ІНФОРМАЦІЙНА БЕЗПЕКА В СУЧАСНОМУ СВІТІ ТА ЇЇ ВПЛИВ НА КОНСТИТУЦІЙНИЙ ЛАД В УКРАЇНІ: ТЕОРІЯ Й ПРАКТИКА: ЕЛЕКТРОННЕ ВИДАННЯ МАТЕРІАЛІВ ВСЕУКРАЇНСЬКОЇ КОНФЕРЕНЦІЇ 20 ЧЕРВНЯ 2019 РОКУ

м. Івано – Франківськ, 2019

УДК 342.(081)
Р43

Р 48 **Інформаційна безпека в сучасному світі та її вплив на конституційний лад в Україні: теорія й практика** : матеріали всеукраїнської конференції (м. Івано-Франківськ, 20 червня 2019 року) / упорядник В. І. Розвадовський. Івано-Франківськ : ДВНЗ «Прикарпатський національний університет імені Василя Стефаника», 2019.116 с.

В цьому збірнику вміщені матеріали наукових доповідей, повідомлень та інформацій, представлених на всеукраїнські конференції, організованій кафедрою конституційного, міжнародного та адміністративного права навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника» і проведеному в Івано-Франківську 20 червня 2019 року.

Для державних та муніципальних службовців, науковців, аспірантів та студентів вищих навчальних закладів, усі хто цікавиться проблемами інформаційної безпеки у сучасному світі.

УДК 342.(081)

Електронне видання
ISBN-978-966-640-456-8

ЗМІСТ

ВСТУПНЕ СЛОВО……... **8**

ВІД ОРГАНІЗАТОРІВ……. **10**

НАПРЯМОК І. ТЕОРЕТИКО-ПРАКТИЧНІ ПІДХОДИ ДО ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ В УКРАЇНІ ТА СВІТІ

1. Албу Андрій Аркадійович, викладач кафедри конституційного, міжнародного та адміністративного права навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника», кандидат юридичних наук.
«Особливості створення та використання електронного цифрового підпису»…….. **12**

2. Дерев'янко Сергій Миронович, професор кафедри політичних інститутів та процесів факультету історії, політології і міжнародних відносин ДВНЗ «Прикарпатський національний університет імені Василя Стефаника», заслужений працівник освіти України, доктор політичних наук.
«Конституційне право громадян на інформацію: політико-правові особливості реалізації в умовах гібридної війни»…… **16**

3. Книш Віталій Васильович, професор кафедри конституційного, міжнародного та адміністративного права навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника», доктор юридичних наук, доцент.
«Місце інформаційної безпеки в системі національної безпеки»……. **27**

4. Зінич Любомир Васильович, викладач кафедри конституційного, міжнародного та адміністративного права навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника», кандидат юридичних наук.
«Правові засади взаємодії громадянського суспільства та держави у забезпеченні інформаційної безпеки»…… **32**

5. Петровська Ірина Ігорівна, доцент кафедри конституційного, міжнародного та адміністративного права навчально-наукового

юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника», кандидат юридичних наук, доцент.
Поварчук Роман Ігорович, студент 2 курсу магістратури, спеціалізація 01 «Публічна служба», навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника».
«Особливості використання інформації з обмеженим доступом при здійсненні контрольного провадження» …..... **37**

НАПРЯМОК ІІ. ІНФОРМАЦІЙНА БЕЗПЕКА ТА КОНСТИТУЦІЙНИЙ ЛАД УКРАЇНИ В ПРОЦЕСІ ІМПЛЕМЕНТАЦІЇ ЄВРОПЕЙСЬКОГО ЗАКОНОДАВСТВА

6. Петровська Ірина Ігорівна, доцент кафедри конституційного, міжнародного та адміністративного права навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника», кандидат юридичних наук, доцент.
«Особливості забезпечення інформаційної безпеки у сучасному суспільстві: Україна та ЄС»…… **40**

7. Збирак Тетяна Вікторівна, викладач кафедри конституційного, міжнародного та адміністративного права навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника», кандидат юридичних наук.
«Інформаційна безпека в Україні: деякі аспекти її забезпечення при реалізації права на свободу слова»…… **45**

8. Войтович Романа Ярославівна, студентка 1 курсу групи ПР-14 навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника» (наук. керівник: викл. Федорончук А.В.).
«Інформаційна безпека: підходи до визначення понять»…… **49**

НАПРЯМОК ІІІ. ІНФОРМАЦІЙНІ ВІДНОСИНИ В

СУЧАСНОМУ СУСПІЛЬСТВІ ТА ЇХ ВПЛИВ НА ПУБЛІЧНЕ УПРАВЛІННЯ ДЕРЖАВИ

9. Федорончук Андрій Володимирович, викладач кафедри конституційного, міжнародного та адміністративного права навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника», кандидат юридичних наук.
«Окремі аспекти діяльності Міністерства інформаційної політики України щодо гарантування інформаційної безпеки держави»……..... **54**

10. Янцаловська Віталіна Олександрівна, приватний нотаріус Деражнянського районного нотаріального округу Хмельницької області.
«Кібербезпека та захист інформації в сфері нотаріату»…….. **61**

11. Бойцан Любомир Іванович, студент 2 курсу магістратури, спеціалізація 01 «Публічна служба» навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника» (наук. керівник: доц. Петровська І.І.).
«Правовий режим інформації про корупційні правопорушення»……. **63**

12. Михаць Олег Володимирович, студент 4 курсу групи ПР-42 навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника» (наук. керівник: доц. Петровська І.І.).
«Застосування інформаційних технологій при наданні адміністративних послуг»…… **66**

13. Московчук Ірина Ярославівна, студентка 1 курсу групи ПР-15 навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника» (наук. керівник (наук. керівник: Федорончук А.В.).
«Окремі питання інформаційної безпеки України»…….. **74**

14. Дирда Діана Володимирівна, студентка 2 курсу магістратури, спеціалізація 01 «Публічна служба» навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний

університет імені Василя Стефаника» (наук. керівник: доц. Петровська І.І.).
«Поняття та види публічної служби в Україні…… **78**

15. Капустяк Ірина Ігорівна, студентка 2 курсу магістратури, спеціалізація 01 «Публічна служба» навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника» (наук. керівник: доц. Петровська І.І.).
«Банківська таємниця: поняття та особливості правового забезпечення»…… **84**

16. Петрованчук Галина Романівна, студентка 2 курсу магістратури, спеціалізація 01 «Публічна служба» навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника» (наук. керівник: викл. Зінич Л.В.).
«Інтелектуальна власність як об'єкт адміністративно-правового регулювання»…… **88**

НАПРЯМОК IV. КОНСТИТУЦІЙНА ЮСТИЦІЯ ТА ЇЇ РОЛЬ ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СУЧАСНОМУ СУСПІЛЬСТВІ

17. Розвадовський Володимир Іванович, завідувач кафедри конституційного, міжнародного та адміністративного права навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника», кандидат юридичних наук, доцент.
«Проблеми урегулювання доступу до публічної інформації: теорія і практика»…… **92**

18. Костенко Світлана Олексіївна, доцент кафедри правознавства Житомирського національного агроекологічного університету, кандидат юридичних наук.
«Роль Конституційного Суду України в забезпеченні інформаційної безпеки в Україні»…… **99**

19. Бабак Віталій Михайлович, студент 4 курсу групи ПР-41 навчально-наукового юридичного інституту (наук. керівник: доц.

Розвадовський В.І.).
«Інформаційна безпека України в умовах євроінтеграції»……..... **103**

20. Панкевич Іван Миронович, доцент кафедри конституційного права Львівського юридичного інституту імені Івана Франка, доктор юридичних наук.
«Про основні засади розвитку інформаційного суспільства в Україні після революції гідності»…… **108**

РЕКОМЕНДАЦІЇ УЧАСНИКІВ КОНФЕРЕНЦІЇ ……..…….. **112**

ВСТУПНЕ СЛОВО

Сучасний період розвитку інформаційної сфери характеризується якісно новим підходом до збирання, зберігання та обробки інформації. Поява нових засобів поширення інформації дозволяє не тільки задовольнити інформаційні потреби громадян, а й створює небезпеку для національного інформаційного простору. Підтвердженням цього є наявний стан інформаційної безпеки України, який характеризується втратою впливу на інформаційні процеси, відсутністю національного інформаційного виробництва. Протистояння загрозам, що існують в сучасному світі вимагають від держав дієвого механізму протидії та забезпечення інформаційних прав і свобод людини. Важливим засобом захисту національних інтересів у інформаційній сфері, повинно стати ефективна інформаційна політика

Зростає потреба у засобах структурування, накопичення, зберігання, пошуку та передачі інформації – задоволення саме цих потреб і є метою суб'єктів інформаційної діяльності. Саме тому надзвичайної актуальності набувають проблеми регулювання інформаційної сфери, створення відповідних умов для випередження розвитку вітчизняного інформаційного виробництва. Провідним інструментом реалізації національних інтересів у такій галузі суспільних відносин, як інформаційна сфера, повинно стати право.

Проблемність розвитку інформаційної безпеки пов'язана з тим, що Україна за час незалежності не присвячувала належної уваги питанням інформаційної політики, концепції розвитку правового регулювання інформаційної безпеки та відсутністю розвинутих структур громадянського суспільства. Переломним моментом в усвідомленні і визнанні цінності інформаційної безпеки стала Революція Гідності. Сама ідея інформаційної безпеки держави та суспільства на той момент вступала в суперечність з державним управлінням, інститутом свободи слова, незалежністю ЗМІ.

Проблемні питання в інформаційній сфері привертають значну увагу науковців досить тривалий час, тому проведення наукового заходу кафедрою конституційного, міжнародного та адміністративного права «Інформаційна безпека в сучасному світі та її вплив на конституційний лад: теорія і практика» є сьогодні надзвичайно актуальним.

Саме такі заходи, дають змогу правникам поділитися досвідом, взаємно збагатити знання і визначити тенденції розвитку юридичної науки, обговорити проблемні питання в інформаційній сфері, теоретично-правові аспекти інформаційної діяльності, вплив інформаційної безпеки на публічне управління. Участь молодих дослідників дозволить віднайти оригінальні рішення завдань, які ставить перед собою наука. Висловлюємо сподівання, що представленні напрацювання знайдуть відображення не тільки у науці, але й на практиці.

Сподіваємося, що плідна робота конференції залишить тільки позитивні враження та дасть поштовх для нових наукових досліджень.

Васильєва В. А. *директор навчально - наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника», Заслужений юрист України, доктор юридичних наук, професор.*

ВІД ОРГАНІЗАТОРІВ

Колективом вчених кафедри конституційного, міжнародного та адміністративного права навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника» було запропоновано провести всеукраїнську конференцію на тему: «Інформаційна безпека в сучасному світі та її вплив на конституційний лад в Україні: теорія і практика». Такий захід відбувся 20 червня 2019 року на базі навчально-наукового юридичного інституту та за участю Житомирського національного агроекологічного університету, нотаріусів, представників Івано-Франківської обласної ради.

Метою конференції є обмін науковими поглядами та ідеями з приводу інформаційної безпеки, обговорення наукових проблем, студенти мають можливість опанувати практичні навички у сфері наукової діяльності та ін..

Інформаційна безпека в XXI столітті виходить на перше місце в системі національної безпеки держави, тому лише та держава може розраховувати на лідерство в економічній, військово-політичній та інших сферах, мати стратегічну і тактичну перевагу, гнучкіше регулювати економічні витрати на розвиток озброєнь і військової техніки, підтримувати перевагу з ряду передових технологій, яка має перевагу в засобах інформації та інформаційної боротьби.

Інформаційна безпека є невід'ємним напрямом розбудови інформаційного суспільства, розвиток якого повинен відбуватись не тільки через нарощування технологічних можливостей здійснення інформаційного обміну, але й через глибоке усвідомлення усіма суб'єктами інформаційних відносин – власниками інформації та її користувачами, виробниками інформаційних технологій і засобів, постачальниками послуг, державою – необхідності здійснення всіх заходів щодо інформаційних ресурсів та забезпечення інформаційної безпеки держави.

Отже, інформаційна безпека є однією із складових стійкого розвитку всієї держави, а процес забезпечення інформаційної безпеки необхідно розуміти як: «…одне з глобальних і пріоритетних завдань органів державного управління, вирішенню якого мають бути підпорядковані політична, економічна, воєнна, культурна та інші види діяльності системи державного управління».

За таких обставин було вирішено опублікувати матеріали всеукраїнської конференції, оскільки в них знайшли обґрунтування шляхи підвищення інформаційної безпеки, удосконалення існуючих

юридичних механізмів закріплення та реалізацій інформаційних прав і свобод.

Вважаємо за доцільне висловити щиру подяку ректорату ДВНЗ «Прикарпатський національний університет ім.В.Стефаника», особисто професору Цепенді І.Є., директору навчально-наукового юридичного інституту, професору Васильєвій В.А. – за сприяння і допомогу в організації та проведеннівсеукраїнської конференції: «Інформаційна безпека та її вплив на конституційний лад в Україні: теорія і практика».

***Розвадовський В.І**., завідувач кафедри конституційного, міжнародного та адміністративного права навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет ім.В.Стефаника», кандидат юридичних наук, доцент, модератор конференції.*

НАПРЯМОК І. ТЕОРЕТИКО-ПРАКТИЧНІ ПІДХОДИ ДО ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ В УКРАЇНІ ТА СВІТІ

Албу Андрій Аркадійович
Викладач кафедри конституційного, міжнародного та адміністративного права навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника»,
кандидат юридичних наук.

ОСОБЛИВОСТІ СТВОРЕННЯ ТА ВИКОРИСТАННЯ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

Розвиток і впровадження практично у всі сфери діяльності інформаційних технологій суттєво змінює структуру суспільства, а також трансформує міжнародні відносини. В умовах сьогодення з урахуванням розвитку економіки та науково-технічного прогресу кожне підприємство тією чи іншою мірою використовує сучасну техніку та технології для активізації бізнес-процесів та комунікації з контрагентами, обслуговуючими організаціями, контролюючими органами та потенційними споживачами тощо. Обмін електронними даними прискорює рух інформації як всередині підприємства, так і з зовнішнім середовищем, сприяє поліпшенню процесів управління та контролю. Він виключає викривлення інформації сторонніми особами та помилки, що трапляються під час оброблення паперових документів, сприяє підвищенню ефективності та якості ділових стосунків, а також дає змогу позбутися великої кількості паперових документів. Безумовною перевагою електронного обміну даними є те, що дані, які передаються, не залежать від особливостей програмного та апаратного забезпечення, яким володіють партнери, адже інформація проходить шифрування засобами численних стандартизованих довідників та кодів, після чого передається у структурованому вигляді.

В умовах обміну електронними даними між контрагентами великого значення набуває захищення інформації від стороннього

втручання та викривлення, а також надання інформації юридичної сили. Інструментом, що дає змогу створити правові основи для електронного обміну даними (зокрема, в мережі Інтернет), є електронний цифровий підпис. Юридична сила електронного документа, підписаного електронним цифровим підписом, еквівалентна юридичній силі паперового документа з власноручним підписом правоздатної особи та печаткою. Тому в сучасних умовах підприємства зацікавлені у придбанні електронних цифрових підписів з метою організації електронного документообігу. В таких умовах актуальним завданням в Україні є розвиток інфраструктури електронного документообігу.

Метою роботи є визначення сутності електронного цифрового підпису як елементу інформаційної безпеки та особливостей його облікового відображення й оподаткування в інформаційній системі підприємства.

В науковій літературі є багато праць вітчизняних та закордонних вчених, присвячених питанням походження електронного цифрового підпису та його використання. Серед закордонних вчених, які вивчали застосування електронних цифрових підписів, варто відзначити таких, як Ю.М. Батуріна, І.Л. Бачило, Г.Г. Абрамкін, Ю. Хаяші. Серед вітчизняних дослідників, які займалися вивченням питань сутності електронного цифрового підпису, слід згадати таких вчених, як В.І. Волинець, А.А. Гринович, Ю.І. Горбенко, М.Р Макарова. Правовим питанням використання електронного цифрового підпису присвячені праці А.О. Борисенко, Н.Б. Новицької, В.Б. Чередниченко, Т.А. Чернової та інших науковців. Питанням захисту інформації з використанням електронного цифрового підпису присвятили свої праці А.О. Азарова, А.Д. Кожухівський, О.Б. Кукарін, В.А. Лужецький, О.М. Роїк, А.В. Сагун та інші вчені.

Законодавство України дає змогу використовувати електронний цифровий підпис під час пересилання документів для забезпечення електронного документообігу. Правові основи створення та використання електронних документів і електронного документообігу визначаються Законом України «Про електронні документи та електронний документообіг» [1]. Розділ 2 Закону України «Про електронні документи та електронний документообіг» присвячено

[1] Про електронні документи та електронний документообіг: Закон України від 22 травня 2003 року № 851-IV. Сайт Верхов-ної Ради України. URL: http://zakon0.rada.gov.ua/laws/show/851-15.

електронному документу, але він не має чітких правових норм щодо його складу та структури, а також порядку розміщення обов'язкових реквізитів. У цьому ж розділі зазначено, що створення електронного документа завершується накладанням електронного цифрового підпису.

Правові основи застосування електронного цифрового підпису визначаються Законом України «Про електронний цифровий підпис»[2], який пояснює його призначення та особливості застосування, правовий статус електронного цифрового підпису, права та обов'язки підписанта, а також надає інформацію про вимоги до сертифікату та акредитовані центри сертифікації електронних ключів, роз'яснює відповідальність за порушення законодавства про електронний цифровий підпис.

Крім того, варто зазначити, що Інформаційно-довідковий департамент Державної фіскальної служби України у загальнодоступному інформаційно-довідковому ресурсі постійно розміщує відповіді на запитання про отримання, внесення змін, блокування електронних цифрових підписів, а також податковий облік операцій з придбання електронних цифрових підписів[3]. Однак податкові консультації містять спірні питання обліку електронних цифрових підписів відповідно до міжнародних стандартів бухгалтерського обліку.

В Україні правові основи використання електронного цифрового підпису встановлено у 2003 році з прийняттям Закону України «Про електронний цифровий підпис» та Закону України «Про електронні документи та електронний документообіг».

Відповідно до ст. 1 Закону України «Про електронний цифровий підпис» електронний цифровий підпис - це вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується, а також дає змогу підтвердити його цілісність та ідентифікувати підписувача. Він є самостійним аналогом власноручного підпису правоздатної особи поряд з аналогом,

---

[2] Про електронний цифровий підпис: Закон України від 22 травня 2003 року № 852-IV. Сайт Верховної Ради України. URL: http://zakon5.rada.gov.ua/laws/-show/852-15.

[3] Інформаційно-довідковий департамент Державної фіскальної служби України. Загальнодоступний інформаційно-довід-ковий ресурс. URL: http://zir.sfs.gov.ua/main/bz/view/?src=ques.

отриманим в результаті факсимільного відтворення підпису за допомогою засобів механічного або іншого копіювання.

Безумовною перевагою використання електронного цифрового підпису є те, що він поєднує всі реквізити електронного документа в єдине ціле і робить неможливою зміну будь-якого реквізиту документа без порушення оригінальності цифрового підпису правоздатної особи.

Алгоритм генерації електронного цифрового підпису здійснюється таким чином: на першому кроці визначається хеш-функція (контрольна сума невеликого фіксованого розміру) електронного документа, яка ідентифікує його зміст; на другому кроці хеш-функція шифрується особистим ключем електронного цифрового підпису та в зашифрованому вигляді додається до даних електронного документа[4].

Алгоритм перевірки даних та підпису здійснюється таким чином: на першому кроці визначається хеш-функція отриманого електронного документа (даних електронного документа без даних електронного цифрового підпису); на другому кроці здійснюється розшифрування зашифрованої хеш-функції, яка міститься в отриманому електронному документі, за допомогою відкритого ключа електронного цифрового підпису; на третьому кроці здійснюється порівняння хеш-функцій, визначених на попередніх кроках. Їх збіг підтверджує справжність змісту документа та його авторство[5].

Після придбання електронного цифрового підпису на підприємстві постає питання їх обліку. Основою для розрахунку податку на прибуток є прибуток, розрахований за правилами бухгалтерського обліку (ст. 134 Податкового кодексу України) [5][6]. Але якщо річний дохід підприємства більше 20 млн. грн., то

---

[4] Електронний цифровий підпис (ЕЦП) - як отримати електронний підпис за 6 кроків: інструкція для новачків + огляд ТОП-3 засвідчувальних центрів для отримання ЕЦП. URL: http://bigenergy.com.ua/fnansi/bznes-dlya-pdpri/948-elektronnij- pidpis-ecp-otrimati-elektronnij-cifrovij-pidpis.html.

[5] Волинець В.І. Електронний цифровий підпис: сутність, принципи дії та порядок отримання. URL: http://dspace.tneu.edu.ua/ bitstream/316497/23292/1/111-112.pdf.

[6] Податковий кодекс України від 2 грудня 2010 року № 2755-VI. Сайт Верховної Ради України. URL: http://zakon5.rada.gov.ua/ laws/show/2755-17/page.

підприємство має застосовувати податкові різниці відповідно до ст. 138 Податкового кодексу України. З одного боку, амортизаційні витрати за електронний цифровий підпис відносять до податкових різниць, а з іншого боку, ні, оскільки строк амортизації нематеріального активу 6 групи встановлюється відповідно до правовстановлюючого документа, а отже, збігається з бухгалтерським (за умови, що в бухгалтерському обліку електронний цифровий підпис є нематеріальним активом або обліковується у складі витрат майбутніх періодів).

Отже, дослідження сутності та практичного використання електронних цифрових підписів довело, що електронний цифровий підпис спрямований на спрощення та прискорення документообігу між суб'єктами господарювання, що має зміцнити конкурентоспроможність вітчизняних підприємств, адже пришвидшиться процедура укладення цивільно-правових та господарських договорів, оформлення експортно-імпортних операцій, надання електронних банківських послуг, обміну документів між контрагентами. Схема використання електронного цифрового підпису доводить простоту його використання та підвищення достовірності даних. Крім того, доведено що використання електронного цифрового підпису підвищує інформаційну безпеку як всередині підприємства, так і в умовах передачі електронних даних інформаційними каналами зв'язку. Крім того, електронний цифровий підпис вирішує питання відповідальності за складення та затвердження електронних документів, адже після його накладання відповідальність правоздатної особи очевидна.

Дерев'янко Сергій Миронович
професор кафедри політичних інститутів та процесів факультету історії, політології і міжнародних відносин ДВНЗ «Прикарпатський національний університет імені Василя Стефаника»,
Заслужений працівник освіти України, доктор політичних наук.

КОНСТИТУЦІЙНЕ ПРАВО ГРОМАДЯН НА ІНФОРМАЦІЮ: ПОЛІТИКО-ПРАВОВІ ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Перспективи повноцінного входження України до європейського простору безпосередньо пов'язані зі становленням інформаційного суспільства. Це актуалізує потребу ширшого забезпечення права громадян на свободу думки і слова. Для його реалізації за Конституцією України «кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір» (частина друга статті 34). Показово, що це формулювання в істотному збігається із положеннями «Загальної декларації прав людини» (прийнята Генеральною Асамблеєю ООН 10 грудня 1948 року) «Кожна людина має право на свободу переконань і на вільне їх виявлення; це право включає свободу безперешкодно дотримуватися своїх переконань та свободу шукати, одержувати і поширювати інформацію та ідеї будь-якими засобами і незалежно від державних кордонів» – стверджується у статті 19 цього акту[7]. Порівняльний аналіз обох документів дає підстави стверджувати про прагнення українських законотворців імплементувати апробовані загальноприйняті міжнародно-правові норми й розширити їх розуміння в новітніх умовах.

Конституція України не тільки декларує права громадян, але й визначає конкретний механізм їх реалізації, встановлює вичерпний перелік підстав обмеження. Це норми Конституції України, що містять пряму заборону щодо втручання в особисте і сімейне життя громадян, у зв'язку з чим «не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини» (частина друга статті 32). Частиною третьою цієї ж статті кожному громадянину надано «право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею». Основний Закон гарантує кожному «судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації» (частина четверта статті 32). Крім того, конституєдавець

[7] Загальна декларація прав людини: Прийнята і проголошена Генеральною Асамблеєю ООН 10.12.1948 р. (Док. ООН/PES/217 A). URL: http://zakon.rada.gov.ua/laws/show/995_015.

гарантує кожному громадянину й право «вільного доступу до інформації про стан довкілля, про якість харчових продуктів і предметів побуту, а також право на її поширення. Така інформація ніким не може бути засекречена» (частина друга статті 50).

Загалом названі конституційні норми, що конкретизовані у низці інших законів України та численних підзаконних нормативно-правових актах, набули офіційного тлумачення в окремих рішеннях Конституційного Суду України, створюють надійну основу для реалізації та дієвої охорони конституційного права громадян на інформацію.

Однак, у новітніх геополітичних та суспільно-політичних реаліях існує реальна пряма загроза інформаційній безпеці Української держави та її громадян. Широкий перелік цих загроз містив Закон України «Про основи національної безпеки України» від 19.06.2003 р. № 964-IV. У статті 7 (із змінами, внесеними згідно із Законом № 1170-VII від 27.03.2014 р.) такими загрозами національним інтересам і національній безпеці України в інформаційній сфері названі: «прояви обмеження свободи слова та доступу до публічної інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп`ютерна злочинність та комп`ютерний тероризм; розголошення інформації, яка становить державну таємницю, або іншої інформації з обмеженим доступом, спрямованої на задоволення потреб і забезпечення захисту національних інтересів суспільства і держави; намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації» [8].

Попри те, що, вважаємо, названі загрози не зникли, виникають й нові, їх переліку не знаходимо у новому Законі України «Про національну безпеку України» за № 2469-VIII від 21 вересня 2018 року [9]. Пояснюється це очевидно тим, що чинний нині Закон прийнятий в умовах збройної агресії проти нашої держави. Російська загроза, що має довгостроковий характер, інші докорінні зміни у зовнішньому та внутрішньому безпековому середовищі України обумовили

---

[8] Про основи національної безпеки України : Закон України від 19.06.2003 р. № 964-IV. *ВВ*. 2003. № 39. Ст. 351. . URL: https://zakon.rada.gov. ua/laws/show/ 964-15.

[9] Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII**.** *ВВР*. 2018. № 31. Ст. 241. URL: https://zakon.rada.gov.ua/laws/show/ 2469-19.

необхідність створення нової системи забезпечення національної безпеки України. Війна, яку такою не визнають ні очільники України, ні Росії та й європейських країн, означена науковцями та політиками поняттям «гібридна війна». Серед її вимірів виокремимо – інформаційний, який несе істотну загрозу національній безпеці та й конституційному ладу України.

Вихідним є розуміння гібридної війни як політико-правового феномена. Науковці шукають його витоки у глибокій давнині та у різних цивілізаціях, аналізують причини виникнення, принципи і особливості ведення, прогнозують формат завершення та наслідки. Запропоновано чимало більш чи менш об'ємних і змістовних визначень, однак поза актуальністю та частотою вживання кожного – єдиного розуміння не вироблено. Не вдаючись до дискусії щодо їх сутності, використаємо сформульоване у монографії «Світова гібридна війна: український фронт», під якою розуміють «воєнні дії, що здійснюють шляхом поєднання мілітарних, квазімілітарних, дипломатичних, інформаційних, економічних та інших засобів з метою досягнення стратегічних політичних цілей» [10].

Натомість, у чинному законодавстві України поняття «гібридна війна» не вживається взагалі. Проте, певною мірою можна використати наведене у тексті нової редакції «Воєнної доктрини України»[11] означення однієї із головних тенденцій, яка впливає на формування та розвиток безпекового середовища у світі, а саме «перенесення ваги у воєнних конфліктах на асиметричне застосування воєнної сили не передбаченими законом збройними формуваннями, зміщення акцентів у веденні воєнних конфліктів на комплексне використання воєнних і невоєнних інструментів (економічних, політичних, інформаційно-психологічних тощо), що принципово змінює характер збройної боротьби» (пункт 6).

---

[10] Світова гібридна війна: український фронт : монографія / за заг. ред. В. П. Горбуліна. Національний інститут стратегічних досліджень. Київ : НІСД, 2017. С.19.

[11] Воєнна доктрина України : Затверджена Указом Президента України "Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року "Про нову редакцію Воєнної доктрини України" від 24.09.2015 р. № 555/2015. *Офіційний вісник Президента України*: офіц. вид. від 05.10.2015. № 22. С. 19, Ст. 1291. URL: https://zakon.rada.gov.ua/laws/show/555/2015.

Зауважимо, що близьке за змістом визначення характерних рис і особливостей сучасних військових конфліктів виписано й у «Воєнній доктрині Російської Федерації». Першою з них названо «комплексне застосування воєнної сили, політичних, економічних, інформаційних та інших заходів невійськового характеру, які реалізуються з широким використанням протестного потенціалу населення і сил спеціальних операцій»[12].

Із сукупності застосовуваних дій акцентуємо на інформаційних. «Інформаційна війна Російської Федерації проти України» визначена у «Воєнній доктрині України» серед «головних тенденцій, що впливають на воєнно-політичну обстановку в регіоні довкола України». Далі по тексту документу конкретизуються сутність і особливості ведення такої війни, визначаються заходи щодо протидії її виявам.

Зокрема, у пункті 10 серед воєнно-політичних викликів, які можуть перерости в загрозу застосування воєнної сили проти України виокремлено «цілеспрямований інформаційний (інформаційно-психологічний) вплив з використанням сучасних інформаційних технологій, спрямований на формування негативного міжнародного іміджу України, а також на дестабілізацію внутрішньої соціально-політичної обстановки, загострення міжетнічних та міжконфесійних відносин в Україні або її окремих регіонах і місцях компактного проживання національних меншин».

Доктрина містить перелік ймовірних сценаріїв, які можуть бути реалізовані, й серед них, другим у пункті 11 – «окрема спеціальна операція Російської Федерації проти України із застосуванням військових підрозділів та/або частин, вогневих ударів, інформаційних, інформаційно-психологічних операцій (дій) у сукупності з використанням невоєнних заходів, у тому числі миротворчих сил за відсутності відповідного рішення Ради Безпеки ООН».

Небезпека таких дій об'єктивується внутрішніми економічними та соціально-політичними факторами, що впливають на спроможність України щодо адекватного реагування на виклики та ризики воєнній безпеці. До них відносять, зокрема, й недостатній рівень готовності Збройних Сил України та інших утворених відповідно до законів України військових формувань, а також правоохоронних органів спеціального призначення до ведення сучасної збройної боротьби, а

---

[12] Военная доктрина Российской Федерации : Утверждена Президентом Российской Федерации 25.12.2014 г. № Пр-2976. URL: http://static.kremlin.ru/ media/events/files/41d527556bec8deb3530.pdf.

також «недостатні та непрофесійні зусилля органів державної влади України у сфері протидії пропаганді та інформаційно-психологічним операціям Російської Федерації» (пункт 12).

До того ж, істотну роль відграє те, що, як визнає українська влада, «порівняно з Російською Федерацією економічні, воєнні, людські, інформаційні та інші ресурси України є значно меншими. З урахуванням наявності в Російській Федерації стратегічної ядерної зброї та зловживання нею статусом постійного члена Ради Безпеки ООН обмеженою також стає і реакція світової спільноти на російську агресію проти України» (пункт 42).

Тому, одним із основних завдань воєнної політики України у найближчий час і в середньостроковій перспективі повинно стати «попередження та ефективна протидія інформаційно-психологічним впливам іноземних держав, спрямованим на підрив обороноздатності, порушення суверенітету і територіальної цілісності України, дестабілізацію внутрішньої соціально-політичної обстановки, провокування міжетнічних та міжконфесійних конфліктів в Україні» (пункт 17). Першочерговими ж названі у пункті 32 заходи, які спрямовані на "підвищення ефективності спеціальних інформаційних заходів впливу в районі проведення антитерористичної операції в Донецькій та Луганській областях і на тимчасово окупованій території та зосередження сил і засобів для організації ефективної протидії проведенню ворожих інформаційно-психологічних операцій проти України" та ін. Доцільним видається й анонсоване «розроблення комплексного нормативного документа щодо проведення спеціальних інформаційних операцій, передбачивши узгодження понятійного апарату, визначення профільних структурних підрозділів державних органів та їх завдань і повноважень у мирний, воєнний час» (пункт 47).

Отже, аналіз «Воєнної доктрини України» дає підстави стверджувати про розуміння політичним керівництвом держави сутності інформаційного виміру гібридної війни, причин, що поглиблює її небезпеку для суверенітету та територіальної цілісності, певною мірою вироблено бачення протидії. Однак, практика реалізації положень цього документу, зокрема, в частині, інформаційної складової, свідчить про низьку ефективність такої протидії. Означення подій 2014-2019 року на сході та півдні України як «гібридна війна» є «зручним» для української влади, яка всупереч реаліям уперто не визнає факту російсько-української війни.

Тому, очевидно, можновладцям слід при прийнятті політичних рішень слід звіряти свої дії з вимогами засадничого характеру, які містить стаття 17 Конституції України: «захист суверенітету і

територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу». Серед принципів державної політики у сферах національної безпеки і оборони Закон України «Про національну безпеку» називає «забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо» (пункт 4 статті 3)[13].

З точки зору нормотворчої техніки названий Закон вирізняється в масиві нормативно-правових актів статтею 1, що містить визначення термінів. З огляду на предмет дослідження використаємо наступне: «загрози національній безпеці України – явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України» (пункт 6 частини першої статті 1). Самі ж загрози національній безпеці України та відповідні пріоритети державної політики у сферах національної безпеки і оборони – відповідно до припису частини п'ятої статті 4 цього Закону – визначаються у Стратегії національної безпеки України, Стратегії воєнної безпеки України, Стратегії кібербезпеки України, інших документах з питань національної безпеки і оборони, які схвалюються Радою національної безпеки і оборони України і затверджуються указами Президента України.

Новий перелік загроз, вважаємо, хоча і вимагає розширення, але досить змістовно виписаний у «Стратегії національної безпеки України», що затверджена Указом Президента України від 26 травня 2015 року [14]. Насамперед, це інформаційно-психологічна війна, приниження української мови і культури, фальшування української історії, формування російськими засобами масової комунікації альтернативної до дійсності викривленої інформаційної картини світу. Загрозами інформаційній безпеці держави є ведення інформаційної війни проти України та відсутність цілісної комунікативної політики

---

[13] Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII**.** *ВВР*. 2018. № 31. Ст. 241. URL: https://zakon.rada.gov.ua/laws/show/ 2469-19.

[14] Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України" : Указ Президента України від 26.05.2015 р. № 287/2015. *Офіційний вісник Президента України:* офіц. вид. 03.06.2015. № 13, С. 50. Ст. 874. URL: https://zakon.rada.gov. ua/laws/show/287/2015/paran29#n29.

держави, недостатній рівень медіа-культури суспільства. У документі виокремлено загрози кібербезпеці і безпеці інформаційних ресурсів, а саме «уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом». У Стратегії визначені пріоритети забезпечення інформаційної безпеки, а також забезпечення кібербезпеки і безпеки інформаційних ресурсів.

Серед інших нормативно-правових актів України, з огляду на предмет дослідження, привернемо уваги до чинного Кримінального кодексу України. Це, насамперед, стаття 111 «Державна зрада», яку законодавець кваліфікує, як "діяння, умисно вчинене громадянином України на шкоду суверенітетові, територіальній цілісності та недоторканності, обороноздатності, державній, економічній чи інформаційній безпеці України: перехід на бік ворога в умовах воєнного стану або в період збройного конфлікту, шпигунство, надання іноземній державі, іноземній організації або їх представникам допомоги в проведенні підривної діяльності проти України" (частина перша). Стає кодекс і на захист недоторканості приватного життя громадян, кваліфікуючи як злочин «незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації, крім випадків, передбачених іншими статтями цього Кодексу» (частина перша статті 182)[15].

Для характеристики інформаційної війни доцільно використати систематизовані науковцями всі основні принципи гібридної війни: раптовість, багатовимірність, багатовекторність, тотальність, темпоральна невизначеність, інституційність, асиметричність, симулятивність та ін [16]. Підтвердженням цього стало загострення збройного конфлікту внаслідок нападу ВМС Російської Федерації на українські судна в Азовському морі і, як наслідок, введення в Україні воєнного стану згідно з Указом Президента України П. Порошенка від

---

[15] Кримінальний кодекс України від 05.04.2001 р. № 2341-III. *ВВР*. 2001. № 25-26. Ст.131; поточна ред. – Ред. від 25.09.2019 р. URL: https://zakon5.rada. gov.ua/laws/show/2341-14.

[16] Магда Є. М. Гібридна війна: сутність та структура феномену. *Міжнародні відносини. Серія "Політичні науки"*. 2014. № 4. URL: http:// journals.iir.kiev.ua/index.php/pol_n/article/view/2489/2220.

26 листопада 2018 року[17]. Подія ця неоднозначно сприйнята і політикумом і громадянами загалом. Думки полярні – від повної підтримки дій Глави держави до сприйняття введення воєнного стану як PR-акції влади чи прагнення відтермінувати проведення виборів Президента України, що за Конституцією держави мали відбутись 31 березня 2019 року. Дорікають й, що це слід було зробити раніше (у 2014 році), та й війна державою офіційно не оголошена.

Конституція України містить вичерпний перелік статей, за якими здійснення прав громадян може бути обмежене законом. Зокрема, здійснення прав, передбачених названими вище частинами першою та другою статті 34, «може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя» (частина третя статті 34). Воєнний стан як чинник обмеження конституційних прав і свобод названий у статті 64 чинної Конституції України. Статтею встановлено, що «конституційні права і свободи людини і громадянина не можуть бути обмежені, крім випадків, передбачених Конституцією України» (частина перша).

Наведені конституційні норми конкретизовані у чинному Законі України «Про правовий режим воєнного стану» від 12 травня 2015 року за № 389-VIII[18]. Із сукупності його норм і приписів проблеми дослідження стосуються, зокрема, вимоги до змісту Указу Президента України про введення воєнного стану, у якому повинні бути зазначений «вичерпний перелік конституційних прав і свобод людини і громадянина, які тимчасово обмежуються у зв'язку з введенням воєнного стану із зазначенням строку дії цих обмежень, а також тимчасові обмеження прав і законних інтересів юридичних осіб із зазначенням строку дії цих обмежень» (пункт 5 частини першої статті 6).

---

[17] Про введення воєнного стану в Україні : Указ Президента України від 26.11.2018 р. № 393/2018. *Голос України*. 2018. 28 листоп. URL: https://www. president.gov.ua/documents/3932018-25594.

[18] Про правовий режим воєнного стану : Закон України від 12.05.2015 р. № 389-VIII. *ВВР.* 2015. № 28. Ст.250; поточна ред. – Ред. від 26.05.2018. URL: http://zakon.rada.gov.ua/laws/show/389-19

Певною мірою може бути використано і припис пункту 12 частини першої цієї ж статті згідно з яким «у разі порушення вимог або невиконання заходів правового режиму воєнного стану вилучати у підприємств, установ і організацій усіх форм власності, окремих громадян телекомунікаційне обладнання, телевізійну, відео- і аудіоапаратуру, комп'ютери, а також у разі потреби інші технічні засоби зв'язку».

Заборону роботи приймально-передавальних радіостанцій особистого і колективного користування та заборону на передачу інформації через комп'ютерні мережі повинні забезпечити Міністерство інформаційної політики України, МВС, Міністерство оборони України, СБУ, Адміністрація Держспецзв'язку, Нацрада України з питань телебачення і радіомовлення, Держкомтелерадіо та Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації (пункт 11). На МВС, Національну гвардію, Адміністрацію Держприкордонслужби, Державну фіскальну службу, СБУ покладено забезпечення «вилучення у підприємств, установ і організацій усіх форм власності, окремих громадян телекомунікаційного обладнання, телевізійної, відео- і аудіоапаратури, комп'ютерів, а також у разі потреби інших технічних засобів зв'язку у разі порушення вимог або невиконання заходів правового режиму воєнного стану» (пункт 12).

Запровадження та здійснення заходів правового режиму воєнного стану провадиться регламентується типовим планом, який розроблений урядовцями та затверджений Постановою Кабінету Міністрів 22 липня 2015 року[19]. Виконання заходів покладено на «військове командування, військові адміністрації (у разі їх утворення), які діють самостійно або із залученням органів виконавчої влади, Ради міністрів Автономної Республіки Крим, органів місцевого самоврядування» (абзац перший частини першої статті 8). При цьому Закон зобов'язує громадян «сприяти діяльності військового командування та військових адміністрацій у запровадженні та здійсненні заходів правового режиму воєнного стану на відповідній території» (частина перша статті 17).

---

[19] Про затвердження типового плану запровадження та забезпечення заходів правового режиму воєнного стану в Україні або в окремих її місцевостях: Постанова Кабінету Міністрів України від 22.07.2015 р. № 544. *Офіційний вісник України*. 2015. № 62. Ст. 2018.

26 грудня 2018 року дію воєнного стану в Україні – припинено. Обмеження ж конституційних прав громадян, зокрема, на інформацію – фактично не застосовувалось, що зумовлено низкою причин, які здебільшого виходять за межі даного дослідження й проаналізовані нами окремо[20].

І ще один вияв інформаційної агресії. Застосування противником звичайних і нетрадиційних засобів в адаптивний спосіб для досягнення своїх цілей знайшло вираз у широкій інформаційній інтервенції на українство, в т.ч. і закордонне. І така діяльність принесла їм певні результати. Прагнення лідерів самопроголошених республік надати легітимності їх утворенням спонукали до спроб використання ними апробованих світовому конституціоналізмі та міжнародному праві форм народного волевиявлення – виборів та референдумів. І хоча, світова спільнота, не визнала їх результатів, проведене голосування стали підставою для приєднання Криму до Російської Федерації, утворення ДНР та ЛНР. Більше того, сьогодні ведеться масована психологічна атака щодо проведення повторних референдумів і виборів, які б закріпили особливий статус окремих територій Донецької та Луганської областей. Об'єктивно оцінюючи ситуацію в ОРДЛО мусимо визнати, шо проросійське «зомбування» дало змогу рекрутувати сепаратистам певне число прихильників. Тому принципово важливим, вважаємо, є наголошення у «Воєнній доктрині України» на потребі посилення заходів з реалізації державної інформаційної політики на тимчасово окупованій противником території і міжнародній арені з метою досягнення переваги над воєнним противником.

Потужна пропагандистська машина країни-агресора зуміла створити негативний образ українців у свідомості знаної частини росіян і цим забезпечити, якщо не підтримку, то відсутність у Російській Федерації масових акцій протесту проти війни. Нестійкою є підтримка й частини громадян окремих європейських країн попри позицію глав держав ЄС та санкції.

Вершиною майстерності у війні з давніх часів вважають використання ресурсів противника та їх використання проти нього

---

[20] Дерев'янко С. М. Обмеження політичних прав громадян в умовах воєнного стану : політико-правові підстави. *Держава і право: зб. наук. пр. Серія. Політичні науки.* Вип. 93 / Ін-т держави і права ім. В. М. Корецького НАН України. Київ: Вид-во "Юридична думка", 2019. С. 26–38.

самого. Така стратегія отримала нині назву «розумного енергоменеджменту впливу»[21]. Окремі громадяни України самі, здебільшого несвідомо, поширюють фейкові новини. Невичерпним джерелом їх стали соціальні мережі.

Таким чином, вторгнення Російської Федерації на територію України, окупація та наступна анексія українського півострова Крим, спровоковане державою-агресором збройне протистояння у південно-східних областях, що триває вже шостий рік, невизначеність реальних перспектив їх завершення викликали глибоке розчарування й обурення в суспільстві в дієздатності влади. Інформаційна війна, яка інтенсивно ведеться проти України Російською Федерацією стала істотним компонентом гібридної війни. Втягнутими в неї виявились фактично, усвідомлено чи ні, більшість громадян держави. Результати виборів Президента України та народних депутатів України у 2019 році переконливо свідчать про домінуючий суспільний запит на здійснення корінних змін у всіх сферах державотворення. Істотним є звинувачення владі у відсутності дієвих гарантій щодо реалізації конституційних прав і свобод громадян, в т.ч. й на інформацію. Ми повинні виграти інформаційну війну, виграти всю війну. А далі складний й тривалий процес «гуманітарного розмінування» тимчасово окупованих територій.

Книш Віталій Васильович
Професор кафедри конституційного, міжнародного та адміністративного права навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника»,
доктор юридичних наук, доцент.

МІСЦЕ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

[21] Гибрессия Путина. Невоенные аспекты войн нового поколения / Центр глобалистики “Стратегія XXI”. М. Гончар. 2016. URL: http://geostrategy.org.ua/ images/Hybression_finversion.pdf.

Провідну науково-методологічну роль у визначенні місця інформаційної безпеки відіграє співвідношення понять «безпека – національна безпека – інформаційна безпека». Тому доцільно спочатку дослідити зміст поняття безпека як найзагальнішої суспільної категорії.

У науковій та довідково-енциклопедичній літературі зазначається, що термін «безпека» (від грецького – «володіти ситуацією») почав вживатися з 1190 р. і означав спокійний стан духу людини, яка вважала себе захищеною від будь-якої небезпеки.

Однак у цьому значенні він не прижився в лексиці народів Західної Європи і тому до XVII ст. вживався рідко. Порівняно нечасте використання цього терміна протягом майже шести століть пояснюється, зокрема, тим, що з середини XII ст. більше розповсюдження отримав інший феномен - «поліція». Зміст його був надзвичайно широким. Він трактувався як державний устрій, державне управління, мета якого - всезагальне благо та безпека.

У XVII-XVIII ст. практично в усіх країнах стверджується точка зору, що держава має за головну мету всезагальний добробут та безпеку. Тому термін «безпека» отримує в цей час нове трактування – стан, ситуація спокою, що з'являється в результаті відсутності реальної небезпеки, а також матеріальні, економічні, політичні умови, відповідні органи та організації, що сприяють утворенню такої ситуації[22].

На сьогодні існує майже шість різних трактувань поняття «безпека», в залежності від галузі яка розглядає це питання (правознавство, політологія, філософія, біологія тощо). Основними з них є наступні розуміння безпеки:

1) *загальносуспільне розуміння* - стан захищеності особи, суспільства, держави від зовнішніх та внутрішніх загроз, який ґрунтується на діяльності людей, суспільства, держави, світового співтовариства щодо виявлення, запобігання, послаблення, усунення і відбиття небезпек і загроз здатних їх знищити позбавити фундаментальних матеріальних та духовних цінностей, нанести неприйнятні збитки, закрити шлях до виживання та розвитку;

2) *технологічне розуміння* – відсутність неприпустимого ризику, пов’язаного з можливістю завдання будь-якої шкоди;

---

[22] Головні визначення – безпека, загроза, небезпека, надзвичайна ситуація, ризик. URL: https://studfiles.net/preview/5704573/page:3/.

3) *державно-політичне розуміння* – органічна система організації державної влади щодо реалізації потреб та інтересів людини;

4) *системно-функціональне розуміння* – тип динамічної рівноваги, характерний для складних саморегульованих систем, що полягає у підтриманні істотно важливих для системи параметрів у допустимих межах [21] .

Поняттю «безпека» протиставляється термін «небезпека», що розглядається у наступних значеннях:

1) *у загальносуспільному розумінні* – як подія, умова або ситуація яка існує в навколишньому середовищі і здатна призвести до фізичної, психічної моральної шкоди та різної тяжкості поранень (включаючи смертельні);

2) *у гуманітарному розумінні* – як наслідок дії окремих чинників на людину.

Розрізняють політичні небезпеки, економічні, екологічні, харчові, криміногенні небезпеки інформаційні тощо [21].

У свою чергу, можна виділити *національне* та *міжнародно-правове* розуміння безпеки. Національне розуміння зазначеного найзагальнішого поняття закріплене у Державному стандарті України 2293-99, який визначає термін «безпека» як стан захищеності особи та суспільства від ризику зазнати шкоди[23].

У цьому визначенні поняття «безпека» присутній термін «ризик». Тут же зазначимо, що ризик виникнення аварій, пошкоджень або виходу з ладу простих технічних пристроїв визначити не досить складно. Для складних же технічних систем, а тим більше для людини чи суспільства ризик – це категорія, яка має велику кількість індивідуальних ознак і характеристик, і математично точно визначити його надзвичайно складно, а інколи неможливо. В таких випадках ризик може бути оцінений лише завдяки експертній оцінці.

У міжнародно-правовому розумінні, безпека людини – це поняття, що відображає саму суть людського життя, її ментальні, соціальні і духовні надбання. Безпека людини невід'ємна складова характеристика стратегічного напряму людства, що визначений ООН як «сталий людський розвиток» (Sustainable Human Development), тобто такий розвиток, який веде не тільки до економічного, а й до

---

[23] ДСТУ 2293-99. Охорона праці. Терміни та визначення основних понять. URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=21726.

соціального, культурного, духовного зростання, що сприяє гуманізації менталітету громадян і збагаченню позитивного загальнолюдського досвіду[24].

Родовим поняттям у контексті досліджуваної проблематики виступає поняття «*національна безпека*». Згідно п. 9 ст. 1 Закону України «Про національну безпеку України» від 08.07.2018 року, національна безпека України – захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз [25].

Враховуючи зміст вищенаведеного нормативного визначення, доцільно виокремити наступні ознаки поняття «національна безпека»:

1) воно походить від загального поняття «безпека», враховує та інтегрує в собі його національне та міжнародно-правове розуміння та носить родовий характер;

2) метою національної безпеки є захищеність держави та громадянського суспільства України від реальних чи потенційних загроз;

3) об'єктом національної безпеки виступають державний суверенітет, територіальна цілісність, демократичний конституційний лад та інші національні інтереси України.

По відношенню до загального поняття «безпека» та родового поняття «національна безпека» термін «інформаційна безпека» є поняттям видовим.

Саме ж поняття *інформаційної безпеки* можна розглядати удвох основних аспектах:

1) інформаційна безпека як стан захищенності інформаційного середовища суспільства, який забезпечує його формування, використання й розвиток в інтересах громадян, організацій, держави. У даному випадку мова йде про захист інформаційного простору як об'єкта;

2) інформаційна безпека як стан захищеності потреб в інформації особи, суспільства й держави, при якому забезпечується їхнє існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз. У цьому аспекті

---

[24] Коптєва О. О. Безпека людини як концепція міжнародного права. URL: Nzizvru_2014_6_14.pdf.

[25] Про національну безпеку України: Закон України від 08.07.2018 року. URL: https://zakon.rada.gov.ua/laws/show/2469-19.

головний акцент робиться на захисті суб'єктів інформаційного права, а також їх правового статусу в інформаційній сфері.

В цілому, в інформаційному праві інформаційна безпека – це одна із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позиції захисту життєво важливих інтересів особистості, суспільства, держави і акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами [26].

На забезпечення інформаційної безпеки відповідно до п. 21 ст. 1 та ст. 31 Закону України «Про національну безпеку України» розробляється та реалізується «Стратегія кібербезпеки України», під якою розуміється документ довгострокового планування, що визначає загрози кібербезпеці України, пріоритети та напрями забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Таким чином, за результатами дослідження можна зробити наступні висновки:

1) загальне поняття «безпека» переважно тлумачиться у міжнародно-правовому розумінні, обґрунтованому ООН, як «сталий людський розвиток», тобто такий розвиток, який веде не тільки до економічного, а й до соціального, культурного, духовного зростання, що сприяє гуманізації менталітету громадян і збагаченню позитивного загальнолюдського досвіду. Тут зазначене розуміння акцентує увагу на окремих сферах суспільного життя;

2) родове поняття «національна безпека» акумулює в собі основні ознаки загального, визнаного на міжнародному рівні поняття «безпека», деталізуючи на рівні національного права сфери суспільної безпеки та безпекової політики;

3) видове поняття «інформаційна безпека» уособлює окрему сферу національної безпекової політики – інформаційну (інформаційно-комунікативну) сферу, окремим напрямом якої є кібербезпека.

---

[26] Інформаційна безпека. URL: https://sites.google.com/site/infobezpekaosobu/informacijna-bezpeka.

Зінич Любомир Васильович
викладач кафедри конституційного, міжнародного та адміністративного права навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника»,
кандидат юридичних наук.

ПРАВОВІ ЗАСАДИ ВЗАЄМОДІЇ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА ТА ДЕРЖАВИ У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сучасні реалії розвитку інформаційних процесів в Україні підтверджують, що інформаційна безпека є такою ж важливою складовою національної безпеки, як економічна, політична чи військова. Проте, в умовах зовнішніх впливів вона стала найменш захищеним її елементом. Протидія інформаційним загрозам можлива шляхом ефективної взаємодії громадянського суспільства та держави, адже саме на суспільство спрямований інформаційний вплив.

Найбільш знаковою подією стало прийняття Доктрини інформаційної безпеки України[27], яка у п.3 визначила, що налагодження ефективної взаємодії органів державної влади та інститутів громадянського суспільства під час формування та реалізації державної політики в інформаційній сфері є найважливішим інтересом суспільства.

Слід зазначити, що різним аспектам дослідження питань взаємодії громадянського суспільства та держави присвячували увагу велика кількість науковців. Однак, на сьогодні ще залишається значна кількість проблемних питань при взаємодії громадянського суспільства і держави у забезпеченні інформаційної безпеки.

Громадянське суспільство як зазначено в Указі Президента України «Про сприяння розвитку громадянського суспільства в

[27] Указ Президента України №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про доктрину інформаційної безпеки України». URL: https://www.president.gov.ua/documents/472017-21374

Україні»[28] – це такий стан суспільства, в якому вільно реалізуються основоположні права і свободи людини і громадянина через різноманітні форми публічної громадської активності та самоорганізації. Громадянське суспільство виступає гарантією демократичного розвитку держави.

Суспільство і держава перебувають у тісному взаємозв'язку і не можуть існувати окремо. Завдяки державі спільнота набуває цивілізованості і стає суспільством. Водночас держава не може існувати поза суспільством. Вона похідна від нього і покликана йому слугувати.

Закон України «Про засади внутрішньої та зовнішньої політики» [29] передбачає ряд засад внутрішньої політики у сфері формування інститутів громадянського суспільства до яких слід віднести наступні:

- Утвердження громадянського суспільства як гарантії демократичного розвитку держави;
- Посилення взаємодії органів державної влади, місцевого самоврядування та об'єднань громадян та запровадження громадянського контролю за їх діяльністю;
- Забезпечення незалежної діяльності об'єднань громадян, посилення їх впливу на прийняття суспільно важливих рішень;
- Створення умов для забезпечення широкого представництва громадян у органах державної влади;
- Проведення регулярних консультації з громадськістю з важливих питань суспільства та держави;
- Проведення всеукраїнських та місцевих референдумів як ефективних форм народного волевиявлення, участі народу у прийнятті суспільно важливих рішень.

Принцип утвердження громадянського суспільства як гарантії демократичного розвитку держави є загальним, оскільки він спирається на конституційний та міжнародний принцип свободи слова. Цей принцип прямо закріплений у Конституції України та міжнародних актах.

---

[28] Указ Президента України №68/2016 «Про сприяння розвитку громадянського суспільства в Україні». URL: https://zakon.rada.gov.ua/laws/show/68/2016

[29] Закон України №2411-VI від 08.07.2018 «Про засади внутрішньої і зовнішньої політики». URL: https://zakon.rada.gov.ua/laws/show/2411-17

Даний принцип передбачає, що держава створює умови для формування та розвитку організацій громадянського суспільства, забезпечення ефективних процедур участі громадськості, під час формування та реалізації державної, регіональної політики, розв'язання питань місцевого значення, стимулювання участі організацій громадянського суспільства у соціально-економічному розвитку України.

Посилення взаємодії органів державної влади, місцевого самоврядування та об'єднань громадян та запровадження громадянського контролю за їх діяльністю, яка здійснюється за допомогою презумпції відкритості інформації та є необхідною умовою для забезпечення реалізації права на інформацію. Натомість необґрунтоване віднесення органами державної влади відомостей до категорії інформації з обмеженим доступом негативним чином впливає на реальність здійснення зазначеного права. Важливу роль у забезпеченні відкритості інформації та гарантуванні здійснення права громадян на інформацію відіграє заборона засекречування деяких категорій відомостей. Їх перелік зафіксований у законодавстві України, зокрема у ч. 4 ст. 30 Закону України «Про інформацію» [30], ч. 2 ст. 50 Конституції України [31], Постанові Кабінету Міністрів України від 9 серпня 1993 р. № 611 «Про перелік відомостей, що не становлять комерційної таємниці» [32]. На даний час такий порядок визначається рядом нормативно-правових актів, зокрема Законом України «Про державну таємницю» [33]. Тому закріплення у законодавстві переліку відомостей, які не можуть бути віднесені до інформації з обмеженим доступом, є важливим та необхідним. Доступність інформації є властивість системи (середовища, засобів і технології її обробки), в якій здійснює обіг інформація, що характеризується здатністю забезпечувати своєчасний безперешкодний доступ суб'єктів до

---

[30] Закон України № 2657-XI від 02.10.1992 «Про інформацію». URL: https://zakon.rada.gov.ua/laws/show/2657-12

[31] Конституція України. Закон України №254к-96ВР від 28.06.1996. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80

[32] Про перелік відомостей, що не становлять комерційної таємниці. Постанова Кабінету Міністрів України №611 від 09.08.1993. URL: https://zakon.rada.gov.ua/laws/show/611-93-%D0%BF

[33] Про державну таємницю. Закон України №3855-XII від 21.01.1994. URL: https://zakon.rada.gov.ua/laws/show/3855-12

зацікавленої інформації, а також постійна готовність відповідних автоматизованих служб до обслуговування отриманих від суб'єктів запитів, коли в цьому виникає необхідність. Доступність саме цієї інформації, яка в юридичній літературі отримала назву офіційна інформація чи урядова інформація є необхідною передумовою реалізації права на інформацію та багатьох інших суб'єктивних прав.

Реалізація права на доступ до інформації багато в чому залежить від способів її здобування. Для всебічної поінформованості недостатньо мати змогу діставати інформацію лише за інформаційним запитом або тільки знайомитися з потрібною інформацією на сайті органу державної влади. Реалізація цих можливих способів діставати інформацію гарантує право на доступ до інформації. Фахівці у сфері доступу до інформації розрізняють «активний» і «пасивний» спосіб реалізації права на доступ до інформації. Проте автори по-різному визначають, які форми доступу до інформації слід відносити до пасивною способу, а які до активного. Зокрема фахівці дотримуються погляду де, пасивний спосіб здобуття інформації вони визначають як отримання інформації через створені органами державної влади й місцевого самоврядування канали комунікації, а активний доступ до інформації – як здобуття інформації шляхом інформаційних запитів щодо отримання відомостей або про доступ до матеріалів. Питання доступності принципів інформаційних відносин передбачає аналіз усіх матеріалів, які стосуються проблем правового регулювання доступу до публічної інформації.

Ефективною формою громадського контролю діяльності органів місцевого самоврядування є громадські експертизи нормативно-правових актів, ухвалених органами самоврядування. Громадська експертиза є механізмом громадської експертної діяльності з аналізу й оцінки впливу нормативних та інших управлінських рішень влади усіх рівнів на умови життя і реалізацію прав та законних інтересів широких верств громадян і конкретних соціальних груп.

Для діяльності інститутів громадянського суспільства в Україні характерним є недостатній рівень інституційної, кадрової та фінансової спроможності. У зв'язку з цим міжнародними та вітчизняними неурядовими організаціями визначається досить низький рівень суспільно важливої добровільної активності громадян. Розвиток громадянського суспільства в Україні повинен орієнтуватися на європейські стандарти захисту прав і свобод людини: запровадження практики належного врядування, відкритості, доброчесності, прозорості та підзвітності інститутів влади, забезпечення умов для реалізації різних суспільних інтересів, у тому числі соціальних,

економічних, екологічних, релігійних, культурних, територіальних тощо, а також форм їх прояву (суспільні рухи, громадські ініціативи, об'єднання. асоціації). Оптимальне поєднання контролю за діяльністю влади та громадського впливу на прийняття рішень може збільшити рівень суспільної компетентності й довіри до органів влади, а також сприяти становленню демократії в Україні.

Важливим компонентом взаємодії громадянського суспільства та держави є достовірність інформації, при цьому достовірність інформації є досить істотним принципом інформаційних відносин та основоположною вимогою щодо інформації, у зв'язку з чим потребує свого законодавчого визначення у Законі України «Про інформацію», зокрема, у такому формулюванні як відповідність, та ідентичність отриманих даних фактичним умовам або є властивістю інформації, яка визначає ступінь об'єктивного, точного відображення подій, фактів, що мали місце. Надання або поширення недостовірної інформації є підставою для застосування до винних у цьому осіб встановленої законодавством відповідальності. Передбачено також порядок спростування інформації, яка не відповідає дійсності, відшкодування майнової й моральної шкоди, завданої її поширенням. Повнота є також однією зі складових умов щодо інформації.

Тому на основі всього сказаного вище, можна стверджувати, що важливими аспектами протидії інформаційній війні у сучасних умовах є активна взаємодія громадянського суспільства та держави. Держава і громадянське суспільство в межах демократичного устрою зацікавлені в діалозі та партнерстві. Також вони повинні прагнути до підвищення ефективності взаємодії. Але без розвиненого громадянського суспільства, без створення належних умов для забезпечення свободи думки і слова, свободи об'єднань, вільного вираження поглядів свободи зборів, участі громадян в управлінні державними справами та місцевому самоврядуванні, держава не може забезпечити інформаційну безпеку.

Вважаємо, що дотримання описаних у дослідженні засад взаємодії громадянського суспільства і держави дасть можливість (поряд з іншими заходами) на якісно новому рівні забезпечити інформаційну безпеку України.

Проведений аналіз взаємодії держави і громадянського суспільства з метою забезпечення інформаційної безпеки є невичерпаним, а подальші дослідження дадуть змогу розробити практичні рекомендації щодо вдосконалення законодавства України.

Петровська Ірина Ігорівна
доцент кафедри конституційного, міжнародного та адміністративного права навчально-наукового юридичного інституту ДВНЗ «Прикарпатського національного університету імені Василя Стефаника», кандидат юридичних наук, доцент.
Поварчук Роман Ігорович
Студент 2 курсу магістратури, спеціалізація 01 «Публічна служба» навчально-наукового юридичного інституту ДВНЗ «Прикарпатського національного університету імені Василя Стефаника».

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ ПРИ ЗДІЙСНЕННІ КОНТРОЛЬНОГО ПРОВАДЖЕННЯ

Правовий режим інформації в інформаційному суспільстві включає досить об'ємний перелік нормативно-правових актів та методів правозастосування, групу відносин з притягнення видних осіб до всіх видів юридичної відповідальності та застосування адміністративно-господарських санкцій. Також, контрольні відносини пов'язані зі значним комплексом заходів, процедурно-процесуальних дій уповноважених суб'єктів. Тому дослідження питань використання інформації з обмеженим доступом при здійсненні контрольного провадження є актуальним у відносинах публічної служби.

У сучасних правових документах немає визначення контрольного провадження, здебільшого визначається тільки комплекс заходів процедурного характеру. Науковці визначають контрольне провадження як регламентовану адміністративно-процесуальними нормами послідовну діяльність органів публічної адміністрації із забезпечення законності і дисципліни в сфері публічного управління [34]; контрольно-наглядові провадження – вид провадження за ініціативою органу владних повноважень, регламентовані адміністративно-процесуальними нормами дії органу владних повноважень щодо

[34] Кузьменко О.В., Гуржій Т.О. Адміністратино-процесуальне право України / за ред. Кузьменко О.В. К.: Атіка, 2008. 416 с

здійснення контролю, нагляду та перевірки виконання законів, інших нормативних актів у сфері господарювання, забезпечення громадського порядку і громадської безпеки, порядку управління [35].

Для характеристики інформації з обмеженим доступом при здійсненні контрольного провадження варто проаналізувати зміст публічної інформації. Публічна інформація – це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених Законом «Про доступ до публічної інформації».

Серед видів інформації з обмеженим доступом при здійсненні контрольного провадження можна виділити, службову інформацію, державну таємницю, персональні дані, адвокатську таємницю, комерційну таємницю та ін.

Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень [36]. Чинне законодавство замість «конфіденційної інформації» використовує поняття «службова» або «інформація для службового використання». Ці поняття схожі, але не тотожні. Віднесення інформації до службової і відповідно присвоєння документу, що містить таку інформацію, грифу «для службового користування», має відбуватись відповідно до вимог статей 6 і 9 Закону України «Про доступ до публічної інформації». Основною метою прийняття нового законодавства було якомога більше розширення доступу до інформації та зменшення дискреційних повноважень органів влади для її обмеження[36]. Наприклад, Івано-Франківська міська рада затвердила Примірний Перелік відомостей, що становлять службову інформацію, до якого віднесла документи та інформацію, що не підлягають наданню для ознайомлення за запитами та включила до цих документів таємну, державну і конфіденційну інформацію, а також інформацію про особисте життя особи,

---

[35] Демський Е.Ф. Адміністративне процесуальне право України: навч.пос. К.: Юрінком Інтер, 2008. 496 с.

[36] Службова інформація: порядок віднесення та доступу. Практичний посібник / За редакцією Д. М. Слизьконіс. Автори-укладачі: О.Л. Огданська, В.В. Таран, В.В. Щербаченко. К.: Центр політичних студій та аналітики, 2014. 76 с .

інформацію про оперативну і слідчу роботу органів прокуратури, МВС, СБУ, відомості про заходи мобілізаційної підготовки, мобілізаційного плану міста [36].

Таємна інформація – інформація, яка містить державну, професійну, банківську таємницю, таємницю слідства та іншу, передбачену Законом таємницю, розголошення якої може завдати шкоди особі, суспільству і державі (ст. 8 Закону України «Про доступ до публічної інформації»)[36]. Обмеження доступу до інформації здійснюється відповідно до закону при дотриманні сукупності таких вимог: 1) виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя; 2) розголошення інформації може завдати істотної шкоди цим інтересам; 3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні [36]. Не може бути обмежено доступ до інформації про розпорядження бюджетними коштами, володіння, користування чи розпорядження державним, комунальним майном, у тому числі до копій відповідних документів, умови отримання цих коштів чи майна, прізвища, імена, по батькові фізичних осіб та найменування юридичних осіб, які отримали ці кошти або майно. Зазначене положення не поширюється на випадки, коли оприлюднення або надання такої інформації може завдати шкоди інтересам національної безпеки, оборони, розслідуванню чи запобіганню злочину. Не належать до інформації з обмеженим доступом відомості, зазначені у декларації про майно, доходи, витрати і зобов'язання фінансового характеру, оформленої за формою і в порядку, що встановлені Законом України «Про запобігання корупції» (ч. 5 і 6 статті 6 Закону України «Про доступ до публічної інформації» [37]).

Дії чи бездіяльність суб’єктів владних повноважень щодо недотримання режиму доступу до інформації, в тому числі і при здійсненні контрольного провадження є правопорушеннями і тягнуть за собою юридичну відповідальність.

---

[37] Про доступ до публічної інформації: Закон України від 13.01.2011 року. URL: https://zakon.rada.gov.ua/laws/show/2939-17

НАПРЯМОК ІІ. ІНФОРМАЦІЙНА БЕЗПЕКА І КОНСТИТУЦІЙНИЙ ЛАД УКРАЇНИ В ПРОЦЕСІ ІМПЛЕМЕНТАЦІЇ ЗАКОНОДАВСТВА УКРАЇНИ ДО ЄВРОПЕЙСЬКОГО ЗАКОНОДАВСТВА

Петровська Ірина Ігорівна
доцент кафедри конституційного, міжнародного та адміністративного права навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника»,
кандидат юридичних наук, доцент

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СУЧАСНОМУ СУСПІЛЬСТВІ: УКРАЇНА ТА ЄС

У сучасному суспільстві з питаннями безпеки пов'язаний великий комплекс заходів та напрямків діяльності як кожної людини (задля забезпечення особистої безпеки) так і їх об'єднань (національних та міжнародних), держав, міжнародних організацій, що покликані забезпечити громадську та національну безпеку, визначити основи безпеки на міжнародному рівні. Інформаційна безпека, яка вступає видом національної безпеки є предметом внутрішньої та зовнішньої політики. Зокрема, підходи до забезпечення інформаційної безпеки, які застосовуються у країнах Східної Європи, є не уніфікованими, що зумовлено геополітичною специфікою відповідних країн, одні з яких входять до Північноатлантичного Альянсу (НАТО) та Європейського Союзу (ЄС), інші – прямують до членства у вказаних організаціях, а деякі – входять до євразійських міждержавних утворень. Обравши євроінтеграційний курс та визначивши вступ до НАТО своїм стратегічним пріоритетом, Україна має орієнтуватися передусім на стратегію розвитку країн-учасниць ЄС та НАТО в

інформаційній сфері[38]. Україна має співпрацювати з іншими країнами Європи у розбудові систем регіональної та міжнародної інформаційної безпеки з метою протидії загрозам стратегічній стабільності, таким, як кібертероризм та кіберзлочинність, орієнтуючись при цьому на стандарти ЄС та НАТО. В цьому контексті для України є важливим досвід країн Східної Європи щодо приведення національного законодавства у відповідність до вимог вказаних міжнародних організацій, передусім –щодо забезпечення балансу між свободою й безпекою в інформаційній сфері на законодавчому рівні [39].

Інформаційна безпека, яка є складовою національної безпеки, визначається як захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз. Закон «Про національну безпеку України» [40], у статті 31, містить положення щодо стратегії кібербезпеки України. Кібербезпека є частиною інформаційної безпеки. Інформаційна безпека стосується інформації в цілому, а кібербезпека – інформації в ІТ системах. Зазначено, що ця стратегія є документом довгострокового планування, в якому визначаються пріоритети національних інтересів України у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози життєво важливим інтересам людини і громадянина, суспільства та держави в кіберпросторі, пріоритетні напрями, концептуальні підходи до формування та реалізації державної політики щодо безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, підвищення ефективності основних суб'єктів забезпечення кібербезпеки, насамперед суб'єктів сектору безпеки і оборони, щодо виконання завдань у кіберпросторі, а також потреби

---

[38] Політанський В.С. Інформаційне суспільство в Україні : від зародження до сьогодення. Науковий вісник Ужгородського національного університету. (Серія "Право"). Вип. 42. 2017. С. 16-22

[39] Ткачук Т.Ю. Забезпечення інформаційної безпеки:досвід окремих країн східної Європи. *Інформація і право*. № 4(23)/2017. С.62-72. URL: http://ippi.org.ua/tkachuk-tyu-zabezpechennya-informatsiinoi-bezpeki-dosvid-okremikh-krain-skhidnoi-%D1%94vropi-st-62-72 (дата звернення: 11.04.2019).

[40] Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII. Відомості Верховної Ради (ВВР), 2018, № 31, ст.241. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 11.04.2019).

бюджетного фінансування, достатні для досягнення визначених цілей і виконання передбачених завдань, та основні напрями використання фінансових ресурсів. Організація підготовки Стратегії кібербезпеки України здійснюється за дорученням Президента України Національним координаційним центром кібербезпеки після затвердження Стратегії національної безпеки України. Стратегія кібербезпеки України схвалюється рішенням Ради національної безпеки і оборони України та затверджується указом Президента України, є основою для підготовки державних програм та нормативно-правових актів, що стосуються забезпечення кібербезпеки України. Реалізація цієї стратегії здійснюється на основі національного оборонного, безпекового, економічного, інтелектуального потенціалу з використанням механізмів державно-приватного партнерства, а також із залученням міжнародної консультативної, фінансової, матеріально-технічної допомоги[40]. Стратегія кібербезпеки України - документ довгострокового планування, що визначає загрози кібербезпеці України, пріоритети та напрями забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави (ст.1 Закону «Про національну безпеку»). Про необхідність розробки стратегії інформаційної/кібербезпеки науковці говорили протягом тривалого часу. Тому передбачення таких положень у законодавстві є позитивним кроком. Варто якнайскоріше її розробити та почати впроваджувати.

У законодавстві України визначено також основні напрямами державної інформаційної політики, а саме: забезпечення доступу кожного до інформації; забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації; створення умов для формування в Україні інформаційного суспільства; забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень; створення інформаційних систем і мереж інформації, розвиток електронного урядування;

постійне оновлення, збагачення та зберігання національних інформаційних ресурсів; забезпечення інформаційної безпеки України;

сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору [41].

Один з напрямків інформаційної діяльності щодо забезпечення національної безпеки України є ведення інформаційна війни з Росією. Мета інформаційної війни – послабити моральні і матеріальні сили супротивника або конкурента та зміцнити власні[42]. Політика безпеки інформаційно-телекомунікаційних технологій включає правила, директиви та практику, що визначають засоби управління, захисту та розподілення активів, у тому числі критичної інформації, в інформаційних мережах[43]. В країнах ЄС та НАТО правова основа інформаційної безпеки включає досить об'ємний масив конвенцій, рекомендацій та інших матеріалів.

Загрози національній безпеці України нормативно визначено як явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України. А національні інтереси України – це життєво важливі інтереси людини, суспільства і держави, реалізація яких забезпечує державний суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності і добробут її громадян[40]. До сектору безпеки і оборони включено систему органів державної влади, Збройних Сил України, інших утворених відповідно до законів України військових формувань, правоохоронних та розвідувальних органів, державних органів спеціального призначення з правоохоронними функціями, сил цивільного захисту, оборонно-

---

[41] Про інформацію: Закон України від 2 жовтня 1992 року №2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 11.04.2019).

[42] Горбань Ю.О. Інформаційна війна проти України та засоби її ведення. *Вісник Національної академії державного управління при Президентові України*. №1. 2015. С. 136-141. URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Vnadu_2015_1_21.pdf (дата звернення: 11.04.2019).

[43] Синєокий О.В. Інформаційне право України та електронне право високих технологій: електронний курс лекцій українською мовою. Запоріжжя : ЗНУ, 2010. 215 ел. с http://www.kul-lib.narod.ru/bibl.files/ILaw/10sovipu.pdf (дата звернення: 11.04.2019).

промислового комплексу України, діяльність яких перебуває під демократичним цивільним контролем і відповідно до Конституції[44] та законів України за функціональним призначенням спрямована на захист національних інтересів України від загроз, а також громадяни та громадські об'єднання, які добровільно беруть участь у забезпеченні національної безпеки України[3]. Серед спеціалізованих суб'єктів варто виділити Державну служба спеціального зв'язку та захисту інформації України, яка є державним органом, призначеним для забезпечення функціонування і розвитку державної системи урядового зв'язку, національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, а також інших завдань відповідно до закону (стаття 22 Закону «Про національну безпеку»).

Варто погодитись з твердженням, що розвиток технологій, зокрема телекомунікаційних систем та електроніки, привів до надзвичайно швидкого зростання комунікаційних можливостей. Особливим полем для маневру є розвиток інформаційних технологій, що дає змогу придбати інформацію віддалено, без фізичної присутності в місці зберігання. Це є викликом не тільки для підприємців, які дбають про свої власні інтереси, але й для держави, яка повинна побудувати ефективну правову систему для захисту від шпигунських дій[45].

В правових актах України визначено напрямки державної політики, публічних посадовців, основні методи забезпечення національної безпеки та територіальної цілісності країни, зокрема при здійсненні інформаційної діяльності. Державна політика з національної

---

[44] Конституція України від 28 червня 1996 року. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 11.04.2019).

[45] Муравська (Якубівська) Ю.Є. Інформаційна безпека суспільства: концептуальний аналіз. Економіка та управління національним господарством №9. 2017. С. 289-294. URL: http://economyandsociety.in.ua/journal/9_ukr/50.pdf (дата звернення: 11.04.2019).

безпеки спрямовується на забезпечення державної, економічної, інформаційної, воєнної, зовнішньополітичної, екологічної безпеки, кібербезпеки України тощо.

Для забезпечення територіальної цілісності та національної безпеки як основ соборності України в інформаційній діяльності публічних службовців важливо втілити в життя положення чинного законодавства (реалізувати юридичні норми) з високою результативністю. Досягнення цього є можливим тільки за умов подальшого вдосконалення методів та форм публічного адміністрування суб'єктів владних повноважень, їх високої правової культури та професійної компетентності, подальшого розвитку електронного урядування в нашій країні.

Збирак Тетяна Вікторівна
Викладач кафедри конституційного, міжнародного та адміністративного права навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника»,
кандидат юридичних наук.

ІНФОРМАЦІЙНА БЕЗПЕКА В УКРАЇНІ: ДЕЯКІ АСПЕКТИ ЇЇ ЗАБЕЗПЕЧЕННЯ ПРИ РЕАЛІЗАЦІЇ ПРАВА НА СВОБОДУ СЛОВА

Одним із найважливіших завдань держави на сучасному етапі є створенням належних умов для вільного вираження кожною особою своїх поглядів та переконань, усунення перешкод при реалізації цього права та притягнення винних осіб до відповідальності. Однак гарантуючи свободу слова українська держава зіткнулася із іншою проблемою – спотворення інформації та використання її у якості зброї в інформаційній війні. Тому на сьогодні не менш важливим завданням є забезпечення інформаційної безпеки України. В цьому контексті повинен бути віднайдений баланс між реалізацією права на свободу слова та інформаційною безпекою.

Варто зазначити, що органи державної влади України поки що не належним чином забезпечують реалізацію державної інформаційної політики, спрямованої на утвердження свободи слова, плюралізму і демократичних засад інформаційної діяльності, інформаційного суверенітету та інформаційної безпеки України, зміцнення і розвиток її інформаційної інфраструктури. Поряд з цим чиновники користуються

недосконалістю законів, на свій розсуд часто необґрунтовано засекречують інформацію, встановлюючи обмеження її поширення під грифами «для службового користування» чи «не для друку» та ховають непопулярні рішення, інколи з ознаками корумпованості. Правове поле частково регулював Закон України «Про доступ до публічної інформації», однак, як свідчить практика його застосування, наразі він потребує вдосконалення, зокрема положення, які стосуються внесення плати за надання інформації, процедури інформування запитувача інформації про розмір плати за надання інформації (оскільки поряд з фактичними витратами на копіювання і друк існують ще й фактичні витрати на пересилання відповіді, що складає значну частку вартості такої послуги, а їх відшкодування цим законом не передбачено). Крім того, Закон України «Про доступ до публічної інформації» не враховує, що іншими законами встановлено спеціальні процедури доступу до інформації, яка зберігається в архівах, державних реєстрах, базах персональних даних тощо.

Правом на свободу думки і слова, на вільне вираження своїх поглядів і переконань може користуватися кожен, не зважаючи на те, чи є він громадянином України чи ні, адже це право закріплене в Конституції України і наша держава зобов'язалася його гарантувати так само, як й інші основоположні права людини. Українське суспільство усвідомило необхідність утвердження загальновизнаних норм свободи слова, прийнятих міжнародною спільнотою, що підтверджується не лише ратифікацією міжнародних документів та приведенням у відповідність до них національного законодавства, а включенням цього права до програмних документів більшості політичних партій та громадських об'єднань [46].

Під свободою слова слід розуміти правовий інститут міжнародного права та національних правових систем, який складається з правових норм, що мають на меті забезпечити право особи вільно думати про різні суб'єкти, об'єкти, явища, відносини та відомості, на підставі її уявлень і переконань, освіти, психологічного стану й середовища, в якому вона живе, а також можливість вільно виражати свої думки у словесній чи знаковій формах, вільно збирати, зберігати, використовувати, поширювати та отримувати інформацію у будь-якій формі, будь-якого змісту та обсягу, в межах, визначених чинним законодавством.

---

[46] Тарадай С.М. Адміністративні процедури забезпечення права громадян на доступ до публічної інформації: дис. … канд. юрид. наук: 12.00.07 / С.М. Тарадай. - Київ, 2012. - 217с.

Наголошується, що обмеження на свободу слова мають відповідати трьом міжнародно-правовим вимогам: легітимності, необхідності та доцільності, які повинні бути чітко виписані в національному законі, зрозумілими та гарантувати правовий захист від довільного втручання з боку влади, мають бути необхідними в демократичному суспільстві, під яким Європейський суд з прав людини розуміє панування плюралізму та верховенства права, а також повинні відповідати встановленим міжнародним правом цілям.

Загалом як можна побачити, реалізація права громадян на доступ до публічної інформації в Україні забезпечується недостатньо та зумовлена недоліками правового регулювання, зокрема сфери соціального управління, дій органів державної влади та самоврядування [47]. Тому з метою ефективного забезпечення прав громадян на доступ до публічної інформації необхідно передбачити на законодавчому рівні пошук інформації як самостійного різновиду інформаційної діяльності. Водночас потребує подальшого розвитку і вдосконалення інформаційне законодавство як окрема галузь, що об'єднує у собі самостійні правові інститути. Тому й надалі актуальною залишається розробка та впровадження нових законодавчих актів, спрямованих на врегулювання статусу суб'єктів правовідносин у мережі Інтернет.

Вважаю, що не потрібно приймати нові закони у сфері інформації, а варто систематизувати існуючі, визначаючи у них правові зв'язки, з метою подальшого їх кодифікування на рівні Інформаційного кодексу України. Цей кодифікований нормативний документ має об'єднати в одному законодавчому акті регулювання провідних суспільних відносин, об'єктом яких є інформація, незалежно від форми, способу, засобу чи технологій її прояву в суспільних відносинах. Серед провідних завдань кодифікування інформаційного законодавства визначення консенсусу у суспільних відносинах, узгодженості розуміння та застосування юридичних норм, правомірної поведінки учасників відносин в інформаційній сфері; забезпечення інформаційного суверенітету, незалежності України у міжнародних відносинах; забезпечення інформаційної безпеки громадян, їх окремих спільнот, суспільства та держави як складових національної безпеки

[47] Калюжний Р.А. Питання концепції реформування інформаційного законодавства України / Р.А. Калюжний, В.Д. Гавлонський, В.С. Цимбалюк, В.М. Гуцалюк. URL http:// www.crime-rsearch.ru/library/Rost.htm.

України; визначення правомірної поведінки учасників інформаційних відносин в Україні; захист інформації від несанкціонованого доступу, правопорушень (знищення, модифікації, перекручування тощо) [48].

Інформаційний кодекс має розроблятися з урахуванням європейських стандартів та розвитку інформаційних відносин в Україні. Тому розробка та введення його в дію сприятиме побудові розвинутого інформаційного суспільства нашої держави як органічного сегменту глобального інформаційного співтовариства, забезпеченню реалізації права на свободу слова та вільний доступ до публічної інформації, розвитку національних інформаційних ресурсів та інфраструктури, впровадженню новітніх інформаційних технологій.

Тому з метою ефективного забезпечення прав громадян на доступ до публічної інформації необхідно передбачити на законодавчому рівні пошук інформації як самостійного різновиду інформаційної діяльності. Водночас потребує подальшого розвитку і вдосконалення інформаційне законодавство як окрема галузь, що об'єднує у собі самостійні правові інститути. Тому й надалі актуальною залишається розробка та впровадження нових законодавчих актів, спрямованих на врегулювання статусу суб'єктів правовідносин у мережі Інтернет, а для цього необхідно ввести в дію Інформаційний кодекс України. В цьому кодексі необхідно визначити та уніфікувати загальні положення інформаційного законодавства, а також засади та норми регулювання інформаційних відносин у різних галузях суспільної діяльності. Це сприятиме побудові в Україні розвинутого інформаційного суспільства як органічного сегменту глобального інформаційного співтовариства, забезпеченню реалізації конституційних прав на свободу слова та вільний доступ до інформації, що становить суспільний інтерес, а також до публічної інформації, розвитку національних інформаційних ресурсів та інфраструктури, впровадженню новітніх інформаційних технологій тощо. Вирішення цих питань дасть змогу забезпечити реальне здійснення передбаченого Конституцією України права людини на свободу слова.

---

[48] Боднар Ю. Свобода слова: історичний аспект і розуміння в контексті формування сучасної демократичної політичної культури / Ю. Боднар // Освіта регіону. Політологія, психологія, комунікації. - Київ, 2011. - №4. - С.199-202.

Войтович Романа Ярославівна
студентка групи ПР-14 1 курсу навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника» (науковий керівник: викл. Федорончук А.В.).

ІНФОРМАЦІЙНА БЕЗПЕКА: ПІДХОДИ ДО ВИЗНАЧЕННЯ ПОНЯТТЯ

Розуміння поняття «інформаційна безпека» є важливим завданням наукового аналізу. Сутність самого поняття проявляється у вираженні родового поняття, а таким є поняття безпеки, яке в широкому розумінні характеризується як певний процес управління загрозами та небезпеками. «Інформаційна безпека», відповідно, означає процес управління загрозами та небезпеками в інформаційному полі [49].

Інформаційна безпека являє собою одне з найважливіших понять у науці і різних сферах людської діяльності.

Аналіз поняття «інформаційна безпека» передбачає розгляд сукупності таких чинників:

- потреби громадян, суспільства, держави і світового співтовариства;
- вплив інформаційних технологій на індивідів, суспільство і державу;
- наявність загроз і небезпек, якими повинна управляти система забезпечення інформаційної безпеки.

Осягнення сутності змісту поняття «інформаційна безпека» є важливим завданнями наукового аналізу. Будь-яке вчення лише тоді досягає зрілості і досконалості, коли розкриває сутність досліджуваних явищ, має можливість передбачати майбутні зміни не лише у сфері явищ, а й у сфері сутностей. Пізнання сутності інформаційної безпеки можливо лише на основі абстрактного мислення, створення теорії досліджуваного предмета, усвідомлення внутрішнього змісту,

[49] Конституція України. Прийнята Верховною Радою України 28 червня 1996 року // Відомості Верховної Ради України. – 1996. - №30 – ст. 141

виявлення характерних ознак, розкриття сутнісних характеристик поняття, що досліджується.

В історичному процесі складається структура предмета, тобто єдність внутрішнього змісту і зовнішніх проявів, співпадаючих і неспівпадаючих суперечливих сутностей. Сутність — сукупність глибинних зв'язків , відносин і внутрішніх законів, які визначають основні риси і тенденції розвитку системи. Сутність може вважатися пізнаною, коли відомі причини виникнення і джерела розвитку розглядуваного об'єкта, шляхи його формування або технічного репродукування, якщо в теорії або на практиці створена його достовірна модель. Одна й та сама сутність може мати множину різних явищ. Сутність проявляється і осягається в порівнянні яке виражає родове поняття. Таким щодо інформаційної безпеки є поняття безпеки, яке характеризує певний процес управління загрозами та небезпеками. Відповідно видове поняття «інформаційна безпека» означає процес управління загрозами та небезпеками в інформаційній сфері. Саме тому інформаційна безпека є невід'ємною частиною загальної безпеки, чи то національної, чи то регіональної, чи то міжнародної.

Поняття «інформаційна безпека» з'явилося наприкінці 80-х років у праці німецького вченого Г.Одермана. У ній йдеться про важливий інформаційний компонент у міжнародній безпеці та робиться спроба розглянути проблеми безпеки, які пов'язані з інформаційними загрозами комплексно. А у вітчизняній пресі починаючи з кінці 1991 – початку 1992 року спостерігається тенденція до відкритого дослідження проблеми інформаційної безпеки як окремого питання [50].

Слід зазначити, що у науковій літературі поки бракує єдиного консолідованого погляду на зміст поняття «інформаційна безпека». Так, наприклад, В. Богуш під поняттям інформаційна безпека розуміє стан захищеності інформаційного середовища, який відповідає інтересам держави, за якого забезпечується формування, використання і можливості розвитку незалежно від впливу внутрішніх та зовнішніх інформаційних загроз[51].

---

[50] Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник / Ліпкан В.А., Максименко Ю.Є., Желіховський В.М. – К.: КНТ, 2006. – С.140.

[51] Богуш В. Інформаційна безпека держави / Володимир Богуш. Олександр Юдін; Гол. ред. Ю.О. Шпак. – К.: «МК-Прес», 2005. – С.248.

В. А. Ліпкан зазначає, що інформаційна безпека – це стан захищеності життєво важливих інтересів особи, суспільства та держави, який виключає можливість заподіяння їм шкоди через неповноту, невчасність і недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок поширення законодавчо забороненої чи обмеженої для поширення інформації[52].

На думку Р. Калюжного інформаційна безпека – це стан захищеності інформаційного простору, який забезпечує формування та розвиток цього простору в інтересах особистості, суспільства та держави [53].

Я.М. Жарков під інформаційною безпекою розуміє стан правових норм і відповідних їм інститутів безпеки, які гарантують постійну наявність даних для прийняття стратегічних рішень та захист інформаційних ресурсів країни [54].

На думку Б.А. Кормича інофрмаційна безпека – це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, всього суспільства та держави [55].

О.І. Барановський вважає, що інформаційна безпека – це стан захищеності національних інтересів України в інформаційному середовищі, за якого не допускається (або зводиться до мінімуму)

---

[52] Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник / Ліпкан В.А., Максименко Ю.Є., Желіховський В.М. – К.: КНТ, 2006. – С.148.

[53] Калюжний Р. Питання концепції реформування інформаційного законодавства України / Калюжний Р., Говловський В., Цимбалюк В., Гузалюк М. // Збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». К.: НТУУ «КПІ», Міністерство освіти і науки України, СБУ. – К. – 2000. – С. 17-21.

[54] Жарков Я.М., Бєсєдіна Л.М. Напрямки зовнішнього інформаційно-психологічного впливу на Україну / Жарков Я.М., Бєсєдіна Л.М. // Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка. – 2009. - №19 [Електронний ресурс] Режим доступу: http//www.nbuv.gov.ua / portal / natural / znpviknu / 2009-19 / vip19-21.pdf.

[55] Кормич Б.А. Інформаційна безпека: організаційно-правові основи: навч. Посібник для студ. вищих навч. закл. / Б.А. Кормич. – К.: Кондор, 2004. – С.186.

завдання шкоди особі, суспільству, державі через неповноту, несвоєчасність, недостовірність інофрмації й несанкціоноване поширення та використання, а також через негативний інформаційний вплив та негативні наслідки функціонування інформаційних технологій [56].

На підставі аналізу поняття «інформаційна безпека», ми можемо зробити висновок, що для одних науковців воно відображає стан, для інших процес, діяльність, здатність, систему гарантій, властивість, функцію тощо. Вітчизняні науковці і дослідники пов'язують інформаційну безпеку саме з національною безпекою – як частину з цілим. Її визначають як невід'ємну складову національної безпеки, самостійним напрямком національної безпеки.

На нашу думку, розглядати безпеку лише в якості стану не є доречним, оскільки губиться динамізм як самої безпеки так і тієї системи, для якої безпека виступає функцією її подальшого розвитку та існування.

Саме поняття «процес» відрізняється від поняття «стан», оскільки поняття «процес» означає послідовність станів, зв'язок між стадіями зміни і розвитку. Тобто, на відміну від поняття «стан», поняття «процес» акцентує увагу на моменті спрямованості в зміні об'єкта. Водночас «стан» відображає лише один момент безпеки, а тому не вичерпує її повністю.

Що стосується законодавчого визначення поняття «інформаційна безпека», ми можемо відмітити, що в законах України та відповідних інших нормативно-правових актах досить часто згадується дане поняття, але його визначення закріплене тільки у Законі України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки». Так, Законом України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» запропоноване наступне визначення поняття «інформаційна безпека»: «інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних

[56] Барановський О.І. Фінансова безпека / О.І. Барановський. – К.: Фенікс, 1999. – С.212.

технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» [57].

Отже, проаналізувавши різні підходи до визначення поняття «інформаційна безпека» ми можемо зрозуміти недоцільність обрання тієї чи іншої позиції. Вищевказані підходи до визначення поняття інформаційна безпека дають можливість зрозуміти це явище комплексно і системно. Крім того, ми вважаємо, що інформаційна безпека не може розглядатися лише у якості окремого стану. Вона є властивістю та атрибутом інформаційного суспільства, діяльністю та результатом діяльності людини, яка спрямована на забезпечення безпеки в інформаційній сфері. Інформаційна безпека є не станом, а являється процесом, оскільки вона повинна враховувати майбутнє. Разом з тим, об'єктами інформаційної безпеки є людина, суспільство та держава, а суб'єктами – інформація у всіх її проявах, джерела інформації, механізми та засоби її створення, доступу і розповсюдження та наслідки її використання, а також установчі і регуляторні нормативно-правові та адміністративно-організаційні норми і правила, які визначають порядок їх формування, використання та припинення дії.

[57] Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 р. №537-V // Відомості Верховної Ради України. – 2007. - №12. – Ст. 102.

НАПРЯМОК ІІІ. ІНФОРМАЦІЙНІ ВІДНОСИНИ В СУЧАСНОМУ СУСПІЛЬСТВІ ТА ЇХ ВПЛИВ НА ПУБЛІЧНЕ УПРАВЛІННЯ ДЕРЖАВИ

Федорончук Андрій Володимирович
викладач кафедри конституційного, міжнародного та адміністративного права навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника», кандидат юридичних наук.

ОКРЕМІ АСПЕКТИ ДІЯЛЬНОСТІ МІНІСТЕРСТВА ІНФОРМАЦІЙНОЇ ПОЛІТИКИ УКРАЇНИ ЩОДО ГАРАНТУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Згідно ст. 17 Конституції України, захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу [58].

Значення інформаційної безпеки держави важко переоцінити, оскільки ми продовжуємо жити в умовах інформаційної війни. Війни, головним завданням якої є вплив на свідомість громадян з метою розпалювання національної і релігійної ворожнечі, пропаганди дозволених агресивних дій, зміни конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України. Тому, суб'єкти реалізації державної інформаційної політики, інститути громадянського суспільства та кожен із нас, повинні зробити все для того, щоб правда про агресію Російської Федерації відносно нашої держави була почута.

Держава посідає особливе місце як серед суб'єктів державної інформаційної політики, так і серед суб'єктів забезпечення інформаційної безпеки, оскільки вона володіє унікальними засобами і

[58] Конституція України. – С.: ТОВ «ВВП Нотіс», 2017 – 56 с.

силами протидії загрозам у даній сфері [59]. Загальна структура державної системи забезпечення інформаційної безпеки включає чотири основні владні підсистеми, що утворюють гілки влади, які різняться функціями у сфері забезпечення інформаційної безпеки відповідно до компетенції: голови держави, законодавча влада, виконавча влада, судова влада [60]. У доповіді свою увагу ми приділимо діяльності органів виконавчої влади, а саме Міністерства інформаційної політики України.

Реалізацію державної політики в означеній сфері покладено на центральний орган виконавчої влади – Міністерство інформаційної політики України (далі – МІП), який з 2015 року є головним органом у забезпеченні інформаційної безпеки держави. Згідно з Положенням про Міністерство інформаційної політики України, основним завданням МІП є забезпечення формування та реалізація державної політики у сферах інформаційного суверенітету України та інформаційної безпеки, зокрема з питань поширення суспільно важливої інформації в Україні та за її межами [61]. Разом з тим, згідно Закону України «Про національну безпеку України» МІП не є складовою частиною сектору безпеки і оборони держави [62].

Незважаючи на те, що Міністерство інформаційної політики України існує всього лише декілька років, воно було об'єктом дисертаційного дослідження проведеного Бериславською О. М.

---

[59] Михайлов А.О. Оптимізація причинно-наслідкового зв'язку функцій держави та механізмів державного управління в Україні: автореферат дис. … канд. наук з держ. упр.: 25.00.02 / А.О. Михайлов; Акад. муніц. Управління. – К., 2015. – 20 с.

[60] Опанасенко Я.О. Роль і місце організаційної, соціальної й інформаційної складових у реалізації державної регіональної політики в умовах невизначеності регіонів / А.Л. Помаза-Пономаренко, Р.Т. Лукиша, Я.О. Опанасенко // Вісник Національного університету цивільного захисту України (Серія: Державне управління), 2016. - №1 (4). – С. 203-209.

[61] Положення про Міністерство інформаційної політики України, затверджене постановою Кабінету Міністрів України від 14.01.2015 №2 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2-2015-%D0%BF

[62] Про національну безпеку України: Закон України від 21.06.2018 №2469-VIII [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19

(12.00.07 – адміністративне право і процес; фінансове право; інформаційне право) на тему: «Адміністративно-правовий статус Міністерства інформаційної політики України» 2017 рік, а також дисертаційного дослідження проведеного Антонюком В. В. (25.00.02 – механізми державного управління) на тему: «Організаційно-правові засади формування та реалізації державної політики інформаційної безпеки України» 2017 рік.

Варто зазначити, що одним із успіхів діяльності МІП є ухвалення Доктрини інформаційної безпеки України. Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» введено в дію указом Президента України від 25 лютого 2017 року №47/2017. Метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни. Проте, чи вироблені на сьогодні організаційно-правові механізми, завдяки яким положення Доктрини можна було б втілювати в життя?

14 червня 2019 року українське суспільство сколихнула звістка про те, що новим власником телеканалу «ZIK» став Тарас Козак, який є народним депутатом VIII-го скликання Верховної Ради України від фракції «Опозиційний блок» та правою рукою Віктора Медведчука (проросійський політик та член партії «Опозиційна платформа - «За життя»). Як відомо Тарас Козак 5 жовтня 2018 року викупив телеканал «NewsOne» (провідний проросійський телеканал, який дуже прихильно ставиться до політики Кремля та агресії Росії в Україні), а 14 грудня 2018 року став власником телеканалу «112 Україна» (саме Віктора Медведчука найчастіше показують в ефірі цього телеканалу) [63].

Таким чином, Віктор Медведчук фактично контролює вже три інформаційні телеканали, які пропагують ідеї «руского міра», ідеї близькі Путіну. Зрозуміло, що в умовах демократії добро і зло має рівні умови на розвиток. Але, якщо таке зло підриває основоположні засади розбудови української державності, тоді його слід поміщати у певні рамки, рамки визначені законом і підкріплені адекватним реагуванням на відповідні загрози і виклики органів державної влади.

---

[63] Які канали перебувають під контролем Медведчука [Електронний ресурс]. – Режим доступу: https://24tv.ua/yaki_kanali_perebuvayut_pid_kontrolem_medvedchuka_n1166693

Першою на цю подію, зрозуміло відреагувала журналістська спільнота, а саме Медіарух «Журналісти за усвідомлений вибір» у заяві до Національної ради України з питань телебачення і радіомовлення, Служби безпеки України, Президента України та усієї української влади [64]. Також, голова Антимонопольного комітету України заявив, що буде проведено перевірку інформації щодо купівлі телеканалу, адже сторони угоди не зверталися до комітету за узгодженням. Це можливо лише коли сума угоди не перевищує 4 млн. євро [65]. Нагадаємо, що саме Антимонопольний комітет України має здійснювати контроль за дотриманням законодавства про захист економічної конкуренції.

Також, з приводу цієї ситуації мала б бути відповідна реакція правоохоронних органів держави, зокрема Служби безпеки України. Адже саме Служба безпеки України згідно Закону України «Про Службу безпеки України» наділена повноваженнями щодо здійснення профілактики, виявлення, припинення та розкриття кримінальних правопорушень у сфері інформаційної безпеки держави. Окрім того, Національна рада України з питань телебачення і радіомовлення має здійснювати постійний офіційний моніторинг телепрограм на відповідність українському законодавству.

Згідно п. 4 Доктрини інформаційної безпеки України, актуальними загрозами національним інтересам та національній безпеці України в інформаційній сфері є інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах та недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України

---

[64] Зосередження каналів у руках оточення Віктора Медведчука – загроза для національної безпеки та інформаційного простору України [Електронний ресурс]. – Режим доступу: https://cedem.org.ua/news/zoseredzhennya-kanaliv-u-rukah-otochennyaviktora-medvedchuka-zagroza-dlya-natsionalnoyi-bezpeky-ta-informatsijnogo-prostoru-ukrayiny/

[65] АМКУ проведе перевірку через купівлю Козаком каналу Zik [Електронний ресурс]. – Режим доступу: https://detector.media/infospace/article/168247/2019-06-19-amkuprovede perevirku-cherez-kupivlyu-kozakom-kanalu-zik/

ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України [66].

З огляду на те, що МІП відповідало за розробку Доктрини, у підсумку на нього було покладено низку зобов'язань щодо організації та забезпечення моніторингу засобів масової інформації та загальнодоступних ресурсів вітчизняного сегмента мережі Інтернет з метою виявлення інформації, поширення якої заборонено в Україні, а також моніторингу загроз національним інтересам і національній безпеці в інформаційній сфері.

Аналізуючи офіційний веб-сайт Міністерства інформаційної політики України [67] та мережу Інтернет, станом на 18 червня 2019 року, ми не знайшли жодної публічної реакції цього відомства щодо купівлі телеканалу «Zik». Що з огляду на положення Доктрини викликає сумніви в ефективності здійснення діяльності МІП у даній сфері.

Як зазначає Володимир Копчак (керівник Південно-Кавказької філії Центру досліджень армії, конверсії та роззброєння): «на п'ятий рік зовнішньої агресії в Україні до кінця не вирішена проблема функціонування в медіа-просторі російських або відверто проросійських ресурсів. Ситуація ускладнюється слабкою позицією державних ЗМІ, в першу чергу, основних державних телеканалів на тлі відсутності «деолігархізації» ключових телевізійних медіа» [68]. Слід доповнити, що ситуація ускладнюється також слабкою позицією (неможливістю своєчасно та адекватно реагувати на загрози та виклики національним інтересам та інформаційній безпеці України) органів державної влади, які наділені повноваженнями щодо гарантування інформаційної безпеки, зокрема Міністерства інформаційної політики України.

---

[66] Доктрина інформаційної безпеки України: затверджена указом Президента України від 25.02.2017 №47/2017 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/47/2017

[67] Офіційний веб-сайт Міністерства інформаційної політики України [Електронний ресурс]. – Режим доступу: https://mip.gov.ua/

[68] «Україна стала полігоном інформаційної війни, яку розв'язав кремль у світовому інформпросторі» - експерт (виступ Володимира Копчака) [Електронний ресурс]. – Режим доступу: https://irrp.org.ua/ukrayina-stala-poligonom-informatsiynoyi-viyni-yaku-rozv-yazav-kreml-u-svitovomu-informprostori-ekspert/

Зважаючи на те, що координацію діяльності органів виконавчої влади щодо реалізації Доктрини та забезпечення національної безпеки в інформаційній сфері має здійснювати Рада національної безпеки і оборони України, саме Міністерство інформаційної політики України у разі виявлення загроз національним інтересам і національній безпеці в інформаційній сфері повинно було звернутися до РНБО із пропозицією скликати засідання для розгляду питання про вплив факту купівлі телеканалу «Zik» проросійськими силами на інформаційну безпеку держави, а не народні депутати України [69]. Станом на 18 червня 2019 року, засідання РНБО щодо обговорення цієї ситуації так і не відбулося.

Важливо зазначити, що за своєю правовою сутністю Доктрина не є нормативним актом прямої дії, який регулює виключно всі аспекти діяльності щодо забезпечення інформаційної безпеки. Вона окреслює стратегічні питання, а центральні органи виконавчої влади, зокрема Міністерство інформаційної політики України, структури сектору безпеки та оборони мають деталізувати та конкретизувати її положення в інших нормативних документах.

Як зазначає низка експертів з інформаційної безпеки: «Доктрина має винятково декларативний характер. Для того, щоб Доктрина запрацювала потрібно трансформувати її в конкретні механізми і закони» [70].

І дійсно, ми можемо відмітити відсутність у Доктрині реально працюючих механізмів координації діяльності у сфері інформаційної безпеки. Безумовно, необхідність централізації діяльності, дієвих алгоритмів координації та контролю в тексті Доктрини задекларовані (п. 6 Механізм реалізації Доктрини). Але, з іншого боку, механізми зазначеного не прописані. Міністерство інформаційної політики в такій ситуації не може виконувати ті завдання, які визначені для нього у

---

[69] Від Зеленського вимагають скликати засідання РНБО через купівлю кумом Путіна ще одного телеканалу в Україні [Електронний ресурс]. – Режим доступу: http://buknews.com.ua/page/vid-zelenskoho-vymahayut-sklykaty-zasidannia-rnbo-cherez-kupivlyu-kumom-putina-shche-odnoho-telekanalu-v-ukraini.html

[70] Тарасенко Н. Доктрина інформаційної безпеки України в оцінках експертів [Електронний ресурс] / Н. Тарасенко // Резонанс. – 2017. - №18. – С. 3-14. – Режим доступу: http://nbuviap.gov.ua/images/rezonans/2017/rez18.pdf.

Доктрині. І якщо МІП серед інших міністерств і відомств виконавчої влади визнано фактично головним суб'єктом забезпечення інформаційної безпеки, то це накладає певні зобов'язання. Особливо щодо проблематики активних заходів інформаційного спротиву, необхідності координації діяльності силових структур. Тобто, одночасно із розробкою проекту Доктрини інформаційної безпеки України одночасно мали бути розроблені зміни у нормативно-правові акти, які визначають правовий статус МІП, зокрема зміни до Положення про Міністерство інформаційної політики України. В якому конкретизувати механізм реалізації положень Доктрини у випадку виявлення загроз національним інтересам і національній безпеці в інформаційній сфері Міністерством інформаційної політики України та механізм взаємодії з правоохоронними органами у зазначеній сфері.

Маємо погодитися, що завдання, які стоять перед МІП можуть бути такими ж, як і завдання правоохоронних органів у сфері захисту інформаційної безпеки. У той же час, повноваження є різними. Так, відповідні структурні підрозділи Служби безпеки України можуть не лише виявляти інформаційні атаки на нашу державу, а й у межах свого відомства проводити досудове розслідування. МІП такими можливостями не наділене, воно не може займатися оперативно-розшуковою діяльністю чи досудовим розслідуванням і в певній частині просто повторює повноваження Служби безпеки України щодо моніторингу.

Отже, на сьогоднішній день для України надзвичайно актуальним є завдання із виявлення та аналізу загроз, які існують в інформаційній сфері. Незважаючи на створення великої системи органів, які покликані гарантувати інформаційну безпеку держави, ми й надалі продовжуємо зіштовхуватися із випадками, коли діяльність цих органів в силу різних причин є малоефективною. Дослідивши окремі аспекти діяльності Міністерства інформаційної політики України можемо відмітити, що є очевидною необхідність удосконалення організаційно-правових механізмів взаємодії даного Міністерства із іншими органами, які мають гарантувати інформаційну безпеку держави. Проте, слід пам'ятати, що наявність у майбутньому цих механізмів не гарантуватиме успіху в інформаційній боротьбі, було б бажання діяти та змінювати ситуацію на користь нашої держави.

Янцаловська Віталіна Олександрівна
Приватний нотаріус Деражнянського районного нотаріального округу Хмельницької області.

КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ В СФЕРІ НОТАРІАТУ УКРАЇНИ

Відповідно до вимог національного, чинного законодавства на нотаріусів, які працюють у державних нотаріальних конторах або займаються приватною нотаріальною діяльністю, законом покладено обов'язок посвідчувати права, а також факти, що мають юридичне значення, та вчиняти інші нотаріальні дії, передбачені законодавцем, з метою надання їм юридичної вірогідності (ст.1 Закону про нотаріат) [1]. Таким чином нотаріуси, несуть величезну відповідальність, адже мають доступ до державних реєстрів, і в зв'язку з цим виникає питання, як себе захистити від кіберзлочинців» та захистити наявну інформацію. Адже ми розуміємо, що механізми, які використовує держава і нотаріуси, не є абсолютно досконалими і тому виникають питання», про важливість синхронності законодавчих і технічних ініціатив для забезпечення належного захисту в сфері нотаріальної діяльності.

Сьогодні не є секретом, що проблеми, які виникають при реєстрації власності та бізнесу – системні, тому потребують системних рішень. За таких обставин необхідно розробити дієві механізми для кращого забезпечення безпеки і якості процесу реєстрації, а головне – один тип даних повинен вноситися з використанням відповідних єдиних правил, і це завдання потрібно вирішувати як найшвидше, а ніж організація ефективного обміну даними.

На мою думку потрібно активніше інтегрувати національне законодавство з міжнародним, особливо практику реалізації позитивного права щодо захисту від кіберзагрози. Так, захищеність нотаріального процесу в Іспанії гарантується тим, **що мережа іспанських реєстрів є локальною, а не використовується через Інтернет, як це в Україні**. Саме в цьому напрямку держава повинна вжити реальні та дієві заходи щодо забезпечення нам, нотаріусам здійснювати реєстри відповідних документів у локальній мережі і цим здійснити заслін від незаконного впливу хакерів, а чи інших шахраїв.

Правда, комісія Нотаріальної Палати України з питань запобігання та протидії кіберзлочинності постійно привертає до проблем забезпечення кібербезпеки робочого місця нотаріуса, зокрема, розроблено рекомендації для нотаріусів на випадок критичних ситуацій. Однак, технологічний прогрес наразі дуже стрімкий, хакери постійно вдосконалюють свої навички та засоби, тому часто законодавець не встигає адекватно відреагувати на потреби часу. Наприклад, державний реєстратор зараз не має повноважень скасувати незаконну дію в реєстрі, а може лише звернутися до правоохоронних органів, але за час проведення розслідування відповідне майно залишається незахищеним. Фактично, ми жодним чином не маємо права вплинути на прискорення процедури слідства. Виходить що нотаріус, самотужки, повинен здійснювати превентивний захист своїх професійних повноважень від кіберзлочинців.

Окрім того, беззаперечним залишається той факт, що ми нотаріуси не досить обізнані в технологічних нюансах кібербезпеки, тому виникає ряд проблем, для вирішення яких нотаріальній спільноті, державним органам та IT-компаніям необхідно терміново шукати спільні рішення, для виправлення цієї проблеми.

Наступною проблемою у нашій повсякденній роботі, залишається наш захист від кіберзлочинців. Фактично, правоохоронні органи намагаються всі звинувачення спрямувати на нас (нотаріусів).

Отже, безпека – це особиста справа кожного, тому необхідно вжити всіх заходів, аби мати необхідний захист, а саме:

- нотаріус повинен мати належний рівень знать комп'ютерної «гігієни»;
- використовувати лише актуальне і сертифіковане програмне забезпечення;
- обов'язкова наявність антивірусної програми;
- щотижнево змінювати пароль доступу до реєстрів;
- не користуватись ПК, на якому встановлені реєстри, для відвідування будь-яких інших сайтів в мережі, включаючи користування електронною поштою;
- щоденно робити звіт виконаних дій по реєстру.

Це лише короткий перелік необхідних дій, аби хоч якось застерегти себе і свою справу від хакерської атаки та своєчасного її виявлення, у разі, якщо така сталась.

Необхідним та важливим фактором кібербезпеки нотаріату, має бути підтримка з боку держави, а саме прийняття ряду нормативно-правових актів, для забезпечення безпечної роботи реєстрів, одним з яких є запропонована система блокчейн.

Підсумовуючи вищевикладене, необхідно зауважити, що лише особиста свідомість кожного нотаріуса та спільна співпраця МЮУ з Нотаріальною палатою України, можуть дати результат надійного захисту нотаріальної сфери, а отже і надійного захисту інтересів, прав та майна фізичних та юридичних осіб, та й держави в цілому.

Бойцан Любомир Іванович
Студент 2 курсу магістратури, спеціалізація 01 «Публічна служба» навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника,
(наук. керівник: доц. Петровська І.І.).

ПРАВОВИЙ РЕЖИМ ІНФОРМАЦІЇ ПРО КОРУПЦІЙНІ ПРАВОПОРУШЕННЯ

Відповідно до ст. 1 Закону України «Про запобігання корупції»[71] (далі – Закон), корупція - це використання посадовою особою наданих їй службових повноважень або пов'язаних з ними можливостей з метою одержання неправомірної вигоди або прийняття такої вигоди чи прийняття обіцянки / пропозиції такої вигоди для себе чи інших осіб або відповідно обіцянка / пропозиція чи надання неправомірної вигоди посадовій особі, або на її вимогу іншим фізичним чи юридичним особам з метою схилити цю особу до протиправного використання наданих їй службових повноважень або пов'язаних з ними можливостей. Тобто, якщо вам відомо про те, що мали/мають місце такі діяння як отримання посадовцем (будь-який державний службовець, суддя, прокурор, слідчий, працівник поліції, тощо) неправомірної вигоди (грошових коштів, переваг, пільг, тощо); використання посадовцем будь-якого державного чи комунального майна або коштів в приватних інтересах; наявність конфлікту інтересів; порушення обмеження спільної роботи близьких осіб (ст. 27 Закону); порушення обмеження щодо сумісництва та суміщення з іншими видами діяльності а також обмеження після припинення діяльності посадової особи (статті 25, 26 Закону); надання

[71] Про запобігання корупції: Закон України від 14.10.2014 року. URL: https://zakon.rada.gov.ua/laws/show/1700-18

керівництвом незаконних доручень (стаття 44 Закону) варто повідомити про це у встановленому порядку [72], уповноваженим органам.

Спеціально уповноваженим суб'єктам у сфері протидії корупції, а це:

- Органи прокуратури – зокрема, органи Спеціалізованої антикорупційної прокуратури (спочатку треба звертатися до територіальних філій Спеціалізованої прокуратури);
- Національне антикорупційне бюро України (НАБУ);
- Національне агентство з питань запобігання корупції (НАЗК);
- Служба безпеки України (СБУ).

До прокуратури, органів внутрішніх справ, СБУ, НАБУ треба звертатися, коли відомі факти корупційних злочинів або адміністративних правопорушень.

До компетенції та підслідності НАЗК відносять ведення Єдиного державного реєстру декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування, та Єдиного державного реєстру осіб, які вчинили корупційні або пов'язані з корупцією правопорушення; перевірка відповідності декларацій способу життя чиновників; контроль дотримання обмежень щодо фінансування політичних партій; недопущення конфлікту інтересів у чиновників; прийняття повідомлень про можливі випадки корупції; розробка проектів Антикорупційної стратегії та державної програми з її виконання, проектів нормативно-правових актів з цих питань; видання обов'язкових для виконання приписів; здійснення співпраці з викривачами корупції, вжиття заходів щодо їх правового та іншого захисту, притягнення до відповідальності осіб, винних у порушенні цих прав.

Уповноважені на те посадові особи НАЗК складають протоколи у справах про такі адміністративні правопорушення, які передбачені Кодексом України про адміністративні правопорушення (КпАП)[73]: стаття 188-46 «Невиконання законних вимог (приписів) Національного агентства з питань запобігання корупції», стаття 172-4 «Порушення

---

[72] Як, коли і кому повідомити про корупцію (антикорупційний сайт). URL: https://anticorruption.in.ua/instructions/yak-koli-i-komu-povidomiti-pro-koruptsiyu.html

[73] Кодекс України про адміністративні правопорушення. URL: https://zakon.rada.gov.ua/laws/show/80731-10

обмежень щодо сумісництва та суміщення з іншими видами діяльності»; стаття 172-5 «Порушення встановлених законом обмежень щодо одержання подарунків»; стаття 172-6 «Порушення вимог фінансового контролю»; стаття 172-7 «Порушення вимог щодо запобігання та врегулювання конфлікту інтересів»; стаття 172-8 «Незаконне використання інформації, що стала відома особі у зв'язку з виконанням службових повноважень»; стаття 172-9 «Невжиття заходів щодо протидії корупції»; стаття 212-15 «Порушення порядку надання або отримання внеску на підтримку політичної партії, порушення порядку надання або отримання державного фінансування статутної діяльності політичної партії, порушення порядку надання або отримання фінансової (матеріальної) підтримки для здійснення передвиборної агітації або агітації з всеукраїнського або місцевого референдуму»; стаття 212-21 «Порушення порядку подання фінансового звіту про надходження і використання коштів виборчого фонду, звіту партії про майно, доходи, витрати і зобов'язання фінансового характеру».

Компетенція НАБУ:

- вживає заходів щодо розшуку та арешту коштів та майна, які можуть бути предметом конфіскації, або спеціальної конфіскації у кримінальних правопорушеннях, віднесених до його підслідності,

- здійснює оперативно-розшукові заходи і досудове розслідування кримінальних правопорушень, віднесених до його підслідності (ст. 216 Кримінального процесуального кодексу).

У підслідності НАБУ статті 191, 206-2, 209, 210, 211, 354, 368, 368-2, 369, 369-2, 410, Кримінального кодексу України (ККУ).

Уповноважені на те посадові особи НАБУ складають протоколи у справах про адміністративне правопорушення, яке передбачене статтею 185-13 КпАП «Невиконання законних вимог посадових осіб Національного антикорупційного бюро України».

Інші органи та організації, яким можна повідомити про факти корупції

Уповноважені підрозділи з питань запобігання та виявлення корупції органів державної влади

До зазначених підрозділів слід звертатись у випадку, якщо корупційне правопорушення стосується посадових чи службових осіб, які працюють у органах влади. Керівники підприємств, установ, організації незалежно від підпорядкованості та форми власності, якщо корупційне правопорушення стосується робітників цих підприємств.

Звернутись необхідно у письмовій формі. У заяві необхідно у довільній формі викласти всі відомі Вам факти корупційного

порушення. При наявності до заяви можна прикласти докази на підтвердження викладених у ній обставин. Фактами, що вказують на наявність корупційного правопорушення, можуть бути документи, що підтверджують витрачання коштів, посилання на журналістські розслідування у пресі, аудіо- чи відеозаписи, Ваші власні розслідування тощо.

Михаць Олег Володимирович
Студент 4 курсу групи ПР-42 навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника»,
(науковий керівник: доц. Петровська І.І.).

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПРИ НАДАННІ АДМІНІСТРАТИВНИХ ПОСЛУГ

Широке використання досягнень інформаційно-комунікаційних технологій у сфері публічної адміністрації розглядається як необхідний компонент розвитку електронного урядування. Сучасний стан надання адміністративних послуг в електронній формі характеризується певними зрушеннями. Новації українського законодавства свідчать про підвищення уваги держави до формування інформаційного суспільства в Україні, розширення сфери застосування інформаційно-комунікаційних технологій у публічному секторі тощо. Однак розвиток електронного врядування в Україні, у тому числі надання адміністративних послуг в електронній формі, стримується наявністю великої кількості проблем правового, організаційного й матеріального-технічного характеру.

Наведене зумовлює актуальність дослідження надання адміністративних послуг в електронній формі з урахуванням досвіду країн Європейського Союзу, що сприятиме підвищенню якості надання адміністративних послуг населенню та адаптації українського законодавства до законодавства ЄС.

Метою доповіді є визначення сучасного стану правового регулювання та практики надання адміністративних послуг із застосуванням інформаційних технологій та з урахуванням останніх новацій українського законодавства, а також виокремлення основних

перспектив розвитку системи електронних адміністративних послуг з огляду на позитивний досвід країн Європейського Союзу.

1.Правове забезпечення надання адміністративних послуг із застосуванням інформаційних технологій

Правові передумови запровадження електронного врядування й надання адміністративних послуг органами державної влади в Україні із застосуванням інформаційних технологій обумовлені прийняттям Закону України «Про електронні документи та електронний документообіг» від 22 травня 2003 року № 851-IV, Закону України «Про електронний цифровий підпис» від 22 травня 2003 року № 852-IV й Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 9 січня 2007 року № 537-V.

На виконання вимог зазначених Законів прийнято велику кількість підзаконних нормативно-правових актів, зокрема Постанови Кабінету Міністрів України: «Про заходи щодо створення електронної інформаційної системи «Електронний уряд» від 24 лютого 2003 року № 208, «Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади» від 28 жовтня 2004 року № 1453, «Про електронний обмін службовими документами в органах виконавчої влади» від 17 липня 2009 року № 733, а також Розпорядження Кабінету Міністрів України: «Про схвалення Концепції розвитку електронного урядування в Україні» від 13 грудня 2010 року № 2250-р, «Про схвалення Концепції Державної цільової програми створення та функціонування інформаційної системи надання адміністративних послуг на період до 2017 року» від 24 липня 2013 року № 614-р, «Про затвердження Плану дій із впровадження Ініціативи «Партнерство «Відкритий Уряд» у 2014–2015 роках» від 26 листопада 2014 року № 1176-р тощо.

На окрему увагу заслуговує Розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку системи електронних послуг в Україні» від 16 листопада 2016 року № 918-р, де надано визначення поняття «електронна послуга», що розглядається як адміністративна й інша публічна послуга, яка надається суб'єкту звернення в електронній формі за допомогою засобів інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем [74].

[74] Кодекс адміністративного судочинства України від 06.07.2005 р. № 2747-IV [Електрон. ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2747- 15/print1370431715462163.

Отже, сфера застосування Концепції стосується надання публічних послуг, що є ширшим поняттям, ніж адміністративні послуги, оскільки останні розглядаються як різновид публічних послуг.

Однак зазначеним Розпорядженням Кабінету Міністрів України «Про схвалення Концепції розвитку системи електронних послуг в Україні» від 16 листопада 2016 року № 918-р основну увагу приділено саме забезпеченню надання адміністративних послуг в електронній формі та не враховано створення передумов для надання інших публічних послуг в електронній формі. Про зазначене свідчать, зокрема, визначені напрями реалізації Концепції розвитку системи електронних послуг в Україні. Порядок реалізації зазначених напрямів сфокусований виключно на формуванні передумов для надання саме адміністративних послуг в електронній формі й не враховує широкого спектру інших видів публічних послуг і забезпечення їх надання в електронні формі.

Сьогодні в Україні створено велику кількість електронних порталів надання адміністративних послуг, зокрема на загальнодержавному рівні функціонує «Кабінет електронних сервісів» і нещодавно запрацював «Он-лайн будинок юстиції», які забезпечують надання електронних адміністративних послуг Міністерства юстиції України, а також працює портал «Електронні сервіси», що забезпечує надання електронних адміністративних послуг Державною фіскальною службою України. Окремі електронні адміністративні послуги Державної служби України з питань геодезії, картографії та кадастру надаються через розроблений із цією метою «Електронний сервіс».

На регіональному рівні органами місцевого самоврядування та місцевими органами виконавчої влади утворюються окремі електронні портали (сервіси) надання адміністративних послуг, наприклад, Регіональний віртуальний офіс електронних адміністративних послуг Дніпропетровської області, окремі адміністративні послуги в електронній формі надаються через веб-сайт Центру надання адміністративних послуг м. Івано-Франківськ тощо.

Як недержавний проект функціонує Портал державних послуг iGov.org.ua.

Відповідно до положень Закону України «Про адміністративні послуги» в редакції, що діяла до 10 грудня 2015 року, надання адміністративних послуг в електронній формі передбачалося здійснювати виключно через Єдиний державний портал адміністративних послуг. Однак Законом України «Про внесення змін до деяких законодавчих актів України щодо розширення повноважень органів місцевого самоврядування та оптимізації надання

адміністративних послуг» від 10 грудня 2015 року № 888-VIII установлено, що адміністративні послуги в електронній формі надаються через Єдиний державний портал адміністративних послуг, у тому числі через інтегровані з ним інформаційні системи державних органів та органів місцевого самоврядування. Хоча окремі електроні сервіси надання адміністративних послуг розпочали свою роботу до прийняття вказаного Закону, зокрема «Кабінет електронних сервісів».

На виконання вимог указаного Закону України від 10 грудня 2015 року № 888-VIII спільним Наказом Міністерства економічного розвитку і торгівлі України й Міністерства регіонального розвитку, будівництва та житлово-комунального господарства України від 8 вересня 2016 року № 1501/248 затверджено Порядок інтеграції інформаційних систем державних органів та органів місцевого самоврядування до Єдиного державного порталу адміністративних послуг, у якому встановлено вимоги до процедури інтеграції інформаційних систем державних органів та органів місцевого самоврядування до Єдиного державного порталу адміністративних послуг з метою забезпечення надання адміністративних послуг в електронній формі за принципом «єдиного вікна» [75].

2.Єдиний державний портал адміністративних послуг

Єдиний державний портал адміністративних послуг створено на вимогу Закону України «Про адміністративні послуги». Ведення Єдиного державного порталу адміністративних послуг здійснюється відповідно до Порядку затвердженого постановою Кабінету Міністрів України від 3 січня 2013 р. № 13.

Цілі Порталу:

- впорядкування та надання вичерпної інформації про адміністративні послуги;
- надання адміністративних та інших публічних послуг в електронному вигляді.

Функціональні елементи

Персональний кабінет – створюється для одержувачів послуг та використовується як механізм спілкування між заявником та надавачем послуг.

---

[75] Про схвалення Концепції розвитку системи електронних послуг в Україні : Розпорядження Кабінету Міністрів України від 16 листопада 2016 року № 918-р // Офіційний вісник України. – 2016. – № 99. – С. 259.

Ідентифікація – процедура розпізнавання особи. На даному етапі буде використовуватись електронний цифровий підпис. З часом доступними стануть різні методи ідентифікації, по мірі технічної та юридичної готовності.

Подача документів – форми заяв та документи подаються в електронному вигляді. Електронний підпис засвідчує автентичність документів.

Отримання послуги - відбуватиметься в персональному кабінеті шляхом надання результату послуги в електронному вигляді.

Зворотній зв'язок здійснюється через електронну пошту заявника.

Етапи розвитку Порталу:

- Робота Порталу в інформаційному режимі та забезпечення вичерпної інформації про:

о адміністративну послугу

о список, шаблони та зразки документів необхідних для отримання послуги

о контактну інформацію та місце отримання послуги

- Надання послуг в електронному вигляді:

о Послідовне впровадження послуг в електронному вигляді (по мірі готовності суб'єктів надання)

о Розширення способів ідентифікації одержувачів послуг

о Впровадження механізмів сплати за послуги

3.Європейський досвід надання адміністративних послуг із застосуванням інформаційно-комунікативних технологій

Аналізуючи досвід держав-членів ЄС у досліджуваній сфері, варто зазначити, що надання адміністративних послуг в електронній формі зазвичай відбувається через єдині он-лайн сервіси, на яких зібрана велика кількість популярних електронних послуг як для громадян, так і для бізнесу. Надання електронних послуг на загальнодержавному рівні за допомогою єдиного веб-порталу сприяє підвищенню зручності пошуку необхідної послуги й уніфікації вимог для отримання подібних послуг, незалежно від органу державної влади, який надає ці послуги. Однак на локальному рівні органи місцевого самоврядування створюють можливості щодо надання додаткових адміністративних послуг, що належать до їхньої компетенції і здійснюється з урахуванням місцевих особливостей і потреб.

Надання електронних адміністративних послуг характеризується популярністю серед громадян ЄС, зокрема у Великобританії портал надання електронних послуг загалом на рік відвідує понад сімдесят

мільйонів користувачів [76], у Норвегії до загальнодержавного порталу надання послуг адміністративними органами здійснено понад сто десять мільйонів звернень [77].

Отже, європейський досвід надання послуг адміністративними органами із застосуванням інформаційних технологій свідчить про те, що більшість послуг надаються через єдиний загальнодержавний веб-портал надання адміністративних послуг та інтегровані до нього веб-портали надання адміністративних послуг місцевих органів влади, які розробляються з подібним інтерфейсом і зовнішньою архітектурою сайту, що сприяє легкому орієнтуванню споживачів послуг у пропонованих можливостях порталу надання адміністративних послуг і спрощує процедуру отримання необхідної послуги.

Створення в Україні окремих електронних сервісів, які забезпечуватимуть надання адміністративних послуг органами державної влади й місцевого самоврядування, є позитивним явищем на початковому етапі реформування системи електронних адміністративних послуг. Ураховуючи європейський досвід організації системи електронних адміністративних послуг, кінцевою метою розвитку їх надання стала інтеграція окремих електронних сервісів надання адміністративних послуг у єдиний загальнодержавний веб-портал, функції якого взяв на себе Єдиний державний портал адміністративних послуг.

Надання певних адміністративних послуг із застосуванням інформаційних технологій за допомогою офіційних веб-сайтів органів державної влади або через окремі веб-портали надання електронних адміністративних послуг також не видавалося доцільним із погляду необхідності інтеграції процедур надання адміністративних послуг в електронній формі, створювало передумови для розпорошеності інформації про електронні адміністративні послуги, тягнуло за собою додаткові витрати бюджетних коштів на створення нових веб-ресурсів, що забезпечували їх надання, викликало необхідність у додатковій електронній ідентифікації споживачів послуг тощо.

---

[76] Про адміністративні послуги : Закон України від 06.09.2012 р. № 5203-VI [Електрон. ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/5203-17.

[77] Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI [Електрон. ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2939- 17/print1370431715462163.

4.Надання транскордонних адміністративних послуг у країнах ЄС

Реалізація Концепції розвитку системи електронних послуг в Україні передбачена на період до 2020 року, її кінцевою метою є забезпечення надання електронних послуг у всіх сферах суспільного життя, надання інтегрованих електронних послуг, а також запровадження транскордонних електронних послуг.

Натепер правове регулювання надання транскордонних адміністративних послуг в Україні відсутнє, однак інтеграція України до ЄС, адаптація українського законодавства до законодавства держав-членів ЄС зумовлює необхідність розвитку зазначеного інституту і створення як правових, так організаційних передумов його впровадження в практичну діяльність органів публічної адміністрації.

Як зазначається в юридичній літературі, «сучасним напрямом реформування надання електронних послуг у ЄС є передусім створення єдиного цифрового ринку публічних послуг. Зважаючи на те, що ринок електронних публічних послуг у країнах ЄС стрімко розвивається, важливим завданням на сьогодні видається забезпечити сумісність між системами надання електронних публічних послуг різних країнчленів» [78].

Надання транскордонних адміністративних послуг у країнах ЄС передбачено Регламентом Європейського Парламенту й Ради «Про електронну ідентифікацію і трастові послуги для електронних угод на внутрішньому ринку і скасування Директиви 1999/93/ЕС» від 23 липня 2014 року № 910/2014, Рішенням Європейського парламенту й Ради «Про створення програми сумісності рішень і загальних рамок для європейських публічних адміністрацій, підприємств і громадян (ISA2 програма) в якості засобу для модернізації публічного сектору» від 25 листопада 2015 року № (ЄС) 2015/2240 тощо.

На виконання вимог зазначених нормативно-правових актів у ЄС запроваджена програма «STORK», яка «з урахуванням технології ІД-ідентифікації є доступною в кожній країні й забезпечує систематизацію даних згідно із загальноприйнятою технічною та

[78] Про державну реєстрацію речових прав на нерухоме майно та їх обтяжень : Закон України від 1 липня 2004 року № 1952-IV // Голос України. – 2004. – № 142. – С. 9–12.

юридичною схемами, що забезпечує розуміння між користувачами один із одним»[79].

Окрім того, з метою надання транскордонних електронних послуг у ЄС працює електронний сервіс «SPOCS (Simple Procedures Online for Cross-Border Services)», що забезпечує здійснення простих он-лайн процедур для транскордонних послуг, електронний портал "e-CODEX (e-Justice Communication via Online Data Exchange)", створений з метою забезпечення електронної взаємодії у сфері юстиції через он-лайн обмін даними, а також програма «epSOS», що забезпечує доступ до транскордонних послуг у сфері охорони здоров'я, та електронний сервіс «PEPPOL (Pan-European Public Procurement Online)», запроваджений з метою он-лайн доступу до публічних закупівель.

Сучасний стан надання транскордонних послуг адміністративними органами в країнах ЄС характеризується об'єднанням окремих електронних сервісів надання зазначених послуг у єдиний веб-портал, функції якого забезпечуватимуть надання широкого спектру публічних послуг в електронній формі на території всього ЄС. Зокрема, на цей момент розробляється портал «e-SENS (Electronic Simple European Networked Services)», що об'єднуватиме функції вищезазначених електронних сервісів та «утворюється з метою забезпечення надання транскордонних публічних послуг в електронній формі за допомогою загальних і повторно використовуваних технічних компонентів»[80].

Отже, основу розв'язання проблем надання адміністративних послуг із застосуванням інформаційних технологій покладений комплексний підхід, що включає широкий спектр заходів, а саме:

- удосконалення чинного законодавства, у тому числі закріплення еквівалентності юридичної сили результатів надання адміністративних послуг в електронній формі й письмовій формі на паперових носіях в єдиному законодавчому актів щодо регулювання адміністративних процедур;

---

[79] Про засади державної регуляторної політики у сфері господарської діяльності : Закон України від 11.09.2003 р. № 1160-IV [Електрон. ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/1160-15.

[80] Про заходи щодо впровадження Концепції адміністративної реформи в Україні : Указ Президента України від 22.07.1998 р. № 810/98 [Електрон. ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/810/98/print1366915713988680.

- формування механізмів ефективної взаємодії та інтеграції інформаційних систем органів державної влади й органів місцевого самоврядування на базі Єдиного державного порталу надання адміністративних послуг;

- широке інформування споживачів адміністративних послуг про можливість отримати їх в електронній формі та розроблення заходів заохочення отримувати послуги саме в електронній формі;

- розроблення ефективних механізмів електронної ідентифікації й автентифікації споживачів адміністративних послуг в електронній формі з метою безпечного користування електронними сервісами надання адміністративних послуг;

- створення правових і організаційних передумов для надання органами публічної адміністрації транскордонних адміністративних послуг;

- приділення достатньої уваги спеціальному навчанню й перекваліфікації державних службовців та інших осіб, які надають адміністративні послуги на підставі закону.

Московчук Ірина Ярославівна
Студентка 1 курсу групи ПР-15, навчально-наукового юридичного інституту, ДВНЗ «Прикарпатський національний університет імені Василя Стефаника»,
(наук. керівник: викл. Федорончук А.В.).

ОКРЕМІ ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

В умовах сучасних глобальних та регіональних інформаційних протистоянь, деструктивних комунікативних впливів, зіткнення різновекторних національних інформаційних інтересів, поширення інформаційної експансії та агресії, захист національного інформаційного простору та гарантування інформаційної безпеки стають пріоритетними стратегічними завданнями сучасних держав у системі глобальних інформаційних відносин. Збереження інформаційного суверенітету, формування ефективної системи безпеки в інформаційній сфері є актуальною проблемою і для України, яка часто є об’єктом зовнішньої інформаційної експансії, маніпулятивних

пропагандистських технологій та руйнівного інформаційного вторгнення [81].

Під інформаційною безпекою держави слід розуміти такий стан інформаційного простору держави, при якому гарантується захищеність від будь-яких загроз. Інформаційна безпека в загальній системі національної безпеки України посідає особливе місце. З урахуванням темпів інформатизації та розвитку інформаційних технологій, широкого втілення таких технологій у виробництво, оборону, науку, освіту тощо, інформаційна діяльність стає обов'язковим і, часто-густо, вирішальним елементом усіх сфер діяльності суспільства, тому інформаційна безпека є елементом всіх складових національної безпеки країни. В цих умовах проблема інформаційної безпеки все більше набуває самостійного суспільного значення. У той же час система зовнішніх і внутрішніх загроз інформаційній безпеці носить комплексний характер і здійснення цих загроз має на меті нанесення збитків у політичній, економічній, соціальній, військовій, екологічній, науково-технічній сферах.

Безумовно інформаційна безпека відіграє одну з ключових ролей у забезпеченні життєво важливих інтересів країни. «Це в першу чергу обумовлено швидким розвитком сучасних інформаційно-телекомунікаційних технологій, засобів зв'язку й інформатизації і, як наслідок,-істотним зростанням впливу інформаційної сфери на життя нашого суспільства. У сучасному світі інформація стає стратегічним національним ресурсом - одним з основних багатств економічно розвинутої держави, головним джерелом економічної і військової мощі держави. Національний інформаційний ресурс повинен стати одним із вирішальних ресурсів розвитку країни, привабливою сферою вкладення капіталів суб'єктів господарської діяльності» [82]. Зокрема, причинами невдач України в перші місяці гібридної війни, значною мірою є невдачі на інформаційному фронті.

Упродовж останніх десятиліть невід'ємним складником будь-якого збройного конфлікту є інформаційні війни. Характер та

---

[81] Дмитренко М. А. Політична система України: розвиток в умовах глобалізації та інформаційної революції: [монографія] / М. А. Дмитренко ; Нац. пед. ун-т ім. М. П. Драгоманова, Ін-т дослідж. пробл. держ. безпеки. – 2-ге вид., допов. та переробл. – К. : Ун-т «Україна», 2011. – С.630.

[82] Домарев В. Безпека інформаційних технологій. – К.: «Діа Софт», 2003. – С.130.

особливості ведення російсько-української війни свідчать, що її метою є зміна самоідентифікації населення і перетворення східного регіону нашої держави на «сіру зону», яка залишить РФ важелі свого впливу через постійну загрозу поширення нестабільності на всю Україну. Це війна не за території, а за світогляд, думки і душі людей. А оскільки контроль над інформаційною інфраструктурою дає підстави для формування суспільної думки, яка завжди спочатку виявляється в певних переконаннях, а вже потім у конкретних діях то в умовах конкурентної боротьби контроль над інформаційною сферою перетворюється на один із основних ресурсів влади.

Причин «чутливості» Донбасу до інформаційної війни на противагу іншим регіонам України кілька: значна частка (понад 30%) російськомовного населення, традиційні родинні, освітні і економічні зв'язки з Росією, включаючи трудову міграцію, транскордонні поїздки, господарську кооперацію [83].

Аналіз міжнародного інформаційного простору дає підстави стверджувати, що Україна стала об'єктом інформаційних атак (інформаційно-психологічних акцій), спрямованих на встановлення контролю над усіма сферами існування незалежної держави. Нерозуміння важливості проведення з боку України акцій інформаційного впливу задля підтримки наших національних інтересів і державної політики за кордоном, як засвідчують останні події, завдає державі величезних економічних, політичних, іміджевих та інших збитків. Російська Федерація, наприклад, не обмежується проведенням інформаційних атак на українське населення. Через мережу російського мовлення за кордоном – потужну систему інформаційного впливу – вона проводить інформаційні операції для формування негативного іміджу нашої держави.

Однією з найвагоміших причин ситуації, що склалася, є те, що в нашій державі на інституційному рівні забезпеченням окремих напрямів інформаційної безпеки опікується низка органів державної влади, зокрема Міністерство інформаційної політики, Національна рада України та Державний комітет з питань телебачення й радіомовлення, Національна комісія державного регулювання у сфері зв'язку та інформатизації, МЗС України, МВС України, СБ України, Державна служба спеціального зв'язку та захисту інформації, МО

[83] Дмитренко М. Причини воєнного конфлікту на Донбасі та заходи з попередження таких конфліктів у майбутньому // Освіта регіону. – 2016. - № 2. – С. 69-81.

України, СЗР України тощо. Проте, всі вони виявилися неготовими з об'єктивних і суб'єктивних причин до протидії сучасним викликам і загрозам. Проблема в тому, що жоден із державних органів, які беруть участь у забезпеченні інформаційної безпеки України, не відповідає за незадовільний стан протидії інформаційній агресії через відсутність суб'єкта юридичної координації зусиль забезпечення національної безпеки в інформаційній сфері. Кожен виконує виключно свою функцію, не знаючи, що роблять інші відомства в цій сфері.

Слід пам'ятати, що при подальшому удосконаленні державної системи інформаційної безпеки України необхідно зберігати баланс між демократією і безпекою і не допускати створення одноособового органу державної влади, що здійснює діяльність у сфері інформаційної безпеки, варто дотримуватися колективних основ, тобто зміцнювати систему всіх державних органів, покликаних вирішувати проблеми інформаційної безпеки, ні в якому разі не допускати монополізму одного з них. На закінчення також слід зазначити, що Україна повинна брати активну участь у розробці і прийнятті міжнародних домовленостей, спрямованих на розвиток системи міжнародної взаємодії органів державної влади, що здійснюють діяльність у сфері інформаційної безпеки, зокрема, по запобіганню і припиненню правопорушень у світовому інформаційному просторі.

Отже, проти України широко використовують сучасні технології негативних інформаційно-психологічних впливів, які стають загрозою українському національному інформаційному простору та суверенітету держави. Гарантування інформаційної безпеки України в умовах дестабілізаційних негативних інформаційно-психологічних впливів та експансіоністської агресивної інформаційної політики Російської федерації, потребує консолідації зусиль на усіх рівнях державної влади та громадянського суспільства. Як протидія масштабним негативним інформаційно-психологічним впливам, операціям та війнам, пріоритетними напрямами державної інформаційної політики та важливими кроками з боку владних органів України мають бути: 1) інтеграція України до світового та регіонального європейського інформаційного просторів; 2) інтеграція у міжнародні інформаційні та інформаційно-телекомунікаційні системи та організації; 3) створення власної національної моделі інформаційного простору та забезпечення розвитку інформаційного суспільства; 4) модернізації усієї системи інформаційної безпеки держави та формування й реалізація ефективної інформаційної політики; 5) удосконалення законодавства з питань інформаційної безпеки, узгодження національного законодавства з міжнародними стандартами та дієве правове регулювання

інформаційних процесів; 6) розвиток національної інформаційної інфраструктури; 7) підвищення конкурентоспроможності вітчизняної інформаційної продукції та інформаційних послуг; 8) впровадження сучасних інформаційно-комунікативних технологій у процеси державного управління; 9) ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації та коригуванні державної політики в інформаційній сфері.

Дирда Діана Володимирівна
Студент 2 курсу магістратури, Навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет ім. Василя Стефаника»,
(наук. керівник доц.. Петровська І.І.).

ПОНЯТТЯ ТА ВИДИ ПУБЛІЧНОЇ СЛУЖБИ В УКРАЇНІ

Сучасний етап формування публічної служби характеризується посиленням уваги до питань забезпечення її ефективності, взаємозв'язку різних видів публічної служби, модернізації правового статусу публічного службовця. Реальний стан публічної служби не відповідає запитам держави та українського громадянського суспільства, не повною мірою відповідає основам Конституції України, в якій права і свободи людини і громадянина оголошені вищою цінністю і їх захист становить основну мету і сенс діяльності державних органів і органів місцевого самоврядування. У зв'язку сьогодні перед українськими державцями стоїть стратегічна задача – поставити роботу держави на службу інтересам всього суспільства, подолати її корумпованості на основі нових принципів кадрової політики, відбору та ротації чиновників, критеріїв їх ефективності і форм персональної відповідальності.

Дослідженням даного питання були присвячені деякі праці вітчизняних науковців, такихяк: В. Б. Авер'янова, Ю. П. Битяка, І. І. Боршуляка,Р. З. Голобутовського,А.О. Гончарова, Б.І.Гуменюка, О. В.Щерби, Н. І. Карпи, О. П. Ковальчука, В. Я. Малиновського та інших.

Система державного управління та організація державного апарату, що дісталась Україні у спадок від радянських часів, не відповідала вимогам часу та новим політичним реаліям. Саме тому впродовж багатьох років постійно змінюється структура та функції

органів публічної влади на всіх її рівнях. Ринкова економіка та розвиток громадянського суспільства вимагали перетворення бюрократичного апарату на ефективну систему урядування, що слугуватиме людям. У зв'язку з цим постала необхідність переосмислення призначення держави та публічної влади[84]. .Для сучасної України багато викликів державотворення були над звичайно складними через тягар радянського минулого та відсутність достатніх знань у сфері урядування, до таких не досліджуваних питань на лежав і інститут публічної служби.

Н.Т.Гончарук зазначає, що за роки незалежності в Україні в основному сформовано інститут публічної служби, яка включає службову діяльність фізичних осіб на державних політичних посадах, у державних колегіальних органах, органах судової влади, прокуратури, а також військову службу, альтернативну (невійськову) службу, іншу службову діяльність у державних органах, органах місцевого самоврядування щодо виконання повноважень суб'єктів публічного права[1].

Проблематику публічної служби з наукової точки зору в Україні почали досліджувати відносно недавно. Але ще в 50-х роках XX ст. Ю.Л. Панейко визначав поняття «публічної служби» крізь призму дефініції держави як «корпорації публічних служб»[85]. Науковець стверджував, що публічна служба повинна змінюватися відповідно до потреб загального інтересу.

Відповідно до інституційного підходу публічна служба здійснюється працівниками всіх організацій публічного сектору: органів державної влади, державних підприємств та установ, органів місцевого самоврядування, комунальних підприємств та установ.

Варто зазначити, що вперше поняття «публічна служба» на законодавчому рівні було закріплено в Кодексі адміністративного судочинства України: публічна служба – діяльність на державних політичних посадах, професійна діяльність суддів, прокурорів, військова служба, альтернативна (невійськова) служба, дипломатична

---

[84] Теорія та практика публічної служби: матеріали наук.-практ. конф.,Дніпро,21грудня2018р./за заг. ред.С.М. Серьогіна. Дніпро:ДРІДУНАДУ, 2018.264с.

[85] Панейко Ю.Л. Наука адміністрації і адміністративного права: підручник у 2-х томах. Загальна частина. Авґсбурґ, 1949. 115 с.

служба, інша державна служба, служба в органах влади Автономної Республіки Крим, органах місцевого самоврядування[86].

С.Серьогіна, зазначає що, до основних завдань публічної служби належать: захист прав, свобод і законних інтересів громадян; створення та забезпечення умов для розвитку громадянського суспільства, політичного та соціального партнерства; формування суспільно-політичних і правових умов для практичного досягнення цілей та здійснення завдань і функцій органів державної влади та місцевого самоврядування, дотримання законності; забезпечення ефективного функціонування механізму держави та державного апарату, публічних службовців тощо[87].

Отже, можна зазначити, що публічна служба – це професійна, політично нейтральна діяльність осіб, на адміністративних посадах в органах виконавчої влади та органах місцевого самоврядування.

Публічний службовець – це особа, що обіймає посаду в органі виконавчої влади, апараті органів влади чи органі місцевого самоврядування на підставі фактичного складу, обов'язковим елементом якого повинен бути акт призначення на посаду, який здійснює професійну виконавчо-розпорядчу адміністративну діяльність на постійній основі, виходячи з публічних інтересів.

Професор Ю.П.Битяк зазначає, що правовий статус державних службовців відображає сутність і зміст державно-службових відносин, він поєднує елементи інституту державної служби від вступу на державну службу до її завершення[88]. Основу правового статусу публічного службовця визначають обов'язки публічного службовця, права, обмеження, гарантії, соціально-матеріальне забезпечення, відповідальність, що в сукупності забезпечують відповідне правове положення особи у публічно-службових відносинах і створюють умови для виконання завдань і функцій держави.

На сучасному етапі інститут державної служби регламентується Законом України «Про державну службу» від 10.12.2015 р., який визначає, що державна служба – це публічна, професійна, політично

---

[86] Кодекс адміністративного судочинства: Закон від 06.07.2005 № 2747-IV. URL: https://zakon2.rada.gov.ua/laws/show/2747-15/

[87] Серьогін С.М. Мета, завдання та функції державної служби. *Аспекти публічного управління*. 2013. № 1. С. 58-65. URL:http://nbuv.gov.ua/UJRN/aplup_2013_1_12.

[88] Битяк Ю. Державна служба в Україні: організаційно-правові засади: монографія. Харків: Право, 2005. 304 с.

неупереджена діяльність із практичного виконання завдань і функцій держави[89].

Проблемним моментом в окресленні чітких меж публічної служби є необхідність розмежування політичних та адміністративних (службових, чиновницьких) посад в органах виконавчої влади та в органах місцевого самоврядування. Існує цілий ряд ознак, зокрема, порядок призначення та звільнення з посад, характер виконуваних повноважень, види та підстави притягнення до відповідальності тощо[90].

Таким чином, політична служба – діяльність на державних політичних посадах, що спрямована на визначення (формування) та реалізацію державної політики у різних сферах суспільного життя, здійснення політичної діяльності, характеризується політичною відповідальністю, а також особливим порядком вступу на службу, її проходження та припинення.

З аналізу законодавчих положень та доктринальних позицій Р. З. Голобутовський формулює висновок, що під публічною службою в органах судової влади слід розуміти політично-нейтральну професійну службу на посаді судді в судах, в інших органах суддівського врядування, державних органах та установах системи правосуддя задля організації та забезпечення діяльності судів та суддів[91]. Професійна діяльність суддів (суддівська служба) – діяльність громадян України, які відповідно до Конституції України та Закону України «Про судоустрій і статус суддів» призначені на посаду судді та займають штатну суддівську посаду в одному з судів України, що спрямована на здійснення правосуддя на професійній основі. Судді мають особливий статус, що визначається насамперед Законом України «Про судоустрій і статус суддів».

Публічна служба в органах прокуратури є спеціалізованою та професійною, адже має ознаки професійної діяльності державного службовця. На службу в органах прокуратури як на вид публічної служби вказує І.І.Боршуляк, який стверджує, що прокуратура – це

---

[89] Про державну службу: Закон України від 10 груд. 2015 р. № 889-VIII. URL: https://zakon.rada.gov.ua/laws/show/889-19

[90] Битяк Ю. Державна служба в Україні: організаційно-правові засади: монографія. Харків: Право, 2005. 304 с.

[91] Голобутовський Р.З. Публічна служба в органах судової влади як адміністративно-правова категорія. Юридичний науковий електронний журнал. 2019. № 1. С.127-129.

комплексний та багатогранний правовий інститут, який виконує особливий вид державної діяльності із забезпечення верховенства закону, єдності, зміцнення законності, захисту прав та свобод людини і громадянина[92] .

Професійна діяльність прокурорів (прокурорська служба) – діяльність громадян України, які згідно Конституції України та Закону України «Про прокуратуру» займають посаду прокурора, що спрямована на реалізацію на професійній основі функцій прокуратури. Прокурори здійснюють діяльність на посадах в Генеральній прокуратурі України, регіональних та місцевих прокуратурах, військових прокуратурах, а також Спеціалізованій антикорупційній прокуратурі.

Захист Вітчизни є конституційним обов'язком кожного громадянина. Так, у Законі України «Про військовий обов'язок та військову службу» зазначено, що військова служба є державною службою особливого характеру, яка полягає у професійній діяльності придатних до неї за станом здоров'я і віком громадян України (за винятком випадків, визначених законом), іноземців та осіб без громадянства, пов'язаній із обороною України, її незалежності та територіальної цілісності[93].

У своєму дисертаційному дослідженні В. М. Александров розкриває військову службу як особливий вид діяльності осіб, які обіймають посади у визначених державою військових організаціях і структурах, мають військові звання, виконують завдання та функції держави щодо забезпечення її суверенітету, територіальної цілісності та недоторканності специфічними методами і засобами[94]. Взамін проходження строкової військової служби в Україні була запроваджена альтернативна (невійськова) служба – це служба, яка має на меті виконання обов'язку перед суспільством. На альтернативну службу направляються громадяни, які підлягають призову на строкову

---

[92] Боршуляк І.І. До теми служби в органах прокуратури як різновиду державної служби. *Право.ua*. 2015. № 3. С.12-17

[93] Про військовий обов'язок та військову службу: Закон України від 25.03.1992 № 2232-XII. URL: https://zakon.rada.gov.ua/laws/show/2232-12.

[94] Александров В. М. Військова служба як особливий вид державної служби в Україні: автореф. дис. ... канд. юрид. наук : 12.00.07 / Нац. юрид. акад. України ім. Я. Мудрого. Харків, 2009. 20 с.

військову службу і особисто заявили про неможливість її проходження, бо це суперечить їхнім релігійним переконанням.

Дипломатична служба є особливим різновидом державної служби, яка безпосередньо пов'язана з реалізацією зовнішньої політики держави, спрямованої на зміцнення її зовнішньополітичного авторитету у світі. Закон України «Про дипломатичну службу» 2018 р. пов'язує цей вид державної служби також із захистом національних інтересів України у сфері міжнародних відносин, а також із захистом прав та інтересів громадян і юридичних осіб України за кордоном[95]. Таким чином,дипломатична служба України – це складова частина державної служби, що призначена забезпечувати практичну реалізацію зовнішньої політики України, представляти та захищати національні інтереси України у сфері міжнародних відносин, а також права та інтереси юридичних осіб і громадян України за кордоном.

Поняття «служба в органах місцевого самоврядування» відносно нове для законодавства України. Його поява зумовлена необхідністю органів місцевого самоврядування мати власний корпус професійних службовців. У ст. 6 Європейської хартії місцевого самоврядування передбачено, що органи місцевого самоврядування повинні мати можливість визначати внутрішні адміністративні структури, що вимагає формування службового корпусу для забезпечення діяльності цих структур[96]. Так, служба в органах місцевого самоврядування (муніципальна служба) – професійна, на постійній основі діяльність громадян України, які займають посади в органах місцевого самоврядування, що спрямована на реалізацію територіальною громадою свого права на місцеве самоврядування та окремих повноважень органів виконавчої влади.

Підсумовуючи, можна сказати, що поняття публічної служби не так давно закріплено в законодавстві України, але і закріплене визначення не є досконалим. Під публічною службою слід розуміти політично-нейтральну, професійну та результативну службу в органах публічної влади, задля задоволення публічних інтересів.

---

[95] Про дипломатичну службу України: Закон України від 07.06.2018 № 2449-VIII. URL: https://zakon.rada.gov.ua/laws/show/2449-19

[96] Європейська хартія місцевого самоврядування: Міжнародний документ від 15.10.1985.URL: https://webcache.googleusercontent.com/search?q=cache:k-mp2ktGrjcJ:https://zakon.rada.gov.ua/go/994_036+&cd=1&hl=uk&ct=clnk&gl=ua&client=firefox-b-d

Система публічної служби в широкому розумінні охоплює такі основні складові: політичну службу; державну службу; професійну діяльність суддів, прокурорів; службу в органах місцевого самоврядування; військову, альтернативну службу; дипломатичну службу; патронатну службу в державних орнанах.

Капустяк Ірина Ігорівна
Студентка 2 курсу магістратури, спеціалізація 01 «Публічна служба», навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника»,
(Наук. керівник: доц. Петровська І.І.).

БАНКІВСЬКА ТАЄМНИЦЯ: ПОНЯТТЯ ТА ОСОБЛИВОСТІ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ

Банківська таємниця відноситься до видів інформації з обмеженим доступом. Основним правовим актом, який визначає цей вид інформації є Закон України «Про банки і банківські діяльність» [97]. Відповідно до статті 60 цього акту, банківською таємницею є інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку. Окремо деталізують такі види інформації, що є банківською таємницею:

1) відомості про банківські рахунки клієнтів, у тому числі кореспондентські рахунки банків у Національному банку України;

2) операції, які були проведені на користь чи за дорученням клієнта, здійснені ним угоди;

3) фінансово-економічний стан клієнтів;

4) системи охорони банку та клієнтів;

5) інформація про організаційно-правову структуру юридичної особи - клієнта, її керівників, напрями діяльності;

[97] Про банки і банківську діяльність: Закон України від 7.12.2000 року зі змінами. URL: https://zakon.rada.gov.ua/laws/show/2121-14

6) відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація;

7) інформація щодо звітності по окремому банку, за винятком тієї, що підлягає опублікуванню;

8) коди, що використовуються банками для захисту інформації;

9) інформація про фізичну особу, яка має намір укласти договір про споживчий кредит, отримана під час оцінки її кредитоспроможності.

Також становить банківську таємницю інформація про банки чи клієнтів, що збирається під час проведення банківського та валютного нагляду, отримана Національним банком України відповідно до міжнародного договору або за принципом взаємності від органу банківського нагляду іншої держави для використання з метою банківського нагляду або запобігання легалізації (відмиванню) доходів, одержаних злочинним шляхом, чи фінансуванню тероризму.

Винятком є інформація, яка підлягає опублікуванню (є публічною). Перелік інформації, що підлягає обов'язковому опублікуванню, встановлюється Національним банком України (НБУ) та додатково самим банком на його розсуд. НБУ видає, також, нормативно-правові акти з питань зберігання, захисту, використання та розкриття інформації, що становить банківську таємницю, та надає роз'яснення щодо застосування таких актів. Банк має право надавати інформацію, яка містить банківську таємницю, приватним особам та організаціям для забезпечення виконання ними своїх функцій або надання послуг банку відповідно до укладених між такими особами (організаціями) та банком договорів, у тому числі про відступлення права вимоги до клієнта, за умови, що передбачені договорами функції та/або послуги стосуються діяльності банку, яку він здійснює. Отримана органами державної влади, юридичним та фізичним особам, які при виконанні своїх функцій, визначених законом, або наданні послуг банку безпосередньо чи опосередковано інформація, що містить банківську таємницю, не може бути розголошена і використана ними на свою користь чи на користь третіх осіб.

Банківські установи зобов'язані забезпечити збереження банківської таємниці шляхом: (1) обмеження кола осіб, що мають доступ до інформації, яка становить банківську таємницю; (2) організації спеціального діловодства з документами, що містять банківську таємницю; (3) застосування технічних засобів для запобігання несанкціонованому доступу до електронних та інших носіїв інформації; (4) застосування застережень щодо збереження

банківської таємниці та відповідальності за її розголошення у договорах і угодах між банком і клієнтом (стаття 61 Закону «Про банки і банківську діяльність»). Службовці банку при вступі на посаду підписують зобов'язання щодо збереження банківської таємниці. Керівники та службовці банків зобов'язані не розголошувати та не використовувати з вигодою для себе чи для третіх осіб конфіденційну інформацію, яка стала відома їм при виконанні своїх службових обов'язків.

У разі заподіяння банку чи його клієнту збитків шляхом витоку інформації про банки та їх клієнтів з органів, які уповноважені здійснювати банківський нагляд, збитки відшкодовуються винними органами.

Порядок розкриття банківської таємниці описано в статті 62 Закону «Про банки і банківську діяльність». Зокрема, ця інформація розкривається на письмовий запит або з письмового дозволу відповідної юридичної чи фізичної особи; за рішенням суду; органам прокуратури України, Служби безпеки України, Державному бюро розслідувань, Національної поліції, Національному антикорупційному бюро України, Антимонопольного комітету України - на їх письмову вимогу стосовно операцій за рахунками конкретної юридичної особи або фізичної особи - суб'єкта підприємницької діяльності за конкретний проміжок часу; центральному органу виконавчої влади, що реалізує державну податкову політику на його письмову вимогу щодо наявності банківських рахунків; центральному органу виконавчої влади, що реалізує державну політику у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму, на його запит щодо фінансових операцій, пов'язаних з фінансовими операціями, що стали об'єктом фінансового моніторингу (аналізу) згідно із законодавством щодо запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму, а також учасників зазначених операцій; органам державної виконавчої служби, приватним виконавцям на їхню письмову вимогу з питань виконання рішень судів та рішень, що підлягають примусовому виконанню тощо. Правила зберігання, захисту, використання та розкриття банківської таємниці затверджені Постановою Правління НБУ [98].

[98] Про затвердження Правил зберігання, захисту, використання та розкриття банківської таємниці: Постанова Правління Національного

Вимога відповідного державного органу на отримання інформації, яка містить банківську таємницю, повинна бути викладена на бланку державного органу встановленої форми, надана за підписом керівника державного органу (чи його заступника), скріпленого гербовою печаткою, містити передбачені Законом «Про банки і банківську діяльність» підстави для отримання цієї інформації, посилання на норми закону, відповідно до яких державний орган має право на отримання такої інформації, містити прізвище, ім'я, по батькові та реєстраційний номер облікової картки платника податку клієнта банку - фізичної особи або серію та номер паспорта/номер паспорта у формі картки (для фізичних осіб, які через свої релігійні переконання відмовилися від прийняття реєстраційного номера облікової картки платника податків, повідомили про це відповідний контролюючий орган і мають відмітку в паспорті про право здійснювати платежі за серією та номером паспорта, або для фізичних осіб - нерезидентів), або найменування та ідентифікаційний код в Єдиному державному реєстрі юридичних осіб, фізичних осіб - підприємців та громадських формувань клієнта банку - юридичної особи. Довідки по рахунках (вкладах) у разі смерті їх власників надаються банком особам, зазначеним власником рахунку (вкладу) у відповідному розпорядженні банку, державним нотаріальним конторам або приватним нотаріусам, посадовим особам органів місцевого самоврядування, уповноваженим на вчинення нотаріальних дій, іноземним консульським установам для вчинення такими особами нотаріальних дій з охорони спадкового майна, з видачі свідоцтв про право на спадщину, про право власності на частку в спільному майні подружжя в разі смерті одного з подружжя. Довідки щодо рухомого майна померлих клієнтів, що перебуває на збереженні та/або у заставі банку в якості закладу, щодо наявності індивідуального банківського сейфа та/або договорів про надання в майновий найм (оренду) індивідуального банківського сейфа надаються банком державним нотаріальним конторам або приватним нотаріусам, посадовим особам органів місцевого самоврядування, уповноваженим на вчинення нотаріальних дій, іноземним консульським установам для вчинення такими особами нотаріальних дій з охорони спадкового майна, з видачі свідоцтв про право на спадщину, про право власності на частку в спільному майні подружжя в разі смерті одного з подружжя.

Банку України від 14.07.2006 № 267. URL: https://zakon.rada.gov.ua/laws/show/z0935-06

Забороняється надавати інформацію про клієнтів іншого банку, навіть якщо їх імена зазначені у документах, угодах та операціях клієнта.

Банк має право надавати інформацію, що становить банківську таємницю, іншим банкам та Національному банку України в обсягах, необхідних при наданні кредитів, банківських гарантій, а також при здійсненні валютного нагляду, у тому числі в разі запровадження Національним банком України заходів захисту відповідно до Закону України «Про валюту і валютні операції» [99].

Петрованчук Галина Романівна
Студентка 2 курсу магістратури,
Спеціалізація 01 «Публічна служба»
Навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника»,
(науковий керівник: викл. Зінич Л.В.).

ІНТЕЛЕКТУАЛЬНА ВЛАСНІСТЬ ЯК ОБ'ЄКТ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ

Навколишній світ стрімко змінюється, перетворюючись на світ електронного бізнесу, електронної комерції, нової економіки й управління, на світ, рушієм якого є інформаційні технології, що стрімко увійшли у сферу інтелектуальної творчості, охопивши значний спектр понять, зазначених у ст. 1 Закону України «Про авторські та суміжні права», що вимагають пошуку і вибору комплексних підходів у вирішенні складного завдання – захисту авторських прав. Європейський Союз регулярно здійснює заходи, покликані підтверджувати зобов'язання щодо дотримання свободи засобів масової інформації та виробляти напрямки подальшої діяльності Ради Європи в галузі засобів масової інформації, захисту авторських прав у сфері застосування новітніх інформаційних технологій, що в контексті

[99] Про валюту і валютні операції: Закон України від 21.06.2018 року. URL: https://zakon.rada.gov.ua/laws/show/2473-19

адаптації національного законодавства впливає на адміністративно-правові засоби захисту інтелектуальних прав.

Наука адміністративного права на сучасному етапі свого розвитку перебуває в пошуках нових науково-практичних підходів до характеристики відносин, що виникли у сфері діяльності органів державного управління та пов'язані із захистом прав, свобод і законних інтересів громадян України. Одним з актуальних напрямів наукового дослідження є розв'язання проблем, дотичних до адміністративно-правового забезпечення права інтелектуальної власності в Україні. Правовідносини майнового характеру, а саме категорія власності, виступає об'єктом регулювання з боку адміністративного та інших галузей права. Її законодавче забезпечення втілюється в Основному законі держави, що передбачає захист приватної власності, і щодо набуття, і щодо розпоряджання. Інститут інтелектуальної власності з усіма його складовими елементами потребує не лише вдосконалення, а й нових кроків у здійсненні правової охорони та захисту об'єктів інтелектуальної власності[100].

Охорона прав на об'єкти інтелектуальної власності на сьогоднішній день є пріоритетним напрямком діяльності Української держави. Це продиктовано рядом об'єктивних факторів. По-перше, Конституція України гарантувала громадянам захист прав інтелектуальної власності, який має здійснюватися саме державою; по-друге, держава сама зацікавлена у належній правовій охороні інтелектуального капіталу, оскільки останній є найважливішою передумовою забезпечення подальшого сталого соціально-економічного і культурного розвитку країни; по-третє, необхідність виконання зазначеного завдання обумовлена також міжнародними зобов'язаннями держави у сфері інтелектуальної власності. У зв'язку з цим Україна взяла курс на побудову дієвого механізму гарантування та охорони прав на об'єкти інтелектуальної власності. Історично склалося так, що змістом даного механізму стали переважно норми цивільного права і заснована на них діяльність суб'єктів цивільно-правових відносин. Однак сучасний стан справ у сфері охорони прав на об'єкти інтелектуальної власності свідчить, що цього замало, оскільки саморегуляція відносин у зазначеній сфері не задовольняє потреби сучасного суспільства. Це обумовлює необхідність активізації участі державних органів у процесі охорони прав на об'єкти інтелектуальної

[100] Кодекс України про адміністративні правопорушення (статті 1 - 212-20) (ст.213 - ст.330)

власності, функціонування яких вже набуває управлінського аспекту. У цьому контексті, а також враховуючи проблеми здійснення адміністративної реформи, надзвичайно актуальним є дослідження адміністративно-правового регулювання у сфері охорони прав на об'єкти інтелектуальної власності, оскільки недосконаліть державної діяльності у цій сфері перешкоджає ефективній охороні зазначених прав[101].

Адміністративно-правове забезпечення права інтелектуальної власності – це здійснюване державою за допомогою правових норм, приписів і сукупності засобів упорядкування суспільних відносин, їх юридичне закріплення, охорона, реалізація і розвиток.

Здійснено порівняльно-правовий аналіз понять «адміністративно-правовий захист права інтелектуальної власності» та «адміністративно-правова охорона права інтелектуальної власності»,

Адміністративно-правова охорона права інтелектуальної власності передбачає надання гарантії та юридичне закріплення відповідних прав та обов'язків суб'єктів права інтелектуальної власності, тоді як під адміністративно-правовим захистом права інтелектуальної власності розуміють діяльність правоохоронних органів та судових установ щодо профілактики незаконних посягань на права власника об'єкта інтелектуальної власності, а також дії на припинення адміністративних проступків та відновлення порушеного права.

Зміст поняття адміністративно-правового забезпечення права інтелектуальної власності охоплює комплекс правотворчих та правозастосовних заходів з боку органів державної влади та управління, правоохоронних органів та судової влади, спрямованих на введення правових гарантій, реалізацію функції адміністративно-правової охорони та адміністративно-правового захисту права інтелектуальної власності.

На підставі розмежування понять «адміністративно-правова охорона права інтелектуальної власності» і «адміністративно-правовий захист права інтелектуальної власності» визначено, що адміністративно-правова охорона – це дії у сфері надання (гарантії) та юридичного закріплення відповідних прав та обов'язків суб'єктів права інтелектуальної власності. Натомість адміністративно-правовий

---

[101] . Конституція України. Прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 року, №254/96-ВР

захист охоплює діяльність правоохоронних органів та судових установ задля профілактики незаконних посягань на права власника об'єкта права інтелектуальної власності, а також дії на припинення адміністративних проступків та відновлення порушеного права.

Ознаки суспільної небезпеки та шкоди є безпосереднім наслідком вчинення протиправного діяння з настанням негативного результату для будь-якого виду суспільних відносин (у цьому контексті це відносини у сфері інтелектуальної власності).

Аргументовано, що на сьогодні законодавство у сфері протидії правопорушенням у царині інтелектуальної власності перебуває в стані «замороження», оскільки серйозні правові прогалини, зокрема на місцевому та регіональному рівнях, не заповнені відповідними нормами права, а також немає чітко визначеного плану заходів щодо боротьби з правопорушеннями у сфері інтелектуальної власності.

До найефективніших форм і методів різнорівневої профілактичної діяльності у сфері інтелектуальної власності зараховано: ведення державних реєстрів об'єктів права інтелектуальної власності; розробку нормативно-правової бази для посилення системи забезпечення прав на об'єкти права інтелектуальної власності; правозастосовну діяльність судових органів; введення структурно-організаційних змін в апаратах органів місцевого самоврядування та правоохоронних органів; посилення співпраці органів державної влади з обміну інформацією щодо стану правопорядку під час реалізації індивідами прав на об'єкти права інтелектуальної власності; активізація діяльності засобів масової інформації з громадськими діячами, науково-дослідними співробітниками, представниками органів державної влади, судовим апаратом щодо протидії злочинності та моніторингу дотримання виконання положень ратифікованих міжнародних актів у сфері права інтелектуальної власності на території України.

Запорукою забезпечення права інтелектуальної власності є тісна взаємодія і співпраця між органами державної влади, їх постійний взаємозв'язок та обмін інформацією щодо стану правовідносин. Саме комплексний підхід слугує гарантією забезпечення права інтелектуальної власності[102].

---

[102] Закон України «Про авторське право і суміжні права» (Відомості Верховної Ради України (ВВР), 1994

НАПРЯМОК IV. КОНСТИТУЦІЙНА ЮСТИЦІЯ ТА ЇЇ РОЛЬ ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СУЧАСНОМУ СУСПІЛЬСТВІ

Розвадовський Володимир Іванович
Завідувач кафедри конституційного, міжнародного та адміністративного права, навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника»,
кандидат юридичних наук, доцент.

ПРОБЛЕМИ УРЕГУЛЮВАННЯ ДОСТУПУ ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ: ТЕОРІЯ ТА ПРАКТИКА

Сучасний бурхливий розвиток інформаційних технологій значною мірою впливає на політичну, економічну, соціальну, культурну, безпекову та інші складові розвитку суспільства і держави, а інформаційні ресурси стають системоутворюючим фактором їх життєдіяльності.

Окрім того в Конституції України закладено базовий принцип свободи на інформацію та заборону цензури державою (ч.3. ст. 15) Відповідно до ст. 34 Основного закону кожному гарантується право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово, або в інший спосіб на свій вибір. Таким чином положення передбачені цими статтями Основного закону України, є першоосновою для таких, пов»язаних між собою прав, а саме: свобода вираження поглядів на певну інформацію, та право на доступ до публічної інформації. Також Конституція України забезпечує кожному право знайомитись в органах державної влади, місцевого самоврядування , установах організаціях з відомостями про себе (ч.3 ст. 32)[103].

---

103 Конституція України : Закон України від 28 червня 1996 р. // Відомості Верховної Ради України. – 1996. –№ 30. – Ст. 141.

На переконання О. Шпортько, Основним Законом України забезпечено право людини, громадянина впливати на якість роботи державного апарату, рівень освіченості і правосвідомості політиків, які ухвалюють політичні рішення, а також мати змогу слідкувати за діями представників органів державної влади та місцевого самоврядування шляхом відкритого доступу до їх діяльності, особливо якщо наслідком цих дій є зміни в їх правах і свободах [104].

На наш погляд відкритість влади не можна зводити лише до взаємин між владою та окремими громадянами. Тобто, необхідно відслідковувати конкретні суспільні інституції, які забезпечують і здійснюють тиск на владу, забезпечують певну спрямованість влади і, нарешті, формують всю архітектуру владної системи стосовно громадянина. Поряд з цим держава в цілому повинна переглянути першочергово політику щодо установлення зворотного зв'язку з громадськістю, домагатись публічного діалогу, партнерства на рівні місцевого самоврядування та інститутів громадянського суспільства. Відповід-но залучення громадськості до розроблення та реалізації державної політики – питання першочергової ваги, від яких залежатимуть усі подальші дії влади щодо доступності до публічної інформації. Звісно, що для досягнення всьому цьому буде сприяти якісна нормативно-правова база та європейський досвід.

Досліджуючи проблему доступу людини, громадянина до публічної інформації необхідно проаналізувати відповідні органічні закони України.

Як, відомо, перший крок реформи у сфері доступу до інформації про діяльність влади в Україні забезпечив закон України «Про інформацію»[105]. Однак названий закон не тільки не створив гарантій забезпечення права на доступ до інформації, але значною мірою став причиною ускладнень, що виникали внаслідок спроб отримати інформацію про діяльність органів публічної влади. Таким чином, даний закон став об'єктом критики з боку вітчизняних науковців конституціоналістів. Так, на думку В. Серьогіна інформаційне чинне законодавство певною мірою залишається декларативним та не отримує повноцінної його реалізації, особливо у

---

104 Шпортько О. Поле публічної політики / О. Шпортько // Політ. менеджмент. – 2010. – № 5(44). – С. 90–96.

105 Про інформацію : Закон України від 2 жовтня 1992 р. №2657-XII // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.

відносинах між органами публічної влади й пересічними громадянами[106]. Аналогічні судження стосовно проблем у сфері правового регулювання інформаційно-правових відносин висловлювали Є. Захаров; Л. Задорожня; Р. Калюжний; А. Марущак; О. Марцеляк; В. Речицький; Т. Слінько та інші.

В. Речицький звертає увагу на те що Закон України в редакції 1992 року «Про інформацію» вичерпав свій потенціал, він суттєво розходиться з європейськими стандартами щодо забезпечення доступу населення до урядової та іншої офіційної інформації[107].

Другий крок, щодо досліджуваної проблем, реалізується прийнятим 13 січня 2011 року Закону України «Про доступ до публічної інформації»[108].

Цей закон встановив нові правила гри у сфері інформаційних відносин між громадськістю та владою, в підґрунтя яких покладено принцип максимальної відкритості влади. Таким чином законом передбачено відкритість держави про всю інформацію щодо її діяльності за виключенням окремих обмежень в інтересах та безпеки людини, громадянина й держави. Визначено короткі терміни для відповіді на запити (5 робочих днів та до 48 годин) та інші новели.

Однак і черговий правовий акт засвідчив про відсутність суттєвих зрушень у бік більшої відкритості української держави, особливо щодо доступу фізичних та юридичних осіб до публічної інформації.

У свою чергу О. В. Нестеренко наголошує, що значна кількість новел повинні були розв»язати стратегічні завдання в царині транспарентності державного управління, передбачених в проекті Закону України «Про доступ до публічної інформації», але вони були вилучені законотворчою владою[109]. Для прикладу можна використати

---

106 Серьогін В. О. Конституційний принцип гласності у діяльності органів державної влади України: дис. канд. юрид. Наук: 12.00.02. – с. 174.

107 Речицький В. В. Пояснювальна записка до проекту ЗУ «Про інформацію»//Свобода інформації та право на приватність в Україні. – Т.1. доступ до інформації: hic et nuncl – с.161.

108 Про доступ до публічної інформації: закон України від 13.01.2011 № 2939-VI [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2939-1.

109 Нестеренко О. В. Інформація в Україні: право на доступ Наукове видання, Х. 2012 с.174.

дослідження національного незалежного центру політичних досліджень в якому значиться, що чинне законодавство з досліджуваної теми , органи влади використовують на 50% [110].

На наш погляд результативність Закону України «Про доступ до публічної інформації» був би значно дієвим, якщо б Кабінет Міністрів України скасував постанову № 1893 від 27 листопада 1998 року «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, визнаних такими, що містять конфіденційну інформацію, яка є власністю держави»[111]. Підтримуючи думку вчених, цей піднормативний правовий акт за духом суперечить Закону України «Про доступ до публічної інформації». Адже згадана постанова Кабінету Міністрів України надає право державним органам влади та місцевого самоврядування на власний розсуд присвоювати гриф «для службового користування» любому офіційному документу що не узгоджується з вимогами та концепцією Закону України «Про доступ до публічної інформації». Така невідповідність законотворців порушує основну ідею згаданого закону - подолання надмірної таємності держави, обмежень щодо можливості зарахувати публічну інформацію до інформації з обмеженим доступом та інше.

Як зауважує А.І. Буханевич на даний час існує нерозв'язана проблема забезпечення пасивного доступу до інформації, зокрема несвоєчасне або неповне оприлюднення на офіційних веб-сайтах органів державної влади та місцевого самоврядування інформації щодо прийнятих рішень, ухвалених нормативно-правових актів, оприлюднення системи обліку документів тощо, яке є швидше винятком, ніж повсякденною нормою. Крім того, інформація яка оприлюднюється на веб-сайтах, іноді викладається не повністю, або її надзвичайно важко знайти, особливо пересічному громадянину, який

---

[110] Закон о доступе к публичной информации выполняется на 50% - эксперт.(Електорнний ресурс – Режим доступу; http:nbnews.com.ua /news/27350

[111] Постанова Кабінету Міністрів України № 1893 від 27 листопада 1998 р. «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, визнаних такими, що містять конфіденційну інформацію, яка є власністю держави».

не орієнтується в функціях та повноваженнях конкретного органу [112]. В законі України «Про доступ до публічної інформації» зазначено, що за неповне та несвоєчасне надання інформації відповідальність несе структурний підрозділ або відповідальна особа з питань доступу до публічної інформації розпорядників інформації. Хоча, на нашу думку, у законі доцільно передбачити спільну відповідальність керівника організації – розпорядника інформації та відповідальної особи.

У той же час аналіз практики свідчить, що відповідь на запит не завжди містить повний обсяг запитуваної інформації, інколи органи влади обмежуються формальною відпискою або відсилають для ознайомлення з інформацією до офіційного веб-сайту, що є неправомірною відмовою в наданні інформації. Ще однією проблемою є те, що часто органи влади допускають затримку з відповіддю на запит у декілька днів, при цьому не повідомляючи про таку затримку запитувача інформації.

А. І. Кохан стверджує, що на практиці не досить ефективно реалізується законодавче право громадян, передбачене статтею 19 закону України «Про доступ до публічної інформації», отримувати відповідь на інформаційні запити в письмові, електронній чи іншій довільній формі на вибір запитувача[113]. Особливо ця негативна практика з боку публічної влади продовжує мати місце і після Революції Гідності.

З огляду проаналізованого чинного законодавства випливає, що важливим елементом змін в сфері доступу до публічної інформації є можливість отримання інформації в електронному вигляді. Так, 21 жовтня 2015 р. Кабінет Міністрів України ухвалив Постанову «Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних», якою передбачається відкриття у формі відкритих даних 331 набору державних даних, а також встановлюються вимоги до формату та структури таких наборів

---

112 Буханевич А. І. Забезпечення принципів відкритості та прозорості при налагодженні діалогу між владою та громадськістю / А. І. Буханевич // Державне управління: удосконалення та розвиток. – 2010. – № 3 [Електронний ресурс]. – Режим доступу : www.dy. .com.ua/?op=1&z=133.

113 Кохан А. І. Державна комунікативна політика –механізм ефективної діяльності інституту публічної влади в Україні / А. І. Кохан [Електронний ресурс]. – Режим доступу : http://www.academy.gov. ua/ej/ej13/txts/zmist. Htm

даних. Так, протягом 6 місяців розпорядники інформації повинні оприлюднити та забезпечити подальше оновлення на єдиному державному веб-порталі відкритих даних та своїх офіційних веб-сайтах відповідних наборів даних, серед яких Єдиний державний реєстр юридичних осіб та фізичних осіб – підприємців; Єдиний реєстр підприємств, щодо яких порушено провадження у справі про банкрутство; звіти про використання бюджетних коштів; інформація про стан аварійності на автошляхах України; Державний реєстр лікарських засобів; інформація про хід ліквідації ямковості на основних дорогах міжнародного, національного та регіонального значень; Реєстр платників податку на додану вартість та багато інших важливих для громадян державних даних [114].

Наявна в розвинених країнах концепція електронного врядування передбачає забезпечення повнішого доступу до інформації через Інтернет; сприяння громадянській участі в державному житті засобом створення можливостей для більш зручної комунікації з державними службовцями через електронні канали [10]. В Україні розвиток електронного урядування було запроваджено шляхом схвалення Концепції розвитку електронного урядування в Україні [115].

Водночас окремий авторський інтерес викликає відсутність чіткої процедури забезпечення доступу до публічної інформації в діяльності органів місцевого самоврядування. Досліджуючи такі нормативні акти, як Закони України «Про місцеве самоврядування в Україні» та «Про службу в органах місцевого самоврядування» [116], можна зробити висновок, що норми цих законів визначають тільки декларативні положення щодо обміну інформацією між органами місцевого самоврядування, фізичними і юридичними особами, а також представниками органів виконавчої влади. Так, представницькі органи місцевого самоврядування мають засновувати власні засоби масової

---

[114] Постанова Кабінету Міністрів України від 21 жовтня 2015 року «Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних».

[115] Мельниченко В. І. Прозорість і відкритість публічного управління як об'єкт законодавчого регулювання / В. І. Мельниченко [Електронний ресурс]. – Режим доступу : www.academy.gov.ua/ej/ej5/txts/07mviozr.htm.

[116] Про службу в органах місцевого самоврядування: Закон України від 7 червня 2001 р. № 2493-III // Відомості Верховної Ради України. – 2001. – № 33. – Ст. 175.

інформації та сприяти взаємодії з центральними органами виконавчої влади у сфері інформації. Органи місцевого самоврядування в особі своїх голів мають звітувати про свою роботу перед територіальною громадою на відкритій зустрічі з громадянами, а секретарі відповідних рад забезпечують своєчасне доведення рішень ради до виконавців і населення та організують контроль за їх виконанням, оприлюднення рішень ради відповідно до Закону України «Про доступ до публічної інформації» [117].

Висновки

1. Під час удосконалення нормативно-правової бази законодавства у сфері доступу до публічної інформації в діяльності органів державної влади та місцевого самоврядування необхідно враховувати не тільки необхідність гармонізації всього пласту загальних і спеціальних правових актів у цій сфері, але і відсутність прозорого механізму доведення до громадськості інформації органами влади та місцевого самоврядування попри спроби запровадити механізми зворотного зв'язку влади та громадян.

2. Вирішення проблем публічної влади в інформаційній сфері призведе до таких важливих наслідків, як зменшення кількості ухвалених незаконних рішень влади шляхом оприлюднення планів виконання поточних завдань і загальних звітів про діяльність органів публічної влади; попередження незаконності та проявів корупції в діях чи бездіяльності посадових осіб органів державної влади та місцевого самоврядування; підвищення правосвідомості як самих представників органів влади та місцевого самоврядування, так і громадськості шляхом створення при окремих державних органах громадських і експертних рад, комісій та інших громадських утворень; спрощення доступності публічної інформації для пересічних громадян шляхом доступу до мережі Інтернет, а саме – до створених веб-сайтів із системно викладеною публічною інформацією про діяльність органів влади та місцевого самоврядування.

---

117 Про додаткові заходи щодо забезпечення відкритості у діяльності органів державної влади: Указ Президента України: за станом на 1 серпня 2002 р. № 683/2002 // Урядовий кур'єр. – 2002. – № 140.

Костенко Світлана Олексіївна
Житомирський національний агроекологічний університет, доцент кафедри правознавства, кандидат юридичних наук.

РОЛЬ КОНСТИТУЦІЙНОГО СУДУ УКРАЇНИ В ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

З розвитком суспільних відносин та поглибленням процесів глобалізації у світі право на інформаційну безпеку набуває все більшої актуальності. Загострює актуальність даної тематики різноманіття сфер інформаційної діяльності, в яких суб'єкт інформаційних правовідносин потребує безпеки: воєнна сфера, науково-технічна, екологічна, економічна, соціальна, внутрішньо-політична та зовнішньополітична сфери, тощо. Відповідно, для кожної з вище названих сфер мають бути розроблені індивідуальні способи та методи забезпечення інформаційної безпеки. Тобто, зміст інформаційної безпеки є настільки об'ємним та носить комплексний характер, що потребується мобілізація зусиль науковців з різних сфер науки. Проблематику даного дослідження становить також недосконаліть нормативно-правового регулювання відповідних правовідносин, що утруднює реалізацію державою такого конституційного обов'язку як забезпечення інформаційної безпеки.

Для розкриття обраної теми дослідження необхідно розглянути такі питання як повноваження Конституційного суду України, поняття інформаційної безпеки та, наостанок, роль Конституційного суду України у забезпеченні державою інформаційної безпеки.

Розпочнемо дане дослідження з аналізу повноважень Конституційного суду України, які закріплені в Законі України «Про Конституційний Суд України» [118]. Так, ст.7 вказаного Закону передбачено перелік повноважень Суду: вирішення питань про відповідність Конституції України законів України та інших правових актів; офіційне тлумачення Конституції; надання висновків про відповідність Конституції України чинних міжнародних договорів України або тих міжнародних договорів, що вносяться до Верховної

[118] Закон України «Про Конституційний Суд України» від 05.08.2018 // Відомості Верховної Ради (ВВР), 2017, № 35, ст.376

Ради України для надання згоди на їх обов'язковість; надання висновків про відповідність Конституції України законопроекту про внесення змін до Конституції України вимогам статей 157 і 158 Конституції України; вирішення питань про відповідність Конституції України (конституційність) законів України (їх окремих положень) за конституційною скаргою особи, яка вважає, що застосований в остаточному судовому рішенні в її справі закон України суперечить Конституції України та інші. З аналізу вказаної статті немає будь-якого посилання на роль єдиного конституційного юрисдикційного органу - Конституційного Суду України в забезпеченні інформаційної безпеки держави.

Більше того, в розробленому проекті Концепції інформаційної безпеки України [119] за сприянням ОБСЄ вказано перелік суб'єктів забезпечення інформаційної безпеки (це - громадяни України, об'єднання громадян, громадські організації та інші інститути громадянського суспільства; Президент України, Верховна Рада України, Кабінет Міністрів України, інші центральні органи виконавчої влади та органи сектору безпеки і оборони України; засоби масової інформації та комунікації різних форм власності, підприємства, заклади, установи та організації різних форм власності, що здійснюють інформаційну діяльність; наукові установи, освітні і навчальні заклади України, які, зокрема, здійснюють наукові дослідження та підготовку фахівців за різними напрямами інформаційної діяльності, в галузі інформаційної безпеки) і в ньому взагалі відсутні такі суб'єкти забезпечення інформаційної безпеки як судові органи.

Що, однак, не узгоджується з Законом України «Про національну безпеку України» [120]. Очевидно, що поняття «національна безпека» ширше ніж поняття «інформаційна безпека» та включає в себе останнє, тому положення Закону «Про національну безпеку України» природно застосовувати і до інформаційних правовідносин. Про це також йдеться у п.4 ст.3 зазначеного закону: «*Державна політика у сферах національної безпеки і оборони спрямовується на*

---

[119] Проект Концепції інформаційної безпеки України. URL: https://www.osce.org/uk/fom/175056?download=true (дата звернення: 15.06.2019 р.)

[120] Закон України «Про національну безпеку України» від 21.06.2018 // Відомості Верховної Ради (ВВР), 2018, № 31, ст.241.

забезпечення воєнної, зовнішньополітичної, державної, економічної, *інформаційної*, екологічної *безпеки,* кібербезпеки України тощо.»

Так, зазначений закон містить таке поняття як «демократичний цивільний контроль» під яким розуміється комплекс здійснюваних відповідно до Конституції і законів України правових, організаційних, інформаційних, кадрових та інших заходів для забезпечення верховенства права, законності, підзвітності, прозорості органів сектору безпеки і оборони та інших органів, діяльність яких пов'язана з обмеженням у визначених законом випадках прав і свобод людини, сприяння їх ефективній діяльності й виконанню покладених на них функцій, зміцненню національної безпеки України. А ст.4 Закону України «Про національну безпеку України» чітко вказує хто такий контроль може здійснювати – це Президент України, Верховна Рада України, Рада національної безпеки і оборони України, Кабінет Міністрів України, органи виконавчої влади та органи місцевого самоврядування, судові органи та громадяни. Отже, фактично, розглядуваним законом встановлено, що національну безпеку, а значить і інформаційну безпеку також, забезпечують судові органи, у тому числі Конституційний Суд України.

Для підтвердження даної тези потрібно проаналізувати поняття «інформаційної безпеки». Якщо лишити поза увагою згадуваний вище Проект Концепції інформаційної безпеки України, то єдине нормативно-правове визначення інформаційної безпеки міститься в Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» [121], де зазначено, що інформаційна безпека – *це стан захищеності* життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації. А стан захищеності досягається, в тому числі, наявністю закріплених на нормативно-правовому рівні способів захисту порушеного права, серед яких, зокрема, судовий.

---

[121] Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09.01.2007 // Відомості Верховної Ради України (ВВР), 2007, № 12, ст.102

Більше того, якщо заглибитися в сутність повноважень Конституційного Суду України, а саме офіційного тлумачення Конституції та вирішення питань про конституційність законів України (їх окремих положень) за конституційною скаргою особи, яка вважає, що застосований в остаточному судовому рішенні в її справі закон України суперечить Конституції України, то можна зрозуміти, що Конституційний Суд України виконує превентивну функцію в забезпеченні інформаційної безпеки.

Так, Рішенням Конституційного Суду України від 20.01.2012 року у справі № 1-9/2012 за конституційним поданням Жашківської районної ради Черкаської області було встановлено що слід розуміти під інформацією про особисте і сімейне життя, зокрема, чи належить така інформація до конфіденційної інформації про особу та чи є збирання, зберігання, використання та поширення інформації про особу втручанням в її особисте і сімейне життя, зокрема посадової особи. Завдяки цьому рішенню вдалося запобігти порушенню прав особи в інформаційній сфері в конкретно цьому випадку та у всіх інших потенційних випадках, коли йдеться про поширення конфіденційної інформації про особу, у тому числі державного службовця, без її згоди державою, органами місцевого самоврядування, юридичними або фізичними особами.

Ще одним прикладом виконання Конституційним Судом України вже не лише превентивної функції, а й захисної у сфері забезпечення інформаційної безпеки є Рішення Конституційного Суду України від 30.10.1997 року у справі № 18/203-97 за конституційним зверненням Устименка К. Г. Так, Устименко К. Г. звертався до головного лікаря психіатричного диспансеру, на обліку якого він раніше перебував з певним переліком питань щодо себе особисто, однак лікар відмовив йому у наданні відповідної інформації, посилаючись на лікарську таємницю. Конституційний Суд України встановив, що в даній ситуації медична установа у своїй діяльності використовувала відомчі нормативні акти СРСР, які суперечили вимогам норм Закону України «Про інформацію», однак в таких та подібних випадках потрібно керуватися останнім вказаним нормативно-правовим актом.

Таких прикладів безпосередньої участі Конституційного Суду України у забезпеченні інформаційної безпеки можна навести ще багато, однак усі вони свідчать про те, що Конституційний Суд України у перспективному законодавстві обов'язково повинен бути визнаний одним із суб'єктів забезпечення інформаційної безпеки, оскільки він, ґрунтуючись на своїх повноваженнях, виконує

регулятивну (завдяки офіційному тлумаченню Конституції регулює відповідні правовідносини, у тому числі, інформаційні), захисну та превентивну функції в реалізації такого конституційного завдання як забезпечення інформаційної безпеки. Більше того, Конституційний Суд України може також працювати в напрямку перейняття позитивного досвіду функціонування, наприклад, Федерального конституційного суду Німеччини, який розробив концепцію конкретних безпекових гарантій конституційних цінностей у випадках, коли виникає загроза з боку держави або приватних осіб [122], що є безцінним вкладом в розвиток інформаційних правовідносин та забезпечення інформаційної безпеки в цілому.

Бабак Віталій Михайлович
Студент 4 курсу групи ПР-41 навчально-наукового юридичного інституту ДВНЗ «Прикарпатський національний університет імені Василя Стефаника»,
(науковий керівник: доц. Розвадовський В.І.).

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В УМОВАХ ЄВРОІНТЕГРАЦІЇ

Події 2013-2014 років відіграли надзвичайно важливу роль у трансформації поглядів громадян України на геополітику, засоби масової інформації та обороноздатність держави. Досягненням, здобутим завдяки Революції гідності є усвідомлення необхідності підтримки обороноздатності та національної безпеки.

У 21 столітті поняття обороноздатність та національна безпека вже не можуть обмежуватися лише Збройними силами, їх матеріально-технічним оснащенням та підготовкою бійців. Унаслідок

[122] Райнер Арнольд. «Права людини і національна безпека: роль органу конституційної юрисдикції»: Міжнародна конференція з нагоди Дня Конституції України. URL: http://www.ccu.gov.ua/novyna/prava-lyudyny-i-nacionalna-bezpeka-rol-organu-konstytuciynoyi-yurysdykciyi-mizhnarodna-0 (дата звернення: 15.06.2019 р.)

інформаційної глобалізації, здійснення більшості комунікацій у мережі Інтернет важливу увагу слід приділяти інформаційній безпеці.

Враховуючи той факт, що саме завдяки нормам права можна забезпечити практичну реалізацію заходів спрямованих на практичне посилення інформаційної безпеки, вивчення питань нормативно-правового регулювання питань інформаційної безпеки є важливим та актуальним.

Більше того, в контексті підписання Угоди про асоціацію між Україною та ЄС, наша держава повинна привести своє законодавство до європейських стандартів, що означає врахування європейського досвіду у покращенні регулювання питання інформаційної безпеки. Все це свідчить про неабияку актуальність даного дослідження.

Проблеми нормативно-правого регулювання інформаційної безпеки, захисту інформаційного простору досліджували багато науковців. Зокрема, проблему відображено у працях А. Марущака, В. Петрика, В. Ліпкана, Б. Кормича, В. Почепцова та інших фахівців.

Відповідно до ст. 1 Закону України «Про основи національної безпеки України» національна безпека - захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються в тому числі і забезпечення свободи слова та інформаційної безпеки.

Що стосується тлумачення поняття інформаційна безпека, то на доктринальному рівні існує декілька підходів його визначення. Не вдаючись до дискусії щодо тлумачення, оскільки це не є предметом даного дослідження, ми погоджуємося із запропонованим В.І. Гурковським визначенням, відповідно до якого національна інформаційна безпека - це суспільні відносини, пов'язані із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в інформаційному просторі, що є необхідною умовою збереження та примноження духовних і матеріальних цінностей державоутворюючої нації, її існування, самозбереження і прогресивного розвитку України як суверенної держави, що залежить від цілеспрямованої інформаційної політики гарантій, охорони, оборони, захисту її національних інтересів[123]

[123] Гурковський В. Т. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки: Дис... канд... юрид. Наук. 25.00.02 - К. 2004. 225 с, С 35.

Інформаційна безпека є складною та багатогранною за своєю суттю, а тому складається із багатьох елементів. Комплекс питань інформаційної безпеки держави включає такі сфери державної діяльності, як: захист та обмеження обігу інформації; захист інформаційної інфраструктури держави; захист персональних даних; безпека розвитку інформаційної сфери держави; захист національного інформаційного ринку; попередження інформаційного тероризму та інформаційної війни[124].

У даному дослідженні нам хотілося б детальніше зупинитися на особливостях регулювання питання захисту персональних даних у ЄС, оскільки дане питання стосується кожного громадянина, а захист персональних даних індивіда є первинним елементом інформаційної безпеки в цілому.

Перш за все, потрібно проаналізувати джерела нормативно-правового регулювання захисту персональних даних у ЄС. Вперше норми, що регулювали дане питання були складовою права на приватність та були вперше закріплені у Міжнародному Пакті про громадянські та політичні права 1966 р.

У Конвенції про захист прав людини і основоположних свобод 1950 р. міститься норма, що: «Кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції».

У Конвенції № 108 Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» закріплено ключові принципи обробки персональних даних, права особи у зв'язку з обробкою її персональних даних, базові норми щодо транскордонної передачі даних.

8 листопада 2001р., було прийнято Додатковий протокол до цього міжнародного договору, який деталізував положення Конвенції в частині, що стосується транскордонної передачі даних.

На сьогоднішній день найактивнішу діяльність у сфері захисту персональних даних здійснює Європейський Союз. Директива 95/46/ЄС Європейського Парламенту та Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року (далі – Директива) була базовим документом, який встановлює достатньо детальні вимоги щодо того, як має бути організована система захисту персональних даних у державі.

---

[124] Соснін О. В. Інформаційна політика України: проблеми розбудови URL: http://www.niisp.gov.ua/vydanna/panorama

Цей документ був ключовим у системі захисту персональних даних держав-членів Європейського Союзу, який є орієнтиром розвитку законодавчої бази. Також Закон України «Про захист персональних даних» базується фактично повністю на положеннях Директиви[125].

26 квітня 2016 р. Європейським Союзом було прийнято Загальний регламент захисту даних №2016/679, який став найсучаснішим документом у цій сфері. Даний регламент скасував описану вище Директиву 95/46/ЄС.

Основними положеннями цього регламенту є те, що його положення розповсюджуються на компанії, які займаються обробкою даних резидентів і громадян ЄС, при чому незалежно від місцезнаходження такої компанії. Тому всі компанії, які надають послуги, здійснюють продаж товарів або моніторинг поведінки суб'єктів даних на території ЄС повинні відповідати новим вимогам. Також нові правила захисту розповсюджується навіть на компанії, які на своєму офіційному сайті лише пропонують свої послуги на таких мовах, як, наприклад, англійська, німецька, французька та ін[126] .

Що стосується практики ЄСПЛ, то основним рішенням, що регулює дане питання є рішення у справі «Леандер проти Швеції», де суд вирішив, що зберігання державними органами інформації про особу є втручанням у її право на повагу до приватного життя.

Суд вказав, що держава повинна також вживати розумних заходів із метою дотримання права особи на повагу до її приватного життя (а відтак і права на захист персональних даних) із боку приватних суб'єктів[3].

На національному рівні ключовими документами у сфері захисту персональних даних є Конституція України, Закон України «Про захист персональних даних», документи у сфері захисту персональних даних, прийняті Уповноваженим Верховної Ради України з прав людини. Варто зазначити, що закон «Про захист

---

[125] Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. К. К.І.С., 2015. 220 с.

[126] Аліна Моргунова. Набрав чинності європейський GDPR. Закон і Бізнес. URL:https://zib.com.ua/ua/print/133036-nabrav_chinnosti_reglament_pro_zahist_fizosib_u_zvyazku_iz_o.html

персональних даних» дуже багато своїх положень запозичив від Директива 95/46/ ЄС.

Станом на сьогоднішній день виникла ситуація, при якій на практиці неможливо притягнути до відповідальності за незаконне поширення персональних даних у мережі Інтернет. Так, особу, яка поширила персональні дані, як правило, просто неможливо встановити, оскільки доменне ім'я сайту, де незаконно поширені персональні дані, зареєстроване зазвичай в іншій державі.

Більше того, інформація, надана хостинг-провайдером щодо особи, яка зареєструвала доменне ім'я, також не завжди відповідає дійсності. В інших державах у таких випадках є можливість заблокувати доступ до веб-сторінки чи видалити її.

В Україні станом на сьогодні відсутні будь-які юридичні механізми такого характеру. Як наслідок, ні встановити особу, яка причетна до незаконного поширення інформації, ні заблокувати доступ до такої інформації немає можливості. При цьому усвідомлюючи такий стан справ, правопорушники часто навіть не намагаються приховати незаконність розміщеної інформації.

На даний час абсолютна безкарність поширення інформації в Інтернеті призводить до частих порушень права особи на приватність і відповідальність за такий стан справ повністю лежить на державі.

Отже, підсумувавши все вищесказане, можемо зробити наступні висновки. Основним нормативним актом ЄС, що регулює питання захисту персональних даних є Регламент №2016/679. Не зважаючи на те, що він був прийнятий у 2016 році, тобто про його імплементацію не йшлося під час підписання договору про Асоціацію, варто зазначити, що у разі вступу України до ЄС у нашої держави все ж виникне обов'язок розробити заходи щодо його імплементації.

Цінність Регламенту №2016/679 також полягає у тому, що він пропонує механізми притягнення до відповідальності осіб, які незаконно обробляють чи розповсюджують персональні дані, а тому може стати не лише декларативним, а й ефективним нормативним актом.

Панкевич Іван Миронович
доцент кафедри конституційного права Львівського юридичного інституту імені Івана Франка,
доктор юридичних наук.

ПРО ОСНОВНІ ЗАСАДИ РОЗВИТКУ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА В УКРАЇНІ ПІСЛЯ РЕВОЛЮЦІЇ ГІДНОСТІ

Становлення і розвиток інформаційного суспільства є характерною рисою XXI століття. Саме в інформаційному суспільстві активно розвиваються інформаційні і комунікаційні технології, створюються умови для ефективного використання знань в рішенні найважливіших завдань управління суспільством і демократизації суспільного життя. В широкому значенні під інформаційним суспільством слід розуміти: – суспільство нового типу, яке формується внаслідок глобальної соціальної революції та породжується вибуховим розвитком і конвергенцією інформаційних та комунікаційних технологій; – суспільство знання, тобто таке, в якому головною умовою добробуту кожної людини й кожної держави стає знання, здобуте завдяки безперешкодному доступу до інформації та вмінню працювати з нею; – глобальне суспільство, в якому обмін інформацією не матиме ні часових, ані просторових, ані політичних меж, яке, з одного боку, сприяє взаємопроникненню культур, а з іншого – відкриває кожному співтовариству нові можливості для самоідентифікації[127]. Виходячи із зазначених методологічних міркувань можна визначати поняття інформаційного суспільства як «суспільство з розвиненою інфраструктурою, що формується на основі комп'ютерних засобів телекомунікації, створення, передавання, отримання, зберігання інформації, з високим рівнем інформаційної культури більшості громадян при задоволенні їх різноманітних правомірних потреб, інтересів»[1].

Отже, головними ознаками інформаційного суспільства, що розкривають його сутність в поєднанні різних аспектів є: – індустрія

[127] Гурковський В.І. Державне управління розбудовою інформаційного суспільства в Україні (історія, теорія, практика)/ В.І.Гурковський – «Видавництво «Науковий світ»» МНДЦ з проблем боротьби з організованою злочинністю при РНБ України. 2010. – 396 с.

інформаційних послуг; – інформаційні технології та технології зв'язку (телекомунікації), що постійно розвиваються завдяки науково - технічному прогресу в таких галузях, як електроніка, і наукам, що її забезпечують, а також наукам, що пов'язані з розвитком електроніки: автоматика, інформатика, кібернетика тощо; – зростання потенціалу науки (перехід її у виробничу сферу) для задоволення потреб людей інформацією з подальшим перетворенням її в масові (масово-доступні) знання; – постійне зростання рівня інформаційної культури всіх суб'єктів інформаційних відносин, у тому числі в структурах державного управління1 .

Становлення ІС в різних країнах є передумовою еволюційного переходу до наступної стадії розвитку людства, технологічною основою якої є індустрія створення, оброблення і передачі інформації. Державі належить провідна роль у формуванні ІС, що координує діяльність різних суб'єктів суспільства у процесі його становлення, сприяє інтеграції людей у нове інформаційно-технологічне оточення, розвитку галузей інформаційної індустрії, забезпеченню прогресу демократії і дотримання прав особистості в умовах ІС.

Інформаційна взаємодія держави, суспільства і особистості є найоптимальнішою за використання інформаційних і телекомунікаційних технологій з метою підвищення загальної ефективності діяльності державного механізму, створення інформаційно-відкритого суспільства, розвитку інститутів демократії. На думку Е. Тоффлера перехід від індустріального до інформаційного суспільства несе повністю новий устрій життя, заснований на різноманітних поновлюваних джерелах енергії; на методах виробництва, які виключають доцільність та необхідність більшості фабричних конвеєрів; на новій структурі, яку можна назвати електронним котеджем "; на радикально змінених школах і об'єднаннях майбутнього"[128]. Це приведе до обмеження впливу бюрократії та національних держав, в результаті чого зросте значення демократичних інститутів. На сьогодні стає очевидним, що розвиток ІС в Україні має здійснюватися за допомогою заходів правового забезпечення. Неабияку роль тут повинні відігравати й стратегічні політичні рішення стосовно обрання векторів розвитку ІС.

Сучасний етап розвитку України неможливий без створення ефективної, дієвої інформаційно - комунікативної системи, яка

---

[128] Тоффлер Э. Третья волна: Пер. с англ. / Э. Тоффлер. – М., 2004. – 781 с.

неможлива без активного залучення до процесу прийняття рішень інститутів громадянського суспільства – органів місцевого самоуправління, громадських асоціацій та й самого громадянина. Для цього в країні повинна діяти розвинута система громадянської комунікації, яка передбачає суб'єкт-об'єктну взаємодію, де суб'єктом виступають органи державної влади і різного роду корпоративні організації, а об'єктом – громадськість. В цьому контексті цілком виправданою, на наш погляд, є необхідність удосконалення механізму регулювання процесу обміну інформацією, зокрема обґрунтування впровадження принципу партнерської взаємодії, що передбачає не тільки інформування населення, а і налагодження ефективного зворотного зв'язку, проведення відповідної роз'яснювальної роботи, встановлення громадського контролю за діяльністю органів державної влади та органів місцевого самоврядування.

Основними завданнями громадської комунікації є забезпечення підтримки суспільством дій влади, що досягається підвищенням рівня довіри громадян до державних інституцій; реалізація єдиної державної комунікативної політики шляхом створення системи 96 впливу на громадську думку; формування та підтримка ефективного зворотного зв'язку із громадянами для моніторингу ситуації й оцінювання результатів своєї роботи; налагодження співпраці із громадськими організаціями задля забезпечення інформування громадськості про здійснювану політику та створення й підтримки позитивного іміджу влади. Переваги застосування органами державної влади інформаційних технологій є особливо відчутними, коли необхідно провести консультації із залученням усіх рівнів суспільства. Інформаційна взаємодія органів влади та зацікавленої громадськості має передбачати застосування різних видів консультування - внутрішньо урядових («міжміністерських»), владно-політичних (між різними органами влади), публічних консультацій (з різними суспільно-політичними групами, державними і незалежними, громадськими організаціями, науковими закладами тощо), що можуть відбуватися на всіх етапах прийняття рішень. Зокрема, розроблення на Матеріали всеукраїнської конференції 20 червня 2019 року 103 офіційному веб-сайті органу влади рубрики опитування, яке дає чіткий результат і може бути використане в подальшій роботі[129].

---

[129] Афонін, Е. А. Громадська участь у творенні та здійсненні державної політики / Е. А. Афонін, Л. В. Гонюкова, Р. В. Войтович. - К. : Центр сприяння інституц. розвитку держ. служби, 2006. - 160 с.

Таким чином, Україна обрала курс на входження до загальносвітового інформаційного простору, побудову інформаційного суспільства та створення в управлінні державою так званого відкритого електронного врядування[130]. Це означає розширення кола можливостей використання інформаційно-комунікаційних технологій (далі – ІКТ) для підвищення ефективності діяльності органів державної влади й місцевого самоврядування. По суті, створення сучасної контрольованої державою технологічної основи інформаційнокомунікаційного середовища для оперативної та інтенсивної взаємодії суспільства з державною владою стає запорукою успіху. Саме у цій сфері сьогодні розгортається боротьба за світове лідерство, однак надалі під час реалізації програм упровадження новітніх ІКТ в Україні постає питання розширення функціонального потенціалу інформаційного суспільства щодо забезпечення ефективності функціонування сучасної держави. У цьому контексті концептуального значення для загальної системи комунікації і, зокрема, державного управління набувають питання комунікативної етики, що охоплюють комплекс проблем виховання в людині в умовах розвитку сучасного інформаційного суспільства, спрямована на реалізацію потреб та інтересів сучасної людини.

Отже, можна зробити висновок, що специфічна роль громадянської комунікації полягає в тому, що вона забезпечує поширення, передачу політичної інформації як між елементами політичної системи, так і між політичною системою і навколишнім середовищем. Нерозвиненість даної комунікації є однією з важливих причин низького рівня адаптації політичної системи в цілому та . системи державного управління зокрема, що призводить до втрати її підтримки в суспільстві і їх нестабільності. Тому, дослідження впливу процесу становлення та розвитку інформаційного суспільства на систему державного управління, розширення можливостей для зворотних зв'язків (комунікації) органів державної влади з громадянами на сьогоднішній час дуже важливе і актуальне.

---

[130] 124 Відкрите урядування: колективна робота, прозорість і дієва участь / За ред. Д. Латропа і Л. Руми / Переклад з англ. А. Іщенка. – К.: Наука, 2011. – 536 с.

РЕКОМЕНДАЦІЇ
учасників всеукраїнської конференції «Інформаційна безпека в сучасному світі та її вплив на конституційний лад в Україні: теорія і практика»

1. У результаті проведення конференції учасники відзначили багатозначність інформаційної безпеки, її комплексний та всеохоплюючий характер. Автори висловили наступні міркування:

- загальне поняття «безпека» переважно тлумачиться у міжнародно-правовому розумінні, обґрунтованому ООН, як «сталий людський розвиток», тобто такий розвиток, який веде не тільки до економічного, а й до соціального, культурного, духовного зростання, що сприяє гуманізації менталітету громадян і збагаченню позитивного загальнолюдського досвіду. Тут зазначене розуміння акцентує увагу на окремих сферах суспільного життя;

- родове поняття «національна безпека» акумулює в собі основні ознаки загального, визнаного на міжнародному рівні поняття «безпека», деталізуючи на рівні національного права сфери суспільної безпеки та безпекової політики;

- видове поняття «інформаційна безпека» уособлює окрему сферу національної безпекової політики – інформаційну (інформаційно-комунікативну) сферу, окремим напрямом якої є кібербезпека.

2. Варто висловити підтримку позиції учасників конференції щодо:

Інформаційна війна, яка інтенсивно ведеться проти України Російською Федерацією стала істотним компонентом гібридної війни. Втягнутими в неї виявились фактично, усвідомлено чи ні, більшість громадян держави. Результати виборів Президента України та народних депутатів України у 2019 році переконливо свідчать про домінуючий суспільний запит на здійснення корінних змін у всіх сферах державотворення. Істотним є звинувачення владі у відсутності дієвих гарантій щодо реалізації конституційних прав і свобод громадян, в т.ч. й на інформацію. Ми повинні виграти інформаційну війну, виграти всю війну. А далі складний й тривалий процес “гуманітарного розмінування” тимчасово окупованих територій.

3 Для виявлення та аналізу загроз, які існують в інформаційній сфері необхідно удосконалити організаційно-правові механізми взаємодії даного Міністерства із іншими органами, які мають гарантувати інформаційну безпеку держави. Проте, слід пам’ятати, що

наявність у майбутньому цих механізмів не гарантуватиме успіху в інформаційній боротьбі, було б бажання діяти та змінювати ситуацію на користь нашої держави.

4. Основу розв'язання проблем надання адміністративних послуг із застосуванням інформаційних технологій покладений комплексний підхід, що включає широкий спектр заходів, а саме:

- удосконалення чинного законодавства, у тому числі закріплення еквівалентності юридичної сили результатів надання адміністративних послуг в електронній формі й письмовій формі на паперових носіях в єдиному законодавчому актів щодо регулювання адміністративних процедур;

- формування механізмів ефективної взаємодії та інтеграції інформаційних систем органів державної влади й органів місцевого самоврядування на базі Єдиного державного порталу надання адміністративних послуг;

- широке інформування споживачів адміністративних послуг про можливість отримати їх в електронній формі та розроблення заходів заохочення отримувати послуги саме в електронній формі;

- розроблення ефективних механізмів електронної ідентифікації й автентифікації споживачів адміністративних послуг в електронній формі з метою безпечного користування електронними сервісами надання адміністративних послуг;

- створення правових і організаційних передумов для надання органами публічної адміністрації транскордонних адміністративних послуг;

- приділення достатньої уваги спеціальному навчанню й перекваліфікації державних службовців та інших осіб, які надають адміністративні послуги на підставі закону.

5. У сфері нотаріату лише особиста свідомість кожного нотаріуса та спільна співпраця МЮУ з Нотаріальною палатою України, можуть дати результат надійного захисту нотаріальної сфери, а отже і надійного захисту інтересів, прав та майна фізичних та юридичних осіб, та й держави в цілому.

6. Рекомендаціями щодо протидії корупційним проявам можуть бути такі: Звернутись необхідно у письмовій формі. У заяві необхідно у довільній формі викласти всі відомі Вам факти корупційного порушення. При наявності до заяви можна прикласти докази на підтвердження викладених у ній обставин. Фактами, що вказують на наявність корупційного правопорушення, можуть бути документи, що підтверджують витрачання коштів, посилання на журналістські

розслідування у пресі, аудіо- чи відеозаписи, Ваші власні розслідування тощо.

7. Під час удосконалення нормативно-правової бази законодавства у сфері доступу до публічної інформації в діяльності органів державної влади та місцевого самоврядування необхідно враховувати не тільки необхідність гармонізації всього пласту загальних і спеціальних правових актів у цій сфері, але і відсутність прозорого механізму доведення до громадськості інформації органами влади та місцевого самоврядування попри спроби запровадити механізми зворотного зв'язку влади та громадян.

Вирішення проблем публічної влади в інформаційній сфері призведе до таких важливих наслідків, як зменшення кількості ухвалених незаконних рішень влади шляхом оприлюднення планів виконання поточних завдань і загальних звітів про діяльність органів публічної влади; попередження незаконності та проявів корупції в діях чи бездіяльності посадових осіб органів державної влади та місцевого самоврядування; підвищення правосвідомості як самих представників органів влади та місцевого самоврядування, так і громадськості шляхом створення при окремих державних органах громадських і експертних рад, комісій та інших громадських утворень; спрощення доступності публічної інформації для пересічних громадян шляхом доступу до мережі Інтернет, а саме – до створених веб-сайтів із системно викладеною публічною інформацією про діяльність органів влади та місцевого самоврядування.

8. Для протидії використанню сучасних технології негативних інформаційно-психологічних впливів, які стають загрозою українському національному інформаційному простору та суверенітету держави. Гарантування інформаційної безпеки України в умовах дестабілізаційних негативних інформаційно-психологічних впливів та експансіоністської агресивної інформаційної політики Російської федерації, потребує консолідації зусиль на усіх рівнях державної влади та громадянського суспільства. Як протидія масштабним негативним інформаційно-психологічним впливам, операціям та війнам, пріоритетними напрямами державної інформаційної політики та важливими кроками з боку владних органів України мають бути: 1) інтеграція України до світового та регіонального європейського інформаційного просторів; 2) інтеграція у міжнародні інформаційні та інформаційно-телекомунікаційні системи та організації; 3) створення власної національної моделі інформаційного простору та забезпечення розвитку інформаційного суспільства; 4) модернізації усієї системи інформаційної безпеки держави та формування й реалізація ефективної

інформаційної політики; 5) удосконалення законодавства з питань інформаційної безпеки, узгодження національного законодавства з міжнародними стандартами та дієве правове регулювання інформаційних процесів; 6) розвиток національної інформаційної інфраструктури; 7) підвищення конкурентоспроможності вітчизняної інформаційної продукції та інформаційних послуг; 8) впровадження сучасних інформаційно-комунікативних технологій у процеси державного управління; 9) ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації та коригуванні державної політики в інформаційній сфері.

Інформаційне видання

Інформаційна безпека в сучасному світі та її вплив на конституційний лад в Україні: теорія й практика:

Матеріали всеукраїнської конференції
(м. Івано-Франківськ, 20 червня 2019 року)

Електронне видання

Видавець
Прикарпатський національний університет
імені Василя Стефаника
76025, м. Івано-Франківськ,
вул. С.Бандери, 1, тел.: 71-56-22
E-mail: vdvcit@pu.if.ua
Свідоцтво суб'єкта видавничої справи ДК № 2718
від 12.12.2006

ISBN-978-966-640-456-8