УДК 342.9
DOI https://doi.org/10.32844/2618-1258.2020.3.29

ТКАЧУК Т.Ю.

АДМІНІСТРАТИВНО-ПРАВОВІ ЕЛЕМЕНТИ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Створення належних умов для реалізації державної політики, спрямованої на захист національних цінностей та реалізацію національних інтересів України, на забезпечення безпеки особистості, суспільства та держави від зовнішніх та внутрішніх загроз в інформаційній сфері, потребує розвитку сучасних ефективних механізмів інформаційної безпеки, які відповідають природі та масштабам викликів сучасності. Складна військово-політична, оперативно-стратегічна та економічна ситуація, що виникла внаслідок збройної агресії Російської Федерації проти нашої держави, набула небезпечних проявів у інформаційному просторі.

Доктринальне та нормативне визначення такої фундаментальної категорії, як «система інформаційної безпеки», стає надзвичайно актуальною, оскільки інформаційна безпека – це системне, багаторівневе явище, на яке впливають зовнішні та внутрішні фактори, зокрема: політична ситуація у світі; внутрішньополітична ситуація в державі; стан та рівень інформаційно-комунікаційного розвитку країни тощо.

Розмежування інформаційної безпеки як динамічної системи та забезпечення інформаційної безпеки як процесу підтримки цього стану (включаючи самовідтворення, збереження та розвиток) є важливим для усунення суперечності між організаційно-структурними та функціонально-діяльнісними підходами до визначення сутності явища інформаційної безпеки та її системи.

Так, система інформаційної безпеки включає захист інформації, захист від інформаційних впливів, а також захист інформаційних прав та належний порядок реалізації інтересів суб'єктів інформаційної сфери. Що стосується об'єктів, то система інформаційної безпеки на національному рівні відповідає класичній формулі об'єктів національної безпеки «територія – населення – система державного управління», але замість території для інформаційної безпеки ми вважаємо використовувати «інформаційний простір», який охоплюватиме інформаційну модель території та її інформаційне обслуговування.

Ключові слова: *безпека, інформація, інформаційний простір, забезпечення.*

Creating the proper conditions for the implementation of the state policy aimed at protecting national values and realizing Ukraine's national interests, ensuring the security of the individual, society and the state from the external and internal threats in the information sphere, requires the development of modern effective information security mechanisms that respond to the nature and scale of the challenges the present The complex military-political, operational-strategic and economic situation, which arose as a result of the armed aggression of the Russian Federation against our state, has come to perilous manifestations in the information space.

The doctrinal and normative definition of such a fundamental category as the "information security system" becomes extremely relevant, since information security is a systemic, multilevel phenomenon influenced by external and internal factors, in particular, the political situation in the world; internal political situation in the state; the state and level of information and communication development of the country, etc.

The separation of information security as a dynamic system and the ensuring of information security as a process to maintain this state (including self-reproduction, preservation and development) is important for eliminating the contradiction between organizational-structural and functional-activity approaches to defining the essence of the phenomenon of information security and its system.

© ТКАЧУК Т.Ю. – доктор юридичних наук, доцент, заступник завідувача кафедри (Навчально-науковий інститут інформаційної безпеки Національної академії Служби безпеки України)

So, the system of information security includes security of information, security against information influences, as well as the protection of information rights and proper order of realization of interests of subjects of the information sphere. As for objects, the system of information security at the national level corresponds to the classical formula for the objects of national security "territory – population – the system of state administration", but instead of the territory for information security, we consider to use the "information space", which will cover the information model of the territory and its informational service.

Key words: *security, information, information space, provision.*

Вступ. Виходячи з комплексного визначення інформаційної безпеки з функціональної точки зору як безперервного процесу діяльності уповноважених органів, спрямованої на запобігання та протидію загрозам в інформаційній сфері, на вжиття активних заходів інформаційного впливу, а також як сукупності умов такої діяльності, що реалізуються й контролюються тривалий час, можемо виокремити активний (створення інформаційних загроз) та пасивний (протидія інформаційним загрозам) елементи інформаційної безпеки.

Постановка завдання. Метою статті є здійснення правового аналізу основних складників системи забезпечення інформаційної безпеки.

Результати дослідження. У найзагальнішому розумінні глобальна інформаційна сфера має дві компоненти, котрі водночас є *основними складниками інформаційної безпеки: технічну* – антропогенне штучне середовище техніки й технологій і *психологічну* – світ природи з його емоціями.

Принципові відмінності між названими складниками інформаційної безпеки та зміст інформаційно-психологічного складника схематично зображено на рис. 1.

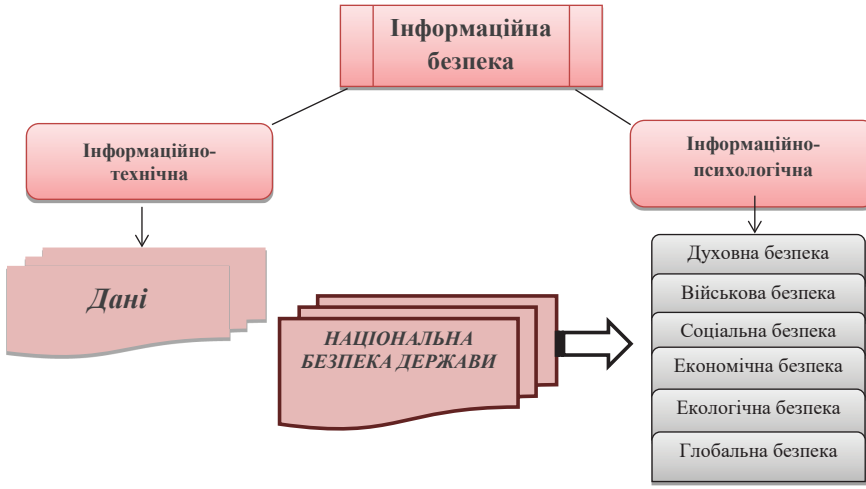

Рис. 1. Складники інформаційної безпеки

Отже, предмет правового забезпечення інформаційної безпеки держави – це пов'язані з інформаційною сферою суспільні відносини, які виникають у двох її складниках: технічному – комп'ютерні системи, телекомунікаційні мережі та інформаційно-психологічному – національні цінності, суспільна думка, індивідуальна та суспільна психологія.

У цьому дослідженні розглянемо детальніше інформаційно-психологічні аспекти інформаційної безпеки України, тобто захищеність головної національної цінності – психічного здоров'я людини й суспільства, а також національних інформаційних ресурсів, до яких належать насамперед державні секрети та комерційна таємниця, втрата чи розголошення котрих може істотно зашкодити національним інтересам і національній безпеці держави.

Не зайве підкреслити, що пріоритетному захисту в цьому разі підлягає саме суспільна свідомість українців. Адже сьогодні вже маємо безліч переконливих прикладів, як маніпулювання суспільною свідомістю та інші деструктивні інформаційно-психологічні впливи викликають, провокують або сприяють серйозним дисфункційним суспільно-політичним процесам, котрі

можуть призвести до розбалансованості та імпотенції владних структур, соціально-політичних напружень, безладів, потрясінь і т.п.

Як один з окремих фундаментальних елементів системи національної безпеки України інформаційна безпека нерозривно пов'язана з усіма іншими складниками безпеки, успішне функціонування яких значною мірою залежить від рівня її забезпечення. Ми погоджуємося з О. Корейком, що сьогодні інформаційний складник не існує поза межами загальної національної безпеки, так само як і національна безпека не буде всеосяжною без інформаційного свого складника [1, с. 9].

Саме нині, в епоху бурхливого зростання обсягів застосування інформаційних технологій у всіх сферах життєдіяльності, успішне вирішення проблем у галузі правового забезпечення інформаційної безпеки держави передбачає більш ефективну діяльність у процесі забезпечення національної безпеки. Зупиняючись на найважливіших питаннях з погляду безпечного розвитку, виділимо роль інформаційної безпеки в процесі забезпечення кожного з безпекових видів у системі інформаційної безпеки.

Розглянемо докладніше кожен із видів інформаційної безпеки.

Пріоритетними об'єктами забезпечення *духовної безпеки* є: мова як головна ознака нації, основа національна культура та історична спадщина народу; наука, освіта, мистецтво, а також головне джерело інформування суспільства – засоби масової комунікації. Інформаційно-психологічне протиборство та пропаганда вважаються найбільш ефективними з-поміж методів захисту духовної сфери.

Основними засобами інформаційно-психологічного впливу є дезінформація і різноманітні методики маніпулювання свідомістю людини й суспільства з метою їх деморалізації та прихованого керування поведінкою. Головним завданням таких впливів є формування у людини й соціуму в цілому спотворених поглядів на навколишній світ і самих себе шляхом пропагування, навіювання фальшивих цінностей, хибних пріоритетів і цілей.

Забезпечення *військової безпеки* визначальною мірою пов'язане сьогодні з упровадженням інформаційних технологій. Отже, небезпека від ураження сучасних комп'ютеризованих систем управління військом, систем озброєння, логістики тощо кібернетичною зброєю противника, його інформаційними атаками значно підвищується. Недооцінка цих реалій стала одним із найвагоміших чинників трагічних подій на півдні та сході нашої країни.

Економічна безпека як складова частина інформаційної безпеки в системі національної безпеки пов'язана з так званою інформаційною економікою, котра виникла як результат прогресу інформаційних технологій, створення глобальних інформаційно-телекомунікаційних систем, зростання потреб населення в інформаційних послугах. А про визначальний вплив економіки на всі сфери суспільного розвитку, напевно, не варто зайвий раз говорити [2, с. 370].

Натепер, як слушно зазначають фахівці, інформаційна безпека національної економіки є атрибутивною ознакою суверенітету держави та її цілісності. При цьому стабільний соціально-економічний і політичний прогрес країни на основі сучасних інновацій багато в чому залежить від формування ефективної системи інформаційної безпеки [3, с. 45]. Розвиток інформаційної економіки стає стратегічно важливим чинником сучасної геополітики. Тому актуалізується також потреба унормування таких економічних явищ, як, наприклад, криптовалюта, електронна комерція, Інтернет-розрахунки та інших нових суспільних відносин.

У свою чергу формування глобального інформаційного простору, базисом якого є комп'ютерна мережа, ставить перед державою низку серйозних питань щодо забезпечення економічної безпеки. Вказані проблеми стосуються методів і технологій захисту інформаційних ресурсів, що концентруються в інформаційних мережах. Ця ситуація пов'язана з формуванням інформаційної політики держави стосовно забезпечення захищеності життєво важливих інтересів країни у сфері інформаційної безпеки.

Соціальна безпека як складова частина інформаційної безпеки передбачає захист інтересів населення у цій сфері, суспільних відносин, способу життя, функціонування громадських структур, систем життєзабезпечення, адекватних сучасному етапу цивілізаційного розвитку.

Людина й людські спільноти завжди є головним об'єктом усіх форм управління, в тому числі й механізмів інформаційного керування. Сучасні інформаційні технології значно розширили можливості й підвищили ефективність впливу на психіку і свідомість людей завдяки впровадженню новітніх методів, засобів і прийомів латентного маніпулювання. Отже, загроза дегуманізації настільки актуалізувалася, що саме життя людини вийшло на передній план у структурі сучасних цінностей. При цьому в контексті державно-правового захисту зазіхання на психіку людей вважаються, як правило, другорядними порівняно з фізичними посяганнями. І якщо пра-

вове забезпечення взагалі зазвичай не встигає за процесами суспільного розвою, то про духовну сферу, особливо щодо безпекових проблем, годі й говорити. Тому питання правової захищеності свідомості людей є сьогодні серед головних пріоритетів.

Зловмисне використання інформаційних технологій задля провокування соціального розшарування суспільства шляхом розподілу інформаційного продукту, диссолюції інститутів, спрямованих на розвиток особистості, інспірування розколу суспільства на підставі етнонаціональних, ідеологічних, мовних, конфесійних та інших чинників призводить до негативних деформацій соціальної сфери. Отруйні «плоди» такої інформаційної агресії Російської Федерації вже багато років лихоманять українське суспільство.

Атрибутом інформаційного суспільства є засоби масової інформації, котрі сьогодні є фактично монополістами на ринку задоволення інформаційних потреб соціуму, як на рівні окремого населеного пункту, регіону, країни, так і у світовому масштабі. Тому вони здатні нав'язувати певні ідеологічні погляди й настанови, формувати громадську думку, виступити надпотужним чинником як стабілізації та згуртування суспільства, так і провокування соціальних заворушень і вибухів. З огляду на це натепер усе частіше порушується питання про достовірність та якість інформації, що ретранслюється ЗМІ, посилення відповідальності за це суб'єктів означеної сфери. Звісно, всі спрямовані на це заходи мають здійснюватися виключно у правовому полі, а тому, як бачимо, досягти бажаного рівня соціальної безпеки неможливо без належного правового забезпечення інформаційної безпеки.

Бурхливий розвиток електронних технології зумовив також виникнення нових серйозних загроз навколишньому природному середовищу, здоров'ю та життю людей, що актуалізувало й глобалізувало питання забезпечення *екологічної безпеки*. Забруднення повітря, землі та водойм, знищення багатьох видів живих організмів і цілих екосистем, руйнування озонового шару планети, техногенні катастрофи (Чорнобиль, Бхопал, Фукусіма та багато інших), створення й застосування нових видів зброї – ось далеко не весь перелік наслідків реалізації подібних загроз.

З-поміж основних шляхів розв'язання безпекових проблем у цій сфері – екологічний моніторинг, моделювання природних процесів, обчислення й урахування антропогенних навантажень і техногенних впливів на навколишнє середовище. Упевнені, що продуктивність таких заходів значною мірою залежить від цілеспрямованого застосування новітніх інформаційних технологій. Отже, безпосередній зв'язок екологічної та інформаційної безпеки цілком очевидний.

Таким чином, унікальна специфіка феномену інформаційної безпеки, котра є атрибутивною ознакою всього безпекового спектру – економічної, соціально-політичної, військової та екологічної безпеки, зумовлює її визначальну роль у процесі забезпечення національної безпеки. Іншими словами, умови та ефективність забезпечення основних видів безпеки людини, суспільства й держави на сучасному етапі розвитку соціуму вирішальною мірою залежать від забезпечення інформаційної безпеки.

Більше того, сьогодні активно дискутується питання про так звану екологію інформації. Показовою з цього приводу є праця Фелікса Сталдера, яка так і називається – «Екологія інформації» [4]. На підставі свого дослідження вчений резюмує, що медіа створюють інтегроване середовище (environment), основу якого становлять потоки інформації. Все частіше в діяльності людини це середовище стає головним. Екологія інформації прагне зрозуміти його властивості, щоб використовувати потенціал цього середовища, уникати небезпек і позитивно впливати на його розвиток.

У цьому контексті ми підтримуємо Р. Проданюка, який зазначає, що інформаційна безпека може розглядатись як одна із соціальних інституцій контролю за підтриманням інформаційної рівноваги, функція якої полягає в підтриманні екологічності інформаційного простору [5, с. 87].

Розвиток інформаційних технологій на початку XXI століття визначив загальні тенденції поступу людства та окреслив характерні проблеми даної епохи, серед яких:

1. Формування нового планетарного простору, в основі якого інформаційні й телекомунікаційні технології забезпечують ефективну взаємодію між людьми. Основними характеристиками таких процесів є безмежність, доступність, гіперпов'язаність, «стирання» територіальних кордонів, рух у масштабі часу, розвиток Інтернету речей тощо. Як наслідок, відбувається становлення нового інформаційного суспільства.

2. Усі без винятку суспільні процеси (політичні, соціальні, економічні) залежать від використання інформаційних технологій, оскільки вони мають вирішальне значення у формуванні існуючої реальності та справляють неабиякий вплив на її розвиток.

3. Недостатня увага з боку як міжнародних інституцій, так і національних урядів, до проблем правового забезпечення інформаційної безпеки стали причиною виникнення та надшвидкого поширення понять «інформаційна зброя», «інформаційний тероризм» та «інформаційна війна», а також деструктивних впливів від позначуваних цими термінами явищ. Значне применшення завдань інформаційної безпеки стало причиною непрогнозованих економічних, соціальних, екологічних, політичних та інших потрясінь у системі безпеки. Унаслідок вирішення питань інформаційної безпеки зі значним запізненням вийшло на перший план в усіх сферах суспільного життя і державної діяльності, як на національному, так і на міжнародному рівнях [6].

Як бачимо, в досліджуваній системі можемо виокремити *глобальну безпеку*, позаяк у загальносвітовому контексті інформаційна безпека набуває статусу всеосяжної проблеми сучасного етапу розвитку людства. Вказаний характер глобальної безпеки зумовлює такі її ознаки, як:

– вона охоплює всі без винятку країни світу;

– вона є об'єктивною передумовою і провідним засобом прогресу світової спільноти;

– як перша стадія ноосфери інформаційна безпека є актуальним завданням в умовах формування світового інформаційного суспільства;

– нехтування питаннями інформаційної безпеки відкриває шлях інформаційним війнам, інформаційному тероризму та іншим загрозам.

Звідси випливає, що для посилення інформаційної безпеки, запобігання негативним інформаційно-психологічним впливам на людину й суспільство та їх припинення потрібні спільні скоординовані зусилля всього міжнародного співтовариства.

Висновки. Таким чином, виникла потреба створення загальносвітової системи інформаційної безпеки, оскільки в реаліях світового інформаційного простору інформаційна безпека може бути ефективно забезпечена лише спільними діями всіх держав. Система глобальної інформаційної безпеки має стати важливим чинником сталого прогресу в глобальних масштабах. Зрозуміло, що така кооперація – справа складна й потребує тривалої, злагодженої, конструктивної співпраці. Убачається, що подібні перемови доцільно починати на рівні підінститутів, як, скажімо, проект Міжмор'я (Intermarium) та аналогічні.

Питаннями, які мають розглядатися в межах таких міжнародних проектів розвитку глобальної інформаційної безпеки, можуть бути, наприклад, такі:

– захист глобального інформаційного середовища від реальних і потенційних загроз і викликів;

– безпечні для людини, суспільства й навколишнього середовища напрями розвитку інформаційного простору;

– розвиток інформаційної культури людини й суспільства.

При цьому важливо пам'ятати, що захист і зміцнення безпеки світового інформаційного простору, який не визнає географічних і державних кордонів, – спільна справа всього міжнародного співтовариства, позаяк його вразливість і шкода від нього відбивається на всіх без винятку країнах. З огляду на це вбачається доцільним висунути на порядок денний питання узгодження національних стандартів і законів, співпраці з їх реалізації, укладання міждержавних угод у соціальній, політичній, культурній, юридичній та інших сферах функціонування міжнародного інформаційного простору.

Список використаних джерел:

1. Корнейко О. Застосування та визначення терміна «інформаційна безпека» в національному законодавстві. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні* : Науково-технічний збірник. 2009. Вип. 2 (19). С. 9–13.

2. Drucker P.F. The Age of Discontinuity. Guidelines to Our Changing Society. London : New Brunswick (US), 1994. P. 370.

3. Білак Ю.Ю. Інформаційна безпека як елемент підвищення ефективності інноваційного розвитку України. *Вісник КНУТД.* 2017. № 4 (113). С. 44–50.

4. Stalder F. Information Ecology; McLuhan Program in Culture and Technology, 1997. URL: http://felix.openflows.com/html/infoeco.html

5. Проданюк Р.І. Інформаційна безпека в соціологічному контексті: до постановки проблеми. *Грані* : Науково-теоретичний альманах. 2018. Т. 21. № 4. С. 84–90.

6. Ткачук Т.Ю. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. *Підприємництво, господарство і право*. 2017. № 10. С. 182–186.