DOI https://doi.org/10.24144/2307-3322.2021.67.65
УДК 338.24

АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ІНТЕРНЕТ ПРОСТОРІ

Бліхар М. М.,
доктор юридичних наук, доцент,
професор кафедри адміністративного та інформаційного права
Національного університету «Львівська політехніка»
(м. Львів, Україна)

Бліхар М.М. Адміністративно-правове забезпечення інформаційної безпеки в інтернет просторі.
У статті досліджено засади адміністративно-правового забезпечення інформаційної безпеки і інтернет просторі. Зокрема відзначено, що сучасні суспільство та держава характеризуються стрімкими темпами технологізації усіх сфер життя. Разом із цим з'явилися нові способи впливу на людину, її підсвідомість, а разом із цим і можливості для маніпулювання людиною з метою задоволення потреб певних політичних груп. В Україні наявний адміністративно-правовий механізм її забезпечення, однак питання, наскільки ефективно він функціонує та чи повною мірою забезпечує безпеку в Інтернет просторі як людини, так і держави залишається відкритим. Систему забезпечення інформаційної безпеки в інтернет просторі формує: 1) сукупність нормативно-правових актів, до якої входить Конституція України, закони України, підзаконні нормативні акти, що стосуються даної сфери; 2) діяльність державних органів, уповноважених законом на проведення роботи із забезпечення інформаційної безпеки в інтернет просторі; 3) діяльність користувача інтернет простору. Отже, забезпечення інформаційної безпеки в інтернет просторі – це діяльність уповноважених органів та посадових осіб, яка здійснюється в межах, визначених законодавством, та спрямована на дотримання прав та свобод людини під час її взаємодії з інформацією, отриманою з інтернет простору (сприйняття, опрацювання та подальші дії, що ґрунтуються на одержаній інформації, захист персональних даних користувача інтернету), а також гарантування безпеки держави від дестабілізаційних впливів інших держав чи певних сил, що розміщуються в інтернет просторі. Відтак, обґрунтовано, що ефективним забезпечення інформаційної безпеки в інтернет просторі буде тільки за умови взаємодії людини та держави. Адже жодна державна політика у сфері забезпечення інформаційної безпеки не принесе позитивних результатів, якщо людина сама не дбатиме про власну інформаційну безпеку. І навпаки, як би людина не прагнула протидіяти негативним інформаційним впливам, самостійно без допомоги держави вона не зможе впоратися зі щоденним потоком інформації, який постійно дискредитує державу та все, що пов'язано з її діяльністю.

Ключові слова: інтернет простір, інформаційна безпека, інформаційна політика, інформаційні технології, мережева комунікація, правове регулювання.

Blikhar M.M. Administrative and legal provision of information security in the internet space.
The article examines the principles of administrative and legal support of information security and the Internet. In particular, it is noted that modern society and the state are characterized by rapid technologicalization of all spheres of life. At the same time, new ways of influencing people, their subconscious, and at the same time opportunities to manipulate people in order to meet the needs of certain political groups. Ukraine has an administrative and legal mechanism to ensure it, but the question of how effectively it functions and whether it fully ensures the security of the Internet space of both man and the state remains open. The system of information security in the Internet space is formed by: 1) a set of normative legal acts, which includes the Constitution of Ukraine, laws of Ukraine, bylaws related to this area; 2) the activities of state bodies authorized by law to carry out work to ensure information security on the Internet; 3) the activities of the user of the Internet space. Thus, the provision of information security on the Internet is the activity of authorized bodies and officials, which is carried out within the limits set by law, and aimed at respecting human rights and freedoms in its interaction with information obtained from the Internet (perception, processing and further actions based on the received information, protection of personal data of the Internet user), as well as guaranteeing the security of the state from the destabilizing influences of other states

or certain forces placed in the Internet space. Therefore, it is substantiated that effective information security in the Internet space will be effective only if the interaction between man and the state. After all, no state policy in the field of information security will bring positive results if a person does not take care of his own information security. Conversely, no matter how much a person tries to counteract the negative information influences, without the help of the state he will not be able to cope with the daily flow of information, which constantly discredits the state and everything related to its activities.

Key words: Internet space, information security, information policy, information technologies, network communication, legal regulation.

Постановка проблеми. Українські суспільство і держава сьогодні перебувають у процесі активної діджиталізації. Усе більше громадян залучені до роботи з інформаційними технологіями, соціальні мережі дедалі частіше стають не просто майданчиками для малого бізнесу, а й засобом інформаційного впливу на значні маси населення. Прикладом такого інформаційного впливу може бути ситуація, пов'язана із вакцинацією від COVID-19, коли переважно молоді люди віком до 35 років слухають порад своїх кумирів – блогерів, які за певну плату просто виконують чиєсь завдання, а не фахівців у сфері медицини. На свідомість людей, які сприймають інформацію з мережі інтернет, здійснюється постійний інформаційний вплив. Для того, щоб відфільтровувати позитивні та негативні впливи, людині необхідно мати власну усвідомлену систему цінностей та пріоритетів, володіти навичками безпечної роботи в інтернеті. З огляду на це, **мета статті** полягатиме у дослідженні адміністративно-правового забезпечення інформаційної безпеки і інтернет просторі.

Аналіз дослідження проблеми. Досягнення обраної мети передбачає аналіз праць дослідників, тих хто тією чи іншою мірою вивчав засади правового забезпечення інформаційної безпеки. Посилання на їхні праці та розробки будуть подані у тексті наукової розвідки з обґрунтуванням основ, що стали теоретико-методологічним підґрунтям цієї статті.

Виклад основного матеріалу. Система забезпечення інформаційної безпеки в інтернет просторі має об'єднувати як зусилля держави, так і людини – користувача інтернету. Завданням держави у цьому процесі є чітка та послідовна політика, яка стосується усіх сфер життя суспільства та держави, спрямування зусиль на підвищення рівня медіаграмотності населення, розробка та ефективне функціонування систем виділення та блокування інформації, яка несе загрозу для безпеки держави. Людина має володіти елементарними навичками безпечної роботи в інтернет просторі, які здатні захистити як її персональні дані, так і її саму від негативного інформаційного впливу.

Завдяки грамотно продуманому та ефективно запущеному в інтернет простір інформаційному впливу стає можливим: впливати на рішення. Під певним інформаційним впливом людина вирішує для себе вчиняти чи не вчиняти певні дії, розуміє або ж не розуміє їх можливі наслідки для себе та свого найближчого оточення. Тим самим з'являється можливість маніпулювати людиною, яка не має власної усвідомленої позиції в певних питаннях, часто невдоволена рівнем свого життя та бажає більшого для себе без жодних фінансових, емоційних та інтелектуальних затрат; створення підґрунтя для певних нововведень чи дій. Інформаційний вплив, який здійснюється поступово, певними хвилями чи етапами має на меті закласти фундамент для подальших нововведень, змін, вигідних певним силам. Завдяки йому поступово формується необхідна громадська думка, відбувається підготовка людей до змін, які вони у подальшому повинні сприйняти без різкої критики чи яскраво вираженого невдоволення, а як такі, які є дійсно необхідними для них, їх подальшого розвитку; виправдання власних дій та засудження дій опонентів. Обґрунтована та подана належним чином інформація може слугувати як піаром, так і антирекламою опонентів. Певні, навіть непопулярні серед населення, рішення та дії провладних сил можна спланово подати як вкрай необхідні, єдино можливі кроки для покращення ситуації в державі загалом чи певних сферах її діяльності зокрема. Те саме стосується і засудження опонентів, коли дії противників подаються виключно у негативному світлі, протиставляються успіхам протилежної сторони; мотивування людей до дій, потрібних певним групам. Інформація виступає для людини певною спонукою до дій. Якщо людина здатна до аналізу, то вона критично сприймає будь-яку інформацію, обмірковує її, а тоді приймає певне рішення щодо своїх дій. Дуже часто «правильно» подана інформація здатна стати мотивом для вчинків значної кількості людей, а ці вчинки будуть вигідними для конкретної сили, яка має на меті не тільки дестабілізувати ситуацію, а мати з неї зиск; вплив на діяльність усіх систем держави. Проблеми в певній галузі державного управління не є поодинокими, адже всі сфери держави зв'язані між собою. Тому коли виникають проблеми в одній галузі, то на інших галузях вони також відбиваються. Так, наприклад, інформаційні повідомлення про політичну кризу в державі негативно відображатимуться на економіці, як найбільш дотичній до неї сфері, а в подальшому й на інших галузях, а також на людині як кінцевому «споживачеві» продуктів діяльності держави; блокування певної інформації, яка

є невигідною тим чи іншим силам. Володіючи засобами масової інформації, можна володіти і свідомістю людей. Допуск або недопуск людей до інформації певного характеру дає її володільцю певну владу, оскільки цю інформацію можна використати собі на благо: при потребі затримати її оприлюднення, заблокувати, створити іншу інформацію, яка нестиме необхідний певній силі посил для забезпечення необхідної суспільної думки.

Систему забезпечення інформаційної безпеки в інтернет просторі формує: 1) сукупність нормативно-правових актів, до якої входить Конституція України, закони України, підзаконні нормативні акти, що стосуються даної сфери; 2) діяльність державних органів, уповноважених законом на проведення роботи із забезпечення інформаційної безпеки в інтернет просторі; 3) діяльність користувача інтернет простору.

Найвищу юридичну силу має Конституція України, яка гарантує людині основні її права та свободи, їх неухильне дотримання з боку держави. Одним із таких прав є право на доступ до інформації: кожний має право вільно збирати, зберігати, використовувати і поширювати інформацію. Це право також закріплено у ЗУ «Про інформацію», «Про доступ до публічної інформації», «Про звернення громадян», «Про захист персональних даних», «Про захист інформації в інформаційно-телекомунікаційних системах», Постанова КМУ «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомінікаційних системах», а також підзаконні нормативно-правові акти, що стосуються доступу до інформації – це інструкції, програми, галузеві стандарти, спрямовані на реалізацію права на доступ до інформації. Однак вітчизняні нормативно-правові акти, що стосуються забезпечення інформаційної безпеки в інтернет просторі, не відповідають перш за все вимогам часу (через стрімкий розвиток інформаційних технологій, вони не можуть ефективно регулювати відносини, що виникають у цій сфері). Відтак, аналіз чинної законодавчої та нормативно-правової бази з позиції забезпечення інформаційної безпеки України свідчить, що у цій галузі характерна термінологічна невизначеність, неоднозначність та певна непослідовність. Покращення існуючого стану інформаційної безпеки потребує розвитку законодавства, де б визначалась сутність державної інформаційної політики України на основі чіткого і коректного понятійного апарату, уточнювались напрями її реалізації, головним із яких має бути забезпечення інформаційної безпеки держави. Україна, її державні інституції та суспільство мають формувати адекватну комплексну систему посиленого оперативного реагування на ризики інформаційної безпеки. При цьому варто перенести акценти з реакції «post factum» на превентивну діяльність, адже усі основні загрози є добре відомі [2, с. 9].

Діяльність державних органів, уповноважених законом на проведення роботи із забезпечення інформаційної безпеки в інтернет просторі, спрямована на моніторинг інтернет простору з метою забезпечення безпеки людини та держави у сфері комп'ютерних технологій. Ці органи та їх посадові особи наділені всіма правами, необхідними для якісного виконання покладених на них обов'язків. Сюди можемо віднести: 1) Міністерство цифрової трансформації України, основним завданням якого є діджиталізація країни, забезпечення безпеки персональних даних кожного користувача інтернету; 2) силові відомства: СБУ, МВС, зокрема підрозділи кіберполіції, їх діяльність спрямована на реалізацію державної політики у сфері протидії кіберзлочинності.

Діяльність користувача інтернет простору є третьою складовою системи забезпечення інформаційної безпеки. Поряд із зусиллями держави, спрямованими на забезпечення інформаційної безпеки, кожен користувач мережі повинен самостійно дбати про свою безпеку [5, p. 490–498; 6]. Починати цей процес, на нашу думку, доцільно із придбання тільки ліцензованого програмного забезпечення, користуватися системами антивірусного захисту та оволодіти елементарними навичками безпечної роботи в інтернет просторі.

Якісна робота кожного складового елемента системи забезпечення інформаційної безпеки і інтернет просторі та їх взаємодія сприятиме значному убезпеченню інтернету, допоможе як захистити свої персональні дані, так і отримувати якісні контент та послуги в мережі інтернет.

Врешті решт, предметом розгляду правового забезпечення інформаційної безпеки є не тільки сама діяльність, але й елементи, включені до системного подання цієї діяльності, тобто повна схема кооперації діяльностей учасників взаємодії при здійсненні такої діяльності – це, зокрема: правозастосовна діяльність органів державної виконавчої влади на які покладено завдання із забезпечення інформаційної безпеки, які виконують її основні функції; діяльність суб'єктів діяльності із забезпечення інформаційної безпеки, яка залучається до системи діяльності органів державної влади на які покладено завдання із забезпечення інформаційної безпеки; правотворча діяльність з питань формування та реалізації інформаційної політики щодо забезпечення інформаційної безпеки; діяльність фахівців, які виконують забезпечувальні (ресурсні) функції із забезпечення інформаційної безпеки; діяльність адміністрації органів державної виконавчої влади на які покладено завдання із забезпечення інформаційної безпеки з організовування, керівництва та управління діяльністю їх органів та підрозділів на різних рівнях системи» [3, с. 184–185].

Діяльність держави, спрямована на правове забезпечення інформаційної безпеки в інтернет просторі, об'єднує у собі як правотворчу, так і правозастосовну діяльність. Правотворча діяльність у цій сфері – це діяльність, спрямована на формування нормативно-правової бази такого рівня, який дозволяв би максимально ефективно використовувати інтернет простір, гарантуючи правовий захист людини і держави. Правозастосовна діяльність полягає в забезпеченні ефективної реалізації державної політики у сфері забезпечення інформаційної безпеки. Тому, «[…] для забезпечення інформаційної безпеки … необхідно визначити ряд основних завдань з реалізації державної інформаційної політики та забезпечення інформаційної безпеки України» таких як: забезпечення постійного об'єктивного моніторингу інформаційного простору (внутрішнього і зовнішнього), систематичний аналіз результатів моніторингу; чітке визначення єдиного загальнодержавного стратегічного наративу та особливостей його трактування різними державними інституціями України; створення механізмів унеможливлення відхилення від наративу при здійсненні інформаційної діяльності різними державними інституціями; скоординована діяльність в інформаційному просторі всіх державних інституцій України; реалізація принципів та методології стратегічних комунікацій всіма державними інституціями, які здійснюють інформаційну діяльність; виявлення, оцінювання та прогнозування наслідків загроз національним інтересам та національній безпеці України в інформаційній сфері; протидія інформаційним впливам на населення України …; захист об'єктів критичної інформаційної інфраструктури України (зокрема від кібератак); підвищення медіаграмотності населення України [1, с. 166].

Власне, якісне виконання завдань, виокремлених О. Войтком, допоможе зробити систему забезпечення інформаційної безпеки в інтернет просторі справді ефективною, адже окрім моніторингу та виявлення інформаційних загроз, з'явиться реальна можливість протидіяти цим інформаційним загрозам. Протидія інформаційним загрозам повинна являти собою чітку та послідовну державну політику в усіх сферах життєдіяльності суспільства та держави, її мета – підвищення, а іноді й формування, у населення основ медіаграмотності. Інформаційна політика в інтернет просторі покликана також представити державу Україна в мережі, адже інформації про нашу державу там вкрай мало.

Певні кроки у цьому напрямку вже зроблено. Так, у квітні 2021 року було презентовано загальнонаціональний проект з медіагрмамотності. Проект реалізовується у трьох напрямках: 1) посилення комунікації з боку держави, 2) розвиток медіаосвіти, 3) стимулювання відповідального та безпечного медіасередовища. Його мета – посилення усвідомленого ставлення населення до споживаної інформації. Вкрай важливим цей проект є для вчителів загальноосвітніх навчальних закладів, адже загальнонаціональний карантин та перехід на дистанційну форму навчання (на тривалий час) показав, що рівень їх медіаграмотності, а відповідно й інформаційної безпеки, є вкрай низьким.

Поряд із позитивними зрушеннями в сфері забезпечення інформаційної безпеки ми все ж спостерігаємо і ті тенденції інтернет простору, які несуть небезпеку як людині, так і державі. «Однією з небезпечних тенденцій, що склалася в сучасних умовах інформатизації суспільства, є випереджальний розвиток форм, способів, технологій і методик впливу на свідомість або підсвідомість, психічний стан людини порівняно з темпами формування й удосконалення методів та інструментів протидії відповідним деструктивним психологічним впливам» [4, с. 14]. З огляду на це, держава повинна всіляко стимулювати наукові пошуки, спрямовані на дослідження можливостей протидії негативного впливу інформаційних технологій в інтернет просторі на людину та державу, їх нейтралізацію, особливо в сьогоднішніх умовах поширення пандемії [7, p. 146–157; 8]. Ці дослідження повинні найперше проводитися у психології, політології та правознавстві. Це безумовна вимога часу, виконання якої є однією з умов існування сучасної держави.

Висновки. Справді ефективним забезпечення інформаційної безпеки в інтернет просторі буде тільки за умови взаємодії людини та держави. Адже жодна державна політика у сфері забезпечення інформаційної безпеки не принесе позитивних результатів, якщо людина сама не дбатиме про власну інформаційну безпеку. І навпаки, як би людина не прагнула протидіяти негативним інформаційним впливам, самостійно без допомоги держави вона не зможе впоратися зі щоденним потоком інформації, який постійно дискредитує державу та все, що пов'язано з її діяльністю. Держава створює умови для забезпеченні інформаційної безпеки в інтернет просторі, а людина бере на себе відповідальність за «роботу» з інформацією, яку вона отримує, та дії, які вчиняє під її впливом. Отже, забезпечення інформаційної безпеки в інтернет просторі – це діяльність уповноважених органів та посадових осіб, яка здійснюється в межах, визначених законодавством, та спрямована на дотримання прав та свобод людини під час її взаємодії з інформацією, отриманою з інтернет простору (сприйняття, опрацювання та подальші дії, що ґрунтуються на одержаній інформації, захист персональних даних користувача інтернету), а також гарантування безпеки держави від дестабілізаційних впливів інших держав чи певних сил, що розміщуються в інтернет просторі.

Список використаних джерел:

1. Войтко О. В. Реалізація державної інформаційної політики та забезпечення інформаційної безпеки в умовах конфлікту з Російською Федерацією. *Міжнародний журнал «Грааль науки»*. 2021. №1. С. 164–166. https://doi.org/10.36074/grail-of-science.19.02.2021.030

2. Грубінко А. Інформаційна безпека України: правове гарантування та реалії забезпечення. *Актуальні проблеми правознавства*. 2019. № 1 (17). С. 5–10.

3. Кунєв Ю. Д., Легеза Є. О. Правове забезпечення інформаційної безпеки як предмет адміністративно-правового дослідження. *Наукові праці Національного авіаційного університету*. Серія: Юридичний вісник. 2021. Т. 1 (58). С. 183–185.

4. Федорова Н. Є., Смєсова В. Л. Інформаційна безпека та шляхи її забезпечення на етапі інформаційно-технологічної революції. *Причорноморська економічні студії*. 2020. Вип. 57. С. 13–16.

5. Budiningsih I., Soehari T.D., Irwansyah I. The Dominant Factor For Improving Information Security Awareness. *Jurnal Cakrawala Pendidikan*. 2019. Vol. 38 (3). P. 490–498.

6. Khando Khando, Shang Gao, Sirajul M. Islam, Ali Salman. Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*. 2021. Vol. 106. https://doi.org/10.1016/j.cose.2021.102267

7. Lidong Wang, Cheryl Ann Alexander. Cyber security during the COVID-19 pandemic. *AIMS Electronics and Electrical Engineering*. 2021. Vol. 5(2). P. 146–157. https://doi:10.3934/electreng.2021008

8. Senol Mustafa, Karacuha Ertugrul. Creating and Implementing an Effective and Deterrent National Cyber Security Strategy. *Journal of Engineering*. 2020. https://doi.org/10.1155/2020/5267564