УДК 342.951
DOI https://doi.org/10.32844/2618-1258.2021.3.25

ЩИГОЛЬ Ю.Ф.

ОСОБЛИВОСТІ ПРИНЦИПІВ ФОРМУВАННЯ ТА РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ УКРАЇНИ У СФЕРІ ЗАХИСТУ ІНФОРМАЦІЇ

PECULIARITIES OF THE PRINCIPLES OF FORMATION AND IMPLEMENTATION OF THE STATE POLICY OF UKRAINE IN THE FIELD OF INFORMATION PROTECTION

Предмет цього наукового дослідження становлять властивості принципів державної політики України у сфері захисту інформації. Мета роботи передбачає висвітлення особливостей визначення принципів формування та реалізації державної політики у сфері захисту інформації.

Як відомо, центральним органом виконавчої влади (із спеціальним статусом) з питань захисту інформації є Адміністрація Державної служби спеціального зв'язку та захисту інформації України (ДССЗЗІ). Саме на неї покладені обов'язки щодо забезпечення, формування та реалізації державної політики із захисту інформації у визначених законодавством сферах діяльності. Проте сама державна політика у сфері інформації значно ширша за діяльність ДССЗЗІ та наразі недостатньо структурована. Водночас реалізація і формування політики вочевидь є різними процесами, які хоча і доповнюють один одного, але мають різне призначення. Отже, враховуючи, що правові принципи є важливою обов'язковою складовою частиною будь-якої політики, виникає необхідність у наданні правової характеристики останніх. Для цього необхідно дослідити зміст таких понять, як: «принципи»; «правові принципи»; «принципи державного захисту інформації».

У ході дослідження шляхом застосування методу аналізу й синтезу даних було розглянуто особливості чинного законодавства та здобутки наукової правової літератури з питання захисту інформації. Проведена робота дозволила структурувати та узагальнити особливості правових принципів, за якими здійснюється формування та реалізація державної політики у сфері захисту інформації в Україні.

Результатом наукової роботи стало авторське визначення поняття «правові принципи державного захисту інформації» та їх класифікація.

Матеріали дослідження будуть корисні для застосування в науковій та нормотворчій діяльності, зокрема у сфері: захисту інформації, інформаційного права, інформаційної політики, а також політики із забезпечення національної безпеки.

Ключові слова: *інформація, політика, національна безпека, правове регулювання, інформаційні відносини, інформаційне право.*

The subject of this research is the properties of the principles of state policy of Ukraine in the field of information protection. The purpose of the work is to highlight the features of determining the principles of formation and implementation of state policy in the field of information protection.

As you know, the central executive body (with a special status) for information protection is the Administration of the State Service for Special Communications and Information Protection of Ukraine (SSSCIP). It is responsible for ensuring, formulating and implementing state policy on information protection in the areas of activity defined by law. However, the state policy in the field of information is much broader than the activities of the SSSCIP and is currently insufficiently structured. At the same time, the implementation and formulation of policies are obviously different processes, which, although complementary but have different purposes. Therefore, given that legal

© ЩИГОЛЬ Ю.Ф. – здобувач (Науково-дослідний інститут публічного права)

principles are an important component of any policy, there is a need to provide a legal description of the latter. To do this, it is necessary to explore the meaning of the concepts: *principles; legal principles; principles of state protection of information.*

In the course of the research, by applying the method of data analysis and synthesis, the peculiarities of the current legislation and the achievements of the scientific legal literature on information protection were considered. This work allowed to structure and generalize the features of the legal principles according to which the formation and implementation of state policy in the field of information protection in Ukraine.

The result of scientific work was the author's definition of *legal principles of state protection of information* and their classification.

The research materials will be useful for application in scientific and rule-making activities, in particular in the field of: information protection, information law, information policy, as well as national security policy.

Key words: *information, policy, national security, legal regulation, information relations, information law.*

Вступ. «Законом України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [1], а також іншими нормативно-правовими актами визначено необхідність розвитку інформаційного суспільства, орієнтованого на інтереси людей, відкритого для всіх, в якому кожна людина може створювати і накопичувати інформацію та знання, мати до них вільний доступ, користуватися і обмінюватися ними, мати можливість повною мірою реалізувати свій потенціал, сприяти суспільному і особистісному розвиткові та підвищувати якість життя» [2]. Навіть одного наведеного нами положення, що визначене Розпорядженням Кабінету Міністрів «Про схвалення Стратегії розвитку інформаційного суспільства в Україні до 2020 року», достатньо, аби продемонструвати, наскільки широким є спектр питань, пов'язаних із «інформацією», та наскільки великим є її значення для сучасного суспільства. Виходячи із цього, цілком закономірним й очікуваним є те, що правові основи з проблем «інформації» закріплені на рівні Основного Закону України.

Постановка завдання. Метою статті є дослідження особливостей принципів формування та реалізації державної політики України у сфері захисту інформації.

Результати дослідження. Стаття 34 Конституції України стверджує, що «кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір…», а стаття 17 визначає, що забезпечення «інформаційної безпеки» України є однією з найважливіших функцій держави та справою всього Українського народу [3, ст. 34, ст. 17].

Наведені вище правові норми дозволяють зробити відразу декілька висновків. По-перше, держава має належним чином регулювати проблеми «інформації» та «інформаційних відносин», а відтак змушена проводити цілеспрямовану політику, направлену на реалізацію «інформаційних прав» громадян, осіб без громадянства, інших осіб, у тому числі не лише фізичних, але й юридичних. По-друге, «інформаційна державна політика» має забезпечувати баланс між публічними та приватними інтересами. По-третє, провадження «інформаційної політики» передбачає створення відповідних державних інститутів та вироблення належного правового інструментарію. І по-четверте, «інформаційна політика» є родовим поняттям по відношенню до «політики інформаційної безпеки», яка виступає важливою функцією та пріоритетом держави. Останнє твердження важливе для нашого дослідження, оскільки дозволяє нам, попри велику кількість різної спрямованості законів, підзаконних нормативно-правових актів, міжнародних документів, а також національних правових положень стратегічного характеру, зосередитись саме на сфері безпеки, до якої за своєю сутністю відноситься «захист інформації».

Зауважимо, що зміст терміну «захист інформації» розкритий законодавцем у Законі України «Про інформацію» та визначається як «сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї» [4, ст. 1].

«Спеціально уповноваженим центральним органом виконавчої влади (ЦОВВ) з питань організації … захисту інформації» [5, ч. 1] є Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ).

На ДССЗЗІ покладаються функції з: «формування та реалізаці(ї) державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, … захисту державних

інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах … і на об'єктах інформаційної діяльності, а також у сферах використання державних інформаційних ресурсів в частині захисту інформації, протидії технічним розвідкам, функціонування, безпеки та розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку; участь у формуванні та реалізації державної політики у сферах електронного документообігу (в частині захисту інформації державних органів та органів місцевого самоврядування), електронної ідентифікації …, електронних довірчих послуг (у частині встановлення вимог з безпеки та захисту інформації під час надання та використання електронних довірчих послуг, контролю за дотриманням вимог законодавства у сфері електронних довірчих послуг); забезпечення в установленому порядку та в межах компетенції діяльності суб'єктів, які безпосередньо здійснюють боротьбу з тероризмом» [6, ст. 3].

У наведених положеннях йдеться про «формування та реалізацію державної політики», проте ми маємо звернути увагу на те, що зміст терміну «політика» не має законодавчо закріпленого визначення. Наразі найближчим за сутністю поняттям (до теми нашого дослідження), що міститься в національній нормативно-правовій базі, є термін «політика інформаційної безпеки». Під останньою слід розуміти політику, яка «визначає підхід підприємства, установи та організації, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури, до інформаційної безпеки, вимоги, правила, обмеження, рекомендації, що регламентують порядок дотримання та забезпечення інформаційної безпеки» [7, ч. 2].

Процитоване визначення закріплене Постановою Кабінету Міністрів України «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури». Тип та призначення цього документу наклали свій відбиток на його зміст і спрямованість. Наголосимо, що запропонований ракурс розгляду означеного поняття влаштовує нас не повною мірою, оскільки зміст «політики інформаційної безпеки» в постанові розкривається лише стосовно «об'єктів критичної інфраструктури», тобто таких, що мають спеціальний статус. А в рамках нашого дослідження інтерес представляє більш узагальнене значення з акцентом на діяльності, в першу чергу саме держави.

Отже, узагальнюючи наведені вище дані, підкреслимо такі характеристики «державної політики у сфері захисту інформації». По-перше, вона представляє з себе регулюючу діяльність уповноважених на те органів держави. По друге, у її межах визначаються правові приписи, правила, обмеження, рекомендації з управлінських, організаційних, технічних, а також інших питань, вимог і заходів, як постійного так і тимчасового характеру.

Наголосимо, що уся сукупність передбачених «державною політикою» правових норм і вимог поділяється на дві великі групи: такі, що розраховані на певний проміжок часу – вони є «стратегічними» і відповідають за «формування державної політики»; та такі, що носять постійний характер – зазвичай регламентовані правовими нормами прямої дії, що спрямовані на «реалізацію державної політики».

Зауважимо, що функції з «формування» та «реалізації» зовсім не обов'язково покладаються на один і той самий державний суб'єкт. Більше того, навіть якщо обидві функції, як це відбувається у випадку із ДССЗЗІ, закріплені за одним органом, при цьому все одно існують вертикальні та інші відносини підпорядкування і зв'язки. Так, діяльність Адміністрації Державної служби спеціального зв'язку та захисту інформації України (Адміністрація Держспецзв'язку): «спрямовується і координується Кабінетом Міністрів України … (Держспецзв'язок) у своїй діяльності керується Конституцією та законами України, указами Президента України та постановами Верховної Ради України, прийнятими відповідно до Конституції та законів України, актами Кабінету Міністрів України, іншими актами законодавства» [5, ч. 1; ч. 2], ДССЗЗІ «є складовою сектору безпеки і оборони України» [6, ч. 2; ст. 2].

Отже, говорячи про «державну політику із захисту інформації», ми одночасно маємо на увазі обидві її частини: і «формування», і «реалізацію». Причому і одна й інша функція регламентуються адміністративно-правовими актами різної сили (від законів до наказів) виданими різними джерелами нормотворчої ініціативи.

Нагадаємо, що при складній системі правових актів, як відомо, інколи виникають невідповідності між закріпленими правовими приписами – так звані правові колізії. Про останні ми згадали лише у якості прикладу, який має підкреслити проблему забезпечення єдності між правовими вимогами із формування та реалізації «державної політики у сфері захисту інформації». Отже, найважливішу роль у вирішенні цієї проблеми відіграють «правові принципи», які визна-

чають не окремі правові норми, а засади й вихідні положення певної діяльності взагалі. Аналіз та порівняння принципів, закріплених у нормативній базі з питань «захисту інформації» дозволить оцінити стан узгодженості й цілісності державної політики в означеній сфері.

Аналіз останніх досліджень. Одразу зауважимо, що «правові принципи», як важлива складова частина «державної політики», досліджувались фактично більшістю вчених-адміністративістів, які вивчали правову «політику» в будь-яких напрямках діяльності держави. Серед дослідників, які внесли свій вклад у розробку теоретичних положень щодо сутності правових принципів, їх систем та значення, такі відомі вчені, як: А. Авер'янов, М. Афанасьєв, О. Бандурка, Д. Бахраха, В. Бевзенко, А. Венгеров, Т. Гуржий, С. Гусаров, О. Джафарова, Т. Коломоєць, В. Колпаков, А. Комзюк, Б. Кормич, В. Ліпкан, Н. Логінова, А. Марущак, В. Настюк, М. Нікулін, С. Шатрава, Ю. Шемшученко та багато інших.

Питання «інформаційної політики», її напрямків та принципів розглядали А. Баровська, С. Гнатюк, О. Голобуцький, Г. Головко, Т. Джига, Д. Дубов, С. Зуєв, Н. Корніловська, О. Крюков, О. Кузьмук, Ю. Машкаров, Д. Мельник, О. Мостовенко, В. Негодченко, Ю. Нестеряк, М. Ожеван, О. Орлов, В. Пожуєв, О. Соснін, В. Стєклов, В. Степанов, О. Орлов, В. Тронь, О. Шевчук, Т. Черненко, С. Чукут та інші вчені.

Проблематика «інформаційної безпеки» взагалі та правового забезпечення «захисту інформації» зокрема привертала увагу дослідників в галузі державного управління, безпеки, інформаційних технологій, технічних наук й інших галузей знань. Наразі питання «захисту інформації» комплексно вивчаються галузевими науковими установами, серед яких слід згадати, наприклад, такі як: «Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації Держспецзв'язку» (ДержНДІ технологій кібербезпеки); Державне підприємство «Український науково-дослідний інститут зв'язку» (ДП УНДІЗ); Державне підприємство «Одеський науково-дослідний інститут зв'язку» (ДП ОНДІЗ); Державне підприємство «Український науково-дослідний інститут радіо і телебачення» (ДП УНДІРТ); Приватне акціонерне товариство «Український інститут із проектування і розвитку інформаційно-телекомунікаційної інфраструктури «Діпрозв'язок» (ПрАТ «Діпрозв'язок»); у галузі зв'язку також провадить діяльність «Фонд нормативних документів», свої функції він виконує за напрямками роботи «проводовий та поштовий зв`язок» у складі ДП УНДІЗ та за напрямками «радіозв`язок і радіомовлення» у складі ДП УНДІРТ. Серед представників перелічених організацій свої роботи питанням правового супроводу «захисту інформації» присвятили, наприклад, такі вчені, як: С. Азаров, О. Верховець, С. Гончар, А. Демків, О. Задунай, Г. Леоненко, О. Липський, А. Мележик, А. Оніськова, В. Сидоренко та інші.

Проблематику правового забезпечення «інформаційної безпеки» та «стандартів захисту інформації» досліджували О. Захарова, М. Ізьо, В. Когут, Я. Кулешник, О. Олійник, А. Рудий, Т. Рудий, В. Сеник, С. Сеник, Р. Тарасенко, В. Цимбалюк та інші науковці.

Попри велику кількість робіт у сфері «інформаційної безпеки», питання принципів формування та реалізації «державної політики України у сфері захисту інформації» наразі залишається недостатньо дослідженим. Разом із тим існує ціла низка факторів, які пояснюють такий стан справ та обґрунтовують актуальність обраної для дослідження теми.

Перш за все, слід відмітити, що, як наголошувала А. Баровська, ще у 2011 році «на офіційному рівні лише Рада національної безпеки і оборони України (РНБО) запропонувала певну ієрархію керівних документів державної політики. (А саме: Доктрина – Концепція – Стратегія – Програма – План. Дослідниця підкреслює, що:) аргументації на користь саме такого підходу наведено не було. Водночас наукові дослідження пропонують й інші підходи до розгортання ієрархії керівних документів державної політики, зокрема: Концепція – Доктрина – Стратегія – Програма (Г. Ситник [8]); Стратегія – Концепція – Доктрина – Програма (А. Кузьменко [9])» [10]. Аналізуючи «доктринальні положення інформаційної безпеки України в умовах сучасності» [11], С. Гордієнко у 2019 році також висловлювався про змістовне наповнення понять *Доктрина, Концепція, Стратегія, Програма, Тактика* та критикував співвідношення їх використання в національній правотворчій практиці.

Отже, відсутність чіткої ієрархії керівних документів формування «політики» не сприяє упорядкуванню її принципів, при цьому залишаючи можливість аналізу ієрархічних співвідношень останніх лише за юридичною силою правових актів, якими закріплені відповідні документи. Ця ситуація ще більше ускладнена у сфері «інформаційної безпеки», оскільки її проблематика знаходиться на перетині «інформаційної політики» держави і правової «політики в сфері безпеки».

Іншим важливим фактором, який зумовлює необхідність уточнення принципів політики із «захисту інформації», є посилення кіберзагроз. Так, Н. Тарасенко, досліджуючи «Доктрину інформаційної безпеки», звертає увагу на оголошення Міноборони Російської Федерації 22 лютого 2017 року про створення військ інформаційних операцій. Науковець підкреслює, що «насправді це не було створення нових, а легалізація вже існуючих підрозділів, які здійснюють інформаційні та кібератаки давно і досить успішно» [12]. Отже, сучасні кіберзагрози це вже не лише випадкові дії поодиноких хакерів, а цілеспрямована організована професійна діяльність відповідних спецслужб. Яка для адекватної відповіді вимагає відповідної державної уваги, формування вимог до безпеки та введення певних обмежень на державному рівні. Усе означене вимагає встановлення відповідних правових принципів.

Певним продовженням означеної проблеми є ріст діджиталізації суспільного життя, наглядним прикладом якої між іншим є додаток «Дія». Або спроби влади створити об'єднані бази даних, безпека існування яких викликала жваві дискусії з боку фахівців із «захисту інформації». Тож цифровізація життя дедалі більшає, що безумовно потребує вироблення відповідних принципів і правил.

Обґрунтувавши таким чином актуальність дослідження, встановимо собі за мету: виявлення особливостей принципів формування та реалізації «державної політики у сфері захисту інформації». Досягнення означеної цілі вимагає виконання таких завдань: розкрити зміст понять «принципи» та «правові принципи»; порівняти між собою принципи, що визначенні у керівних документах, спрямованих на формування та на реалізацію «державної політики у сфері захисту інформації»; сформулювати визначення «принципів державного захисту інформації»; виділити особливості та вивести класифікацію принципів «державної політики у сфері захисту інформації»; зробити висновки та рекомендації з дослідженої проблематики. Для вирішення поставленої мети і завдань у нагоді стане метод аналізу й синтезу особливостей чинного законодавства та здобутків наукової правової літератури з питання «захисту інформації».

Виклад основного матеріалу. Слово «принцип» походить від латинського «principium», а також пов'язується із французьким «principe». У перекладі обидва асоціюються із початком або основою. Літературознавча енциклопедія стверджує, що «античні мислителі розуміли це поняття як відображення первинних ознак, притаманних об'єктивному довкіллю, вважали вказівкою пізнання сутності буття» [13, с. 271].

Академічний тлумачний словник української мови (СУМ) пояснює поняття «принцип» як: «1) основне вихідне положення якої-небудь наукової системи, теорії, ідеологічного напряму; 2) особливість, покладену в основу створення або здійснення чого-небудь, спосіб створення або здійснення чогось; 3) переконання, норму, правило, яким керується хто-небудь у житті чи поведінці» [14, с. 693].

Юридична енциклопедія надає близьке до вже наведених значень визначення терміна «принцип»: «1) основні засади, вихідні ідеї, що характеризуються універсальністю, загальною значущістю, вищою імперативністю і відображають суттєві положення теорії, вчення, науки, системи внутрішнього і міжнародного права, політичної, державної чи громадської організації. Принципам притаманна властивість абстрактного відображення закономірностей соціальної дійсності, що зумовлює їх особливу роль у структурі широкого кола явищ; 2) внутрішнє переконання людини, що визначає її ставлення до дійсності, суспільної ідей і діяльності (наприклад, принцип правомірної поведінки)» [15].

Вільна енциклопедія наводить більш стисле та узагальнене визначення поняття «принцип», розуміючи під ним «твердження, яке сприймається як головне, важливе, суттєве, неодмінне або, принаймні, бажане. (Вікіпедія виділяє також тлумачення поняття «принципів у науці») – це загальні вимоги до побудови теорії, сформульовані як те первинне, що лежить в основі певної сукупності фактів. При характеристиці різноманітних систем принципи відображають ті суттєві характеристики, що відповідають за правильне функціонування системи, без яких вона не виконувала б свого призначення» [16].

Кількість та зміст наведених визначень красномовно свідчать про міждисциплінарне та загально наукове значення терміну «принцип». Проте в рамках дослідження нас цікавлять лише ті «принципи», які використовуються в правових дисциплінах або навіть ще вужче, лише ті, що визначені чинними нормативно-правовими актами. Отже, ми маємо підстави ввести власне позначення та назвати такі принципи «правовими» або «принципами права». Останнє формулювання доречи вже використовується в науці. Так, Юридична енциклопедія Ю. Шемшученка пояснює поняття «принципи права» як: «керівні засади (ідеї), які визначають зміст і спрямо-

ваність правового регулювання суспільних відносин. Значення «принципів права» полягає у тому, що вони в стислому вигляді, концентровано відображають найсуттєвіші риси права, є його квінтесенцією, «обличчям». (Енциклопедія також наводить певним чином класифіковані) види «принципів права»: загальнолюдські (цивілізаційні), типологічні, конкретно-історичні, галузеві, міжгалузеві» [15].

Досліджуючи засади реалізації державної регіональної політики у сфері вищої освіти в Україні, О. Нижник зауважує: «Сьогодні існує багато наукових праць та досліджень де розглядається сутність категорії «принципи». Аналіз різних позицій щодо тлумачення зазначеної категорії свідчить, що вчені одностайні в його розумінні». (Науковець пропонує) під принципами розуміти фундаментальні засади на яких формується певне явище» [17, с. 41].

А. Шпак із цього приводу наголошує: «Відмінності щодо тлумачення категорії «принципи» стосуються лише обрання синонімів, за допомогою яких, може бути додатково позначене назване поняття (вихідні теоретичні положення, основні, керівні засади (ідеї), загальні нормативно-керівні положення, загальноприйняті норми-ідеї, провідні засади, незаперечні вимоги) тощо» [18, с. 39].

У цілому ми погоджуємось із наведеними твердженнями, але маємо зауважити, що база термінів законодавства містить близько півсотні визначень, які мають у своїй назві слово «принцип». Зокрема, звернемо увагу на такі з них: «Наукові принципи – визнані фундаментальні закони і факти природи, відомі через наукові методи» [19], а також «Принципи управління – правила, якими керуються суб'єкти управління. Принципи управління визначають вимоги до системи, процесу та механізму управління» [20]. Останнє визначення доречи зустрічається у п’яти підзаконних актах фактично без відмінностей, що також свідчить про достатньо однорідне сприйняття сутності цього терміну нормотворцями.

Починаючи розгляд «принципів захисту інформації», спочатку зосередимось на тій частині нормативно-правових актів, якою визначається «реалізація державної політики» в означеній сфері. Адже саме змістом цих «принципів» характеризується сьогоднішній стан «захисту інформації» в Україні.

Розгляд доцільно почати із Закону України «Про інформацію». Стаття 2 названого закону визначає основні «принципи інформаційних відносин». До низ відносяться: «гарантованість права на інформацію; відкритість, доступність інформації, свобода обміну інформацією; достовірність і повнота інформації; свобода вираження поглядів і переконань; правомірність одержання, використання, поширення, зберігання та захисту інформації; захищеність особи від втручання в її особисте та сімейне життя» [4, ст. 2]. Зауважимо, що безпосередньо захисту стосується «принцип правомірності захисту інформації». Отже, названий «принцип інформаційних відносин» фактично закладає підґрунтя цілого напрямку «інформаційної політики».

Закон України «Про Державну службу спеціального зв’язку та захисту інформації України» також закріплює досить чіткий перелік «принципів» діяльності ДССЗЗІ. Зокрема, стаття 4 означеного нормативно-правового акта стверджує, що: «1) діяльність ДССЗЗІ ґрунтується на принципах верховенства права, забезпечення дотримання прав і свобод людини і громадянина, безперервності, законності, забезпечення єдності державної політики, відкритості для демократичного цивільного контролю, прозорості, позапартійності; 2) ДССЗЗІ діє за принципом єдиноначальності» [6, ст. 4].

«Принципи» «законності» та «верховенства права» за своєю природою є конституційними. Про них прямо говориться або згадується про їх окремі аспекти у статтях 8, 19, 62, 68, 129 та інших статтях Конституції України. Принцип «забезпечення дотримання прав і свобод людини і громадянина» також витікає безпосередньо з положень Основного Закону, адже увагу на забезпеченні прав людини в Конституції України акцентовано вже в її преамбулі. Отже, згадані принципи спрямовані на забезпечення відповідної спрямованості діяльності держави та на додержання її основного призначення.

Інші перелічені принципи стосуються певних стандартів інституційної діяльності ДССЗЗІ. Наприклад, принцип єдності державної політики підкреслює її узгодженість з іншими напрямками політики держави (інформаційної, у сфері безпеки тощо). А відкритість до демократичного цивільного контролю взагалі є трендом побудови усіх державних інститутів.

Схожу картину розподілу та ґрунтування принципів будемо спостерігати й у Законі України «Про основні засади забезпечення кібербезпеки України». Стаття 7 останнього закріплює такі «принципи»: «1) верховенства права, законності, поваги до прав людини і основоположних свобод та їх захисту в порядку, визначеному законом; 2) забезпечення національних

інтересів України; 3) відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі; 4) державно-приватної взаємодії, широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері; 5) пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам, реалізації невід'ємного права держави на самозахист відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі; 6) пріоритетності запобіжних заходів; 7) невідворотності покарання за вчинення кіберзлочинів; 8) пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу; 9) міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях; 10) забезпечення демократичного цивільного контролю за утвореними відповідно до законів України військовими формуваннями та правоохоронними органами, що провадять діяльність у сфері кібербезпеки» [21].

Особливістю наведеного набору «принципів» є наявність спеціальних норм, обумовлених сферою їх застосування. Прикладом такого положення є «принцип пріоритетності запобіжних заходів». Адже його необхідність продиктована саме специфічними умовами, відносинами та діяльністю, що регулюється в сфері кібербезпеки.

На особливу увагу заслуговує також стаття 2 означеного закону, яка визначає «принципи застосування Закону». А саме: зону його дії а також особливостей провадження. Наприклад, правові норми означеного Закону здійснюються з додержанням принципу «мінімально необхідного регулювання, згідно з яким рішення (заходи) суб'єктів владних повноважень повинні бути необхідними і мінімально достатніми для досягнення мети і завдань, визначених цим Законом» [21]. Отже, область дії певних принципів окреслюється та обмежується.

Цікавою особливістю законодавства також є те, що такий важливий для забезпечення «захисту інформації» закон, як Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», взагалі не містить окремо сформульованих «принципів». Не менш цікавим є нормотворчий прийом, застосований в Указі Президента України «Про Положення про технічний захист інформації в Україні», який закріплює лише посилання на те, що відповідні «організаційно-технічні принципи … визначаються нормативно-правовими актами, прийнятими в установленому порядку відповідними органами» [22].

Переходячи до аналізу правових документів формування «політики у сфері захисту інформації», зауважимо, що європейська техніка законотворчості несхильна закріплювати окремі принципи в нормативно-правових актах. Отже, для нашого аналізу доцільно зосередитись саме на національному законодавстві.

Тож перш за все проаналізуємо «принципи», закріплені у вже згаданій нами раніше «Стратегії розвитку інформаційного суспільства в Україні». У цьому документі визначені такі «принципи», як: рівноправного партнерства державних органів, громадян і бізнесу; прозорості та відкритості діяльності державних органів; гарантованості права на інформацію, вільного отримання та поширення інформації, крім обмежень, установлених законом; свободи вираження поглядів і переконань; правомірності одержання, використання, поширення, зберігання та захисту інформації; інформаційної безпеки; постійного навчання; підконтрольності та підзвітності державних органів громадськості; сприяння пріоритетному розвитку інформаційно-комунікаційних технологій; чіткого розмежування повноважень і скоординованої взаємодії державних органів; гарантованості повного ресурсного забезпечення національних програм та проектів розвитку інформаційного суспільства [2].

Як і у здійсненому раніше аналізі законів, спостерігаємо ту саму ситуацію, коли «принципи» спираються на Конституцію України (наприклад, гарантування права на інформацію) або встановлюють і конкретизують особливості діяльність державних інститутів (наприклад, рівноправне партнерство державних органів з іншими суб'єктами, чи підконтрольності та підзвітності державних органів).

Продовжуючи аналіз, зауважимо, що такий важливий документ, як «Доктрина інформаційної безпеки України», використовує вже знайомий нам прийом визначення правових принципів зазначаючи, що «принципи … забезпечення кібербезпеки України визначені Стратегією кібербезпеки України» [23]. Остання ж стверджує такі «принципи»: «верховенства права і пова-

ги до прав та свобод людини і громадянина; забезпечення національних інтересів України; відкритості, доступності, стабільності та захищеності кіберпростору; державно-приватного партнерства, широкої співпраці з громадянським суспільством у сфері забезпечення кібербезпеки та кіберзахисту; пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам; пріоритетності запобіжних заходів; невідворотності покарання за вчинення кіберзлочинів; пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу; міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в протиправних та воєнних цілях; забезпечення демократичного цивільного контролю над утвореними відповідно до законів України військовими формуваннями та правоохоронними органами держави, що діють у сфері кібербезпеки» [24].

Аналіз «принципів політики» забезпечення «захисту інформації» був би неповним без згадування «принципів», викладених у «Стратегії національної безпеки України». В останній йдеться про два ще не згаданих раніше положення. А саме про намір «утверджувати принцип нульової толерантності до корупції, забезпечувати ефективну діяльність органів, які запобігають корупції та протидіють корупційним правопорушенням; та прискорити оборонну та безпекову реформи за нормами, принципами і стандартами НАТО» [25].

Висновки. Підводячи підсумок здійсненого аналізу особливостей притаманних «принципам» формування та реалізації «державної політики України в сфері захисту інформації», маємо підстави зробити такі висновки.

1. Сукупність положень нормативно-правових актів, які визначають формування та реалізацію «державної політики» у сфері «захисту інформації» дозволяє говорити про існування системи «принципів державного захисту інформації», пов'язаних смисловими зв'язками.

2. Під «принципами державного захисту інформації» доцільно розуміти: вихідні положення, норми, вимоги та правила, які наголошують на пріоритетах та акцентах реалізації правових норм у сфері захисту інформації, закріплених у нормативно-правових актах різного ступеню юридичної сили.

3. «Принципи державного захисту інформації» за їх змістом і спрямованістю можна умовно поділити на загальносистемні особливі та спеціальні.

4. Іншими ознаками для класифікації «принципів державного захисту інформації» є обмеження сфери їх дії (визначене державою або без вказування такого обмеження) та їх основа (джерело походження): Конституція України, міжнародні правові акти, інші національні нормативно-правові акти, вимоги та стандарти продиктовані неправовими джерелами (наприклад, особливості ресурсів і техніки призводять до необхідності принципу «пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам»).

5. Відсутність єдиного нормативно-правового акта, який би регулював діяльність держави в сфері «захисту інформації» ускладнює аналіз системи відповідних «принципів», це важливо тим більше, що принципи зазвичай не містять вказівок на перевагу щодо застосування якогось із них. Отже, з метою вирішення цієї проблеми доцільно в нормотворчій діяльності структурувати принципи за наведеними ознаками та класифікацією, а також уточнювати і розширювати їх склад на рівні підзаконних нормативно-правових актів.

Список використаних джерел:

1. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України від 09.01.2007 № 537-V. *Відомості Верховної Ради України (ВВР)*, 2007, № 12, ст. 102.

2. Про схвалення Стратегії розвитку інформаційного суспільства в Україні : розпорядження Кабінету Міністрів України від 15.05.2013 № 386-р. URL : https://zakon.rada.gov.ua/go/386-2013-%D1%80.

3. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР (із змінами). *Відомості Верховної Ради України (ВВР)*, 1996, № 30, ст. 141.

4. Про інформацію : Закон України від 02.10.1992 № 2657-XII (із змінами). *Відомості Верховної Ради України (ВВР)*, 1992, № 48, ст. 650.

5. Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України : постанова Кабінету Міністрів України від 03.09.2014 № 411 (із змінами). URL : https://zakon.rada.gov.ua/go/411-2014-%D0%BF.

6. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 р. № 3475-IV (із змінами). *Відомості Верховної Ради України (ВВР)*, 2006, № 30, ст. 258.

7. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : постанова Кабінету Міністрів України від 19.06.2019 № 518. URL : https://zakon.rada.gov.ua/go/518-2019-%D0%BF.

8. Ситник Г.П. Державне управління у сфері забезпечення національної безпеки України: теорія і практика : автореф. дис… д-ра наук з держ. управління: 25.00.01. Київ, 2004. 36 с.

9. Кузьменко А. Проблеми відповідності стратегії та системи забезпечення безпеки України національним потребам. *Юридичний Журнал*. 2006. № 10. С. 79–87.

10. Баровська А. Структура керівних документів державної політики в інформаційній сфері: нагальні проблеми та шляхи впорядкування. Аналітична записка. 2011. URL : http://old.niss.gov.ua/articles/572/.

11. Гордієнко С. Доктринальні положення інформаційної безпеки України в умовах сучасності. URL : https://lexinform.com.ua/dumka-eksperta/doktrynalni-polozhennya-informatsijnoyi-bezpeky-ukrayiny-v-umovah-suchasnosti/.

12. Тарасенко Н. Доктрина інформаційної безпеки України в оцінках експертів. *Резонанс*. 2017. № 18. С. 3–14.

13. Літературознавча енциклопедія : у 2 т. / авт.-уклад. Ю.І. Ковалів. Київ : ВЦ «Академія», 2007. Т. 2 : М-Я. 624 с.

14. Словник української мови: в 11 тт. / АН УРСР. Інститут мовознавства; за ред. І.К. Білодіда. К. : Наукова думка, 1970-1980. / Т. 8. ред. тому В.О. Винник, 1977. 927 с.

15. Юридична енциклопедія / ред. Ю.С. Шемшученко [та ін.] ; НАН України, Ін-т держави і права ім. В.М. Корецького. Київ : Вид-во «Українська енциклопедія» ім. М.П. Бажана, 1998-2004. / Т. 5 : П-С. 2003. 736 с.

16. Вікіпедія (Вільна енциклопедія), «Принцип». URL : https://uk.wikipedia.org/wiki/Принцип.

17. Нижник О.С. Адміністративно-правові засади реалізації державної регіональної політики у сфері вищої освіти в Україні : дис. … канд. юрид. наук : 12.00.07. Харків, 2017. 220 с.

18. Шпак А.П. Адміністративно-правова охорона права інтелектуальної власності у сфері освіти : дис. … канд. юрид. наук : 12.00.07. Київ, 2015. 210 с.

19. Міжнародні медико-санітарні правила (2005 р.) : Правила ВООЗ від 23.05.2005 р. URL : https://zakon.rada.gov.ua/go/897_007.

20. Про затвердження Положення про систему управління безпекою судноплавства на морському і річковому транспорті : наказ Міністерства транспорту України від 20.11.2003 р. № 904 (із змінами). URL : https://zakon.rada.gov.ua/go/z1193-03.

21. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII (із змінами). *Відомості Верховної Ради (ВВР),* 2017, № 45, ст. 403.

22. Про Положення про технічний захист інформації в Україні : Указ Президента України від 27.09.1999 р. № 1229/99 (із змінами.) URL : https://zakon.rada.gov.ua/go/1229/99.

23. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 № 47/2017. URL : https://zakon.rada.gov.ua/go/47/2017.

24. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 № 96/2016. URL : https://zakon.rada.gov.ua/go/96/2016.

25. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України від 14.09.2020 № 392/2020. URL: https://zakon.rada.gov.ua/go/392/2020.