УДК 351.078: 681.518

З. О. Надюк
доктор наук із державного управління, доцент,
професор кафедри державного управління
Львівського регіонального інституту державного управління
Національної академії державного управління при Президентові України

УЗГОДЖЕННЯ ПРИНЦИПІВ ВІДКРИТОСТІ І ПРОЗОРОСТІ З БАЗОВИМИ ВИМОГАМИ КІБЕРБЕЗПЕКИ В ДІЯЛЬНОСТІ ОРГАНІВ ПУБЛІЧНОЇ ВЛАДИ В УКРАЇНІ

У статті досліджується сучасний стан здійснення процесу доступу до публічної інформації в Україні. Визначено основні проблеми дотримання принципів відкритості і прозорості в діяльності органів публічної влади. Обгрунтовано потребу узгодження принципів відкритості і прозорості з базовими вимогами кібербезпеки в діяльності органів публічної влади. Надано рекомендації щодо можливих шляхів вирішення цієї проблеми в сучасних умовах державотворення.

Ключові слова: *державні службовці, державне управління, кібербезпека, механізм державного управління, принципи відкритості і прозорості, публічні органи влади, публічна політика.*

Постановка проблеми. Публічна політика держави, як відомо, передбачає максимальну відкритість і прозорість діяльності органів державної влади, прийнятих у межах їх компетентності управлінських рішень [16, с. 246]. Надшвидкий розвиток інформаційно-комунікаційних технологій, упровадження механізмів електронного урядування, дотримання принципів відкритості і прозорості в діяльності органів публічної влади, з одного боку, і вимога забезпечення базових засад кібербезпеки як компонента національної безпеки в сучасних умовах, з іншого боку, потребує розроблення механізмів взаємоузгодження цих процесів у життєдіяльності держави.

Метою статті є виокремлення основних складових частин проблеми узгодження принципів відкритості і прозорості з базовими вимогами кібербезпеки в діяльності органів публічної влади в Україні та обґрунтування шляхів її вирішення.

Аналіз останніх досліджень і публікацій. Теоретичні і практичні аспекти проблеми нормативно-правового забезпечення інформаційної відкритості та прозорості публічних органів влади досліджувалися такими фахівцями, як В.Б. Авер'янов, В.І. Андрейцев, Ю.П. Битяк [1], В.М. Гаращук, Л.П. Горбата [7], С.Г. Гречанюк, Є.В. Додін, В.А. Комаров, Н.П. Матюхіна, О.М. Музичук, В.Ф. Нестерович [18], Н.Р. Нижник, В.П. Петренко, В.М. Сердюк та ін.

Питання вдосконалення політики держави у сфері інформатизації суспільства, взаємодії органів публічної влади з громадськістю, впровадження електронного урядування були предметом досліджень таких вчених, як: А. Акуленко, Є. Болотіна [2], О. Бухтатий [3], А. Вишневський [4], Л. Віткін [5], І. Грабовець [8], В. Даниленко [21], М. Демкова [13], В. Дрешпак [10], П. Клімушин [12], В. Клюцевський [13], І. Колесніченко [14], Д. Коліушко [13], В. Коновал [22], З. Надюк [15], О. Риженко [20], А. Семенченко [22], А. Серенок [12], С. Соловйов [21], О. Тарасова [6], С. Чукут, О. Шевчук та ін. Глобалізаційні виклики сучасності формують потребу дослідження проблем узгодження принципів відкритості і прозорості з базовими вимогами кібербезпеки в діяльності органів публічної влади в Україні, що є особливо актуальним у сучасних умовах розвитку української державності і побудови демократичного суспільства.

Виклад основного матеріалу. Порядок доступу громадян до публічної інформації регламентується такими нормативно-правовими документами, як Конституція України, Закон України «Про доступ до публічної інформації», Закон України «Про інформацію» та ін. Є два основних варіанти отримання громадянами доступу до публічної інформації [25, з посиланням на 6]: активний і пасивний. Це передбачено ст. 5 «Забезпечення доступу до інформації» Закону України «Про доступ до публічної інфор-

мації» [19, ст. 5], зокрема: «Доступ до інформації забезпечується шляхом: систематичного та оперативного оприлюднення інформації: в офіційних друкованих виданнях; на офіційних веб-сайтах у мережі Інтернет; на єдиному державному веб-порталі відкритих даних; на інформаційних стендах; будь-яким іншим способом» – це пасивний спосіб отримання громадянином інформації; а «надання інформації за запитами на інформацію» – активний спосіб. Цей спосіб (активний) передбачає певні дії громадянина (звернення за інформацією) і вимагає певного регламентованого часу на підготовку потрібної громадянинові інформації або обґрунтованої відмови в її наданні.

Іншим аспектом проблеми забезпечення доступу до інформації є власне вид такої інформації. Відповідно до статті 6 Закону України «Про доступ до публічної інформації» [19, ст. 6] до публічної інформації з обмеженим доступом відноситься конфіденційна інформація, таємна інформація і службова інформація, обмеження доступу до яких здійснюється відповідно до закону за умов дотримання сукупності вимог.

Як зазначають фахівці (Даниленко С., 2012), основними видами правопорушень щодо застосування положень Закону України «Про доступ до публічної інформації» є такі [9]:

1) неправомірна відмова публічних органів у наданні інформації через її приналежність до інформації з обмеженим доступом;

2) незаконне застосування грифів обмеження доступу до інформації «опублікуванню не підлягає», «не для друку», «для службового користування»;

3) ігнорування інформаційних запитів;

4) перешкоди в отриманні громадянами локальних нормативно-правових актів місцевих органів влади;

5) неналежне виконання представниками влади вимоги оприлюднювати інформацію про свою діяльність тощо.

У власних попередніх дослідженнях [16] ми рекомендували здійснити низку заходів щодо вдосконалення нормативно-правової бази, зокрема щодо законодавчого визначення базових термінів «публічна інформація», «суспільно необхідна інформація» та ін. Також було наголошено на потребі чіткішого регламентування використання грифу «Для службового користування» для позначення інформації з обмеженим доступом для ознайомлення.

Як зазначає Горбата Л.П. (2018) [7, с. 126], «існує три основні чинники, які визначають відкритість влади: якісне нормативно-правове забезпечення; впровадження дієвих механізмів і процедур для доступу громадян до інформації про діяльність влади, конкретизація реалізації прав; рівень політичної культури в державі і в суспільстві».

На забезпечення принципів відкритості і прозорості в роботі органів публічної влади впливає законодавчо регламентоване зобов'язання надавати чи ні інформацію про свою діяльність. Як зазначають фахівці [9], «позбавлення публічних органів влади обов'язку інформувати громадськість про свою діяльність провокує грубі порушення принципів розвитку демократичного суспільства». Ми погоджуємось із такою думкою, адже для демократичного сталого розвитку держави необхідно забезпечити прозорість і відкритість у роботі органів публічної влади.

В.Ф. Нестерович (2016), визначає три нові механізми в забезпеченні дотримання принципів відкритості і прозорості в діяльності органів публічної влади [18, с. 73]: електронні петиції; ProZorro й електронне декларування.

Проблемним аспектом у забезпеченні прозорості та інформаційної відкритості органів публічної влади є вдосконалення нормативно-правової бази щодо декларування державними службовцями особистого майна і доходів. Зокрема, фахівці [11] зазначають такі дискусійні моменти:

1) зобов'язання декларування власних доходів державними службовцями лише певних категорій;

2) відсутність контролю з боку правоохоронних та контролюючих органів за доходами та витратами державних службовців і достовірністю зафіксованих у деклараціях даних;

3) наявність можливості для державних службовців та інших представників владних структур (депутатів, голів відповідних рад) досить легко приховувати незаконно одержані майно та доходи, зокрема шляхом оформлення їх на інших осіб (знайомих, родичів тощо), які не є суб'єктами декларування.

Згідно зі статтею 4 Закону України «Про основні засади забезпечення кібербезпеки України» об'єктами кібербезпеки та кіберзахисту є [20, ст. 4] «комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів міс-

цевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону», а також «комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу».

Основними суб'єктами забезпечення кібербезпеки в Україні виступають Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України, Розвідувальні органи України, Національний банк України та ін.

У таблиці 1 подані базові завдання основних суб'єктів національної системи кібербезпеки України (згідно зі ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України»).

На нашу думку, доцільно розробити організаційно-методичне забезпечення діяльно-

Таблиця 1

Базові завдання основних суб'єктів національної системи кібербезпеки України [20, ст. 8]

№ з/п	Інституція	Основні завдання
1	Державна служба спеціального зв'язку та захисту інформації України	забезпечує формування та реалізацію державної політики щодо захисту в кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, 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, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA;
2	Національна поліція України	забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; - здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі;
3	Служба безпеки України	здійснює запобігання, виявлення, припинення та розкриття злочинів 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;
4	Міністерство оборони України	відповідно до компетенції здійснює заходи з підготовки держави до відбиття воєнної агресії в кіберпросторі (кібероборони); - здійснює військову співпрацю з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз; - впроваджує заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану;
5	Розвідувальні органи України	здійснюють розвідувальну діяльність щодо загроз національній безпеці України в кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки;
6	Національний банк України	визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки в банківській системі України та для суб'єктів переказу коштів, здійснює контроль за їх виконанням; - створює центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту в банківській системі України; - забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки на об'єктах критичної інфраструктури в банківській системі України.

сті державних службовців, що безпосередньо здійснюють інформаційно-комунікаційну взаємодію з громадськістю в межах дії Закону України «Про доступ до публічної інформації», з урахуванням потреби дотримання принципів відкритості і прозорості, з одного боку, та вимог забезпечення кібербезпеки органів публічної влади – з іншого.

Висновки і пропозиції. У статті досліджено проблему дотримання базових вимог кібербезпеки з погляду забезпечення принципів відкритості і прозорості в діяльності органів публічної влади. Надшвидкий розвиток інформаційно-комунікаційних технологій, упровадження механізмів електронного урядування, дотримання принципів відкритості і прозорості в діяльності органів публічної влади, з одного боку, і вимога забезпечення базових засад кібербезпеки як компонента національної безпеки в сучасних умовах, з іншого, потребує розробки механізмів взаємоузгодження даних процесів у життєдіяльності держави. Визначено основні проблеми дотримання принципів відкритості і прозорості в діяльності органів публічної влади. Обґрунтовано потребу узгодження принципів відкритості і прозорості з базовими вимогами кібербезпеки в діяльності органів публічної влади.

Список використаної літератури:

1. Битяк Ю.П. Пріоритетні напрями забезпечення ефективного функціонування публічної служби в Україні. Теорія та практика правознавства. 2015. Вип. 1. URL: http://nbuv.gov.ua/UJRN/tipp_2015_1_21.
2. Болотіна Є.В., Акуліна А.В. Інформатизація державного управління: сучасні проблеми. Научный вестник ДГМА. 2017. № 2(23Е). С. 134–141.
3. Бухтатий О., Радченко О. Еволюція українського законодавства про електронне урядування: проблеми і перспективи. Теорія та практика державного управління і місцевого самоврядування. 2015. № 2. С. 81–97.
4. Вишневський А., Дунаєв В. Електронне урядування: досвід упровадження в Головдержслужбі України. URL: http://www.guds.gov.ua/control....d=37402.
5. Віткін Л. Розвиток електронного урядування та СУЯ за моделлю CAF в органах влади ЄС. URL: www.dssu.gov.ua:1080/document/143017/Vitkin.52-59.pdf.
6. Головенко Р., Котляр Д., Нестеренко О., Шевченко Т. Науково-практичний коментар до Закону України «Про доступ до публічної інформації» / За заг. ред. Д. Котляра / Під ред. А. Шевченка / Коорд. проекту В. Самохвалов. К.: ГО «Фундація «Центр суспільних медіа»., 2012. 336 с.
7. Горбата Л.П. Інформаційна відкритість як принцип діяльності органів публічної влади. Інвестиції: практика та досвід. 2018. № 3. С. 125–130. URL: http://www.investplan.com.ua/pdf/3_2018/28.pdf.
8. Грабовець І. Тарасова О. Електронне урядування як засіб розвитку демократії. Соціальні технології: актуальні проблеми теорії та практики. 2016. Вип. 69-70. С. 110–117.
9. Даниленко С. Правовий механізм забезпечення інформаційної відкритості та прозорості органів публічної влади. URL: http://www.dridu.dp.ua/vidavnictvo/2012/2012_02(13)/12dsaopv.pdf.
10. Дрешпак В. Розвиток електронного урядування як напрям державної інформаційної політики України: організаційний аспект. Державне управління та місцеве самоврядування. 2012, Вип. 4. С. 78–87. URL: http://nbuv.gov.ua/UJRN/dums_2012_4_12.
11. Забезпечення прозорості та інформаційної відкритості влади. URL: http://sd.net.ua/2012/03/09/zabezpechennya-prozorosti-ta-informacijnoyi.html.
12. Клімушин П., Серенок А. Електронне урядування в інформаційному суспільстві: монографія. Х.: Вид-во ХарРІДУ НАДУ «Магістр», 2010. 312 с.
13. Клюцевський В. Механізми здійснення електронного документообігу в організації діяльності місцевих органів виконавчої влади. Наукові праці. Державне управління. 2012. Випуск 182. Том 194. С. 26–30.
14. Колесніченко І. Розвиток електронного урядування в Україні: інституціональний аспект. Бізнес-Інформ. 2014. № 3. URL: http://business-inform.net.
15. Коліушко Д., Демкова М. Електронне урядування – шлях до ефективності та прозорості державного управління. URL: http://www.isu.org.ua/uploads/publications/20.doc.
16. Надюк З.О. Сучасні проблеми інформатизації державного управління в Україні: публічна політика і «відкритість» інформації; кібербезпека; інформаційне забезпечення і взаємодія територіальних громад. Держава та регіони (серія «Державне управління»). 2017. № 4. С. 244–247.
17. Надюк З.О., Кондаков К.Г. Проблемні аспекти взаємодії органів публічної влади і громадськості в контексті розвитку електронного урядування в Україні. Держава та регіони. (Серія: Державне управління). 2014. № 4. С. 89–91. URL: http://nbuv.gov.ua/UJRN/drdu_2014_4_18.
18. Нестерович В.Ф. Принципи відкритості та прозорості в діяльності органів державної влади

як передумова утвердження демократії участі. Філософські та методологічні проблеми права. 2016. № 2(12). С. 67–77.
19. Про доступ до публічної інформації: Закон України №2939-VI від 13.01.2011 р. Відомості Верховної Ради України. 2011. № 32. Ст. 314.
20. Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII від 05.10.2017 р. Відомості Верховної Ради України від 10.11.2017 р. 2017 р. № 45. С. 42. Ст. 403.
21. Соловйов С.Г., Даниленко В.Г. Проблеми розвитку електронної демократії в умовах модернізації державного управління України: наукова розробка. К.: НАДУ, 2012, 68 с.
22. Семенченко А., Коновал В. Організаційно-правові механізми державного управління розвитком інформаційного суспільства та електронного урядування: проблеми та шляхи розв'язання. Управління сучасним містом. 2012. № 1-4/1-12 (45–48). URL: http://ueuzi.kievcity.gov.ua/files/2014/12/1/konoval_ST_1.pdf.
23. Серенок А., Клімушин П. Електронне урядування в інформаційному суспільстві: [монографія]. Х.: Вид-во ХарРІДУ НАДУ «Магістр», 2010. 312 с.
24. Соловйов С. Концептуальні основи електронної демократії: зарубіжні теорії та впровадження в Україні. Державне управління: удосконалення та розвиток. 2015. № 9. URL: http://www.dy.nayka.com.ua/?op=1&z=885.
25. Стадник Р.І. Відкритість органів влади в контексті законодавства про доступ до публічної інформації // Програма «Відкритість правоохоронної системи» Асоціації українських моніторів дотримання прав людини в діяльності правоохоронних органів. 17.03.2015 р. URL: http://police-access.info/2015/03/vidkrytist-orhaniv-vlady-v-konteksti-zakonodavstva-pro-dostup-do-publichnoji-informatsiji/.

Надюк З. А. Согласование принципов открытости и прозрачности с базовыми требованиями кибербезопасности в деятельности органов публичной власти в Украине

В статье исследуется современное состояние осуществления процесса доступа к публичной информации в Украине. Определены основные проблемы соблюдения принципов открытости и прозрачности в деятельности органов публичной власти. Обоснована необходимость согласования принципов открытости и прозрачности с базовыми требованиями кибербезопасности в деятельности органов публичной власти. Даны рекомендации относительно возможных путей решения этой проблемы в современных условиях государства.

Ключевые слова: *государственные служащие, государственное управление, кибербезопасность, механизм государственного управления, принципы открытости и прозрачности, публичные органы власти, публичная политика.*

Nadiuk Z. O. Crossing the principles of openness and transparency with the basic cybersecurity requirements in the activities of public authorities in Ukraine.

The article deals with the current state of implementation of the process of access to public information in Ukraine. The main problems of adherence to the principles of openness and transparency in the activities of public authorities are outlined. The necessity of harmonizing the principles of openness and transparency with the basic requirements of cybersecurity in the activities of public authorities is substantiated. Recommendations on possible ways of solving this problem in modern conditions of state development are given.

Key words: *civil servants, public administration, cybersecurity, mechanism of public administration, principles of openness and transparency, public authorities, public policy.*