

УДК 340.1+342.951+340.13

ГРИЩЕНКО А.О., аспірант Науково-дослідного інституту
інформатики та права НАПрН України.

ПІДХОДИ ДО РОЗУМІННЯ КАТЕГОРІЇ “ІНФОРМАЦІЙНА БЕЗПЕКА” ТА ПРАВОВІ ЗАСАДИ ЇЇ ЗАБЕЗПЕЧЕННЯ

***Анотація.** Дослідження основних підходів до визначення інформаційної безпеки людини, суспільства та держави в теорії права та правових засад її забезпечення.*

***Ключові слова:** інформаційна безпека, забезпечення інформаційної безпеки, види інформаційної безпеки, об'єкт забезпечення інформаційної безпеки, інформаційна безпека людини, суспільства та держави, правові засади забезпечення інформаційної безпеки.*

***Summary.** Research of the main approaches to defining the personal, social and state information security in theory of law and the legal basis for its ensuring.*

***Keywords:** information security, ensuring information security, types of information security, object of ensuring information security, information security of the person, society and state, legal basis of ensuring information security.*

***Аннотация.** Исследование основных подходов к определению информационной безопасности человека, общества и государства в теории права и правовых основ ее обеспечения.*

***Ключевые слова:** информационная безопасность, обеспечение информационной безопасности, виды информационной безопасности, объект информационной безопасности, информационная безопасность человека, общества и государства, правовые основы обеспечения информационной безопасности.*

Постановка проблеми. Значення інформації для людини, суспільства, держави ще відзначається ще за часів Античності, а перші згадки про інформаційну безпеку сягають корінням сивої данини. Наприклад, ще другий Цар єдиного Ізраїльського царства Давид, який правив приблизно у 1010 – 970 роках до нашої ери, у своїй молитві промовляв: “Ти погубиш тих, хто говорить брехню; кровожерним і підступним гребує Господь”. Якщо розмірковувати над цим виразом через призму сучасних інформаційних процесів, під брехнею можна розуміти “дезінформацію” чи “недостовірну інформацію” [1, с. 82].

Із розвитком інформаційного суспільства, збільшенням обсягу інформації, до якої людина отримує доступ легко та без особливих зусиль, рівень та кількість інформаційних загроз, швидкість їх розповсюдження та масштабність можливих наслідків зростає.

Таким чином, актуальність забезпечення інформаційної безпеки України, особливо в умовах інформаційної агресії, з кожним днем збільшується, а її ефективне нормативно-правове регулювання стає життєво необхідним для забезпечення суверенітету держави.

Результати аналізу наукових публікацій. Незважаючи на велику кількість міжнародних і національних форумів, конференцій, семінарів різних рівнів, опублікованих наукових робіт, присвячених найрізноманітнішим аспектам інформаційної безпеки, досі існують розбіжності як у правовій науці, так і колізії та прогалини у законодавстві щодо визначення основоположної категорії – “інформаційна безпека”. Це затримує розвиток системи забезпечення інформаційної безпеки на національному рівні та цим самим створює фундамент для підриву національної безпеки в умовах інформаційної агресії та його правових засад.

Метою статті є оцінка основних підходів до визначення категорії “інформаційна безпека” в теорії права та правових засад її забезпечення.

Виклад основного матеріалу. Як і про час виникнення інформаційного суспільства, так і про час зародження інформаційної безпеки існують розбіжності в поглядах серед науковців. Деякі науковці притримуються думки, що значення інформаційної безпеки у державотворчих процесах розуміли ще мислителі та правителі держав до нашої ери, хоча саме поняття, таким як ми його сприймаємо сьогодні, виникло пізніше [1, с. 82-83]. Інші ж вважають, що потреба у забезпеченні інформаційної безпеки виникла слідом за доступністю засобів інформаційних комунікацій між людьми, наявністю і розвитком яких забезпечує інформаційний обмін між всіма елементами соціуму, та з усвідомленням людиною можливості завдання збитку шляхом дії на ці засоби [2].

Не зважаючи на відсутність єдиного підходу до розуміння часу виникнення інформаційної безпеки та потреби в її забезпеченні, усі дослідники цього явища підкреслюють актуальність та важливість забезпечення інформаційної безпеки для збереження суверенітету держави. Забезпечення інформаційної безпеки на рівні держави, як і будь-яких інших суспільних відносин, розпочинається із визначення правових засад регулювання відносин між усіма суб'єктами, тобто тих основ та головних принципів, на яких ґрунтується регулювання державою суспільних відносин.

Сукупність ідей та концепцій, що визначають національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері та механізм регулювання суспільних відносин у цій сфері набули нормативного значення у Доктрині інформаційної безпеки України, що була затверджена та введена в дію Указом Президента України від 25 лютого 2017 року № 47/2017 “Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року “Про Доктрину інформаційної безпеки України” [3]. Таким чином, ці положення набули загальнообов'язкового характеру і визначили основні напрями нормотворчості та правозастосування на найближчий час у цьому напрямку.

Метою Доктрини стало “уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни”. Доктриною визначено, що “Російською Федерацією застосовуються проти України найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України” [3].

Незважаючи, на існування цього нормативного акту, що визначає основні засади формування політики в інформаційній сфері, та надзвичайну актуальність здійснення активних дій, спрямованих на захист суверенітету держави, визначення основоположного поняття у цій сфері, такого як “інформаційна безпека”, не набуло законодавчого закріплення, а дискусії щодо нього на доктринальному рівні тривають досі. Зазначене стало однією з основних причин невідповідності інформаційного законодавства України вимогам сучасності [4, с. 19].

Причинами існування різних підходів до формулювання сутності категорії “інформаційна безпека” можна назвати динамічність цього явища, а також структурно-функціональну та системну складність, що виражається у його глобальному і водночас індивідуальному прояві стосовно різних суб'єктів (осіб, організацій, суспільств, держав) і сфер їх життєдіяльності [5, с. 44; 6].

На підставі узагальнення різноманітних поглядів вчених Максименко Ю.Є. через призму змісту категорії “національна безпека” було виокремлено два підходи у визначенні поняття інформаційної безпеки – “статичний” та “динамічний”. “Статичний підхід” пов’язаний з тим, що національна безпека визначається через конструкцію “стан захищеності” (захисту) та “динамічний підхід” – під національною безпекою дослідники розуміють певний процес, діяльність тощо. На його думку, більш адекватним є другий підхід, оскільки розкриття лише однієї сторони – стану захисту при визначенні поняття національної безпеки вважається неповним. За такого розуміння нівелюються і втрачаються такі важливі властивості та функції безпеки, як превентивні дії – звуження, послаблення, усунення і попередження небезпек та загроз [7, с. 16].

Розгляд поняття “інформаційної безпеки” варто розпочати з визначення її місця у сфері забезпечення національної безпеки. У цьому питанні також немає єдиного бачення у юридичній науці та існують три основні погляди на це питання: інформаційна безпека як невід’ємна сфера забезпечення національної безпеки [5; 8 – 10]; інформаційна безпека як окремий самостійний вид безпеки [2; 4; 11 – 14]; інформаційна безпека як інтегруюча складова кожної сфери національної безпеки та водночас і самостійна частка національної безпеки [17 – 20].

Першими спеціальними дослідженнями, у яких розгляд поняття “інформаційна безпека” набув обертів, були дослідження у сфері національної безпеки. Саме завдяки цим роботам підхід, відповідно до якого інформаційна безпека є складовою національної безпеки, залишається поширеним серед науковців і сьогодні [6].

Боднар І.Р. розглядає інформаційну безпеку як національну безпеку в інформаційній сфері, підкреслюючи її суттєве значення у забезпеченні національної безпеки. Це сприяє успішному вирішенню завдань в політичній, соціальній, економічній та інших сферах державної діяльності. На її думку, інформаційну безпеку слід розуміти як “сукупність засобів забезпечення інформаційного суверенітету України, захист інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз”. До завдання інформаційної безпеки автор віднесла створення системи протидії інформаційним загрозам та захист власного інформаційного простору, інформаційної інфраструктури, інформаційних ресурсів держави [8].

Цієї ж позиції притримується Захаренко К.В. Він характеризує інформаційну безпеку як невід’ємну складову національної безпеки, її інтегральну, наскрізну якісну характеристику та показник захищеності громадян, суспільства і держави [5, с. 45].

Під “інформаційною безпекою”, як невід’ємною частиною національної безпеки, Волошина Н.М. пропонує розуміти “захищеність встановлених законодавчо інформаційних процесів в державі, що забезпечують гарантовані Конституцією України умови розвитку людини, суспільства й держави, середовища суспільства, яке забезпечує її використання і розвиток на користь громадян, організацій, держави” [9, с. 55-56].

Корж І.Ф. інформаційну безпеку розглядає як так званий “галузевий” підвид безпеки України, як синонім терміну “національна безпека” [10, с. 71-72].

Дещо інших поглядів притримується Максименко Ю.Є., який у своєму дисертаційному дослідженні розглядає інформаційну безпеку як складову національної безпеки України та відстоює позицію про синонімічність, змістовну однозначність та взаємозамінність понять “інформаційна безпека” та “національна безпека в інформаційній сфері”. Під інформаційною безпекою Максименко Ю.Є. пропонує розуміти “результат управління реальними чи (та) потенційними загрозами (небезпеками) з метою задоволення національних інтересів людини, суспільства та держави в інформаційній сфері” [7, с. 8-10].

Підсумовуючи досліджену інформацію, можна узагальнити погляди на інформаційну безпеку як складову національної безпеки та охарактеризувати їх наступними тезами:

- інформаційна безпека є підвидом безпеки України, що проявляється у інформаційній сфері;
- інформаційна безпека має суттєве значення у забезпеченні національної безпеки та є показником захищеності громадян, суспільства і держави;
- інформаційна безпека передбачає собою систему протидії зовнішнім та внутрішнім інформаційним загрозам;
- метою забезпечення інформаційної безпеки є захист інформаційного суверенітету України, зокрема, власного інформаційного простору, інформаційної інфраструктури та інформаційних ресурсів держави.

Частина інших дослідників явища “інформаційної безпеки”, такі як Довгань О.Д., Ткачук Т.Ю., Фурашев В.М., Гурковський В.Т., Боднар І.Р., Остроухов В.В., Крюков О.І., Сезонова І.К., Нашинець-Наумова А.Ю. та інші розглядають інформаційну безпеку як окремий вид безпеки та самостійну складову національної безпеки.

Крюков О.І. розглядає інформаційну безпеку як “суспільні правовідносини щодо процесу організації створення, підтримки, охорони та захисту необхідних для особи (людини чи юридичної особи, установи, підприємства, організації), суспільства і держави безпечних умов їх життєдіяльності; суспільні правовідносини пов’язані з організацією технологій створення, розповсюдження, зберігання та використанням інформації (відомостей, даних, знань) для забезпечення функціонування і розвитку інформаційних ресурсів людини, суспільства, держави” [11].

На його думку, інформаційна безпека держави – це такий “стан інститутів держави і суспільства, за якого забезпечується надійний захист національних інтересів країни і її громадян в інформаційній сфері, тобто створення і підтримка відповідних інженерно-технічних потужностей та інформаційної організації, що відповідають реальним і потенційним загрозам, а також демографічному й економічному становищу країни” [11].

Остроухов В.В. інформаційну безпеку визначив як “стан захищеності об’єкта (особистості, суспільства, держави, інформаційно-технічної інфраструктури), при якому досягається його нормальне функціонування незалежно від внутрішніх і зовнішніх інформаційних впливів” [12].

Сезонова І.К. запропонувала наступне визначення поняттю “інформаційна безпека” – “це складна система інформаційних правовідносин, яка одночасно повинна задовольняти інформаційні права особистості, організацій та держави й не порушувати інформаційні права держави, організацій та особистості” [2].

На погляд Нашинець-Наумової А.Ю., інформаційну безпеку України можна інтерпретувати як “сукупність життєво важливих умов функціонування суб’єктів (особи, суспільства, держави) в інформаційній сфері та суб’єктивних (правових, політичних, інформаційних, наукових, оперативно-розшукових) можливостей їх усвідомлення й контролю” [13].

Керуючись метою забезпечення інформаційної безпеки, тобто створенням безпечного інформаційного середовища, Довгань О.Д. та Ткачук Т.Ю. визначили інформаційну безпеку України як “стан, за якого в умовах дії реальних та потенційних загроз забезпечується самозбереження, сталий і прогресивний розвиток інформаційної сфери, зокрема захищеність інформаційної інфраструктури, інформаційного простору, інформаційних ресурсів, інформаційних процесів та їх суб’єктів, а також досягнення відповідних національних цілей та реалізація національних інтересів в інформаційній

сфері”. При цьому науковці надали визначення поняттю “забезпечення інформаційної безпеки держави”, під яким вони розуміють “постійний процес діяльності компетентних органів, спрямований на запобігання, протидію загрозам інформаційній сфері, застосування активних заходів інформаційного впливу, а також сукупність умов такої діяльності, які реалізуються і здатні контролюватися тривалий час”. Дане визначення підкреслює підхід, відповідно до якого досягнення ефективності забезпечення інформаційної безпеки держави можливе лише за умови поєднання превентивних та активних контрзаходів у цьому безперервному процесі [4, с. 88].

Забезпечення інформаційної безпеки держави гарантуватиме: безпеку інформації загального доступу, мереж зв'язку, інформаційно-телекомунікаційних систем, технічних та програмних засобів виконання маніпуляцій з інформацією, доступу до інформації; конфіденційність інформації з обмеженим доступом; захищеність особи, суспільства й держави від шкідливого впливу певних видів інформації [4, с. 89].

За результатами дослідження, Фурашев В.М. сформулював визначення поняття “інформаційна безпека” шляхом переліку напрямів завдання можливої шкоди людині, суспільству і державі. Відповідно до цієї дефініції інформаційна безпека – це “стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається завдання шкоди через: негативний інформаційний вплив за допомогою, насамперед, несанкціонованого створення, розповсюдження, використання свідомо спрямованої із визначеною метою неповної, невчасної, невірогідної та упередженої інформації; негативні наслідки застосування інформаційних технологій; несанкціоноване порушення режиму доступу до інформації з подальшим її розповсюдженням та використанням” [14, с. 54].

Згідно з цим визначенням, об'єктами інформаційної безпеки є людина, суспільство та держава, а суб'єктами – інформація у всіх її проявах, джерела інформації, механізми та засоби її створення, доступу і розповсюдження та наслідки її використання, а також установчі і регуляторні нормативно-правові та адміністративно-організаційні норми і правила, які визначають їх формування, використання та припинення дії [14, с. 55].

Гурковський В.Т. у дисертаційному дослідженні розглянув поняття “національної інформаційної безпеки людини”, відповідно до якого це суспільні відносини, пов'язані із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в інформаційному просторі, що є необхідною умовою збереження та примноження духовних і матеріальних цінностей державоутворюючої нації, її існування, самозбереження і прогресивного розвитку України як суверенної держави, що залежить від цілеспрямованої інформаційної політики гарантій, охорони, оборони, захисту її національних інтересів”* [5, с. 218].

Надаючи визначення поняттю “інформаційна безпека”, погляди науковців не збігаються у розумінні суті цього явища та використовують як статичний, так і динамічні підходи. Одні дослідники визначають це як певний стан захищеності об'єкту, інші – як правовідносини.

Законом України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки” розглядається інформаційна безпека в інформаційному суспільстві. Згідно з вказаним законом, інформаційна безпека – це “стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається

* *Примітка від авт.* Цит. за: Гурковський В.Т. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки: дис. ...канд. юрид. наук: 25.00.02. Київ, 2004. 225 с. С. 35.

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” [15].

Законом України “Про національну безпеку України”, що є одним із основних правових актів у сфері забезпечення безпеки України, надано визначення термінам “державна безпека”, “національна безпека”, “воєнна безпека”, “громадська безпека і порядок”. Так відповідно до дефініцій цих термінів, дані явища розглядаються законодавцем як стан захищеності відповідних об’єктів від впливу загроз [16].

Крім того, існують думки щодо доцільності розгляду інформаційної безпеки як невід’ємної складової кожної зі сфер національної безпеки та їх інтегруючого компонента і водночас важливої самостійної частки забезпечення національної безпеки держави [17, с. 1; 18, с. 65; 19].

Так, Олійник О.В., підкреслюючи актуальність питання забезпечення інформаційної безпеки в сучасних умовах для сталого розвитку соціальної системи та її виживання, зазначає, що інформаційна безпека є складовою національної безпеки і системоутворюючим фактором усіх видів безпеки, які складають загальну систему національної безпеки [18, с. 65].

Степко О.М. у роботі “Аналіз головних складових інформаційної безпеки держави” підкреслює, що існує два аспекти вивчення інформаційної безпеки в контексті національної безпеки. З одного боку, це самостійний елемент національної безпеки будь-якої країни, а з іншого – інтегрована складова будь-якої іншої безпеки: військової, економічної, політичної і т.д. На його думку, одним з найбільш повних визначень інформаційної безпеки можна вважати наступне: “це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави, при якому зводиться до мінімуму завдання збитку через неповноту, невчасність і недостовірність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації. Це визначення тією чи іншою мірою охоплює практично всі сфери інформаційної взаємодії суб’єктів держави” [19].

Таке визначення поняття “інформаційної безпеки” охоплює напрямки комплексного вирішення проблеми її забезпечення практично у всіх сферах інформаційної взаємодії суб’єктів держави, шляхом одночасного забезпечення якісного інформування громадян та вільного доступу до різних джерел інформації, а також контролю за непоширенням таємної інформації, сприянню цілісності суспільства, захисту від негативних інформаційних впливів тощо [19].

Домбровська С.М. також підкреслює двоїстий характер інформаційної безпеки, який проявляється в тому, що вона є самостійною складовою державної безпеки та одночасно складовою усіх інших сфер державної безпеки. Це обумовлено тим, що рівень розвитку та безпека інформаційного середовища, які є одними з найвагоміших факторів у всіх сферах державної безпеки, активно впливають на стан політичної, економічної та інших складових державної безпеки України. Інформаційна безпека суспільства, держави характеризується стійкістю головних сфер життєдіяльності у відношенні до небезпечних інформаційних впливів та визначається здатністю нейтралізувати такі впливи. Як загальноприйняте визначення, Домбровська С.М. наводить таке визначення інформаційної безпеки – “стан захищеності життєво важливих інтересів громадян, суспільства та держави в інформаційній сфері” [20].

На нашу думку, зважаючи на щоденне зростання актуальності забезпечення інформаційної безпеки, правові засади регулювання цих суспільних відносин повинні формуватись з позиції приналежності інформаційної безпеки до самостійного виду. Це пояснюється тим, що прийняття єдиного відповідного законодавчого акту, який здійснюватиме правове регулювання комплексно та у взаємозв'язку усіх правовідносин у сфері забезпечення саме інформаційної безпеки, зокрема, в умовах інформаційної агресії, зменшить кількість прогалин та колізій у цій сфері, створить більш ефективну, зрозумілу та зручну у реалізації систему правових норм. Як показує безпосередньо вже досвід нашої держави, недостатня правова визначеність інформаційної безпеки України та неефективне її забезпечення, порушення суверенітету державою-агресором тягне за собою економічні та людські втрати, анексію територій та загалом дестабілізацію обстановки у країні.

До дискусійних тем належать також підходи до співвідношення інформаційної безпеки з безпекою інформації та інформаційних систем, кібербезпекою та комп'ютерною безпекою.

Брижко В.М., Задорожня Л.М., Коваль М.І. розглядають інформаційну безпеку з двох боків: як безпосередньо захист інформації, зокрема, захист таємниці, комерційної інформації, інформації з обмеженим доступом, персональних даних тощо, та як захист інформаційних систем, які фактично є засобом передачі інформації [18].

Кондратюк М.В. розглядає поняття “кібербезпеки”, “комп'ютерної безпеки” та “інформаційної безпеки” як тотожні поняття. Він зазначає, що кібербезпека є найважливішим елементом щодо забезпечення національної безпеки держави в усіх сферах. До факторів, що виводять питання комп'ютерної безпеки на перший план в системі забезпечення національної безпеки, на його думку, можна віднести: національні інтереси, загроза їм і забезпечення захисту від цих загроз, що виражаються, реалізуються і здійснюються через інформаційну сферу; комп'ютерні системи і права на них – це основні об'єкти не тільки кібербезпеки, а й основні елементи всіх об'єктів безпеки в усіх її областях; вирішення завдань національної безпеки пов'язано з використанням інформаційного підходу як основного науково-практичного методу; проблема національної безпеки має яскраво виражений інформаційний характер; інформаційна політика тісно взаємодіє з державною політикою забезпечення національної безпеки країни через систему кібербезпеки, де остання виступає важливою сполучною ланкою всіх основних компонентів державної політики в єдине ціле [21].

Останні роки багатьма дослідниками спростовується отождолення “інформаційної безпеки” з “безпекою інформації та інформаційних систем”, “кібербезпекою”, “комп'ютерною безпекою” та “захистом інформації” тощо.

Наприклад, Максименко Ю.Є. наголошує на помилковості отождолення інформаційної безпеки із забезпеченням безпеки інформації (за Максименко Ю.Є. – інформаційно-технічною безпекою). Він аргументує це тим, що таке твердження не зовсім точно відбиває сутність інформаційної безпеки України, оскільки не враховуються інші складові елементи системи інформаційної безпеки держави, такі як інформаційно-психологічна безпека та інформаційна безпека у сфері прав та свобод людини і громадянина [7, с. 8].

Важливість гуманітарного виміру інформаційної безпеки, тобто захисту від інформації та інформаційна вразливість людини, суспільства, держави, цивілізації, поряд з безпекою інформаційних технологій та інформаційних ресурсів, підкреслюють і Довгань О.Д. разом із Ткачук Т.Ю. у статті “Наукова рефлексія інформаційної безпеки України: від позитивізму до метафізики права” [1, с. 86].

Волошина Н.М також наголошує на розрізненні понять “безпека інформації”, об’єктом якої є інформація, та “інформаційна безпека”, як складова національної безпеки. Під безпекою інформації як поліаспектним поняттям науковець пропонує розуміти, по-перше, “стан інформації, інформаційних ресурсів та інформаційних і телекомунікаційних систем, при якому з необхідною вірогідністю державними і недержавними структурами забезпечується захист інформації від внутрішніх і зовнішніх загроз”, та, по-друге, “стан захищеності інформації, що оброблюється засобами обчислювальної техніки або автоматизованої системи від внутрішніх та зовнішніх загроз” [9, с.55].

Шляхом контекстного аналізу законодавства у сфері забезпечення інформаційної безпеки дає підстави тлумачити поняття “безпека інформації” як стан захищеності інформації в системі. У зв’язку з чим, під “захистом інформації” законодавець має на увазі діяльність із “забезпечення вказаного стану захищеності” [4, с. 88].

Найбільш точно, на думку Довганя О.Д. та Ткачука Т.Ю., діяльність із забезпечення інформаційної безпеки можна відобразити в категоріях “захист” і “охорона”. “Суть охорони інформації полягає у встановленні щодо окремих її видів певного правового режиму, скажімо, державної таємниці. Натомість захист інформації – це сукупність заходів із протидії загрозам та протиправним посяганням на права та законні інтереси суб’єктів в інформаційній сфері” [4, с. 88].

Тихомиров О.О. у своїх роботах зауважує, що по суті забезпечення інформаційної безпеки має гуманітарний вимір, натомість захист інформації безпосередньо пов’язаний із технічною діяльністю. Така позиція дозволяє залишити поза межами теоретико-правового обґрунтування своєрідності забезпечення інформаційної безпеки суто технічні та організаційно-правові аспекти технічного захисту інформації [6].

Кібернетична безпека, або кібербезпека виникла у зв’язку із появою нових потенційних та реальних загроз національній безпеці у кібернетичному просторі (кіберпросторі) – відносно новому та невід’ємному виміру інформаційної сфери, як наслідок стрімкого розвитку інформаційних технологій та широкого їх використання людством, що складається з двох вимірів – людського та технічного [14, с. 168; 22].

На основі зіставлення Барановим О.А. результатів аналізу визначення термінів “кібербезпека” та “інформаційна безпека” у Законі України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки”, можемо зробити висновок про те, що кібербезпека – це окремий випадок інформаційної безпеки, поява якого обумовлена використанням комп’ютерних систем та/або телекомунікаційних мереж. Враховуючи викладене, автор статті пропонує коротке визначення “кібербезпеці” – це “інформаційна безпека в умовах використання комп’ютерних систем та/або телекомунікаційних мереж” [22, с. 60-61].

Шляхом більш детального аналізу явища “кібербезпеки” через призму його правового регулювання, Баранов О.А. сформулював також більш розгорнуте визначення цього поняття: “це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп’ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації” [22, с. 60-61].

На думку Логінова І.В., кібернетична безпека є складовою інформаційної безпеки держави, та являє собою стан захищеності державних електронних інформаційних ресурсів у кіберпросторі та інфраструктури їх оброблення [23, с. 76].

Окрім визначення дефініції “інформаційна безпека”, у наукових працях тривають дискусії щодо об’єктів забезпечення інформаційної безпеки та відповідно її складових елементів. Провідні науковці виділяють наступні складові інформаційної безпеки: інформаційна безпека особи (особистості, людини), інформаційна безпека суспільства, інформаційна безпека організації (комерційних (корпоративних) структур, інформаційно-технічної інфраструктури), інформаційна безпека держави. На думку одних науковців, основними трьома елементами інформаційної безпеки є інформаційна безпека особистості, інформаційна безпека держави та інформаційна безпека організації (комерційних (корпоративних) структур, інформаційно-технічної інфраструктури) [2; 8; 12]. Серед цих трьох елементів Боднар І.Р. та Остроухов В.В. виокремлюють ще інформаційну безпеку суспільства [8; 12]. Інші ж розглядають лише інформаційну безпеку особи, інформаційну безпеку суспільства та інформаційну безпеку держави [1; 14; 25]. При відсутності єдності серед спеціалістів у переліку складових елементів інформаційної безпеки, відсутня єдина думка щодо назв цих елементів, про що свідчить використання синонімів одного поняття, але з різними відтінками.

Під час дослідження питання складових інформаційної безпеки доцільним вважається власне розуміння природи їх виникнення. Причиною виникнення категорії “інформаційна безпека людини, суспільства, держави” стало осмислення людиною її права на інформацію як елемента формування безпечного середовища проживання. Це пояснюється тим, що будь-яка діяльність людини є процесом пізнання, оскільки під час будь-якої діяльності (інтелектуальної чи фізичної) людина завжди зіштовхується та використовує інформацію: у процесі її отримання, обробки, структурування, та навіть під час прийняття будь-якого рішення вона потребує інформаційної підтримки. Усі явища або об’єкти, які їй невідомі, людина прагне зрозуміти і пояснити в своїй свідомості на основі отриманої інформації через інстинкт самозбереження. Так вона формує безпечне середовище для себе, та як наслідок – суспільства і держави [1, с. 81].

Варто зазначити, що усі складові інформаційної безпеки повинні розглядатись з урахуванням дотримання концептуально-теоретичного принципу системності, відповідно до якого жоден елемент не може бути розглянутий та визначений без взаємозв’язку та взаємозалежності з іншими елементами. [5, с. 46]. Кожен елемент інформаційної безпеки тісно пов’язаний з іншим, відповідно зниження ефективності забезпечення одного з них тягне за собою погіршення стану забезпечення іншого.

Пропонуємо більш детально розглянути елементи інформаційної безпеки, їх визначення, їх співвідношення та характеристики, що пропонують провідні спеціалісти у сфері інформаційної безпеки.

Враховуючи природу виникнення інформаційної безпеки, людина є найменшою та найочевиднішою одиницею, інформаційна безпека якої підлягає забезпеченню та повинна розглядатись як “одна з основних детермінант проблеми інформаційної безпеки” [24, с. 109].

Саме право на інформацію виступає певним індикатором стану інформаційної безпеки. Порушення права на інформацію людини, як загроза її інформаційній безпеці, однозначно спричинює уразливість інших елементів інформаційної безпеки, зокрема інформаційної безпеки суспільства і держави, перед зовнішніми та внутрішніми загрозами [1, с. 81], у тому числі перед інформаційною агресією.

Із стрімким прогресом інформаційних технологій ефективність засобів та способів впливу на психіку та свідомість значно зросла, з'явилися нові методи та прийоми прихованого маніпулювання. Людина стала головною ціллю в становленні контролю над механізмами управління [1, с. 87].

Інформаційна агресія, зокрема негативні інформаційно-психологічні впливи, у тому числі технології зомбування, нейролінгвістичного програмування людини тощо, спрямовується на злам природних запобіжників інформаційному насиллю або на їх блокування. Ці запобіжники протидії сучасним інформаційним засобам ураження та інформаційному насиллю на рівні із можливістю сприйняття, вироблення, синтезу, аналізу та використання інформації закладені природою у як у свідомість, так і підсвідомість людини. Вони можуть бути активовані самою людиною або соціальним середовищем, що її оточує [26, с. 17]. Усвідомлюючи це, важливо враховувати значення інформаційної безпеки людини у зв'язку із забезпеченням інформаційної безпеки суспільства та держави, та національної безпеки загалом.

На сьогодні держава шляхом правового регулювання надає перевагу захисту людини від фізичних посягань, ніж від зазіхань на психіку людей, цим самим відстає від процесів суспільного розвитку [1, с. 87].

Усе це вказує на доцільність активізації процесів розробки, встановлення належного правового регулювання, що відповідатиме сучасним інформаційним процесам, впровадження та реалізацію ефективних механізмів та способів регулювання та забезпечення інформаційної безпеки, в першу чергу, саме людини.

Як зазначено вище, науковці, виділяючи категорію інформаційної безпеки людини, використовують і синоніми слова “людина”, такі як “особа” та “особистість”. У зв'язку з цим пропонуємо звернутись до тлумачного словника української мови для визначення найбільш доцільної назви цього явища.

Академічний тлумачний “Словник української мови” надає наступні визначення цим поняттям:

- 1) особа – це окрема людина, індивід; людська індивідуальність, особистість; людина як втілення індивідуального начала в суспільстві;
- 2) особистість – конкретна людина з погляду її культури, особливостей характеру, поведінки і т. ін.; індивідуальність, особа;
- 3) людина – це одиничне до люди; будь-яка особа; кожний; людська постать [27].

Крім того, відповідно до статті 3 Конституції України, саме “людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю”. Розділом 2 Конституції визначаються права, свободи та обов'язки людини і громадянина [28]. Таким чином, в Основному Законі використовується слово “людина” для позначення найменшої одиниці, чий права та свободи гарантуються державою.

Зважаючи на викладене, на нашу думку, найбільш доцільним поняттям при виділенні структурної одиниці інформаційної безпеки є “людина”. Це пояснюється тим, що говорячи про забезпечення інформаційної безпеки найменшої одиниці, ми узагальнюємо цей об'єкт забезпечення, та підкреслення індивідуальності кожної людини в даному випадку не доцільне. У зв'язку з чим, пропонуємо використовувати поняття “інформаційна безпека людини”.

Здійснюючи аналіз ч. 1 ст. 3 Закону України “Про національну безпеку України”, одного із основоположних документів у сфері забезпечення національної безпеки України, варто зазначити, що законодавець виділяє три об'єкти державної політики у сферах національної безпеки і оборони:

- людина і громадянин (захист їхніх життя і гідності, конституційних прав і свобод, безпечних умов життєдіяльності);
- суспільства (захист його демократичних цінностей, добробуту та умов для сталого розвитку);
- держави (захист її конституційного ладу, суверенітету, територіальної цілісності та недоторканності; території, навколишнього природного середовища – від надзвичайних ситуацій) [16].

Крім того, у Розділі 5 “Очікувані результати” Закону України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки” зазначено, що впровадження норм даного закону надасть можливість підвищити рівень інформаційної безпеки саме людини, суспільства, держави [15].

У зв’язку з цим, підтримуючи класичну класифікацію видів інформаційної безпеки, пропонуємо визначити та використовувати для подальшого дослідження наступні види інформаційної безпеки: інформаційна безпека людини, інформаційна безпека суспільства та інформаційна безпека держави.

У контексті “Доктрини інформаційної безпеки України” інформаційна безпека згадується як “національна безпека в інформаційній сфері” [3]. Натомість у Законах України “Про національну безпеку України” та “Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки” вживається власне словосполучення “інформаційна безпека” [15; 16]. По суті, аналіз цих законодавчих актів говорить про тотожність понять “інформаційна безпека”, “національна безпека в інформаційній сфері” та “національна інформаційна безпека”.

З метою уникнення колізій та суперечностей у законодавстві, для забезпечення фундаменту подальшого розвитку правової думки у цій сфері, доцільно використовувати у законодавчих актах одне визначення. На нашу думку, найбільш доцільним буде закріплення на законодавчому рівні термін “національна інформаційна безпека”. Цей термін дозволить виокремити інформаційну безпеку від усіх інших видів безпеки, підкреслить її значення у забезпеченні національної безпеки та дозволить об’єднати у собі на лінгвістичному рівні її складові – інформаційну безпеку людини, інформаційну безпеку суспільства та інформаційну безпеку держави.

Таким чином, беручи до уваги дослідженні доктринальні підходи щодо розуміння інформаційної безпеки та вітчизняні нормативно-правові акти, пропонуємо наступні визначення:

Національна інформаційна безпека – це стан захищеності національних інтересів людини, суспільства і держави в інформаційній сфері, забезпечення якого досягається шляхом попередження, запобігання та нейтралізації загроз та агресії у цій сфері.

Забезпечення національної інформаційної безпеки – це діяльність компетентних органів держави, спрямована на забезпечення стану захищеності національних інтересів людини, суспільства та держави в інформаційній сфері шляхом попередження, запобігання та нейтралізації загроз та агресії у цій сфері.

Об’єктами забезпечення інформаційної безпеки є людина, суспільство та держава, на які спрямована діяльність компетентних органів забезпечення інформаційної безпеки.

Де, згідно з п. 10 ч. 1 ст. 1 Закону України “Про національну безпеку України”, національні інтереси України – це “життєво важливі інтереси людини, суспільства і держави, реалізація яких забезпечує державний суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності і добробут її громадян” [16].

Розгорнутий перелік національних інтересів України в інформаційній сфері наведений у 3 розділі Доктрини інформаційної безпеки. До життєво важливих інтересів особи належить: “забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; забезпечення конституційних прав людини на захист приватного життя; захищеність від руйнівних інформаційно-психологічних впливів”. Життєво важливі інтереси суспільства і держави були законодавцем об’єднані та наведені єдиним переліком: “захист українського суспільства від агресивного впливу деструктивної пропаганди, передусім з боку Російської Федерації; захист українського суспільства від агресивного інформаційного впливу Російської Федерації, спрямованого на пропаганду війни, розпалювання національної і релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України; всебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності у доступі до достовірної та об’єктивної інформації; забезпечення вільного обігу інформації, крім випадків, передбачених законом; розвиток та захист національної інформаційної інфраструктури; збереження і примноження духовних, культурних і моральних цінностей Українського народу; забезпечення всебічного розвитку і функціонування української мови в усіх сферах суспільного життя на всій території України; вільний розвиток, використання і захист мов національних меншин та сприяння вивченню мов міжнародного спілкування; зміцнення інформаційних зв’язків з українською діаспорою, сприяння збереженню її етнокультурної ідентичності; розвиток медіа-культури суспільства та соціально відповідального медіа-середовища; формування ефективної правової системи захисту особи, суспільства та держави від деструктивних пропагандистських впливів; створення з урахуванням норм міжнародного права системи і механізмів захисту від негативних зовнішніх інформаційно-психологічних впливів, передусім пропаганди; розвиток інформаційного суспільства, зокрема його технологічної інфраструктури; безпечне функціонування і розвиток національного інформаційного простору та його інтеграція у європейський і світовий інформаційний простір; розвиток системи стратегічних комунікацій України; ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації державної політики в інформаційній сфері; забезпечення розвитку інформаційно-комунікаційних технологій та інформаційних ресурсів України; захищеність державної таємниці та іншої інформації, вимоги щодо захисту якої встановлені законом; формування позитивного іміджу України у світі, донесення оперативної, достовірної і об’єктивної інформації про події в Україні до міжнародної спільноти; розбудова системи іномовлення України та забезпечення наявності іншомовного українського каналу в кабельних мережах та у супутниковому мовленні за межами України” [3].

Висновки.

Складність явища “інформаційної безпеки” та одночасна надзвичайна актуальність для держави забезпечення такого стану спровокували дискусії у правовій науці та колізії у законодавстві навколо розуміння та трактування цього поняття.

У наукових колах існують три основні підходи до розгляду інформаційної безпеки в контексті забезпечення безпеки держави, суспільства та людини: інформаційна безпека як невід’ємна сфера забезпечення національної безпеки, інформаційна безпека як окремий самостійний вид безпеки та інформаційна безпека як інтегруюча складова кожної сфери національної безпеки.

На нашу думку, підхід, відповідно до якого інформаційна безпека є самостійним видом безпеки, найбільше відповідає сучасним процесам трансформації суспільства.

Таке розуміння дозволяє розглядати усі механізми забезпечення інформаційної безпеки та правові засади їх регулювання у комплексі, в умовах коли усі правовідносини та процеси, що виникають у сфері забезпечення саме інформаційної безпеки, пов'язані між собою. Це особливо актуально в умовах сучасності, де інформаційна агресія, як зовнішня, так і внутрішня, вже не є чимось абстрактним, і кожен зіштовхується із нею протягом свого життя. Прийняття єдиного відповідного законодавчого акту, який здійснюватиме правове регулювання сфери забезпечення інформаційної безпеки, дозволить зменшити кількість прогалин та колізій у цій сфері, створить більш ефективну, зрозумілу та зручну у реалізації систему правових норм.

Варто підкреслити, що багатьма дослідниками спростовується ототожнення “інформаційної безпеки” з “безпекою інформації та інформаційних систем”, “кібербезпекою”, “комп'ютерною безпекою” та “захистом інформації” тощо, та підкреслюється її суттєве значення у забезпеченні національної безпеки України та у визначеності стану захищеності громадян, суспільства і держави.

Для формування єдиного загального поняття “інформаційної безпеки”, що дозволить об'єднати у собі три її складові: інформаційну безпеку людини, інформаційну безпеку суспільства та інформаційну безпеку держави, та підкреслити її значення в контексті забезпечення безпеки держави, пропонуємо розглянути закріплення на законодавчому рівні поняття “національна інформаційна безпека”.

На основі здійсненого аналізу наукових праць та чинного законодавства України, було сформульовано визначення наступних понять:

Національна інформаційна безпека – це стан захищеності національних інтересів людини, суспільства і держави в інформаційній сфері, забезпечення якого досягається шляхом попередження, запобігання та нейтралізації загроз та агресії у цій сфері.

Забезпечення національної інформаційної безпеки – це діяльність компетентних органів держави, спрямована на забезпечення стану захищеності національних інтересів людини, суспільства та держави в інформаційній сфері шляхом попередження, запобігання та нейтралізації загроз та агресії у цій сфері.

Об'єктами забезпечення національної інформаційної безпеки є людина, суспільство та держава, на які спрямована діяльність компетентних органів забезпечення інформаційної безпеки.

Перспективними напрямками подальших наукових досліджень у цій сфері є дослідження сутності інформаційної агресії та визначення її поняття, видів та характеристик, що дозволить продовжити дослідження правових засад забезпечення інформаційної безпеки в умовах інформаційної агресії.

Використана література

1. Довгань О.Д., Ткачук Т.Ю. Наукова рефлексія інформаційної безпеки України: від позитивізму до метафізики права. *Інформація і право*. № 4(27)/2018. С. 79-89.
2. Сезонова І.К., Нестерцова Ю.О. Інформаційна безпека досудового розслідування. *Сучасні проблеми правового, економічного та соціального розвитку держави*. Харків, 2016. С. 349-351.
3. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року “Про Доктрину інформаційної безпеки України”: Указ Президента України від 25.02.17 р. № 47/2017. Дата оновлення: 25.02.2017. URL: <https://zakon.rada.gov.ua/laws/show/47/2017#Text> (дата звернення: 08.09.2020).
4. Довгань О.Д., Ткачук Т.Ю. Концептуальні засади законодавчого забезпечення інформаційної безпеки України. *Інформація і право*. № 1(28)/2019. С. 86-99.

5. Захаренко К.В. Категорія інформаційної безпеки у вітчизняному філософсько-політологічному дискурсі. *Гуманітарний вісник Запорізької державної інженерної академії*. 2018. № 72. С. 44-52.
6. Тихомиров О.О. Забезпечення інформаційної безпеки як функція сучасної держави: монографія. Київ: Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. 196 с.
7. Максименко Ю.Є. Теоретико-правові засади забезпечення інформаційної безпеки України: автореф. дис. ...канд. юрид. наук: 12.00.01. Київ, 2007. С. 22.
8. Боднар І.Р. Інформаційна безпека як основа національної безпеки. *Механізм регулювання економіки*. 2014. № 1. С. 68-75.
9. Волошина Н.М. Поняття “безпеки інформації” та “інформаційна безпека” в сучасному науковому просторі. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2010. № 2(8). С. 53-56. URL: http://nbuv.gov.ua/UJRN/sitsbo_2010_2_14
10. Корж І.Ф. Державна безпека: методологічні підходи до системи складових поняття. *Правова інформатика*. № 4(36)/2012. С. 69-75.
11. Крюков О.І. Інформаційна безпека держави в умовах глобалізації. *Державне будівництво*. 2007. № 2. С. 1-8. URL: http://nbuv.gov.ua/UJRN/DeBu_2007_2_12
12. Остроухов В., Петрик В. До проблеми забезпечення інформаційної безпеки України. *Політичний менеджмент*. 2008. № 4. С. 135-137.
13. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім “Гельветика”, 2017. 168 с.
14. Фурашев В.М. Сутність та визначення понять “інформаційна безпека” і “безпека інформації”. *Правова інформатика*. № 2(34)/2012. С. 51-59.
15. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки: Закон України від 09.01.07 р. № 537-V. Дата оновлення: 09.01.2007. URL: <https://zakon.rada.gov.ua/laws/show/537-16#Text> (дата звернення: 08.09.2020).
16. Про національну безпеку України: Закон України від 21.06.18 р. № 2469-VIII. Дата оновлення: 15.03.2020. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text> (дата звернення: 08.09.2020).
17. Євдовиченко Л.О. Удосконалення системи державного забезпечення інформаційної безпеки України в умовах глобалізації: автореф. дис. ...канд. наук держ. упр.: 25.00.01. Львів, 2011. С. 20.
18. Олійник О.В. Адміністративно-правові засади інформаційної безпеки. *Європейські перспективи*. 2012. № 4(1). С. 65-68.
19. Степко О.М. Аналіз головних складових інформаційної безпеки держави. *Науковий вісник Інституту міжнародних відносин НАУ. Економіка, право, політологія, туризм*. 2011. Вип. 1(3). С. 90-99.
20. Домбровська С.М. Механізми забезпечення інформаційної безпеки як складової державної безпеки України. *Теорія та практика державного управління*. 2015. Вип. 1 (48). С. 1-5.
21. Кондратюк М.В. Комп’ютерна безпека України в системі національної безпеки: матеріали міжн. наук.-практ. конф. *Стан та перспективи реформування сектору безпеки і оборони України*, м. Запоріжжя, 24 лист. 2017 р. У 2 т. Київ: Національна академія прокуратури України, 2017. Т. 2. С. 67-69.
22. Баранов О.А. Про тлумачення та визначення поняття “кібербезпека”. *Правова інформатика*. № 2(42)/2014. С. 54-62.
23. Логінов І.В. Місце кіберрозвідки у виконавчому механізмі розвідувальної діяльності: матеріали всеукр. наук.-практ. конф. *Роль і місце національної спецслужби в історії українського державотворення*, м. Київ, 17 бер. 2017 р. Київ: ВПЦ “Київський Університет”, 2017. С. 76.
24. Захаренко К.В. Категорія “інформаційної безпеки” у вітчизняному науковому дискурсі. *Гуманітарний вісник ДВНЗ. – (Переяслав-Хмельницький державний педагогічний університет імені Григорія Сковороди)*. 2015. № 37. С. 106-117.

25. Олійник О.В. Позитивні та негативні впливи інформаційної революції на забезпечення інформаційної безпеки особи, суспільства, держави. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2011. № 25. С. 321-328.

26. Пилипчук В.Г. Актуальні проблеми становлення і розвитку правової науки в інформаційній сфері. *Інформація і право*. № 1(4)/2012. С. 15-22.

27. Академічний тлумачний словник (1970 – 1980): словник української мови. URL: <http://sum.in.ua> (дата звернення: 08.09.2020).

28. Конституція України: Закон України від 28.06.96 р. № 254к/96-ВР. Дата оновлення: 01.01.2020. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text> (дата звернення: 08.09.2020).

~~~~~ \* \* \* ~~~~~

---

---