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

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 ВДНЗ «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.

УДК 342.(081)
ББК 67.9
Р 43

Матеріали друкуються в авторській редакції.

За повного або часткового відображення матеріалів даної публікації, посилання на видання обов'язкове.

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 : ВДНЗ «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 ВДНЗ «Прикарпатський національний університет імені Василя Стефаника» і проведеній 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.

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

УДК 342.(081)
ББК 67.9