

Спіцина Ганна

докторка юридичних наук, професорка,
професорка кафедри права гуманітарно-правового факультету
Національного аерокосмічного університету ім. М. Є. Жуковського
«Харківський авіаційний інститут»,
м. Харків, Україна
ORCID: <https://orcid.org/0000-0002-6677-6915>
e-mail: spitsyna_hanna@ukr.net

Гуцу Світлана

кандидатка юридичних наук, доцентка, доцентка
кафедри права гуманітарно-правового факультету
Національного аерокосмічного університету
ім. М. Є. Жуковського «Харківський авіаційний інститут»,
м. Харків, Україна
ORCID: <https://orcid.org/0000-0003-1373-6079>
e-mail: s.gutsu@khai.edu

DOI: <https://doi.org/10.32620/pls.2023.2-3.05>

ЛЕГАЛІЗАЦІЯ ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОСОБИСТОСТІ В УКРАЇНСЬКОМУ ЗАКОНОДАВСТВІ

Анотація. Стаття присвячена дослідженню питання інформаційної безпеки особистості через з'ясування сутності поняття інформаційного захисту як важливої складової частини національної безпеки України. Зазначено, що сьогодні в Україні фактично відсутнє визначення інформаційної безпеки особистості яка б могла забезпечити виявлення, аналіз інформаційних загроз, а також протидію цим загрозам. Стверджується, що інформаційну безпеку людини неможливо розглядати відірвано від її прав та свобод у інформаційній сфері, що визначають її правовий статус у суспільстві та державі, а також правових можливостей охорони і захисту цих прав. Проаналізовано науково-теоретичні підходи до визначення сутності «інформаційна безпека» і «інформаційна безпека особистості», а також доведено їх взаємозв'язок. Вказується, що сутність інформаційної безпеки людини як необхідної для існування і розвитку людини властивості, має базуватись на розумінні соціальних, політичних та технологічних процесів, що виникають у зв'язку зі становленням інформаційного суспільства. Обґрунтовується, що інформаційна безпека особистості повинна розглядатися як синтез трьох аспектів: технічного, соціального, біологічного. Автор доводить, що система інформаційної безпеки людини є складовою частиною системи інформаційної та національної безпеки країни. Тому ефективна реалізація стратегічних пріоритетів, основних принципів і завдань державної політики інформаційної безпеки потребує вдосконалення правових та організаційних механізмів управління інформаційною безпекою.

Ключові слова: інформаційна безпека, інформаційна безпека особистості, загрози інформаційній безпеці, національна безпека, стратегія інформаційної безпеки.

Постановка проблеми. Сучасні темпи глобалізації світу, інформатизація всіх сфер функціонування суспільства, економіки і держави породжує створення нової реальності і якості життя. Інформаційні системи різних держав інтегруються до світової інформаційної системи, породжуючи єдиний інформаційний простір без кордонів, меж, контролю і, відповідно, без захисту. Сучасна людина також занурена в світ технологій і надміру інформації. При цьому, інформаційно-комунікаційне насичення суспільних відносин, одночасно створює настання як бажаних так і загрозливих інформаційних наслідків. Глобальний характер інформаційного простору зі

слабкими механізмами ідентифікації користувачів, всесвітній розвиток соціальних мереж, інтернет-бізнес, міжнародна злочинність, уразливість міжнародних та національних інформаційних інфраструктур разом з неможливістю встановити повне обмеження для збору персональних даних загрожують особистій свободі і міжнародній стабільності [1].

Для України проблема правового регулювання інформаційного простору є надзвичайно актуальною. В країні продовжується процес становлення національного інформаційного суспільства, інтеграції до світового інформаційного суспільства. Але інформаційна безпека

людини як складова національної безпеки, наукова і правова категорія все ще перебуває на етапі становлення. Насьогодні, все ще не визначено поняття «інформаційна безпека особистості», національне законодавство не надає критеріїв розмежування інформаційної безпеки держави і особи, не визначає гарантій і відповідальності за створення загроз і нанесення шкоди інформаційній безпеці людини. Все це призводить до ситуації коли не тільки ЗМІ, громадські активісти і державні діячі, а й найвищі посадові особи держави дозволяють собі висловлювання які призводять до послаблення інформаційної захищеності і дестабілізації суспільства. Як, влучно зазначила О. Золотар, в сучасному глобалізованому світі інформаційні права людини неможливо розглядати відокремлено від суспільства і держави. Особистість людини є передумовою й продуктом існування суспільства, держави. оскільки головним джерелом добробуту людини стає інформація, то інформаційна безпека людини має на меті забезпечення збереження цілісності особи та її здатності до розвитку як визначальних категорій буття людини, враховуючи реалії становлення інформаційного суспільства [2].

Аналіз досліджень і публікацій, в яких започатковано розв'язання даної проблеми. Проблематика інформаційної безпеки людини складна і багатоаспектна, що зумовлює необхідність вивчення й узагальнення наукових праць представників різних галузей юридичної науки. Теоретико-правову основу дослідження становлять напрацювання О.А. Баранова, О.Д. Довганя, І.М. Дороніна, В.М. Гаращука, Н.Б. Новицької, А.М. Новицького, В.Я. Тація, А.Ю. Нашинець-Наумової, О.О. Золотар та інших. Окремі аспекти правового регулювання інформаційної сфери були розглянуті в працях українських і зарубіжних дослідників, зокрема І.В. Арістової, В.Г. Пилипчука, Р.А. Калюжного, О.В. Кохановської, А. І. Марущак, В.В. Остроухова та інших. Отже, коло наукових праць в цієї сфері доволі широке, однак не всі проблемні питання визначення інформаційної безпеки особистості дістали свого вирішення. Більшість досліджень присвячені сфері правового регулювання інформаційної (або кібер) безпеки держави, визначенню інформаційних загроз та шляхів боротьби з ними. Тому питання визначення і правового забезпечення особливостей інформаційної безпеки людини потребують більш детального і уважного вивчення у подальших наукових розробках.

Метою статті є дослідження інформаційної безпеки людини через з'ясування сутності інформаційного захисту людини, його особливостей, впливу інформаційних загроз на стан захищеності людини і, як наслідок, на інформаційну безпеку України.

Викладення основного матеріалу. 25 лютого 2017 року Указом Президента України було затверджено Доктрину інформаційної безпеки України, якою було визначено національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної

політики в інформаційній сфері [3]. Документ прямо говорив, що інформаційна сфера є ключовою ареною у боротьбі за національну безпеку. А серед актуальних загроз національним інтересам та національній безпеці України названо недосконалість законодавства стосовно регулювання суспільних відносин в інформаційній сфері. Нажаль, Доктрина інформаційної безпеки України як спеціалізований нормативний акт не мала визначення поняття «інформаційна безпека», що спонукало науковців шукати і пропонувати власний суб'єктивний аналіз цього терміну. Маємо низку поглядів, думок і тлумачень, подекуди дуже подібних один до одного, а інколи – кардинально протилежних. Наприклад, Т. С. Перун визначає інформаційну безпеку як систему суспільних відносин, що виражає зв'язок між інтересами особи, суспільства та держави в сфері інформації та правового забезпечення їхнього захисту, що охоплює стан захищеності інформаційного простору, інформації і інформаційних ресурсів держави, інформаційно-телекомунікаційної інфраструктури від можливих внутрішніх і зовнішніх загроз [4]. В.С. Цимбалюк пропонує визначити інформаційну безпеку як сферу суспільних відносин щодо підтримки на нормативно визначеному рівні співвідношення прав і обов'язків особи, суспільства, держави в інформаційному просторі від загроз, викликів їх суверенітету [5]. Довгань О.Д., під інформаційною безпекою пропонує розуміти результат управління реальними та (або) потенційними викликами і загрозами щодо захищеності важливих інтересів людини і громадянина, суспільства і держави в інформаційній сфері, у т.ч. з використанням правових методів [6].

Вперше термін «інформаційна безпека», було визначено в Концепції Національної програми інформатизації [7]. Відповідно до цього документу інформаційна безпека – це комплекс нормативних документів з усіх аспектів використання засобів обчислювальної техніки для оброблення та зберігання інформації обмеженого доступу; комплекс державних стандартів із документування, супроводження, використання, сертифікаційних випробувань програмних засобів захисту інформації; банк засобів діагностики, локалізації та профілактики комп'ютерних вірусів, нові технології захисту інформації з використанням спектральних методів, високонадійні криптографічні методи захисту інформації тощо. Пізніше, було розроблено проект Закону «Про інформаційний суверенітет та інформаційну безпеку України» [8], який має суттєво іншу інтерпретацію цього терміну – інформаційна безпека розглядається як «захищеність життєво важливих інтересів суспільства, держави і особи, якою виключається заподіяння шкоди через неповноту, несвочасність, недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок розповсюдження інформації, забороненої для розповсюдження законами України».

Чинне законодавство, а саме Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» визначає інформаційну безпеку теж як «стан захищеності», але саме визначення декілька доповнено: «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 технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [9].

28 грудня 2021 року Указом Президента України була затверджена Стратегія інформаційної безпеки, яка, серед іншого визначила стратегічні цілі та завдання, спрямовані на протидію інформаційним загрозам, захист прав осіб на інформацію та захист персональних даних. Документ визначає інформаційну безпеку України як складову частину національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [10]. Отже і в цьому документі не виділяються окремо інформаційна безпека людини і інформаційна безпека держави. Цілком підтримую позицію О.О. Золотар, яка писала, що в законодавстві в один ряд поставлені життєво важливі інтереси людини, суспільства і держави, які в реальності часто є суперечливими і неспіврозмірними. Такий підхід нівелює розуміння людини, гарантування її прав і свобод, як мети забезпечення будь-якого виду інформаційної безпеки – чи то суспільства, чи держави, чи міжнародного співтовариства. Це в свою чергу знаходить відображення в державній інформаційній політиці та законодавстві, що регулює конкретні сфери життєдіяльності людини, коли в пріоритет виносяться інтереси держави і суспільства, а не захист прав і свобод окремої людини [2].

В українській науковій літературі виділяють два основні підходи до інформаційної безпеки людини. Перший підхід (технічний аспект) наголошує на забезпеченні людині здатності вільно і безперешкодно реалізовувати права та свободи в інформаційній сфері, зокрема право на інформацію – вільно збирати, зберігати, використовувати і поширювати інформацію. Другий підхід (гуманітарний) наголошує на

захищеності психіки та свідомості людини від небезпечних інформаційних впливів; маніпулювання, дезінформування, образ, спонукування до самогубства тощо.

На мій погляд, інформаційна безпека особистості повинна розглядатися як синтез трьох аспектів: технічного, соціального, біологічного. Технічна безпека людини включає доступ до інформаційних ресурсів, розвиток і за потреби захист власних інформаційних ресурсів, використання новітніх інформаційних технологій створення, обробки та поширення інформації, забезпечення конфіденційності, цілісності та доступності приватної інформації, в тому числі інтелектуальної власності. Соціальна складова особистості інформаційної безпеки полягає в забезпеченні конституційних прав і свобод людини і громадянина, створення сприятливого правового клімату в національному інформаційному просторі, збереження загальнолюдських та національних моральних цінностей. Біологічний аспект дозволяє виділити людину серед інших учасників інформаційних відносин саме через її природні особливості. Адже тільки на людину можна впливати шляхом маніпулювання свідомістю і дестабілізацією психічного стану. Отже, кожному елементу інформаційної безпеки людини притаманні свої особливості, певні види загроз і впливів і методи захисту від них [11].

14 вересня 2020 року Указом Президента була затверджена Стратегія національної безпеки України [12]. Документ починається зі слів: БЕЗПЕКА ЛЮДИНИ – БЕЗПЕКА КРАЇНИ. І далі говориться, що: «Людина, її життя і здоров'я, честь і гідність, недоторканність і безпека – найвища соціальна цінність в Україні. Реалізація цієї норми Конституції України – головна ціль державної політики національної безпеки». Інформаційна безпека є складовою національної безпеки, а значить забезпечення інформаційної безпеки людини має бути пріоритетною метою державної політики в цій сфері. Досягнення цієї мети має здійснюватися шляхом «створення ефективної системи взаємодії між органами державної влади, органами місцевого самоврядування та суспільством..» (Стратегія інформаційної безпеки). На фоні декларування таких високих цілей, неприпустимими є дії органів державної влади і окремих посадових осіб, спрямовані на дестабілізацію суспільства, залякування громадян шляхом поширення недостовірної інформації. Наприклад, усі пам'ятають обмеження, що ввів уряд навесні 2020 року у зв'язку з поширенням коронавірусної інфекції. Серед обмежень – заборона з'являтися в громадських місцях без маски, ходити групами більше 2 осіб, перебувати на вулиці без документів; заборона на відвідування парків, скверів, зон відпочинку, лісопаркових і прибережних зон. Останнє обмеження здійняло бурю запитань в суспільстві: чому так, якщо на природі між людьми є дистанція, повітря, та і українцям потрібно в час пандемії підтримувати здоров'я? Як з'ясувалось пізніше, парки та сквери на період карантину в Україні закривали не стільки для впливу на епідеміологічний процес, як для психологічного

ефекту на людей. У своїй заяві телеканалу «Україна 24» головний санітарний лікар Віктор Ляшко повідомив, що «Завдяки цьому психологічному ефекту у людей з'явилося відчуття небезпеки і необхідності дотримання карантинних заходів, які впроваджував уряд» [13]. Тобто, влада навмисно застосувала заходи психологічного впливу, обмежила конституційні права громадян, поширила дезінформацію заради того щоб викликати «відчуття небезпеки», а простими словами – залякати людей і примусити виконувати незаконні накази. Слід зазначити, що до сьогодні ні пан Ляшко, який став очільником Міністерства охорони здоров'я, а ні інші посадовці, причепні до цієї ситуації не були притягнуті до відповідальності. Окрім правового аспекту цей випадок має негативні суспільні наслідки – формування недовіри населення до дій уряду і органів державної влади, до заяв державних посадовців і діячів, посилення відчуття незахищеності, послаблення ступеню інформаційної безпеки людей – а значить і суспільства і, як наслідок, держави в цілому. Таких прикладів, нажаль, безліч в сучасному інформаційному полі України. На мій погляд, одна з найважливіших причин такого стану речей – не визнання на законодавчому рівні окремої правової дефініції «інформаційна безпека особистості» і, як наслідок, відсутність механізму захисту інформаційного поля людини від деструктивних інформаційних загроз з боку державних посадовців і притягнення їх до юридичної відповідальності. У тексті Стратегії інформаційної безпеки перераховуються глобальні та національні виклики і загрози інформаційній безпеці. Серед них: - збільшення кількості глобальних дезінформаційних кампаній; - інформаційна політика Російської Федерації; - соціальні мережі; - недостатній рівень інформаційної культури та медіаграмотності в суспільстві для протидії маніпулятивним та інформаційним впливам, тощо. Але жодного слова про зловживання і безвідповідальність в інформаційній сфері з боку органів державної влади і їх посадових осіб. В той час, коли саме державна політика є основним механізмом забезпечення інформаційної безпеки людини, жоден нормативний акт не визначає її як особливу складову інформаційної безпеки і не закріплює гарантії її забезпечення. В сучасному глобалізованому світі інформаційні права людини неможливо розглядати окремо від суспільства і держави. Особистість людини є передумовою й продуктом існування суспільства, держави [2]. Інформаційна безпека особистості і безпека держави тісно пов'язані і взаємозалежні одна від одної. Усі процеси в державі (політичні, економічні, соціальні) впливають на громадян, що призводить до зворотної реакції і впливу громадян на державу і державну політику. А отже, і деструктивні дії уряду в інформаційній сфері спрямовані на громадян (як ті, що наводились у прикладі вище) призводять до зниження стану захищеності всього суспільства і, як наслідок, держави в цілому.

Висновки. Основним складовим елементом інформаційної безпеки є інформаційна захищеність людини. Інформаційна безпека для сучасної людини є необхідною умовою її ефективного включення в соціум і реалізації її прав, свобод та законних інтересів. Внаслідок біологічних і соціальних факторів потенційні інформаційні загрози, методи і засоби впливу на людину мають свої особливості, відмінні від впливів на державу. Таким чином, інформаційна безпека особистості повинна розглядатися в законодавстві як самостійна правова дефініція і визначатися через призму трьох складових: інформаційно-технічної, соціальної і інформаційно-психологічної. Вважаємо, що чинне законодавство не відображає в повній мірі можливі загрози для інформаційної безпеки особистості. Стратегія інформаційної безпеки має бути доповнена гарантіями державного захисту людини від деструктивних інформаційних впливів з боку державних органів влади і їх посадових осіб.

Бібліографічні посилання

1. Гуцу С. Ф. Забезпечення безпеки людини в інформаційному просторі як шлях до євроінтеграції // Науково-практичний семінар: «Забезпечення кібербезпеки: Правові та технічні аспекти», 8 листопада 2018 р., м. Харків. – 2018. – С. 38-44.
2. Золотар О. О. Інформаційна безпека людини: теорія і практика : монографія. – Київ: ТОВ «Видавничий дім «АртЕк», 2018 – 446 с.
3. Доктрина інформаційної безпеки України. Указ Президента України від 25 лютого 2017 року № 47/2017. URL: <https://www.president.gov.ua/documents/472017-21374>
4. Перун Т. С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні: процесі : дис. ... д-ра юрид. наук : 12.00.07. Львів, 2019. 268 с.
5. Цимбалюк В. С. Безпека як інститут інформаційного права та його місце в структурі кодифікації інформаційного законодавства Моделювання колективної безпеки: інформаційний вимір: Мат. міжн. «круглого столу» (м. Київ, 27 квітня 2011 р.). К.: Вид-во «Академпрес», 2011. С. 28–32.
6. Довгань О. Д. Теоретико-правові основи забезпечення інформаційної безпеки України: автореферат... д-ра юрид. наук, спец.: 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право / Ін-т законодавства ВР України. К., 2016. 44 с.
7. Про Національну програму інформатизації. Закон України. Відомості Верховної Ради України (ВВР), 1998, № 27-28, ст.181.
8. Про інформаційний суверенітет та інформаційну безпеку України : Проект Закону України від 12 серпня 1999 р. № 1207-d [Електронний ресурс]. – Режим доступу: <http://www.rada.kiev.ua/>.
9. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 р. № 537-V [Електронний ресурс]. – Режим доступу:

<http://zakon5.rada.gov.ua/laws/show/537-16>.

10. Стратегія інформаційної безпеки. Указ Президента України від 28 грудня 2021 року № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#top>

11. Гуцу С.Ф. Особливості визначення інформаційної безпеки людини // XV Всеукраїнська науково-практична конференція «Теорія та практика сучасної юриспруденції» 25 березня 2018 року у м. Харкові. – 2018. С.

12. Стратегія національної безпеки України. Указ Президента України від 14 вересня 2020 року № 392/2020. URL: <https://www.president.gov.ua/documents/3922020-35037>

13. Головний санлікар визнав, що парки та сквери закривали заради психологічного ефекту [Електронний ресурс]. – Режим доступу: <https://glavcom.ua/country/society/golovniy-sanlikar-viznav-shcho-parki-ta-skveri-zakrivali-zaradi-psihologichnogo-efektu-679123.html>

Hanna Spitsina, Svitlana Gutsu

SOME ISSUES OF LEGALIZATION OF THE CONCEPT OF INFORMATION SECURITY OF THE PERSON IN UKRAINIAN LEGISLATION

Abstract: The article is devoted to the study of the issue of personal information security through understanding the essence of the concept of information protection as an important part of the national security of Ukraine. It is noted that today in Ukraine there is actually no definition of the information security of the individual, which could

ensure the identification, analysis of information threats, as well as counteracting these threats. It is argued that the information security of a person cannot be considered separately from his rights and freedoms in the information sphere, which determine his legal status in society and the state, as well as the legal possibilities for the protection and protection of these rights. Scientific and theoretical approaches to the definition of the essence of "information security" and "information security of the individual" are analyzed, and their relationship is proved. It is indicated that the essence of human information security as a property necessary for the existence and development of a person should be based on an understanding of the social, political and technological processes that arise in connection with the formation of the information society. It is substantiated that the information security of a person should be considered as a synthesis of three aspects: technical, social, biological. The author proves that the human information security system is an integral part of the country's information and national security system. Therefore, the effective implementation of strategic priorities, basic principles and objectives of the state policy of information security requires the improvement of legal and organizational mechanisms for managing information security.

Key words: information security, personal information security, information security threats, state security, information security strategy.