УДК: 34.096+321.01
DOI: https://doi.org/10.32366/2523-4269-2021-77-4-116-126

Веселов Микола Юрійович,
доктор юридичних наук, доцент
(Донецький державний університет внутрішніх справ, м. Кривий Ріг)
ORCID: https://orcid.org/0000-0002-3963-2764

Рекуненко Тетяна Олександрівна,
кандидат юридичних наук, доцент
(Донецький державний університет внутрішніх справ, м. Кривий Ріг)
ORCID: https://orcid.org/0000-0001-7668-0581

Волкова Дар'я Максимівна,
здобувачка вищої освіти
(Національний університет «Одеська юридична академія», м. Кривий Ріг)
ORCID: https://orcid.org/0000-0002-5131-8305

БЕЗПЕКОВИЙ ПІДХІД У ПРАВОВОМУ РЕГУЛЮВАННІ ІНФОРМАЦІЙНИХ ВІДНОСИН

У статті обґрунтовується значення та специфіка «безпекового» підходу в регулюванні інформаційних відносин для досягнення інформаційної безпеки в державі. Цей підхід полягає в тому, що, надаючи правову оцінку і включаючи певні суспільні відносини, пов'язані з обігом інформації, у нормативну площину, законодавець та інші суб'єкти нормотворення спільно з відповідними фахівцями мають попередньо проводити «безпекову» експертизу з метою виявлення і прогнозування всіх можливих загроз інформаційній безпеці, які можуть виникнути або вже де-факто існують на практиці. Результати таких експертних досліджень повинні враховуватися під час вибору методів та форм правового регулювання чинних і нових інформаційних відносин.

Ключові слова: *інформація; інформаційні відносини; правове регулювання; інформаційна безпека; забезпечення інформаційної безпеки.*

Постановка проблеми. На сучасному етапі еволюції суспільства та розвитку ІТ-технологій інформатизація все більше стає глобальним, усеохоплюючим процесом, що проникає в усі сфери суспільного життя. Уважаємо, що не виникне жодних заперечень, якщо припустити, що цей процес перетворюється в один з основних чинників суспільного розвитку і багато в чому характеризує сучасну соціальну динаміку. Завдяки процесу інформатизації відбуваються системні зміни, згідно з якими всі сфери діяльності державних (владних) інституцій, усі сегменти суспільства й кожна окрема людина включаються в глобальний інформаційний простір, стаючи при цьому елементами глобальної інформаційної системи та, відповідно, тією чи іншою мірою залежними від неї.

© Веселов М. Ю., Рекуненко Т. О, Волкова Д. М., 2021

Зазначена інформаційна залежність стосується всього світу в цілому, усіх держав і людей, що беруть участь у процесі виробництва, зберігання і використання інформації під час інформаційного обміну та інформаційної взаємодії. Інформаційна взаємодія та комунікація вже стали планетарними факторами, спричинивши цілу низку соціальних трансформацій і викликавши в системі соціальних відносин такі процеси і поняття, як інформаційні війни, інформаційна зброя, інформаційний тероризм, інформаційна злочинність, і як наслідок – інформаційна безпека. Сучасні соціальні практики та різноманітні дослідження свідчать, що суспільний розвиток на основі глобальної інформатизації створює передумови для появи якісно нових викликів, загроз і ризиків інформаційної безпеки. Указана обставина робить актуальним дослідження цього явища як правової категорії.

В умовах внутрішньої та зовнішньої інформаційної агресії та виникнення нових глобальних викликів у цій сфері, з огляду на потребу ефективного захисту українського суспільства й держави, вагомість функції правового забезпечення безпеки інформаційних відносин зростає. Слід також наголосити, що інформаційна безпека є сьогодні однією з найважливіших складових національної безпеки України, значною мірою визначаючи стан захищеності, зокрема і правової, її життєво важливих інтересів. Окінавська хартія глобального інформаційного суспільства [1] також визнала правове забезпечення інформаційної безпеки одним із пріоритетів у процесі розбудови такого суспільства.

Аналіз останніх досліджень і публікацій. Слід констатувати, що інформаційні відносини, «інформаційна безпека» як їх складова останнім часом привертають усе більше уваги з боку науковців-правників. Дослідженню базових правових засад та категорій, а також окремих проявів забезпечення інформаційної безпеки присвячено праці І. Бачила, К. Бєлякова, Л. Веселової, С. Вітвіцького, А. Гевлич та В. Селиванова, В. Гурковського, О. Користіна та Ю. Кардашевського, І. Коропатника та О. Золотар, В. Ліпкана, Х. Рейнгольда [2–11] тощо. Перераховано лише частину тих наукових праць, матеріали яких були використані під час написання статті. Але, попри наявність начебто великої кількості наукових робіт на заявлену тематику, тема інформаційних відносин та їх правового регулювання від цього не стає менш важливою та обговорюваною, тому що нові виклики безпеці та забезпеченню прав людини в цій сфері генерують актуальні питання, які потребують наукового вивчення та вирішення.

Метою цієї **статті** є обґрунтування значення та специфіки «безпекового» підходу в регулюванні інформаційних відносин для забезпечення інформаційної безпеки в державі.

Виклад основного матеріалу. В історії людства виділяють чотири етапи інформаційно-технологічної революції, які помітно змінили характер цивілізаційного розвитку. Перший етап пов’язується з виникненням та інтенсивним розвитком науки кібернетики, створенням на її основі інформаційних систем управління; другий – характеризується масовим упровадженням персональних комп’ютерів; третій – співвідноситься з розвитком телекомунікаційних технологій, об’єднанням персональних комп’ютерів у комп’ютерні мережі, спочатку в локальні, а потім і глобальні – «Internet», «Fidonet» та ін. При цьому, як слушно зауважує Х. Рейнгольд, вибудовування інформаційних мереж викликало чимало гострих дебатів з приводу допустимості таких термінів (а відповідно і явищ, які вони охоплюють), як «кіберпростір», «інтернет-право», «кіберправо», необхідності правового врегулювання умов використання інформаційних технологій на рівні окремого законодавчого акта тощо [11]. Для четвертого, сучасного етапу, який почався в кінці XX ст. і триває до сьогодні, характерним є формування глобального інформаційного простору. Інформація стає ключовим комунікативним ресурсом у міжнародному та міжрегіональному масштабах, у створенні транснаціональних інформаційних мережевих просторів, у виникненні взаємозалежності держав і соціуму від накопичення та обміну інформацією, у мережевому обслуговуванні всіх видів суспільних відносин.

У загальному значенні інформацією є відомості про навколишній світ і явища, що тривають у ньому, через сприймання їх людиною; повідомлення, що інформують про стан справ, про стан чогось [12, с. 40]. Інформація існує в різних формах. Вона може бути надрукованою або написаною на папері, зберігатися в електронному вигляді, передаватися поштою або з використанням електронних засобів зв'язку, демонструватися на плівці або бути вираженою усно. Нині, коли йдеться про інформаційну безпеку, здебільшого асоціюємо її саме з тією інформацією, яка знаходиться в цифровому комунікативному середовищі, перебуває в електронному форматі. Але це лише частина того об'єкта, що підлягає захисту, стан захищеності останнього охоплюється поняттям кібербезпеки. Законодавство України подає таке визначення інформації, як «будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» [13, ст. 1]. Проте слід зауважити, що всі інші форми інформації сьогодні так чи інакше мають цифрове відтворення та утворюють інформаційний кіберпростір, елементи якого ґрунтовно проникли в усі сфери життєдіяльності людини, суспільства, держави. В одній із наших попередніх публікацій (у співавторстві із С. Вітвіцьким) було наголошено на тому, що рівень розвитку сучасних ІТ-технологій, поява нових способів мобільного пошуку й обміну інформацією чи віртуального спілкування впливають на соціальні процеси та психологію окремих індивідуумів, що активно може бути використано у впровадженні нових форм превентивної (профілактичної) роботи у сфері правоохоронної діяльності [5, с. 155]. І це лише один із багатьох наочних прикладів інтеграції інформаційних відносин у суспільне життя людини та діяльність владних структур.

І. Бачило визначає інформацію «як сприйняту людиною характеристику навколишнього світу, яка виникає в процесі пізнання останнього і дозволяє на основі властивостей предметів, процесів, фактів і відображення їх у різних формах сприйняття відрізняти їх ознаки, значення та встановлювати зв'язки й залежності всього різноманіття прояву матеріального, духовного, ідеологічного світу – формувати світову систему знань» [2, с. 28]. Отже, інформація є головним об'єктом, на основі якого виникають суспільні відносини між різними суб'єктами в інформаційній сфері. Інформаційні відносини як різновид правових відносин регулюються інформаційно-правовими актами, що встановлюють порядок поширення інформації, доступу до неї, обмеження, захисту та ін. Фактично це процес, під час якого позитивне право намагається відповідати тим реаліям сьогодення, які полягають у появі нових і швидкоплинному розвитку (трансформації) вже наявних соціальних процесів в інформаційному середовищі (кібернетичному просторі).

З огляду на вплив інформаційних технологій на розвиток державних і громадських інститутів, світова спільнота прийняла низку правових документів, спрямованих на їх регламентацію. Аналіз цих міжнародно-правових актів дає змогу зробити висновок, що інформаційні відносини є об'єктом особливого правового регулювання. Підтвердженням цьому є Загальна декларація прав людини і громадянина, прийнята Генеральною Асамблеєю Організації Об'єднаних Націй 10 грудня 1948 року, яка закріпила у статті 19 право кожної людини на свободу пошуку, одержання і поширення інформації та ідей будь-якими засобами незалежно від державних кордонів. До того ж в Окінавській хартії глобального інформаційного суспільства підкреслюється, що «інформаційно-комунікаційні технології є одним із найбільш важливих факторів, що впливають на формування суспільства двадцять першого століття. Їх революційний вплив стосується способу життя людей, їх освіти й роботи, а також взаємодії уряду та громадянського суспільства. Інформаційно-комунікаційні технології швидко стають життєво важливим стимулом розвитку світової економіки. Вони також дають можливість усім приватним особам, фірмам і співтовариствам, що займаються підприємницькою діяльністю, більш ефективно та творчо вирішувати економічні й соціальні проблеми» [1].

У результаті впливу інформаційно-правових норм на інформаційні відносини останні набувають форми правовідносин. Термін «інформаційні відносини» юридично

закріплено в рекомендаційному законодавчому акті Міжпарламентської Асамблеї держав-учасниць Співдружності Незалежних Держав від 23.05.1993 р. «Про засади регулювання інформаційних відносин у державах-учасницях Міжпарламентської Асамблеї». Поняття інформаційних відносин у зазначеному документі «розкривається через зв'язки між окремими індивідами, їх колективами та об'єднаннями, підприємствами, державними органами й установами з приводу виробництва, поширення і споживання інформації» [14, с. 25]. Тож, за визначенням Г. Чеботарьової, «інформаційні правовідносини – це суспільні відносини, врегульовані нормами інформаційного права, що виникають у процесі пошуку, отримання, передачі, виробництва і поширення інформації, а також пов'язані з ними відносини» [15, с. 40]. Свого часу К. Бєляков наголошував, що «сучасні суспільно-правові відносини мають інформаційно-комунікативний характер, а будь-які відносини, у тому числі й інформаційні, здійснювалися, здійснюються і будуть здійснюватися як комунікація. Тому основним об'єктом уваги правничої інформаціології (термін, який пропонував запровадити в науку К. Бєляков. – *Прим. авт.*) є інформаційно-комунікативні зв'язки в правничій діяльності та соціальному управлінні, тобто інформаційно-правова реальність» [3, с. 27].

Насамперед інформаційне право як окрема галузь права регулює однорідну групу суспільних відносин. Специфіку цих відносин можна охарактеризувати так: вони виникають, змінюються і припиняються в інформаційній сфері у процесі обігу інформації; володіють певною специфікою об'єктів, до яких належать інформація, інформаційні об'єкти, інформаційні технології. І такі об'єкти, зважаючи на їх особливості, неможливо ототожнити з іншими об'єктами правового регулювання. Інформаційні відносини безпосередньо пов'язані з формуванням, створенням, перетворенням та використанням інформації, зберіганням інформації, передачею і розповсюдженням інформації тощо. На цьому положенні фактично і ґрунтується принциповий розподіл відносин, які мають регулюватися на засадах влади й підпорядкування та на умовах угод. При цьому треба погодитися з А. Гевлич та В. Селивановим, що до такої системи логічно додати відносини, «що виникають з приводу реалізації основних інформаційних прав та інтересів громадян України, інтересів суспільства і держави в інформаційній сфері» [6, с. 11]. Захист прав окремих учасників цих відносин під час обробки та зберігання даних, у процесі яких забезпечується конфіденційність, доступність і цілісність інформації, становить зміст діяльності із забезпечення інформаційної безпеки.

Організаційно-правове забезпечення інформаційної безпеки передбачає реалізацію комплексу законів, нормативів, управлінських рішень, що регламентують як єдину діяльність із забезпечення інформаційної безпеки, так і формування, функціонування спеціалізованих систем захисту даних та інформації. Державна система забезпечення інформаційної безпеки країни – це організаційне об'єднання державних органів, а також сил та засобів інформаційної безпеки, що виконують свої функції на основі закону під контролем і захистом судової влади. Державна система є найважливішою ланкою системи інформаційної безпеки особистості, суспільства й держави в правовій країні. Основними завданнями такої системи є: виявлення і прогнозування факторів та інформаційних загроз, що дестабілізують життєво важливі інтереси особистості, суспільства й держави; здійснення комплексу оперативних і довготривалих заходів з їхнього попередження та усунення; створення і підтримання в готовності сил та засобів забезпечення інформаційної безпеки.

С. Аксьонов зазначив, що «основними принципами становлення організаційно-правового забезпечення інформаційної безпеки є: строгість дотримання загальновизнаних норм і правил захисту баз даних особами, що володіють доступом до конфіденційної інформації; захист відповідними органами; нормативно-правове фіксування норм відповідальності за недотримання режиму й порядку захисту інформації; техніко-математичний підхід до надання юридичної сили у сфері організаційно-правового

забезпечення захисту інформації; процесуальне формування процедур вирішення ситуацій, що реалізуються під час захисту інформації та забезпечення інформаційної безпеки системи» [16].

Необхідно розглянути в змістовному аспекті базові підходи до формулювання визначення інформаційної безпеки. Доктринальних тлумачень цього явища існує дуже багато (наприклад, у наукових працях К. Бєлякова, М. Красноступа [17, 18]), однак на сьогодні немає єдиної думки щодо його сутності. На основі класифікації В. Ліпкана можна виокремити декілька підходів до визначення сутності феномену інформаційної безпеки, за якими останній розуміють як «стан захищеності інформаційного простору; процес управління загрозами та небезпеками, що забезпечує інформаційний суверенітет України; стан захищеності національних інтересів країни в інформаційному середовищі або в інформаційній сфері; захищеність установлених законом правил, за якими відбуваються інформаційні процеси в державі; важливу функцію держави; суспільні відносини, пов'язані із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних і потенційних загроз в інформаційному просторі; невід'ємну частину політичної, економічної, оборонної та інших складових національної безпеки» [10, с. 25–30].

Соціологічний підхід до дослідження інформаційної безпеки, що пропонує В. Шемякін, передбачає «вивчення інформаційної безпеки в рамках інформаційного протиборства, яке є ціннісним й ідеологічним, що виявляється в масмедіа, електронних засобах масової інформації (далі – ЗМІ). Оцінка результатів подібного протиборства проводиться за допомогою виявлення громадської думки, фіксується соціологічними методами» [19]. Разом із соціологічним до методологічних підходів щодо аналізу питань, пов'язаних з інформаційною безпекою, відносять і соціально-психологічний. Прихильники зазначеного підходу намагаються оцінити, наскільки ефективним є інформаційний вплив на людину. На основі досліджень психологічних аспектів інформаційної безпеки О. Войскунський називає цю дефініцію «кібербезпека». Такий підхід орієнтований на «виявлення загроз особистості, обумовлених упередженим відбором й обмеженням інформації, яка надається окремим особам чи соціальним групам людей. Як правило, подібна тенденційність обумовлена тим, що суб'єкти, органи й організації, які проводять відбір інформації, керуються маніпулятивними прагненнями. Загрози особистості пов'язані з відсутністю критичної оцінки під час вибору інформаційних джерел, одностороннім характером подачі інформації, поширенням чуток і дезінформації, неправильної атрибуції інформаційних джерел, зі спробами дискредитації, замовчування або гіперболізації певних подій і фактів» [10, с. 49]. Комп'ютери, смартфони та інші електронні пристрої використовують як спосіб змінити поведінку людини, і на сьогодні це не є чимось незвичним. Нав'язування думки шляхом застосування інтернет-мережі може впливати на різні аспекти життя та розвитку людини, включаючи політику, культуру, релігію, освіту, охорону здоров'я, екологію тощо. Використовуючи технологічні, дизайнерські та психологічні прийоми впливу на свідомість та підсвідомість інтернет-користувачів, переконання завжди має на меті змінити уявлення, ставлення, поведінку як окремої особи, так і невизначеної групи людей, іноді примусити їх до певних дій чи бездіяльності [21, с. 2]. Такі наміри можуть бути суспільно корисними, нейтральними чи, навпаки, шкідливими.

За визначенням В. Гурковського, «інформаційна безпека України – це суспільні відносини, пов'язані із захистом життєво важливих інтересів людини і громадянина, суспільства й держави від реальних та потенційних загроз в інформаційному просторі, що є необхідною умовою збереження і примноження духовних та матеріальних цінностей державоутворювальної нації, її існування, самозбереження і прогресивного розвитку України як суверенної держави, що залежить від цілеспрямованої інформаційної політики гарантій, охорони, оборони, захисту її національних інтересів» [7, с. 74]. Тож цілком закономірною вбачається позиція Ф. Медвідя, який пропонує зарахувати до пріоритетних

напрямів забезпечення інформаційної безпеки України такі: створення законодавчої та нормативної бази; здійснення моніторингу інформаційної безпеки України; стандартизацію, сертифікацію та ліцензування діяльності у сфері забезпечення інформаційної безпеки України; удосконалення та розвиток державної інформаційної інфраструктури з урахуванням вимог інформаційної безпеки України; удосконалення системи освіти, навчання та виховання з урахуванням вимог інформаційної безпеки та мовного законодавства України; розробку міжрегіональних, державних та міждержавних програм розвитку системи інформаційної безпеки держави [22].

Тому погоджуємося, що «нині превалюють практичні підходи – як до законодавчого регулювання сфери інформаційних відносин (формування інформаційного законодавства), так і до проблем впровадження та використання здобутків науково-технічного прогресу в управлінську діяльність (створення спеціалізованих інформаційних систем), а також із питань організаційно-правових та технологічних заходів протидії негативним явищам, що відбуваються в суспільстві через неправомірне використання інформаційних технологій, захисту інформації і т. ін.» [3, с. 24].

Продовжуючи розгляд цієї проблематики, зауважимо, що швидке розповсюдження соціальних мереж як ЗМІ створює низку можливостей і викликів державним інституціям, а також загроз у контексті правоохоронної діяльності. Щодо цього слушно зазначають О. Користін і Ю. Кардашевський: «Незважаючи на те, що багато вебсайтів дозволяють користуватися певною мірою користувальницькими параметрами, вони не входять до більшості визначень соціальних мереж. Натомість соціальні медіа можна розділити на чотири категорії – соціальні мережі, сайти обміну контентом, інструменти для розміщення контенту та інструменти географічних розташувань, кожен з яких має свої особливі характеристики, і тому кожен з них становить різні загрози та можливості» [8, с. 19]. Зважаючи на реалії сьогодення, указані науковці аргументовано доводять, що «існує низка викликів для розслідування правопорушень, скоюваних через ці засоби масової інформації, і це пов'язано, перш за все, із практикою та законодавством (або за деяких обставин відсутністю законодавчих норм). З точки зору практики, інтернет не знає фізичних меж, тому існують очевидні виклики у випадках, коли правопорушник перебуває поза межами країни» [8, с. 19].

Таким чином, як указано в Доктрині інформаційної безпеки України, «в умовах швидкого формування і розвитку інформаційного суспільства в Україні та глобального інформаційного простору, широкого використання інформаційно-комунікаційних технологій у всіх сферах життя особливого значення набувають проблеми інформаційної безпеки» [23], що обумовлює напрацювання шляхів їх вирішення. Така діяльність має ґрунтуватися на поєднанні організаційно-технічних прогресивних заходів із належним нормативно-правовим регулюванням та фінансуванням зазначених проєктів та практики їх впровадження.

Варто звернути увагу, що сучасний стан захищеності прав і законних інтересів людини, суспільства й держави в інформаційній сфері України свідчить про недостатній рівень правового регулювання і забезпечення інформаційної безпеки. Так, непоодинокими є випадки порушення чи безпідставного обмеження вказаних прав та інтересів у нормах, що регулюють інформаційні відносини, у правовому забезпеченні інформаційної безпеки існує чимало казусів і колізій. Наприклад, як це не парадоксально, але до сьогодні немає законодавчого тлумачення такого базового терміна, як «інформаційна безпека», хоча його вжито в Законі України «Про інформацію» [13]. Також у цьому Законі визначено основні засади та види відповідальності за порушення законодавства про інформацію, які деталізуються в нормах відповідних галузевих кодексів.

У Законі України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» інформаційну безпеку розуміють як «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» [24]. Цей закон і нині формально залишається чинним, але з огляду на те, що він був розрахований на визначений термін, який минув більше ніж п'ять років тому, його акутальність залишається сумнівною. Проєкт Закону про внесення змін до законів України щодо інформаційної безпеки (далі – Проєкт), у якому пропонується доповнити Закон України «Про національну безпеку України» та Закон України «Про інформацію» визначенням терміна «інформаційна безпека» [25], значною мірою повторює зазначене вище поняття, однак розширює сферу негативного впливу, зокрема вже згадується про інформаційно-психологічний вплив. Проте, як і в Законі України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», така діяльність має більш оборонний характер, дещо нівелюючи активні заходи забезпечення інформаційної безпеки України. На жаль, Проєкт було відкликано у 2019 році й чинне законодавство залишилося без змін.

Інша проблема, яка потребує законодавчого визначення та врегулювання, – відсутність систематизації законодавства з питань протидії екстремізму в інформаційній сфері. Унаслідок цього матеріали подібного змісту часто розповсюджуються майже безперешкодно, оскільки діяльність із запобігання і припинення різних видів екстремізму здійснюється компетентними державними органами безсистемно й нерідко формально. При цьому важливо пам'ятати, що реальна протидія екстремістським чи іншим негативним проявам в інформаційній сфері не повинна перетворюватися на з'ясування стосунків із журналістами, тиск на опозиційні ЗМІ та придушення свободи слова. До того ж раніше одним із авторів цієї статті було звернуто увагу на такі вади правового регулювання інформаційних відносин в умовах особливих (надзвичайних та «гібридних») адміністративно-правових режимів, як «надмірна розпорошеність окремих норм, що регулюють ці питання в багатьох законах; брак збалансованого врегулювання гарантій та обмежень щодо прав фізичних і юридичних осіб в інформаційній сфері в спеціальних законах, які визначають той чи інший вид особливого адміністративно-правового режиму; «допустимість» установлення певних правил (зокрема й обмежень) у сфері доступу до інформації спеціальними тимчасово створеними органами публічного адміністрування» [26, с. 148]. Ці проблеми не втратили актуальності й дотепер.

Проте необхідно зауважити, що на сьогодні в Україні не прийнято закону, який би визначав концепцію державної інформаційної політики України. Тому в країні немає єдиного плану, єдиної державної позиції чи стратегії розвитку інформаційної галузі, а отже і забезпечення інформаційної безпеки. Такі нормативні акти, як Доктрина інформаційної безпеки України, затверджена Указом Президента України від 25.02.2017 р. № 47/2017, Стратегія кібербезпеки України, затверджена Указом Президента України від 15.03.2016 р. № 96/2016, хоча і є важливими для вирішення цієї проблеми, є необхідними кроками на шляху формування безпечної інформаційної політики в державі, але не доводять це питання національної безпеки до належного рівня нормативно-правового забезпечення. За нашим переконанням, попри те, що в Доктрині згадується про «комплексний характер актуальних загроз національній безпеці в інформаційній сфері», наведені правові акти переважно побудовані з позиції ситуативної протидії загрозам з боку чинного політичного супротивника (Російської Федерації), а не системного та комплексного формування бепекового інформаційного простору в нашій державі в стратегічному контексті на наступні роки.

Підсистема інформаційної безпеки займає особливе місце в системі національної безпеки. Інформаційні відносини і процеси визначають або впливають на всі інші соціальні зв'язки публічного та приватного характеру, які існують у суспільстві, тож інформаційна сфера функціонує одночасно на двох рівнях: самостійно й у взаємозв'язку з

іншими сферами життєдіяльності суспільства шляхом їх інформаційного обслуговування та забезпечення взаємодії за допомогою інформації. Інформація характеризується певним змістовним навантаженням, а отже суть інформаційної сфери – знання (інформація) про інші сфери життєдіяльності суспільства [27, с. 4]. Це забезпечується формуванням інформаційних моделей інших сфер життєдіяльності суспільства, їх інфраструктури, суб'єктів та взаємодії останніх. Як наслідок, інформаційна сфера та її окремі елементи дають змогу чинити опосередкований вплив на соціальну, економічну, політичну, духовну та інші сфери життєдіяльності людського суспільства. Тому фактом, який не вимагає додаткового доведення, є те, що забезпечення інформаційної безпеки є запорукою забезпечення інших складових державної безпеки та національної безпеки в цілому.

Висновки та перспективи подальших розвідок. Отже, на підставі викладеного вважаємо за доцільне наголосити, що пріоритетом у правовому регулюванні інформаційних відносин у країні нині й у майбутньому повинен стати безпековий підхід. Цей підхід полягає в тому, що, надаючи правову оцінку і включаючи певні суспільні відносини, пов'язані з обігом інформації, у нормативну площину, законодавець та інші суб'єкти нормотворення спільно з відповідними фахівцями мають попередньо проводити «безпекову» експертизу з метою виявлення і прогнозування всіх можливих загроз інформаційній безпеці, які можуть виникнути або вже де-факто існують на практиці. Результати таких експертних досліджень повинні враховуватися під час вибору методів та форм правового регулювання чинних і нових інформаційних відносин. Більш детальний аналіз методів та форм такого регулювання має стати предметом самостійних досліджень, що становитиме завдання для подальших наукових розвідок у цьому напрямі.

Список використаних джерел

1. Окінавська хартія глобального інформаційного суспільства (Окінава, 22 липня 2000 року) : хартія, міжнародний документ від 22.07.2000. URL: https://zakon.rada.gov.ua/laws/show/998_163#Text (дата звернення: 22.08.2021).
2. Бачило И. Л. Информационное право : учебник. 2-е изд., перераб. и доп. М. : Юрайт, 2011. 522 с.
3. Бєляков К. І. Сучасна парадигма досліджень інформаційних процесів та явищ у суспільних науках: вступ до соціогуманітарної інформології. *Publishing House "Baltija Publishing"*. 2021. С. 22–32. DOI: https://doi.org/10.30525/978-9934-26-026-1-2.
4. Веселова Л. Ю. Становлення правового інституту кібернетичної безпеки в Україні. *Економічна теорія та право*. 2020. № 1 (40). С. 113–126. DOI: 10.31359/2411-5584-2020-40-1-113.
5. Veselov M., Vitvitsky S. Internet and Juvenile Prevention: A New Format of Prophylactic Activities with Children. *Advances in Economics, Business and Management Research:* Proceedings of the International Conference on Economics, Law and Education Research (ELER 2021). 2021. Vol. 170. P. 152–157. DOI: https://doi.org/10.2991/aebmr.k.210320.027.
6. Гевлич А., Селиванов В. Державна політика України у сфері захисту персональних даних: міжнародно-правовий аспект. *Право України*. 2006. № 1. С. 9–15.
7. Гурковський В. І. Безпека як об'єкт правовідносин в умовах глобального інформаційного суспільства. *Правова інформатика*. 2010. № 2 (26). С. 72–77.
8. Користін О. Є., Кардашевський Ю. Р. Можливості та загрози ефективності правоохоронної діяльності в цифрову епоху. *Наука і правоохорона*. 2018. № 1 (39). С. 16–22.
9. Koropatnik I. M., Zolotar O. O., Zaitsev M. M., Topolnitskyi V. V., Bieliakov K. I. Information security of the defense forces in Ukraine: current state and prospects. *Revista Gênero & Direito*. 2020. Vol. 9. № 05. Special Edition. P. 127–141.
10. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції : навч. посібн. К. : КНТ, 2006. 280 с.
11. Rheingold H. The Virtual Community. Homesteading on the Electronic Frontier. N.Y. : Addison-Wesley Publishing Company Reading, MA, 1993. 282 p.
12. Камышев Э. Н. Информационная безопасность и защита информации : учебное пособие. Томск : ТПУ, 2009. 98 с.
13. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII. Редакція від 16.07.2020. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 22.08.2021).

14. Гаврилов О. А. Курс правовой информатики : учебник для вузов. М. : Издат-во НОРМА, 2002. 432 с.

15. Чеботарева А. А. Информационное право : учебное пособие. М. : Юрид. ин-т МИИТа, 2014. 160 с.

16. Аксенов С. Г. Организационно-правовые основы обеспечения информационной безопасности органов государственной власти. *Налоги*. 2008. № 3 (2). С. 5–11.

17. Беляков К. И. Управление и право в период информатизации : монография. К. : Издат-во «КВІЦ», 2001. 308 с.

18. Красноступ М. Д. Інформаційна безпека України: сутність та проблеми. *Інформаційні технології та захист інформації*. 1999. № 1. С. 108–110.

19. Шемякин В. П. Информационная безопасность в современных российских условиях (социолого-управленческие аспекты) : дис. ... канд. соц. наук : 22.00.08. М., 2004. 131 с.

20. Войскунский А. Е. Информационная безопасность: психологические аспекты. *Национальный психологический журнал*. 2010. № 1 (3). С. 48–53.

21. Kimura H. & Nakajima T. Designing Persuasive Applications to Motivate Sustainable Behavior in Collectivist Cultures. *Psychology Journal*. 2011. Vol. 9 (1). P. 7–28.

22. Медвідь Ф. Інформаційна безпека України: виклики та загрози. URL: https://nato.pu.if.ua/old/journal/2009-2/2009-2-28.pdf (дата звернення: 22.08.2021).

23. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 р. № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text (дата звернення: 22.08.2021).

24. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 09.01.2007 р. № 537-V. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text (дата звернення: 22.08.2021).

25. Проєкт Закону про внесення змін до законів України щодо інформаційної безпеки від 26.11.2018 р. № 9340. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65011 (дата звернення: 22.08.2021).

26. Веселов М. Ю. Правове регулювання інформаційних відносин в умовах особливих (надзвичайних та «гібридних») адміністративно-правових режимів. *Вісник ЛДУВС ім. Е. О. Дідоренка*. 2017. № 4 (80). С. 141–150.

27. Шерстюк В. П. Информационная безопасность в системе обеспечения национальной безопасности России, федеральный и региональный аспекты обеспечения информационной безопасности. *Информационное общество*. 1999. № 5. С. 3–5.

References

1. Okinavska khartiia hlobalnoho informatsiinoho suspilstva (Okinava, 22 lypnia 2000 roku) [Okinawa Charter on the Global Information Society] : khartiia, mizhnarodnyi dokument vid 22.07.2000. URL: https://zakon.rada.gov.ua/laws/show/998_163#Text (data zvernennia: 22.08.2021) [in Ukrainian].

2. Bachilo, I. L. (2011). Informacionnoe pravo [Information law] : uchebnik. 2-e izd., pererab. i dop. M. : YUrajt. 522 s. [in Russian].

3. Bieliakov, K. I. (2021). Suchasna paradyhma doslidzhen informatsiinykh protsesiv ta yavyshch u suspilnykh naukakh: vstup do sotsiohumanitarnoi informolohii [The current paradigm of the development of information processes and phenomena in the suspended sciences: introduction to socio-humanitarian information science]. *Publishing House "Baltija Publishing"*. S. 22–32. DOI: https://doi.org/10.30525/978-9934-26-026-1-2 [in Ukrainian].

4. Veselova, L. Yu. (2020). Stanovlennia pravovoho instytutu kibernetychnoi bezpeky v Ukraini [Formation of Legal Institution of Cybernetics Security in Ukraine]. *Ekonomichna teoriia ta pravo*. № 1 (40). S. 113–126. DOI: 10.31359/2411-5584-2020-40-1-113 [in Ukrainian].

5. Veselov, M., Vitvitsky, S. (2021). Internet and Juvenile Prevention: A New Format of Prophylactic Activities with Children. *Advances in Economics, Business and Management Research:* Proceedings of the International Conference on Economics, Law and Education Research (ELER 2021). Vol. 170. P. 152–157. DOI: https://doi.org/10.2991/aebmr.k.210320.027.

6. Hevlych, A., Selyvanov, V. (2006). Derzhavna polityka Ukrainy u sferi zakhystu personalnykh danykh: mizhnarodno-pravovyi aspekt [State policy of Ukraine in the field of personal data protection: international legal aspect]. *Pravo Ukrainy.* № 1. S. 9–15 [in Ukrainian].

7. Hurkovskyi, V. I. (2010). Bezpeka yak obiekt pravovidnosyn v umovakh hlobalnoho informatsiinoho suspilstva [Security as an object of legal relations in the global information society]. *Pravova informatyka.* № 2 (26). S. 72–77 [in Ukrainian].

8. Korystin, O. Ye., Kardashevskyi, Yu. R. (2018). Mozhlyvosti ta zahrozy efektyvnosti pravookhoronnoi diialnosti v tsyfrovu epokhu [Opportunities and threats to the effectiveness of law enforcement in the digital age]. *Nauka i pravookhorona*. № 1 (39). S. 16–22 [in Ukrainian].

9. Koropatnik I. M., Zolotar O. O., Zaitsev M. M., Topolnitskyi V. V., Bieliakov K. I. Information security of the defense forces in Ukraine: current state and prospects. *Revista Gênero & Direito*. 2020. Vol. 9. № 05. Special Edition. P. 127–141.

10. Lipkan, V. A. (2006). Informatsiina bezpeka Ukrainy v umovakh yevrointehratsii [Information security of Ukraine in terms of European integration]. K. : KNT, 280 s. [in Ukrainian].

11. Rheingold H. The Virtual Community. Homesteading on the Electronic Frontier. N.Y. : Addison-Wesley Publishing Company Reading, MA, 1993. 282 p.

12. Kamyshev, E. N. Informacionnaya bezopasnost' i zashchita informacii [Information security and information protection] : uchebnoe posobie. Tomsk : TPU, 2009. 98 s. [in Russian].

13. Pro informatsiiu : Zakon Ukrainy vid 02.10.1992 r. № 2657-XII [About information : Law of Ukraine]. Redaktsiia vid 16.07.2020. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (data zvernennia: 22.08.2021) [in Ukrainian].

14. Gavrilov, O. A. (2002). Kurs pravovoj informatiki [Course of legal informatics] : uchebnik dlya vuzov. M. : Izdat-vo NORMA. 432 s. [in Russian].

15. Chebotareva, A. A. (2014). Informacionnoe pravo [Information Law] : uchebnoe posobie. M. : YUrid. in-t MIITa. 160 s. [in Russian].

16. Aksenov, S. G. (2008). Organizacionno-pravovye osnovy obespechenija informacionnoj bezopasnosti organov gosudarstvennoj vlasti [Organizational and legal bases of information security of public authorities]. *Nalogi.* № 3 (2). S. 5–11 [in Russian].

17. Belyakov, K. I. (2001). Upravlenie i pravo v period informatizacii : monografiya [Management and law in the period of informatization : monograph]. K. : Izdat-vo «KVIC», 308 s. [in Russian].

18. Krasnostup, M. D. (1999). Informatsiina bezpeka Ukrainy: sutnist ta problemy [Information security of Ukraine: essence and problems]. *Informatsiini tekhnolohii ta zakhyst informatsii.* № 1. S. 108–110 [in Ukrainian].

19. SHemyakin, V. P. (2004). Informacionnaya bezopasnost' v sovremennyh rossijskih usloviyah (sociologo-upravlencheskie aspekty) [Information security in modern Russian conditions (sociological and managerial aspects)] : dis. ... kand. soc. nauk : 22.00.08. M. 131 s. [in Russian].

20. Vojskunskij, A. E. (2010). Informacionnaya bezopasnost': psihologicheskie aspekty [Information security: psychological aspects]. *Nacional'nyj psihologicheskij zhurnal.* № 1 (3). S. 48–53 [in Russian].

21. Kimura H. & Nakajima T. Designing Persuasive Applications to Motivate Sustainable Behavior in Collectivist Cultures. *Psychology Journal*. 2011. Vol. 9 (1). P. 7–28.

22. Medvid, F. (2009). Informatsiina bezpeka Ukrainy: vyklyky ta zahrozy [Information security of Ukraine: challenges and threats]. URL: https://nato.pu.if.ua/old/journal/2009-2/2009-2-28.pdf (data zvernennia: 22.08.2021) [in Ukrainian].

23. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku «Pro Doktrynu informatsiinoi bezpeky Ukrainy» [On the decision of the National Security and Defense Council of Ukraine of December 29, 2016 "On the Doctrine of Information Security of Ukraine"] : Ukaz Prezydenta Ukrainy vid 25.02.2017 r. № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text (data zvernennia: 22.08.2021) [in Ukrainian].

24. Pro Osnovni zasady rozvytku informatsiinoho suspilstva v Ukraini na 2007–2015 roky [On the Basic Principles of Information Society Development in Ukraine for 2007-2015 : Law of Ukraine] : Zakon Ukrainy vid 09.01.2007 r. № 537-5. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text (data zvernennia: 22.08.2021) [in Ukrainian].

25. Proiekt Zakonu pro vnesennia zmin do zakoniv Ukrainy shchodo informatsiinoi bezpeky vid 26.11.2018 r. № 9340 [Projec Law on Amendments to the Laws of Ukraine on Information Security]. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65011 (data zvernennia: 22.08.2021) [in Ukrainian].

26. Veselov, M. Yu. (2017). Pravove rehuliuvannia informatsiinykh vidnosyn v umovakh osoblyvykh (nadzvychainykh ta «hibrydnykh») administratyvno-pravovykh rezhymiv [Legal regulation of information relations in the conditions of special (emergency and "hybrid") administrative-legal regimes]. *Visnyk Luhanskoho derzhavnoho universytetu vnutrishnikh sprav imeni E. O. Didorenka.* № 4 (80). S. 141–150 [in Ukrainian].

27. Sherstjuk, V. P. (1999). Informacionnaja bezopasnost' v sisteme obespechenija nacional'noj bezopasnosti Rossii, federal'nyj i regional'nyj aspekty obespechenija informacionnoj bezopasnosti [Information security in the system of ensuring the national security of Russia, federal and regional aspects of ensuring information security]. *Informacionnoe obshhestvo*. № 5. S. 3–5 [in Russian].

Veselov Mykola,
Doctor of Law, Associate Professor
(Donetsk State University of Internal Affairs, Kryvyi Rih)
ORCID: https://orcid.org/0000-0002-3963-2764

Rekunenko Tetyana,
PhD in Economics, Associate Professor
(Donetsk State University of Internal Affairs, Kryvyi Rih)
ORCID: https://orcid.org/0000-0001-7668-0581

Volkova Daria,
Applicant
(National University "Odesa Law Academy", Kryvyi Rih)
ORCID: https://orcid.org/0000-0002-5131-8305

SAFE APPROACH IN LEGAL REGULATION OF INFORMATION RELATIONS

Due to the process of informatization, systemic changes are taking place, according to which all spheres of activity of state institutions, all segments of society, and each individual are included in the global information space. This determines the need to ensure the reliability and security of information relations, which is achieved in particular through the mechanism of effective and strategic legal regulation. Information security in the conceptual and key legal documents of many states is seen as an important component of national security. New challenges to security and human rights in the field of information relations generate pressing issues that need further scientific study and solution. The article contains a compilation of views available in modern science on the understanding of basic concepts: "information", "information relations", "information security", as well as basic approaches to formulating the definition of information security. Due to the combination of general scientific and special methods of cognition, in particular dialectical, formal-legal, comparative analysis and synthesis, the publication substantiates the importance and specificity of the "security" approach in regulating information relations to achieve information security in the country. This approach is that, providing a legal assessment and, including certain public relations related to the circulation of information in the regulatory sphere, the legislator and other subjects of rule-making together with relevant professionals should pre-conduct a "safe" examination to identify and predicting all possible threats to the information security that may arise or already de facto exist in practice. The results of such expert research should be taken into account when choosing methods and forms of legal regulation of existing and new information relations. Information sphere and its separate elements make it possible to indirect influence on social, economic, political, spiritual and other spheres of life of human society. Therefore, the fact that does not require additional proof is that information security is a guarantee of providing other components of state security and national security as a whole.

Key words: *information; information relations; legal regulation; information security; ensuring information security.*

Надіслано до редколегії 30.08.2021
Рекомендовано до публікації 06.09.2021