
АДМІНІСТРАТИВНЕ ПРАВО. ІНФОРМАЦІЙНЕ ПРАВО

УДК 343.12:004

О. М. Головка, викладач,
Д. С. Бабич, студентка**КРИСТАЛІЗАЦІЯ ДЕФІНІЦІЙ «КІБЕРПРОСТІР» ТА «ІНФОРМАЦІЙНИЙ ПРОСТІР»
ЯК КОНЦЕПТУАЛЬНОГО БАЗИСУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

Анотація. У статті було досліджено концептуальні засади розмежування понять «інформаційний простір» та «кіберпростір» як першооснови інформаційної безпеки. Визначено стан забезпечення інформаційної безпеки суспільства та особи шляхом аналізу законодавчих положень та їх відповідності міжнародним зобов'язанням. Запропоновано шляхи узгодження та координації інтересів держави та соціуму у питаннях гарантування права на безпеку в інформаційній сфері.

Ключові слова: інформаційний простір, кіберпростір, інформаційна безпека, інформаційний вплив, інформаційна система, інформаційне суспільство.

О. М. Головка, преподаватель,
Д. С. Бабич, студентка**КРИСТАЛЛИЗАЦИЯ ДЕФИНИЦИЙ «КИБЕРПРОСТРАНСТВО» И «ИНФОРМАЦИОННОЕ
ПРОСТРАНСТВО» КАК КОНЦЕПТУАЛЬНОГО БАЗИСА ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ**

Аннотация. В статье было исследованы концептуальные основы разграничения понятий «информационное пространство» и «киберпространство» как первоосновы информационной безопасности. Определено состояние обеспечения информационной безопасности общества и личности путем анализа законодательных положений и их соответствия международным обязательствам. Предложены пути согласования и координации интересов государства и социума в вопросах обеспечения права на безопасность в информационной сфере.

Ключевые слова: информационное пространство, киберпространство, информационная безопасность, информационное воздействие, информационная система, информационное общество.

O. M. Golovko, Lecturer,
D. S. Babich, Student**CRYSTALLIZATION DEFINITIONS OF «CYBERSPACE» AND «INFORMATION SPACE»
AS A CONCEPTUAL BASIS OF INFORMATION SECURITY**

Abstract. This article was researched conceptual basis conceptual bases of distinguishing between the concepts «information space» and «cyberspace» as a fundamental principle of information security. Determine the the state of information security of society and individuals by analyzing the legal provisions and their compliance with international obligations. The ways of harmonizing and coordinating the interests of the state and society in terms of guaranteeing the right to security in the information field.

Keywords: information space, cyberspace, information security, informational influence, information system, information society.

Постановка проблеми. Нинішній рівень соціального розвитку характеризується швидким зростанням ролі інформації у всіх сферах суспільних відносин. Науково-технічні перевтілення ХХІ сторіччя викликали суттєві системні зміни в усьому світі. Завдяки новітнім досягненням у сфері інформаційно-комунікаційних технологій (далі – ІКТ) було сформовано віртуальний простір, які

АДМІНІСТРАТИВНЕ ПРАВО. ІНФОРМАЦІЙНЕ ПРАВО

називають інформаційним, кібернетичним тощо. Однак, виникає необхідність чіткого розмежування даних понять, пов'язана зі складністю врегулювання правовідносин у сфері їх використання.

Аналіз останніх досліджень та публікацій. Актуальність даної статті досліджувало багато вчених, зокрема, Засць О. В., Карчевський М. В., Панова І. В., Мельник С. В., Тихомиров О. О., та інші. У правовій доктрині, а саме, в галузі науки інформаційного права, питання співвіднесення визначених термінів були розглянуті такими вченими, як Біловус Л., Буньківська О. В., Бурячок В. Л., Дубов Д. В., Ожеван М. А. та ін. Проте, на жаль, основний акцент був зроблений на тлумаченні вищезгаданих понять, в той час як характеристика основних ознак їх розмежування залишалася без уваги. Це пояснюється, в першу чергу, тим, що вивчення правових аспектів існування людини у сучасному віртуальному просторі неможливо без вивчення та аналізу основних його категорій та дефініцій.

Метою роботи є аналіз підходів до розуміння та розмежування понять «кіберпростір» та «інформаційний простір» в сучасних соціально-політичних умовах, їх деталізація та адаптація до національних та геополітичних умов сучасної Української держави.

Виклад основного змісту матеріалу. Суть запропонованої тематики полягає в тому, що завдяки сьогоdnішньому швидкому прогресу можливостей інформаційних технологій гостро стоїть проблема інформаційного впливу на індивідуальну і суспільну свідомість. Тому нагальною проблемою є забезпечення особистості і суспільства від негативного впливу інформаційного потоку, а для цього необхідно оперувати чітким категоріально-понятійним апаратом.

Щодо визначення порівнюваних понять, слід відмітити неоднорідність їх тлумачень як на законодавчому рівні країн, так і окремими науковцями. Зокрема, Мельник С.В. визначає кіберпростір як простір, сформований інформаційно-комунікаційними системами, в якому проходять процеси перетворення (створення, зберігання, обміну, обробки та знищення) інформації, представленої у вигляді електронних комп'ютерних даних [1].

Відповідно до міжнародного стандарту, кіберпростір – це середовище існування, що виникло в результаті взаємодії людей, програмного забезпечення і послуг в Інтернеті за допомогою технологічних пристроїв і мереж, під'єднаних до них, якого не існує в будь-якій фізичній формі [2, с. 8-9]. За визначенням Міжнародного союзу електрозв'язку, кіберпростір – це фізичний і нефізичний простір, що складається з комп'ютерів, комп'ютерних систем, мереж та комп'ютерних програм, комп'ютерних даних, контенту, даних трафіку та користувачів [3].

Відповідно до нормативної бази США, кіберпростір – це сфера, що характеризується можливістю використання електронних та електромагнітних засобів для запам'ятовування, модифікування та обміну даними через мережні системи та пов'язану з ними фізичну інфраструктуру [2, с. 8-9]. В Стратегіях кібербезпеки Великої Британії та Німеччини даються такі визначення терміну «кіберпростір»: всі форми мережевої, цифрової активності, що охоплюють контент та дії в цифрових мережах; віртуальний простір всіх ІТ-систем, пов'язаних на рівні даних в глобальному масштабі. Основою кіберпростору є мережа Інтернет [3; 4].

Отже, кіберпростір охоплює собою як процеси створення, зберігання, обробки інформації, так і відповідну інфраструктуру: комп'ютерні мережі, системи, програми, пристрої, і, зрештою, людину як користувача таких мереж.

Виходячи з широкого спектру даного простору та неоднорідних відносин, що виникають у ньому пропонуємо здійснити порівняння сутності понять інформаційного простору та кіберпростору (див. табл. № 1).

АДМІНІСТРАТИВНЕ ПРАВО. ІНФОРМАЦІЙНЕ ПРАВО

Таблиця № 1

Критерій	Кіберпростір	Інформаційний простір
Рівні	Інфраструктурний, фізичний, синтаксичний й семантичний.	Глобальний, міжнародний, загальнодержавний, регіональний, локальний.
Доктринальне тлумачення	Форма співіснування сукупності матеріальних та нематеріальних об'єктів і процесів, спрямованих на породження, сприйняття, запам'ятовування, переробку та обмін інформацією [5, с. 165].	Форма співіснування сукупності матеріальних та нематеріальних об'єктів і процесів, спрямованих на задоволення інформаційних потреб всіх живих істот на Землі [5, с. 166].
Об'єкти	Живі істоти та їх угруповання, які спроможні сприймати, запам'ятовувати та переробляти інформацію, а також обмінюватися нею, серед яких, в першу чергу, людина, визначені верстви суспільства та суспільство в цілому, держава, природні та штучні інформаційні відносини між ними та їх формування і використання, а також матеріальні та нематеріальні об'єкти і процеси, спрямовані на породження, сприйняття, запам'ятовування, збереження, переробку та обмін інформацією.	Суб'єкти природного середовища, природні та штучні інформаційні відносини між ними та їх формування і використання, матеріальні та нематеріальні об'єкти і процеси, спрямовані на задоволення інформаційних потреб для забезпечення збереження життя та життєдіяльності живої істоти, угруповання живих істот.
Суб'єкти	Людина, суспільство, держава, жива істота, яка спроможна сприймати, запам'ятовувати та переробляти інформацію, а також обмінюватися нею.	Живі істоти та їх угруповання, які спроможні сприймати, запам'ятовувати та переробляти інформацію, а також обмінюватися нею.
Властивості	<ul style="list-style-type: none"> - протяжність; - єдність дискретності та неперервності; - матеріальність та нематеріальність; - абстрактність і дійсність; - реальність загальнодіючого впливу. 	
Спрямованість	Охоплює лише живі істоти, які спроможні сприймати, запам'ятовувати та переробляти інформацію, а також обмінюватися нею.	Охоплює абсолютно всі джерела інформації без вимог щодо спроможності сприймати, запам'ятовувати та переробляти інформацію, а також обмінюватися нею.

Українські державні відомства, відповідальні за національну безпеку, трактують кіберпростір як сформоване інформаційними, телекомунікаційними та комп'ютерними системами віртуальне середовище, що функціонує як єдине ціле у глобальному масштабі, та в якому відбуваються процеси виробництва, зберігання, обробки, передачі й обміну інформацією. Зокрема, дослідники Національного інституту стратегічних досліджень пропонують таке визначення кіберпростору: це об'єкти інформаційної інфраструктури, що керуються інформаційними (автоматизованими) системами управління, а також інформація, що в них циркулює [6].

Наведені визначення свідчать, що кіберпростір не обмежується мережею Інтернет, а охоплює середовище, створюване сучасними ІКТ, та безпосередньо обладнання, що відноситься до IT-інфраструктури [7, с. 81]. Під інформаційним простором розуміють територію поширення інформації за допомогою конкретних компонентів системи інформації і зв'язку, і функціонування інформаційної діяльності має гарантоване правове забезпечення [8].

АДМІНІСТРАТИВНЕ ПРАВО. ІНФОРМАЦІЙНЕ ПРАВО

Зауважимо, що Біловус Л. визначає інформаційний простір як сукупність суб'єктів інформаційної взаємодії чи впливу; власне інформації, призначеної для використання суб'єктами інформаційної сфери; інформаційної інфраструктури, що забезпечує можливість обміну між суб'єктами; суспільних відносин, котрі формуються як наслідок утворення, передачі, розповсюдження і зберігання інформації, обміну інформацією всередині суспільства [9, с. 189]. Доповнюючи зазначене, автори підручника «Інформаційна та кібербезпека: соціотехнічний аспект» у зміст поняття інформаційного простору вкладають наступне: це глобальне інформаційне середовище, яке в реальному масштабі часу забезпечує комплексну обробку відомостей про протидіючі сторони та їх навколишнє оточення з метою підтримання ухвалюваних рішень щодо створення оптимального задля досягнення поставлених цілей складу сил і засобів та їх ефективного застосування в різних умовах навколишньої обстановки [4, с. 7].

Безпосередньо в руслі інформаційного простору існує таке суспільно-політичне явище як інформаційна безпека – визначальна передумова та наслідок дієвої політики держави у сфері забезпечення конституційних прав громадян. Аналіз наукових публікацій, дає підстави стверджувати про неоднорідність визначеного поняття та можливість виділити основні його передумови. Так, одним з ключових чинників інформаційної безпеки особи є право на достатнє знання, для свідомого і об'єктивного вибору. Держава повинна надавати інформацію кожному праву сутність відносини, щоб отримати повну, точну і своєчасну інформацію; ніхто не має права порушувати інтереси інформації про взаємини будь-яким інформаційного впливу. Для збереження рівноваги між свободою інформації та необхідністю обмежити її в інтересах безпеки, держава створює відповідний правовий механізм, який, з одного боку, забезпечує захист інформаційних прав, з іншого боку, державний контроль над регулюванням інформаційною безпекою [10].

Правила, що стосуються сфери інформаційної безпеки в основному зосереджені на захисті інформації шляхом обмеження доступу осіб до певного типу інформації. Проте, слід зазначити, що основною мішенню негативного впливу інформації є саме людський розум, через який і здійснюється вплив на суспільну свідомість [11].

Одним з перших кроків на шляху до встановлення міжнародних стандартів по боротьбі з злочинним використанням інформаційних технологій була Всесвітня зустріч на вищому рівні з питань інформаційного суспільства (2003) [12]. Це призвело до прийняття Женевської Декларації принципів. Вона закріплює пріоритет приватного життя, що є необхідною умовою для розвитку інформаційного суспільства та підвищення довіри користувачів інформаційних технологій. Крім того, в декларації міститься заклик до необхідності генерування, розробки і впровадження глобальної культури кібербезпеки, поліпшення і забезпечення захисту і конфіденційності даних. Для досягнення цієї мети був зроблений акцент на здійсненні міжнародного співробітництва та імплементації цих стандартів в національне законодавство.

На жаль, стан інформаційної безпеки в Україні не відповідає цим вимогам. Це підтверджується, зокрема, в Аналітичній доповіді Українського центру економічних і політичних досліджень Разумкова, опублікованій в 2001 році, в якій говориться: «Аналіз показує, що рівень інформаційної безпеки в Україні, з незначними ознаками наближається до критичної точки, а саме: втрати демократичних принципів і засад держави, повернення до авторитаризму, ізоляції України на міжнародній арені» [12].

Аналіз національного законодавства дає підстави вважати, що нинішня тенденція розширює зміст законодавчого визначення «інформаційної безпеки». З розвитком інформаційного суспільства та вдосконалення нормативно-правового забезпечення цих процесів, розуміння законодавства з інформаційної безпеки переросла з вузького, простого визначення технічного захисту інформації в складну розгалужену систему.

Характеризуючи сучасне українське кримінальне законодавство слід зазначити, що питанню про інформаційну безпеку особистості як об'єкта кримінально захисту виділеної тільки статтю 163, яка передбачає відповідальність за порушення таємниці листування, телефонних розмов, телеграфної та іншої кореспонденції, що передаються через засоби зв'язку або комп'ютер [13].

АДМІНІСТРАТИВНЕ ПРАВО. ІНФОРМАЦІЙНЕ ПРАВО

З точки зору міжнародного права таке вузьке формулювання даного виду злочинів є недостатнім, з огляду на той факт, що Україна ратифікувала дві основоположні міжнародні угоди, в яких визначена система заходів по боротьбі з комп'ютерною злочинністю.

Так, Угода про співробітництво держав-учасниць Співдружності Незалежних Держав у боротьбі зі злочинністю в сфері комп'ютерної інформації, від 1 червня 2001 року визначає кримінально караними наступні діяння:

а) здійснення несанкціонованого доступу до комп'ютерної інформації захищеної законом, якщо це призвело до знищення, блокування, модифікацію або копіювання;

б) створення, використання або поширення шкідливих програм;

в) нецільове використання комп'ютерів або їх мережевих об'єктів, яке викликало руйнування, блокування або модифікацію інформації, захищеної законом, значний збиток або серйозні наслідки;

г) незаконне використання програмного забезпечення і баз даних, що є об'єктами авторського права, а також привласнення авторства [14].

Конвенція про кіберзлочинність від 23 листопада 2001 року покладає на держави обов'язок використовувати законодавчі та інші заходи, які можуть бути необхідними для визнання національним законодавством кримінальних правопорушень у інформаційній сфері та наступної їх класифікації за групами злочинів:

➤ перша група - злочини проти конфіденційності, цілісності і доступності комп'ютерних даних і систем (незаконний доступ, незаконне перехоплення, втручання в дані, втручання зі зловживанням системними пристроями);

➤ друга група включає в себе злочини, пов'язані з комп'ютерами (підроблення документів, пов'язаних з комп'ютерами, шахрайства, пов'язані з комп'ютерами);

➤ третя група включає злочини, пов'язані зі змістом інформації (злочинів, пов'язані з дитячою порнографією);

➤ четверта група включає злочини, пов'язані з порушенням авторського і суміжних прав [15].

Це дозволяє констатувати, що інформаційна безпека повинна розглядатися як здатність держави, суспільства, соціальної групи, особи з певною ймовірністю забезпечити достатні і захищені інформаційні ресурси та інформаційні потоки для підтримки та функціонування сталого розвитку, протистояти небезпеці і загрози негативного інформаційного впливу на індивідуальну і суспільну свідомість і психіку людей [16, с. 21].

Таким чином, інформаційна безпека вимагає динамічної координації та коригування особистих, соціальних і суспільних інтересів, щоб не допустити виникнення руйнівного конфлікту між ними, локалізації і нейтралізації негативних наслідків нездатності забезпечити баланс інтересів з об'єктивних чи суб'єктивних причин.

Отже, аналіз національного законодавства дає підстави вважати, що нинішня тенденція розширює зміст законодавчого визначення «інформаційної безпеки». З розвитком інформаційного суспільства та вдосконалення нормативно-правового забезпечення цих процесів, розуміння законодавства з інформаційної безпеки переросло з вузького, простого визначення технічного захисту інформації в складну розгалужену систему, вихідними поняттями якої є інформаційний простір та кіберпростір. Аналізуючи наведені тлумачення, можна зробити висновок, що інформаційний простір як сукупність елементів інформаційної взаємодії та безпосередньо інформації, яка використовується суб'єктами інформаційних відносин, співвідноситься з поняттям кіберпростір як ціле та частина. Кіберпростір виступає як сфера соціальної діяльності, пов'язана з обігом інформації у Всесвітній інформаційній павутині, а також в інших інформаційно-комунікаційних мережах.

Література

1. Мельник, С. В., Тихомиров, О. О. До проблеми формування понятійно-термінологічного апарату кібербезпеки / С. В. Мельник, О. О. Тихомиров // [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/portal/natural/Znrviknu/2011_30/Zbirnik_30_28.pdf.

2. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толубка]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с.

3. Even S., Siman-Tov D. Cyber Warfare: Concepts and Strategic Trends [Електронний ресурс]. – Режим доступу: <http://www.inss.org.il/index.aspx?id=4538&articleid=2487>.

АДМІНІСТРАТИВНЕ ПРАВО. ІНФОРМАЦІЙНЕ ПРАВО

4. Дубов, Д. В., Ожеван М.А. Кібербезпека: світові тенденції та виклики для України. Аналітична доповідь. – К. : НІСД, 2011. – 30 с.
5. Фурашев, В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності / В. М. Фурашев // Інформація і право. – 2012. – № 2. – С. 162-169.
6. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування. Аналітична записка [Електронний ресурс]. – Режим доступу: <http://www.niss.gov.ua/articles/454/>.
7. Запорожець, О. Ю. Кібервійна: концептуальний вимір / О. Ю. Запорожець // Актуальні проблеми міжнародних відносин. – 2014. – Вип. 121 (частина I). – С. 80-86.
8. Буньківська, О. В. Інформаційний простір: соціокультура сутність, стан та проблеми функціонування в Україні [Текст]: автореф. дис... канд. мистецтвознав.: 26.00.01 / Буньківська Оксана В'ячеславівна; Київський національний ун-т культури і мистецтв. – К., 2009. – 19 с.
9. Біловус, Л. Український інформаційний простір: сьогодення та перспективи / Л. Біловус // Український інформаційний простір. – 2013. – № 1: Частина 1. – С. 188-191.
10. Заєць, О. В. Захищеність особи від негативного інформаційно-психологічного впливу як напрямок інформаційної безпеки України / О. В. Заєць // Вісник Харківського Національного університету внутрішніх справ. – Х. :Нац. ун-т внутр. Справ – 2010 – № 4 (51) – с. 149-155.
11. Панова, І. В. Захист від впливу інформації, що є шкідливою для особи, як принцип інформаційного права / Панова, І. В. // Право і безпека: Наук. журн. – 2010 – № 3 – с. 69-72.
12. Актуальні проблеми інформаційної безпеки України (аналітична доповідь УЦЕПД) // Національна безпека і оборона – 2001 – № 1 – с. 2-60.
13. Кримінальний кодекс України: Відомості Верховної Ради України / 2001 [Електронний ресурс] – Режим доступу: http://zakon2.rada.gov.ua/laws/show/994_575.
14. Угода про співробітництво держав-учасниць Співдружності Незалежних Держав у боротьбі із злочинами у сфері комп'ютерної інформації / 2001 [Електронний ресурс] – Режим доступу: http://zakon2.rada.gov.ua/laws/show/997_353.
15. Конвенція про кіберзлочинність [Електронний ресурс] – Режим доступу: http://zakon2.rada.gov.ua/laws/show/994_575.
16. Кримінально-правова охорона інформаційної безпеки України: монограф. / М. В. Карчевський; МВС України, Луганськ: РВВ ЛДУВС ім. Е.О. Дідоренка, 2012. – 528 с. – С. 72-77.

Надійшла 9.12.2016