об’єкта адміністративно-правового регулювання. *Юридична наука*. 2020. № 1(103). Т. 2. С. 169–172.

2. Ніколайчик О. С. Адміністративні процедури, пов’язані із захистом інформації, що становить державну таємницю, комунікаційних та технологічних систем, призначених для її оброблення. *Юридична наука*. 2020. № 3(105). Т. 2. С. 61–67.

3. Ніколайчик О. С. Адміністративні процедури, пов’язані зі змістом інформації, що обробляється в комунікаційних або в технологічних системах. *Право і суспільство.* 2021. № 6. С. 207–211.

4. Ніколайчик О. С. Суб’єкти реалізації адміністративних процедур у сфері забезпечення кібербезпеки. *KELM*. 2022. № 7 (51). С. 343–346 (Республіка Польща).

5. Ніколайчик О. С. До характеристики системи правового регулювання реалізації адміністративних процедур у сфері забезпечення кібербезпеки. *Юридичний науковий електронний журнал.* 2023. № 6. С. 850–852.

які засвідчують апробацію матеріалів дисертації:

6. Ніколайчик О. С. Види адміністративних процедур у сфері забезпечення кібербезпеки. *Актуальні проблеми взаємодії правової науки та практики її застосування*: матеріали Міжнар. наук.-практ. конф. (Київ, 16–17 берез. 2022 р.). Київ: Наук.-дослід. ін-т публіч. права, 2022. С. 118–120.

7. Ніколайчик О. С. До характеристики адміністративних процедур забезпечення кібербезпеки, які не пов’язані із проведенням заходів захисту

інформації у комунікаційних, технологічних системах, обробкою та обміном інформацією в кіберпросторі. *Науково-практичні засади розвитку юридичної науки на сучасному етапі державотворення:* матеріали Міжнар. наук.-практ. конф. (Київ, 15–16 лют. 2023 р.). Київ: Наук.-дослід. ін-т публіч. права, 2023. С. 117–121.

8. Ніколайчик О. С. Поняття адміністративних процедур у сфері забезпечення кібербезпеки. *Реформування українського законодавства: проблемні питання та шляхи їх вирішення*: матеріали Міжнар. наук.-практ. конф. (Київ, 7–8 лют. 2024 р.). Київ: Наук.-дослід. ін-т публіч. права, 2024. С. 171–173.