Адміністративно-правові засади захисту інформації в контексті електронного врядування

Крамар Р. І.[1], Бойко Я. А.[2], Черепанич А. М.[3], Пиріг І. В.[4], Голумбівський С. О.[5]

Опубліковано	Секція	УДК
27.01.2023	Економіка	35.078.3

DOI: http://dx.doi.org/10.5281/zenodo.10512210

Ліцензовано за умовами Creative Commons BY 4.0 International license

Анотація. Дана стаття присвячена аналізу актуальних тенденцій стосовно захисту інформації, адміністративно-правових засад дотримання інформаційної безпеки в рамках розвитку електронного врядування в Україні. У статті були досліджені як наявні проблеми та недосконалості нормативно-правового регулювання у сфері захисту інформації, так і досягнення вітчизняних державних органів, котрі не дивляись ні на що продовжують проактивну розбудову взаємодії за системою «держава-громадяни» шляхом імплементації та впровадження покращень до системи електронного врядування. Стаття також присвячена аспектам інформаційної безпеки та прогалинам захисту інформації, новим викликам у сфері інформаційної безпеки в управлінській та адміністративній сферах.

Ключові слова*:* електронне урядування, публічна інформація, інформаційна безпека, адміністративна послуга, електронна послуга, адміністративно-правові заходи.

Administrative and legal principles of information protection in the context of electronic governance

Abstract. Information has always been and remains an important component in achieving the tasks assigned to the state to ensure the full functioning of all institutions of power and state formation. This, in turn, is supported by Art. 17 of the Constitution of Ukraine, in particular, that compliance with information security is the most important element of ensuring the stability and development potential of Ukraine, is the main function of the state and the task of the entire Ukrainian people. Information currently occupies a key place in the creation of such processes as the European integration of Ukraine, improving the population's access to the main state institutions, such as the judicial system, local governance, obtaining legal aid, and also sets the goal of joining the experience of neighboring countries and equalizing the level of informatization in relation to the electoral process (as, for example, in Estonia and Finland). The need to protect and increase the level of information security by legislation and

[1] д.ю.н., професор, ЗВО «Львівський університет бізнесу та права», http://orcid.org/0000-0001-5086-9845
[2] аспірант, ЗВО «Львівський університет бізнесу та права», https://orcid.org/0009-0007-2723-8368
[3] аспірант, ЗВО «Львівський університет бізнесу та права», https://orcid.org/0009-0009-8118-9995
[4] аспірант, ЗВО «Львівський університет бізнесу та права», https://orcid.org/0009-0002-1245-5638
[5] аспірант, ЗВО «Львівський університет бізнесу та права», https://orcid.org/0009-0009-6958-6867

administrative and legal measures in Ukraine should become a cornerstone in the system of all branches of government, and especially where significant development of electronic governance in the form of electronic services is being followed. According to the data of the Government portal of the state authorities of Ukraine, as of 2019, the number of electronic services in Ukraine and their use by citizens had one of the fastest levels of development in the world, and in the course of 2020-2023 the situation had a positive trend, thanks to the approved Action Plan for implementation of the concept of development of the system of electronic services in Ukraine for 2019-2020.

This article is dedicated to analyzing current trends in information protection and the administrative-legal principles of ensuring information security within the development of e-governance in Ukraine. The article explores both existing problems and deficiencies in the regulatory framework for information protection, as well as the achievements of domestic government bodies, which, despite challenges, continue proactive development of interaction within the "state-citizen" system through the implementation and introduction of improvements to the e-governance system. The article also focuses on aspects of information security, information protection gaps, and new challenges in the field of information security in managerial and administrative spheres.

Keywords: electronic government, public information, information security, administrative service, electronic service, administrative and legal measures.

Вступ

*Постановка проблеми***.** Інформація завжди була і залишається вагомою складовою у досягненні покладених на державу завдань щодо забезпечення повноцінного функціонування усіх інститутів влади та державотворення. Це, в свою чергу, підкріплюється ст. 17 Конституції України, зокрема те, що дотримання інформаційної безпеки є найважливішим елементом забезпечення стабільності та потенціалу розвитку України, є основною функцією держави та завданням всього Українського народу [1]. Інформація посідає наразі ключове місце у створенні таких процесів, як євроінтеграція України, покращення доступу населення до основних державних інтитутів, як наприклад судова система, врядування на місцях, отримання правової допомоги, а також ставить за мету доєднатись до досвіду заідних країн та зрівнятись у рівні інформатизації стосовно виборочого процесу (як, наприклад, у Естонії та Фінляндії). Необхідність захисту та підвищення рівней захищеності інформації законодавством та адміністративно-правовими заходами в Україні має стати наріжним каменем у системі усії ланок влади, а в особливості там, де прослідковується значний розвиток електронного врядування у формі електронних послуг. Згідно із даними Урядового порталу органів державної влади України, ще станом на 2019 рік кількість електронних послуг в Україні та їх використання громадянами мала один із найстрімкіших рівнів розвитку у світі, а з плином 2020-2023 років ситуація мала позитивну тенденцію, завдяки затвердженому Плану заходів щодо реалізації концепції розвитку системи електронних послуг в Україні на 2019-2020 роки [2]. Як можна бачити, пріоритетність адміністративно-правового регулювання механізмів захисту інформації в рамках електронного врядування в Україні несе суто утилітарне значення, оскільки без запровадження належних засобів для захисту інформації та інформаційної безпеки в цілому неможливим є сама концепція розвитку е-врядування, котрої притримується Україна у довгстроковій перспективі.

Мета роботи. Дана стаття має на меті аналіз реалій та проблемних питань інформаційної безпеки даних в контексті розвитку та подальшого впровадження концепції електронного врядування в Україні.

*Стан дослідженості тематики***.** Дану та суміжні теми висвітлювали такі вітчизняні науковці, як Бліхар М.М., Ільницький М.П., Олійник О.В., Дзюба С.В., Малашко О.Є., Стародубцев А., Куспляк І.С., Березовська І.Р. але не виключно. Дослідження теми, котра поєднує захист інформації (аспект інформаційної безпеки) та електронне врядування (аспект впровадження інформатизації на рівні державотворення), потребує ретельного ознайомлення із різними науковими думками по суміжним темам, що і було зроблено в рамках даного дослідження.

Результати

Розкриття змісту теми варто почати з визначення термінів, котрі нас цікавлять, а саме «електронне врядування», «інформація (в контексті її правового захисту)» та «інформаційна безпека (в рамках адміністративно-правових засад її забезпечення)». Наприклад, Куспляк І.С. вважає, що електронне урядування – це концептуальний підхід навколо функцій уряду, процес співпраці влади з громадянами за допомогою інформаційно-комунікаційних технологій задля збільшення можливостей для громадян [3]. Із даного визначення слідує, що освновними засадами е-врядування мають виступати принципи гласності, доступу до інформації для громадян, принцип прозорості рішень суб'єктів владних повноважень та принцип всебічної інформатизації владних процесів шляхом впровадження доступних електронних послуг та доступу до владних інститутів для населення.

Поняття інформаційної безпеки розкривається через призму її законодавчого визначення. Так, Рішенням Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки", затвердженого Указом Президента України
від 28 грудня 2021 року № 685/2021, дано визначення інформаційна безпека України, а саме «інформаційна безпека України – складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [4].» Щодо забезпечення інформаційної безпеки засобами адміністративно-правового впливу, то слушної думки у своєму дослідженні дійшов О. В. Олійник. Зокрема, науковець вважає, що застосування методів захисту інформації повинно бути зумволене декількома факторами, серед яких важливість інформації за ступенями її відкритості, реальними та потенційними загрозами для певного виду інформації [5].

Стосовно захисту інформації, то чинним Законом України «Про захист інформації в інформаційно-комунікаційних системах» визначається як «захист інформації від несанкціонованих дій щодо інформації у системі [6].» Тобто, виходячи з даного тлумачення, захист інформації в контексті електронного врядування посідає ключове місце, оскільки без належного захисту інформації всередині відповідних систем, може бути порушена не лише ефективність управління та адміністрування в державі, а й загалом звести на нівець усі здобутки електронного врядування України.

Серед основних недоліків та проблем, котрі виникають у сфері інформаційної бехпеки та захисту інформації, зокрема у царині електронного врядування, можна виділити наступні: ризики пов'язані із захистом особистих даних в системах

електронного врядування, різниця та прогалини між інформатизацією суспільства в цілому та інформатизації державного апарату зокрема, сучасні виклики для додержання інформаційного правопорядку шляхами застосування методів адміністративної відповідальності та примусу. Згідно із дослідженнями О. Хитри та Л. Чистоклетова, наразі існують досить значні прогалини у механізмі адміністративно-правового забезпечення прав та свобод суб'єктів у сфері інформаційного права, що в свою чергу створює перешкоди для подальшого захисту інформації засобами правоохоронної та правозастосовчої діяльності, а також виявлення та превенції несанкціонованих дій відносно інформації, що міститься у системах електронного врядування [7].

Також, не зайвим буде зазначити, що до системи захисту інформації у сфері електронного врядування належать наступні складові: нормативно-правові акти (Конституція України, закони та підзаконні правові акти, що стосуються інформаційної безпеки та захисту інформації); діяльність державних органів, до компетенції котрих належать повноваження із забезпечення захисту інформації (РНБО, Держспецзв'язку, правоохоронні органи в межах компетенцій); діяльність користувача електронного врядування, наприклад, державних електронних послуг, оскільки сам суб'єкт може вживати активних дій задля захисту інформації та попередження несанкціонованого доступу третіх осіб до неї [8].

З іншого боку, нормативно-правові акти України, котрі регламентують та забезпечують захист інформації та інформаційну безпеку, не в повній мірі відповідають викликам часу. В першу чергу, це помітно внаслідок стрімкого розвитку інформаційних технологій, зокрема у царині електронного врядування, загальної інформатизації суспільства. Наразі такі нормативно-правові акти, як то Закони України «Про захист персональних даних», «Про захист інформації в інформаційно-телекомунікаційних системах» та «Про інформацію», не можуть всебічно регулювати відносини, що можуть виникнути з плином часу у цій сфері [8].

Після проведеного аналізу багатьма науковцями складається висновок, що законодавча на нормативно-правова база поки що не має у своєму арсеналі термінологічної визначеності, повної послідовності та однозначності. З огляду на існуючий запит на покращення стану інформаційної безпеки законодавцям та органам державної влади необхідно докласти певних зусиль для розширення вже існуючих адміністративно-правових засобів та засад для захисту інформації. Для цього конче необхідно зайнятись чітким визначенням понятійного апарату, уточнити напрями реалізації державної інформаційної політики [8], в тому числі в рамках електронного врядування, адже саме е-врядування є таким собі «дзеркалом», що відображає актуальний стан інформаційної політики у державі. Електронне врядування в майбутньому повинно краще бути підготоване до існуючих ризиків, пов'язаних із добре відомими прогалинами в системі інформаційної безпеки, такими як «витік даних ("data breach"), несанкціонований доступ до персональних даних, кібернетичними загрозами хакерського характеру, використання інформації в цілях незаконного збагачення, але не виключно.

При цьому, адміністративно-правові засади та засоби реагування на виклики інформаційної безпеки повинні бути перероблені на превентивне реагування та вирішення не «симптомів», а ключових питань захисту інформації. Іншими словами, зміна пріоритетності з реакції пост фактум (коли фактично загроза інформації реально настала разом із негативними наслідками) на реакцію попередження та недопущення можливих порушень [8]. Наприклад, в контексті електронного врядування, подібні пробеми можуть викликати порушення основоположних прав та свобод суб'єктів інформаційного суспільства, призведе до нарощення недовіри населення до використання державних електронних послуг та до інформації адміністративного чи

управлінського характеру, котра поширюватиметься суб'єктами владних повноважень на офіційних джерелах. Так само, потенційною загрозою для подальшого розвитку адміністрування електронного врядування є порушення зв'язку та взаємодії «держава-соціум», котрий прямо виник в результаті запровадження певних елементів електронного врядування в Україні.

В подоланні потенційних проблем захисту інформації суб'єктам інформаційного суспільства мають допомагати державні органи та їх посадові особи, котрі наділені всіма правами, необхідними для якісного виконання покладених на них обов'язків із адміністративно-правового забезпечення інформаційної безпеки в Україні. До таких державних органів відносяться: 1) Міністерство цифрової трансформації України, основним завданням якого є діджиталізація країни, в тому числі і розвиток сфери електронного врядування; 2) правоохоронні органи, такі як СБУ, МВС, зокрема їхні підрозділи кіберполіції, діяльність котрих спрямована на реалізацію державної політики у сфері протидії кіберзлочинності та захисту інформації від незаконного втручання та порущення її цілісності або режиму доступу до неї [8].

Висновки

В результаті проведеного дослідження, автор помітив не лише приділену увагу проблемам, котрі наразі обмежують захист інформації, а й дієві методи кооперування в рамках взаємодії державних органів, котрі впроваджують адміністративно-правові засади захисту інформації та суб'єктів електронного врядування, користувачів дежавних послуг та реципієнтів інформації, розміщеної на офіційних онлайн джерелах органів державної влади. До основних елементів подібної кооперації науковці відносять правозастосовну діяльність органів державної виконавчої влади із забезпечення інформаційної безпеки, діяльність органів влади, завданням котрих є пряме забезпечення захисту інформації та формування інформаційної політики, органи, що забезпечують ресурсні функції захисту інформації [9]. Електронне врядування у свій цій системі має першочерговий пріоритет до захисту інформації всередині своєї системи, адже з плином часу додаються і нові електронні послуги, котрі полегшують взаємодію держави та громадян на інформаційному рівні, і нова інформація до відома громадян, а у майбутньому, на зразок західних країн, імовірно з'являться кібернетичні аналоги цілих державних інститутів, як то електронний виборчий процес.

Список використаних джерел

1. Конституція України : (з офіц. тлумаченням Конституц. Суду України). Київ : Ліра, 2006. 96 с.
2. Е-урядування – ключ до реформ в Україні. *Урядовий портал.* URL: https://www.kmu.gov.ua/news/e-uryaduvannya-klyuch-do-reform-v-ukrayini (дата звернення: 02.01.2024)
3. Куспляк І. С. Електронне урядування як інструмент формування прозорої та відкритої політичної влади : автореф. дис. ... канд. політ. наук : 23.00.02. Одеса, 2012. 17 с.
4. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки" : Указ Президента України від 28.12.2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 02.01.2024).
5. Олійник О. В. Методологічні засади забезпечення системи інформаційної безпеки та її складової – захисту інформаційних ресурсів. *Право і безпека.* 2014. № 1 (52). С. 103–109.

6. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 №80/94-ВР : станом на 01.12.2022 р. URL: https://ips.ligazakon.net/document/Z008000?an=4708 (дата звернення: 02.01.2024)
7. Чистоклетов Л. Г., Хитра О. Л. Адміністративно-правові засоби у забезпеченні інформаційної безпеки Україні. ІТ-право: проблеми та перспективи розвитку в Україні : зб. матеріалів ІІ-ї міжнар. наук.-практ. конф., Львів, 2017. С. 212–217. URL: http://aphd.ua/publication-349/ (дата звернення: 02.01.2024).
8. Грубінко А. Інформаційна безпека України : правове гарантування та реалії забезпечення. *Актуальні проблеми правознавства.* 2019. No 1 (17). С. 5–10.
9. Кунєв Ю. Д., Легеза Є. О. Правове забезпечення інформаційної безпеки як предмет адміністративно-правового дослідження. *Наукові праці Національного авіаційного університету*. *Серія «Юридичний вісник».* 2021. Т. 1 (58). С. 183–185.