ПРИНЦИПИ ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ ЗА ПРАВОПОРУШЕННЯ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ПАРПАН Уляна Михайлівна - доктор юридичних наук, доцент, професор кафедри адміністративного та інформаційного права Навчально-наукового інституту права, психології та інноваційної освіти Національного університету «Львівська політехніка»

МАЛЕЦЬ Марта Романівна - асистент кафедри адміністративного та інформаційного права Навчально-наукового інституту права, психології та інноваційної освіти Національного університету «Львівська політехніка»

ВІТИК Орест Дмитрович – ЗВО «Львівський університет бізнесу та права»

УДК 342.92.2:343.346.8

DOI 10.32782/LAW.2020.3.8

В статье исследуются принципы юридической ответственности за правонарушения в сфере обеспечения информационной безопасности через философский и специально-юридический аспекты. Анализ научной литературы позволяет выделить несколько подходов к пониманию юридической ответственности в сфере обеспечения информационной безопасности, воплощают личностный и государственно-властный подходы, что обусловлено общеправовыми, межотраслевыми и отраслевыми принципами. Категория принципы в сфере обеспечения информационной безопасности позволяет наиболее точно передать правовую природу юридической ответственности, в связи с чем внимание уделено характерным чертам, соотношением с понятием «информационные права» через категорию «информационная безопасность». Выделенные универсальные признаки принципов, которые воплощают правовую природу юридической ответственности независимо от подхода к определению.

Ключевые слова: юридическая ответственность, информационная безопасность, принципы, правонарушения, кибербезопасность, информационная инфраструктура.

Постановка проблеми

Стрімкий розвиток інформаційно-комунікаційних технологій, інформатизація та цифровізація не тільки всіх сфер життєдіяльності, а й окремих напрямів економіки, з одного боку, сприяють розвитку інформаційного суспільства, з іншого? створюють умови для виникнення нових викликів і загроз для інформаційної безпеки в цифровому середовищі та інформаційному просторі. З метою досягнення сталого розвитку сучасного світу та інформаційного простору, всі країни повинні консолідувати зусилля з розробки нових інструментів забезпечення міжнародної інформаційної безпеки, продовжувати вдосконалювати національне законодавства та зміцнювати міжнародну співпрацю.

Стан дослідження

Важливе значення для розробки проблеми мали праці вчених-правознавців: В. Б. Авер'янова, О. Ф. Андрійко, А. І. Берлача, О. П. Віхрова, П. В. Діхтієвського, І. С. Гриценка, Є. В. Додіна, Р. А. Калюжного, С. В. Ківалова, А. А. Козловського, М. І. Козюбри, Т. О. Коломоєць, В. К. Колпакова, О. В. Кузьменко, В. І. Курила, Є. В. Курінного, Р. С. Мельника, В. Я. Настюка, О. І. Остапенка, В. Л. Ортинського, А. О. Селіванова, О. І. Харитонової, В. В. Цвєткова, Я. М. Шевченко, Ю. С. Шемчушенка та інших.

Мета статті – дослідження принципів юридичної відповідальності за правопорушення е сфері забезпечення інформаційної безпеки.

Виклад основного матеріалу

Одним з основних завдань, що сприяють досягненню інформаційної безпеки України, є формування системи інформаційної безпеки не тільки на глобальному рівні, а й у

форматах міждержавного співробітництва в рамках Європейського Союзу та Північно-Атлантичного альянсу. Виходячи з цього, актуальним є дослідження питання про роль принципів правового забезпечення інформаційної безпеки в інформаційному просторі та цифровому середовищі.

Значення загальноправових, галузевих і міжгалузевих принципів сьогодні є не менш актуальним, аніж після Другої світової війни, коли було сформовано сучасну систему міжнародної безпеки та створено Організацію Об'єднаних Націй.

О. В. Зайчук вказує, що принципи права – це ідеї про те, як людське товариство в разі ефективної адаптації до конкретної поточної ситуації може бути організоване за допомогою права найкращим чином, із забезпеченням гідного в поточній і в довгостроковій перспективі існування кожного індивіда, готового слідувати певній моделі поведінки, з оптимальною організацією приватної та публічної сфер, покликаної сприяти гідному існуванню, з профілактикою та мінімізацією особистих і групових конфліктів і оптимальним виправленням наслідків [1, с. 22].

Модель соціальної поведінки, рекомендована об'єктивним принципом, повинна розумітися як абсолютно оптимальна для кожного з представників людства. Вона максимально органічно відповідає людській природі і тільки дотримання здатне забезпечити людині та суспільству кращі з можливих наслідків індивідуальних або групових рішень і дій.

Необхідно зауважити, що сьогодні єдина система принципів інформаційної безпеки на доктринальному та нормативному рівні ще не сформована. У цьому контексті,- Т. С. Перун зазначає, що принципи інформаційного права повинні забезпечувати гармонійну взаємодію різних суб'єктів: власників інформаційних ресурсів й інформаційних систем, держави та споживачів інформаційних послуг, а також безпосередньо інформаційних технологій та інформаційних ресурсів, призначених для забезпечення функціонування інформаційних процесів, зокрема забезпечення створення, поширення, використання, систематизації, збереження і знищення інформації [2, с. 104]. З огляду на те, що принципи як основні засади створюють фундамент правового регулювання, їх можна класифікувати, використовуючи класичний підхід, у такий спосіб.

1. Загальноправові принципи інформаційного права, які одночасно є універсальними для інших галузей права.

До них відносяться законність, рівність усіх перед законом і судом, справедливість, гуманізм і демократизм. Важливим кроком для розвитку права, загальних принципів і людства є Загальна декларація прав людини, прийнята 10 грудня 1948 року Генеральною Асамблеєю ООН, де міститься основа для базового принципу інформаційного права – шукати, одержувати, поширювати інформацію й ідеї будь-якими засобами незалежно від державних кордонів [3].

Подібні положення містяться в Міжнародному пакті про громадянські та політичні права, ухваленому 16 грудня 1966 Резолюцією 2200 (XXI) на 1496-му пленарному засіданні Генеральної Асамблеї ООН, з яких випливає, що користування такими правами накладає особливу відповідальність, яка повинна бути встановлена законом [4].

Принципи права є інструментом системного, телеологічного, логічного тлумачення права, подолання колізій та прогалин у праві, створення в цих умовах норм права. Ці конституційно-закріплені принципи мають ключове значення для подальшого розвитку науки інформаційного права та регулювання правового забезпечення інформаційної безпеки.

Принцип рівності при забезпеченні інформаційної безпеки передбачає рівність усіх перед законом при реалізації прав на безпечне інформаційне середовище, безпечні технології, а стосовно відповідальності – рівність при застосуванні державою щодо суб'єкта примусових заходів при порушенні законодавства в цій сфері.

Принцип справедливості повинен забезпечувати відповідний рівень прав і свобод суб'єктів інформаційного обміну незалежно від їх статусу. Правове регулювання у цьому випадку має справедливо забезпечити інтереси особи, суспільства та держави на основі балансу між можливою поведінкою суб'єктів.

Принцип гуманізму у сфері інформаційної безпеки та відповідальності виражаєть-

ся в необхідності пропорційності обмежень при забезпеченні інформаційної безпеки, заборону застосування технологій, що принижують людську гідність або призначення невідповідного покарання за делікт суб'єкту, який вчинив правопорушення в інформаційній сфері. Як зазначають автори монографії «Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології», виникнення та поширення інформаційних деліктів зумовлено соціальними і технологічними трансформаціями в процесі становлення суспільства нового формату – інформаційного, глобального інформаційного, суспільства знань [5, с. 180].

2. Міжгалузеві принципи забезпечення інформаційної безпеки та інформаційного права загалом.

Передусім, це гласність, презумпція невинуватості, невідворотність покарання. До важливих міжгалузевих принципів можна віднести принцип довіри та принцип державного суверенітету.

Принцип довіри у сфері забезпечення інформаційної безпеки означає, що суб'єкти інформаційного обміну не завдадуть шкоди інформаційної безпеки іншим суб'єктам, інфраструктурі; їх дії матимуть позитивний характер для інших учасників, що виражається в дотриманні прав і свобод та надання взаємної допомоги при виникненні комп'ютерних інцидентів.

Принцип державного суверенітету в інформаційній сфері є одним із найбільш складних. Т. Ю. Ткачук у дисертаційному дослідження «Правове забезпечення інформаційної безпеки в умовах євроінтеграції України» пише, що основною метою державної інформаційної політики України є забезпечення: захисту інформаційного суверенітету держави (особливо захист національного інформаційного простору з інформаційним ресурсом і систем формування масової суспільної свідомості) [6, с. 354].

В умовах глобального інформаційного суспільства кордони держав виявилися розмитими, а з урахуванням непростих міжнародних і міждержавних відносин і сучасної архітектури співпраці у сфері інформаційної безпеки державний суверенітет в інформаційній сфері має безліч правових, політичних та культурних аспектів.

Збереження державного суверенітету в інформаційній сфері доцільно визначити, як можливість захисту держави в інформаційній сфері та самостійне визначення політики в інформаційній сфері, засноване на невтручанні в інформаційний суверенітет інших держав, аналогічно щодо інших держав до власного державного суверенітету в інформаційній сфері.

Цей принцип знайшов відображення в Резолюції Генеральної Асамблеї ООН від 5 грудня 2018 року «Досягнення у сфері інформатизації і телекомунікацій у контексті міжнародної безпеки», в якій довіра та безпека у використанні інформаційно-комунікаційних технологій віднесені до головних опор інформаційного суспільства, стійку глобальну культуру кібербезпеки необхідно заохочувати, формувати, розвивати і активно впроваджувати [7].

3. Галузеві принципи інформаційного права, які сформульовані в теорії інформаційного права та в нормативно-правових актах різного рівня.

Згідно зі ст. 3 Закону України «Про інформацію» від 2 жовтня 1992 року № 2657-XII регулювання відносин у цій сфері базується на таких принципах: свобода пошуку, отримання, передачі, виробництва, поширення інформації будь-яким законним способом; відкритість інформації про діяльність державних органів і органів місцевого самоврядування та вільний доступ до такої інформації, крім випадків, встановлених законами. Вказані принципи співвідносяться з Цілями сталого розвитку України на період до 2030 року [8].

У Законі України «Про основні засади забезпечення кібербезпеки України» закріплено низку принципів, з яких до галузевих можна віднести: принцип безперервності, який передбачає цілодобове функціонування засобів захисту інформаційної інфраструктури від зовнішніх загроз і комп'ютерних атак; принцип комплексності, що означає застосування організаційно-правових, технічних засобів і методів, які в сукупності дозволяють забезпечувати безпеку критичної інформаційної інфраструктури України [9].

Принципом, що має практичне значення, є збереження традиційних для громадян форм отримання інформації. Наприклад,

при функціонуванні інформаційної системи, метою якої є надання адміністративних послуг в електронній формі.

Важливим міжнародним принципом, який може бути застосований у сфері інформаційної безпеки, є принцип загального обов'язку, закріплений у Декларації тисячоліття Організації Об'єднаних Націй, прийнятій резолюцією Генеральної Асамблеї ООН 8 вересня 2000 року № 55/2. Хоча цей принцип не торкається питань інформаційної безпеки безпосередньо, його дотримання сприяє стабілізації міжнародних відносин, зокрема у цій галузі [10].

Визначається цей принцип через необхідність усунення загроз міжнародній інформаційній безпеці. У разі впровадження та розвитку нейромереж принцип достовірності інформації буде вкрай важливим для прийняття на основі великих даних (big data) рішень, в основі яких буде аналіз інформації, проведений нейромережею.

Згідно з прогнозами прискорення темпів зростання та розвитку цивілізації буде відбуватися швидко. Розвиток штучного інтелекту та машинного навчання може дати поштовх для подальшого розвитку людства, але супроводжується певними ризиками. При такій динаміці розвитку технологій залишається відкритим питання про достатність тих основоположних засад, багато з яких були сформовані в римському праві.

Правові засади повинні впливати на статус, функціональний та правовий режим технології (гуманізм, справедливість, невідворотність покарання, пропорційність тощо), а не навпаки.

У найближчому майбутньому можливе формування нових принципів інформаційної безпеки. Проблеми цифрової економіки активно обговорюються в юридичному середовищі, органами державної влади, експертним співтовариством і суспільством загалом.

У 2018 році Кабінетом Міністрів України було схвалено Концепцію розвитку цифрової економіки та суспільства України на 2018–2020 роки та затверджено план заходів щодо її реалізації, яка запустила масштабну системну програму розвитку економіки нового технологічного покоління – цифрової економіки. У Концепції розвитку цифрової економіки було визначено п'ять базових напрямів. До таких напрямів віднесено: нормативне регулювання, кадри, освіта, формування дослідницьких компетенцій і технічних напрацювань, інформаційна інфраструктура та інформаційна безпека [11].

Процес цифровізації, особливо використання низки цифрових технологій, породжує низку ризиків і загроз. У зв'язку з цим питання інформаційної безпеки практично в усіх інформаційних процесах стають ключовими і на національному, і на міжнародному рівнях. Правове регулювання Інтернет–відносин – це комплексна проблема не тільки юридичної науки, а й практики [12, с. 152].

Одним з важливих компонентів системи забезпечення інформаційної безпеки є інститут юридичної відповідальності. Він виконує низку функцій у цій системі: превентивну, охоронну. Цей інститут дозволяє забезпечувати на певному етапі розвитку інформаційного суспільства дотримання більше половини вимог у сфері забезпечення інформаційної безпеки на національному рівні.

Проблематика інформаційної безпеки набуває в умовах розвитку інформаційного суспільства всеосяжний, міжгалузевий характер і тому питання, пов'язані з правовим забезпеченням інформаційної безпеки і юридичною відповідальністю в інформаційній сфері, привертають увагу фахівців різних галузей науки. Важливе теоретико-правове значення для розвитку інституту юридичної відповідальності в галузі забезпечення інформаційної безпеки має оптимізація системи принципів. Для правового регулювання відносин, пов'язаних з юридичною відповідальністю, важлива уніфікація загальновизнаних, загальноправових і закріплених в окремих законодавчих актах галузевих принципів регулювання інфосфері, інформаційно-комунікаційних технологій та захисту інформації.

У контексті Закону України «Про національну безпеку України», який констатує важливість збереження принципу територіальної цілісності та державного суверенітету, доцільно виділити такі важливі принципи, необхідні для подальшого розвитку інформаційного суспільства та забезпечення інформаційної безпеки, як довіра та безпека у використанні інформаційно-комунікаційних

технологій, що випливають з необхідності заохочувати, формувати, розвивати і активно впроваджувати стійку культуру кібербезпеки у контексті європейської інтеграції України на підставі реалізації Угоди про асоціацію між Україною, з одного боку, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншого боку [13; 14].

У сфері безпеки об'єктів критично важливої інформаційної інфраструктури необхідно виділяти два тісно взаємопов'язаних, але різних за змістом напрями: формування та забезпечення безпечного функціонування системи; забезпечення безпеки [15, с. 2004]. З метою вдосконалення системи інформаційної безпеки від різних викликів і загроз пропонується закріпити в інформаційному законодавстві принцип презумпції безпеки об'єктів критичної інформаційної інфраструктури. Принцип встановлює, що об'єкти критичної інформаційної інфраструктури вважаються захищеними, поки організаційно-правове забезпечення безпеки на зазначених об'єктах відповідає вимогам, закріпленим у нормативно-правових актах у сфері забезпечення інформаційної безпеки.

Застосування цього принципу дозволить обґрунтовано кваліфікувати правопорушення з метою підвищення ефективності правозастосовної практики у сфері забезпечення інформаційної безпеки.

Висновки

Підсумовуючи викладене вище, можемо констатувати, що процеси інформатизації та цифровізації, які активно відбуваються в Україні, стосуються всіх сфер життя, включаючи економіку, соціальну сферу, охорону здоров'я і освіту, спрямовані на розвиток інформаційного суспільства, але тягнуть нові ризики, виклики та загрози для інформаційної безпеки в інформаційному просторі та цифровому середовищі. Забезпечення сталого розвитку України, безпеки інформаційного простору можливо лише за умови об'єднання зусиль усіх держав-членів Європейського Союзу та НАТО у створенні нових правових інструментів і механізмів для розвитку ефективної системи міжнародної та інформаційної безпеки, вдосконалення національного законодавства, зміцнення міжнародного співробітництва на основі розвитку базових принципів інформаційної безпеки.

Література

1. Зайчук О. В. Принципи права в контексті розвитку загальної теорії держави і права. URL: http://dspace.nbuv.gov.ua/bitstream/handle/ 123456789/63854/04-Zaychuk.pdf?sequence=1

2. Перун Т. С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні: дис. … канд.. юрид. наук: спец.: 12.00.07. Львів, 2019. 268 с.

3. Загальна декларація прав людини. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/995_015

4. Міжнародний пакт про громадянські та політичні права. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/995_043

5. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології: *монографія*.- І. В. Арістова, О. А. Баранов, О. П. Дзьобань та ін. Київ: КВІЦ, 2019. 344 с.

6. Ткачук Т. Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України: дис. … д-ра юрид. наук: спец.: 12.00.07. Ужгород, 2019. 487 с.

7. Резолюция, принятая Генеральной Ассамблеей 5 декабря 2018 года [по докладу Первого комитета (A/73/505)] 73/27. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. URL: https://undocs.org/pdf?symbol=ru/A/RES/73/27

8. Про Цілі сталого розвитку України на період до 2030 року: Указ Президента України від 30.09.2019 р. № 722/2019. URL: https://zakon.rada.gov.ua/laws/show/722/2019

9. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.

10. Декларації тисячоліття Організації Об'єднаних Націй. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/995_621

11. Про схвалення Концепції розвитку цифрової економіки та суспільства України

АНОТАЦІЯ

У статті досліджуються принципи юридичної відповідальності за правопорушення у сфері забезпечення інформаційної безпеки через філософський та спеціально-юридичний аспекти. Аналіз наукової літератури дозволяє виділити декілька підходів до розуміння юридичної відповідальності у сфері забезпечення інформаційної безпеки, які втілюють особистісний та державно-владний підходи, що зумовлено загальноправовими, міжгалузевими та галузевими принципами. Категорія принципи у сфері забезпечення інформаційної безпеки дозволяє найбільш точно передати правову природу юридичної відповідальності, у зв'язку з чим увага приділена притаманним рисам, співвідношенням із визначенням «інформаційні права» через категорію «інформаційна безпека». Виділені універсальні ознаки принципів, які втілюють правову природу юридичної відповідальності незалежно від підходу до визначення.

Ключові слова: юридична відповідальність, інформаційна безпека, принципи, правопорушення, кібербезпека, інформаційна інфраструктура.

SUMMARY

The article explores the principles of legal responsibility for offenses in the field of information security through philosophical and special legal aspects. The analysis of the scientific literature allows us to identify several approaches to understanding legal responsibility in the field of information security, which embody personal and state-governmental approaches, which are conditioned by generally legal, inter-sectoral and sectoral principles., in connection with which attention is paid to the inherent features, correlation with the definition of «information rights» through the category of in «organizational safety». There are universal features of principles that embody the legal nature of legal liability, regardless of approach to definition.

One of the important components of the information security system is the institution of legal responsibility. It performs a number of functions in this system: preventive, protective. This institute allows to ensure at a certain stage of development of the information society compliance with more than half of the requirements in the field of information security at the national level.

It is noted that the issue of information security in the development of the information society becomes comprehensive, intersectoral in nature, and therefore issues related to the legal provision of information security and legal responsibility in the information field, attract the attention of experts in various fields of science. The optimization of the system of principles is of great theoretical and legal importance for the development of the institution of legal responsibility in the field of information security. For the legal regulation of relations related to legal liability, it is important to unify the generally recognized, common law and enshrined in certain legislation industry principles of regulation of the infosphere, information and communication technologies and information protection.

Key words: legal responsibility, information security, principles, offenses, cyber security, information infrastructure.

на 2018–2020 роки та затвердження плану заходів щодо її реалізації: Постанова Кабінету Міністрів України від 17.01.2018 р. № 67-р. URL: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80

12. Бортник Н., Єсімов С. Відносини в мережі Інтернет як об'єкт правового регулювання. *Вісник Національного університету «Львівська політехніка»*. Юридичні науки. 2019. Вип. 6. № 22. С. 147–153.

13. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.

14. Про ратифікацію Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: Закон України від 16.09.2014 р. № 1678-VII. *Відомості Верховної Ради України*. 2014. № 40. Ст. 2021.

15. Єсімов С., Ковалів М., Скриньковський Р. Правові аспекти формування системи безпеки об'єктів критично важливої інформаційної інфраструктури. *Traektoriâ Nauki = Path of Science*. 2018. Vol. 4. № 7. S. 2001–2018.