Інформаційна і національна безпека

УДК 340+35.078.3

ДОВГАНЬ О.Д., *доктор юридичних наук, старший науковий співробітник,*
НДІ інформатики і права НАПрН України
ТКАЧУК Т.Ю., *кандидат юридичних наук, доцент,*
ННІ інформаційної безпеки НА СБ України

КОНЦЕПТУАЛЬНІ ЗАСАДИ ЗАКОНОДАВЧОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Анотація. *У статті досліджується концептуальні засади правового забезпечення інформаційної безпеки України. На основі теоретичного аналізу запропоновано модель Закону України "Про інформаційну безпеку України" та проаналізовано основні його змістовні частини.*

Ключові слова: *інформаційна безпека України, забезпечення інформаційної безпеки, національна безпека, система, стан, процес, загроза.*

Summary. *The article deals with the conceptual principles of the legal providing of Ukraine's information security. On the basis of theoretical analysis, the model of the Law of Ukraine "On Information Security of Ukraine" is proposed and its main content parts are analyzed.*

Keywords: *information security, information security ensuring, national security, system, state, process, threat.*

Аннотация. *В статье исследуется концептуальные основы правового обеспечения информационной безопасности Украины. На основе теоретического анализа предложена модель Закона Украины "Об информационной безопасности Украины" и проанализированы основные его содержательные части.*

Ключевые слова: *информационная безопасность, обеспечение информационной безопасности, национальная безопасность, система, состояние, процесс, угроза.*

Постановка проблеми. Не викликає сумніву, що будь-яке законодавство має спиратися на чітку, науково обґрунтовану й об'єктивно зумовлену систему права. Тому систематизація інформаційного законодавства потребує створення стрункої комплексної галузі інформаційного права, формування положень, котрі втіляться в конкретні норми законів та підзаконних нормативно-правових актів. А отже розробка й удосконалення вітчизняного законодавства з безпекових питань інформаційної сфери мають відбуватися на міцному теоретичному фундаменті, науковому обґрунтуванні місця в загальній системі права підгалузі правового забезпечення інформаційної безпеки, а також її взаємодії з іншими правовими галузями та інститутами.

Слід зазначити, що теперішній стан захищеності прав і законних інтересів людини, суспільства й держави в інформаційній сфері України свідчить про недостатній рівень правового регулювання й забезпечення інформаційної безпеки. Так, непоодинокими є випадки порушення чи безпідставного обмеження вказаних прав та інтересів, у нормах, що регулюють інформаційні відносини, у правовому забезпеченні інформаційної безпеки існує чимало суперечностей, лакун і колізій, а деякі відносини у цій сфері

взагалі не врегульовані. Убачається, що все це зумовлене насамперед слабким теоретичним обґрунтуванням підгалузі правового забезпечення інформаційної безпеки та іншими системними прорахунками. Стосовно цієї підгалузі спостерігаємо також розсинхронізацію між системами права й законодавства, усунення якої потребує системного підходу до відповідної законотворчості. Саме такий підхід має стати головним методологічним інструментом забезпечення інформаційної безпеки, оскільки за його допомогою можливе розв'язання проблем співвіднесення цілого й частини, організації та дезорганізації, порядку й безладу.

Ефективності інформаційного законодавства в цілому серйозно шкодить також відсутність у нормативно-правових актах з питань забезпечення інформаційної безпеки єдиних для всіх джерел правового регулювання відповідних засадничих нормативних умов.

Результати аналізу наукових публікацій. В основу написання даної статті покладено аналіз чинного інформаційного законодавства, законопроекти, які стосуються предмету дослідження, а також творчий доробок відомих вчених, зокрема О. Баранова [1], Н. Нижника, Г. Ситника та В. Білоуса [2], В. Брижка [3], Є. Захарова та Р. Тополевського [4], В. Пилипчука [5], П. Сніцаренка, Ю. Сарачива, В. Семененка та В. Ткаченка [6], О. Яреми [7] та ін.

Метою статті є визначення концептуальних засад правового забезпечення інформаційної безпеки України на теперішньому етапі, з урахуванням сучасних загроз та євроатлантичної інтеграції нашої держави, та запропонувати модель проекту Закону України "Про інформаційну безпеку України".

Виклад основного матеріалу. Поряд із юридичними конструкціями, правилами та прийомами викладення законодавчих та інших нормативно-правових актів чи не найважливішим засобом юридичної техніки є відповідна термінологія. Система визначень, що характеризує різні аспекти інформаційної діяльності, стає основою формування відповідних безпекових понять, необхідних для розвитку технологій організації і забезпечення інформаційної безпеки. А між тим, термінологія, що застосовується у сфері забезпечення інформаційної безпеки, демонструє на брак єдності, неоднозначні тлумачення, а то й узагалі відсутні визначення багатьох понять, у тому числі ключових. Усе це створює серйозні перешкоди як для правотворчої діяльності в інформаційній сфері, так і для правозастосовної, а також зайвий раз засвідчує відсутність системності у розв'язанні вказаних проблем.

Наприклад, до теперішнього часу немає законодавчого визначення такого базового терміна як "безпека інформації", хоча таке термінологічне сполучення вживається в деяких законах. У Законі України "Про основи національної безпеки", який був основним орієнтиром забезпечення безпеки України, системна сутність безпеки інформації трактувалася як невід'ємна складова національної безпеки України, не даючи при цьому її точного визначення. Крім того, в цьому Законі замість поняття "інформаційна безпека України" використовувався термін "національна безпека України в інформаційній сфері". Визначення поняття "інформаційна безпека", різні за своєю суттю і в Законах України "Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки" та "Про телекомунікації". У більшості наукових праць з питань інформаційної безпеки здебільшого розглядаються суто технічні питання захисту інформації: захист інформаційно-телекомунікаційних систем, каналів передачі інформації, доступ до інформації, розробка засобів захисту баз даних, захист від витоку інформації тощо.

У Законі України "Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015роки" [8], *"інформаційна безпека" визначається як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.*

Проте, слід враховувати, що даний правовий акт розроблявся і був прийнятий до початку явних проявів гібридної війни, і по-друге, на наше переконання даному підходу притаманний однобічний підхід до забезпечення інформаційної безпеки. З врахуванням міжнародного досвіду ми пропонуємо також включати у зміст даного поняття заходи активної оборони.

Проект Закону про внесення змін до законів України щодо інформаційної безпеки, в якому пропонується доповнити Закон України "Про національну безпеку України" визначенням "інформаційна безпека" [9], значною мірою повторює зазначене вище поняття "інформаційна безпека", проте дещо розширює спектр негативного впливу, зокрема вже згадується інформаційно-психологічний вплив. Проте, як і в попередньому, воно займає більш оборонний характер, дещо нівелюючи активні заходи забезпечення інформаційної безпеки України.

Ми визначаємо 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 забезпечення інформаційної безпеки держави, на нашу думку, це *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.*

В основу даного підходу покладено принцип, відповідно до якого основною метою забезпечення інформаційної безпеки є створення безпечного інформаційного середовища. А для цього захищати національні інтереси й цінності, виходячи з виявлення загроз і намірів противника, замало. Даний підхід передбачає також протидію та активні контрзаходи у процесі забезпечення інформаційної безпеки держави.

Контекстний аналіз вживання законодавця поняття "безпека інформації" дає підстави тлумачити його як стан захищеності інформації в системі. Відповідно, "захист інформації" – це діяльність із забезпечення вказаного стану захищеності. Захист інформації як складова діяльності із забезпечення безпеки інформації та інформаційної безпеки є одним із засобів захисту прав і законних інтересів людини, суспільства, держави в інформаційній сфері.

Найбільш точно, на нашу думку, цей процес можна відобразити в категоріях "захист" і "охорона", які разом охоплюють діяльність із забезпечення інформаційної безпеки. 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.

Важливою складовою інформаційної безпеки вбачається комплексний захист зазначених прав і законних інтересів від непередбачуваного й шкідливого впливу

певного інформаційного техніко-технологічного середовища, створеного самим соціумом, тобто від побічних чинників впливу технологічних та організаційних процесів на особу (людину і громадянина), суспільство, державу. При цьому система інформаційної безпеки покликана нейтралізувати вказані негативні впливи на людину та сприяти підтриманню стабільності суспільства й держави, інститути котрої, у свою чергу, повинні цю нейтралізацію забезпечити. Іншими словами, головною ознакою стану захищеності в інформаційній сфері (інформаційної безпеки) є оптимальне співвідношення інтересів людини, суспільства й держави.

Чинниками забезпечення інформаційної безпеки держави є гарантування:

1) безпеки інформації загального доступу, мереж зв'язку, інформаційно-телекомунікаційних систем, технічних та програмних засобів виконання маніпуляцій з інформацією, доступу до інформації;

2) конфіденційності інформації з обмеженим доступом;

3) захищеності особи, суспільства й держави від шкідливого впливу певних видів інформації (в даному разі йдеться не про інформацію, віднесену до категорій з обмеженим доступом, а про такі її види, котрі здатні зашкодити вказаним суб'єктам інформаційних відносин).

На сьогодні зазначені відносини, пов'язані із забезпеченням інформаційної безпеки, далеко не повно законодавчо врегульовані. Можна констатувати лиш загальну регламентацію діяльності щодо захисту інформації. Саме тлумачення змісту поняття "захист інформації" вважаємо не зовсім коректним, позаяк однією із цілей цієї діяльності називається фактично самозабезпечення – захист інформації спрямований на забезпечення захисту інформації, що утруднює не тільки розуміння змісту діяльності, а й оцінювання її результатів. Тому метою цієї діяльності, на наш погляд, слід визнати досягнення стану безпеки інформації як складової інформаційної безпеки.

Описане вище становище спричинене відсутністю сформульованих в одному законі концептуальних аспектів забезпечення інформаційної безпеки держави. При цьому зазначимо, що для розробки такого закону належить виокремити джерела права, котрі містять норми, які відповідають даному інституту, на основі створеної в системі права підгалузі правового захисту інформаційної безпеки. Ці норми, сьогодні розпорошені по багатьох галузевих законах і до того ж нерідко суперечать одна одній.

В умовах, у яких нині опинилася Україна через гібридну агресію Російської Федерації, особливої актуальності набуває протидія поширенню шкідливої для психіки людини інформації, яку без перебільшення можна вважати інформаційною зброєю, а також розвиток відповідного законодавства. У цьому контексті інформаційно-психологічну безпеку можна визначити як стан захищеності від окремих осіб та/або певних груп, а також відповідних життєво важливих інтересів людини, суспільства й держави в інформаційній сфері.

Під негативним інформаційно-психологічним впливом ми розуміємо такий вплив на особу чи групу осіб, який здійснюється на їх психіку, зокрема й усупереч їхній волі, із застосуванням спеціальних засобів і методів, що призводить до шкідливих для людини, суспільства та держави наслідків.

Усю глибину загрози подібних постійних, цілеспрямованих, продуманих і щедро фінансованих впливів з боку РФ Україна повною мірою відчула під час анексії Криму та воєнних дій на сході. Убачається, що всі питання, пов'язані із зазначеними впливами, слід передбачити в межах спеціального закону стосовно забезпечення інформаційної безпеки.

Інша проблема, яка потребує законодавчого визначення та врегулювання, – відсутність систематизації законодавства з питань протидії екстремізму в інформаційній сфері. Внаслідок цього матеріали подібного змісту часто розповсюджуються практично безперешкодно, позаяк діяльність із запобігання й припинення різних видів екстремізму здійснюється компетентними державними органами безсистемно й нерідко формально.

При цьому важливо пам'ятати, що реальна протидія екстремістським чи іншим негативним проявам в інформаційній сфері не повинна перетворюватися на зведення особистих рахунків з "незручними" журналістами, тиск на опозиційні засоби масової інформації та придушення свободи слова.

Таким чином, вважаємо за доцільне з метою чіткого системного врегулювання питань протидії інформаційному екстремізму, що забезпечило б захист законних інтересів людини від негативних інформаційних впливів, суспільної моралі та держави, а також задля усунення колізій і прогалин законодавства регламентувати зазначену діяльність окремим законом з питань забезпечення інформаційної безпеки.

З цього приводу, наприклад, О. Ярема зазначає, що для інституційного розвитку правового забезпечення інформаційної безпеки необхідно прийняти Закон України "Про інформаційну безпеку" [7, с. 250].

Єдності щодо шляхів якісної трансформації інформаційного законодавства України дослідники цієї проблематики допоки не досягли, що не дивно з огляду на складність, динаміку та масштабність сучасних інформаційних процесів, які відбуваються в умовах становлення національної правової системи [7, с. 252].

Одна з основних причин невідповідності інформаційного законодавства України вимогам сучасності є те, як слушно зазначається у [2, с. 89] – те, що у суспільній і науковій думці не сформувалося цілісне уявлення про інформаційну безпеку з позиції права та юридичної науки.

Життєдіяльність інформаційного суспільства потребує чіткого законодавчого врегулювання багатоманітних відносин, що виникають у зв'язку зі створенням, функціонуванням, використанням інформаційних систем і ресурсів, каналів комунікацій, відповідних технологій тощо. Досліджене у попередніх працях формування в системі інформаційного права такої підгалузі, як правове забезпечення інформаційної безпеки, зумовлює потребу виокремлення законодавчих актів, положень, норм, котрі регламентують різні аспекти забезпечення інформаційної безпеки, їхнього аналізу на предмет наявності системних вад, а також систематизації, консолідації на цій основі загальних правових норм у єдиний базовий закон, позбавлений існуючих у теперішній час суперечностей, колізій та прогалин. Це, у свою чергу, має створити передумови для якісної комплексної трансформації законодавства, яке регулює інформаційні відносини в різних сферах життєдіяльності суспільства. Ідеться передусім про прийняття Закону України "Про інформаційну безпеку України".

Зауважимо, що ідея розробки такого закону не є новою, а найбільш результативні спроби її реалізації припадали на 2004 та 2014 роки.

Так, у 2004 році був розроблений проект Закону України "Про інформаційну безпеку України" (від 22 вересня 2004 року № 5732). Фактично зазначений законопроект становив лише словник визначень, що стосуються інформаційної безпеки (ст. 2); перераховував її об'єкти (ст. 3) та суб'єкти (ст. 4); зазначав підстави гарантування державою цілісності інформаційного простору (ст. 5); наводив перелік загроз інформаційному простору й інформаційній безпеці (не розрізняючи їх та не передбачаючи можливості виникнення нових загроз) (ст. 6); загальними фразами окреслював шляхи забезпечення інформаційної безпеки України (ст. 7); визначав

основні напрями державної політики в інформаційній сфері (ст. 9). Відтак, за оцінками експертів, "законопроект справляє враження навчального посібника, присвяченого чи то теорії інформаційної безпеки, чи то інформаційному простору" [4].

Приміром, у ст. 10 "Система забезпечення інформаційної політики та інформаційної безпеки України" систематизовано й наведено повноваження Президента України, Верховної Ради України, Ради національної безпеки і оборони України, Кабінету Міністрів України, міністерств, Служби безпеки України, інших центральних органів виконавчої влади, місцевих державних адміністрацій, органів місцевого самоврядування, правоохоронних органів, судів загальної юрисдикції, Генеральної прокуратури України; окремі права громадян в інформаційній сфері. Вочевидь, закріплення таких норм, які відтворюють уже закріплені законодавчо положення лишень з наголосом на повноваження зазначених суб'єктів в інформаційній сфері, не тільки не врегульовує відповідні суспільні відносини, але й створює можливість обмеження діяльності у сфері інформаційної безпеки виключно наведеними повноваженнями. При цьому значна частина статей законопроекту має бланкетний характер і відсилає до норм чинного законодавства, що аж ніяк не сприяє визначеності правового регулювання.

Фактично законопроект був спрямований на фіксацію рамкових засад інформаційної безпеки і мав переважно декларативний характер. Відсутність конкретизації й орієнтація на загальні положення прийнятна, скажімо, для Концепції забезпечення інформаційної безпеки, але аж ніяк не для закону. Складність і багатоманітність інформаційних відносин зумовлюють необхідність систематизації нормативно-правових актів стосовно інформаційної сфери у вигляді, наприклад, Інформаційного кодексу (статті, присвячені правовому регулюванню інформаційної безпеки, могли би скласти окремий розділ чи книгу цього кодексу) або Закону України "Про інформацію", викладеного в новій редакції.

З огляду на зазначені вище та інші істотні вади проект закону "Про інформаційну безпеку України" було знято з розгляду.

Така ж сама доля спіткала і його більш сучасного "наступника" – проект закону "Про засади інформаційної безпеки України" (реєстр. № 4949 від 28 травня 2014 року) [10]. У цьому законопроекті пропонувалося визначити основні засади державної політики, спрямованої на захист життєво важливих інтересів людини і громадянина, суспільства і держави в інформаційній сфері, порядок забезпечення інформаційної безпеки в умовах формування і розвитку інформаційного суспільства в Україні та глобального інформаційного простору, а також закріпити правові основи інформаційної безпеки України.

Фахівці Головного науково-експертного управління Апарату Верховної Ради України в узагальнюючому висновку від 19 червня 2014 року, погоджуючись з необхідністю врегулювання порушених у законопроекті питань, зауважили, що чимало його положень потребують доопрацювання й уточнення для їх узгодження з іншими законодавчими актами з питань інформаційної безпеки і боротьби з комп'ютерною злочинністю та наповнення конкретним нормативним змістом.

Так, у законопроекті застосовувалася нова для вітчизняного законодавства термінологія. Це, зокрема, поняття "інформаційна безпека", "інформаційна сфера", "кібернетична безпека (кібербезпека)", "кібернетичний простір (кіберпростір)" та низка інших тематичних термінів. Однак при цьому лишилося незрозумілим, чому "інформаційна безпека" тлумачиться як "стан захищеності…", а "кібернетична безпека" – як "здатність людини…". Адже визначення цих споріднених термінів, котрі, очевидно,

співвідносяться між собою як загальне та спеціальне, має ґрунтуватися на одних і тих же вихідних поняттях.

Хоча поняття "кіберзлочинність" і пов'язана з ним термінологія, використовується досить широко, офіційного, закріпленого в міжнародних документах та національному законодавстві його визначення досі не існує. Навіть Конвенція про кіберзлочинність 2001 року і Додаткові протоколи до неї [11] оперують поняттями "комп'ютерна система", "комп'ютерні дані" та передбачають встановлення відповідальності за "правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; за навмисне перехоплення технічними засобами, без права на це передач комп'ютерних даних; за навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це; навмисне серйозне перешкоджання функціонуванню комп'ютерної системи" тощо. Тож запропоновані в законопроекті терміни, зокрема "кіберзлочинність" і "кібертероризм", не узгоджувалися з термінологією, що вже використовується в чинному законодавстві.

Зміст терміна "кібертероризм", крім того, охоплюється поняттям "технологічний тероризм", під яким, зокрема, розуміються "злочини, що вчиняються з терористичною метою із застосуванням… засобів електромагнітної дії, комп'ютерних систем та комунікаційних мереж, включаючи захоплення, виведення з ладу і руйнування потенційно небезпечних об'єктів, які прямо чи опосередковано створили або загрожують виникненням загрози надзвичайної ситуації внаслідок цих дій та становлять небезпеку для персоналу, населення та довкілля; створюють умови для аварій і катастроф техногенного характеру" (ст. 1 Закону України "Про боротьбу з тероризмом" [12]).

Деякі поняття, такі як "об'єкти критичної інформаційної інфраструктури держави", "кібервійська", "кіберпідрозділи" (ст. 5 законопроекту), взагалі не отримали визначень, хоча їхній зміст не є загальнозрозумілим.

До наведених у ст. 3 законопроекту принципів забезпечення інформаційної безпеки, які зведені здебільшого до конституційних гарантій права на інформацію, слід було би додати обов'язкове вжиття заходів щодо інформування про небезпеку та захисту журналістів, які працюють у місцях збройних конфліктів та вчинення терористичних актів, а також при ліквідації небезпечних злочинних груп.

Не можемо погодитися і з тим, що лише створення іншими державами кібервійськ чи кіберпідрозділів є підставою для віднесення цих подій до переліку загроз інформаційній безпеці України. Адже нести загрозу чи завдати державі величезної шкоди може навіть одна людина, котра володіє відповідними знаннями й технічними можливостями.

Зміст ст. 6 проекту, що визначає пріоритети державної політики у сфері інформаційної безпеки, мав би узгоджуватися зі ст. 4, де йдеться про життєво важливі інтереси в інформаційній сфері. На наш погляд, вказані поняття споріднені, а тому автори законопроекту оперують у цих статтях ідентичними положеннями. Зокрема, в обох випадках наголошується на необхідності забезпечення конституційних прав і свобод людини і громадянина в інформаційній сфері; забезпеченні (захисту) інформаційного суверенітету; недопущенні несанкціонованого втручання (забезпечення захисту) у зміст, процеси обробки, передачі та використання персональних даних; розвитку інформаційного суспільства в Україні; збереженні та примноженні духовних, культурних і моральних (національних) цінностей українського народу.

Ст. 7, яка визначає основні напрями діяльності держави у сфері забезпечення інформаційної безпеки, також перевантажена приписами декларативного змісту. Так, в ній відтворюються деякі положення попередніх статей проекту (4 і 6), зокрема, вже

втретє вказується на необхідності "забезпечення неухильного додержання конституційних прав і свобод людини в інформаційній сфері", "формування вітчизняної індустрії високотехнологічної інформаційної продукції (послуг)", "демократичного контролю за діяльністю суб'єктів забезпечення інформаційної безпеки" тощо. Крім того, дев'ять абзаців цієї статті починаються зі слів "удосконалення", "посилення", "поліпшення", "розширення", що свідчить про ненормативний характер відповідних положень, у результаті чого законопроект фактично перетворюється на своєрідну концепцію інформаційної безпеки України. Адже приписів про те, яким чином буде здійснюватися відповідне "удосконалення", "посилення" чи "розширення", документ не містить.

У ст. 8, де називаються об'єкти інформаційної безпеки, вкотре наголошується на необхідності забезпечення "конституційних прав і свобод людини і громадянина, на захищеності від негативного впливу інформаційних технологій та інформаційно-психологічного впливу" (статті 4, 6, 7). Уважаємо, що кількаразове відтворення одного й того ж положення, навіть дуже важливого, в одному законопроекті є очевидною техніко-юридичною помилкою.

Чимало питань виникає і щодо статусу запропонованого до створення аналізованим документом центрального органу виконавчої влади зі спеціальним статусом у сфері інформаційної безпеки – Національної комісії, що здійснює державне регулювання з питань інформаційної безпеки (далі – Нацкомісія інформбезпеки) (ст. 10). Це не повною мірою узгоджується з чинним законодавством, котре визначає порядок створення та формування персонального складу центральних органів виконавчої влади зі спеціальним статусом.

Таким чином, ретроспективний огляд спроб реалізації ідеї щодо розробки єдиного установчого нормативно-правового акту – закону з питань інформаційної безпеки дозволяє дійти висновку, що сьогодні такий закон має чітко визначати сферу правового регулювання, засадничі принципи забезпечення інформаційної безпеки, основні загрози правам та інтересам людини, суспільства й держави, котрі цим законом охороняються, зміст і пріоритетні напрями державної політики у цій сфері та засоби її реалізації, перелік та компетенцію органів державної влади, що забезпечують різні складові інформаційної безпеки. Законом мають також передбачатися правові основи цих складових – захисту державної та іншої таємниці, інформації з різними правовими режимами, персональних даних, а також відповідальності за правопорушення в цій сфері. Нарешті, закон має уніфікувати й удосконалити понятійний апарат і термінологію регульованої сфери, оскільки в теперішній час із цим спостерігаються чималі проблеми.

Ми погоджуємося із фахівцями, що причиною непевного стану щодо забезпечення інформаційної безпеки України стало те, що до сьогодні, незважаючи на конституційну норму, ще не прийнято рамкового закону, яким би стверджувалися основні поняття і положення щодо інформаційної безпеки держави. Це загалом гальмує об'єднавчі процеси та забезпечення їх адекватності як в теоретичному руслі, так і в напрямах практики [6].

Теоретичне обґрунтування вказаного закону має спиратися на сформовану у структурі вітчизняної системи права самостійну підгалузь – правове забезпечення інформаційної безпеки, а також відповідну законодавчу підгалузь, положення якої нині містяться в багатьох законодавчих актах різних галузей. Тому головним завданням законодавця вбачається, як уже зазначалося, саме систематизація й усунення наявних недоліків цих норм і положень з урахуванням комплексної природи вказаної підгалузі права та її взаємодії з іншими правовими галузями і структурними утвореннями. Тобто,

належить виявляти правові джерела не лише забезпечення інформаційної безпеки, а й законодавчих актів, котрі взаємодіють з цією підгалуззю, з метою формування стрункої, позбавленої внутрішніх суперечностей системи відповідного законодавства.

Спробуємо змоделювати структурно-змістову схему пропонованого закону.

Розділ 1. Має розкривати найзагальніші питання, зокрема: мета та сфера дії цього закону; основні поняття (терміни), що в ньому вживаються; принципи забезпечення інформаційної безпеки, його суб'єкти та об'єкти; перелік актів законодавства, котрі цю сферу регулюють; загальна структура законодавства про інформаційну безпеку.

Зрозуміло, що положення цієї глави (як і закону загалом) мають відповідати Конституції України, Доктрині інформаційної безпеки України, а також міжнародно-правовим нормам і принципам.

Мета закону – правове регулювання діяльності із забезпечення інформаційної безпеки держави, тобто стану захищеності й балансу інтересів суб'єктів інформаційної сфери – людини, суспільства, держави.

Понятійний, термінологічний апарат цього системоутворювального закону має бути систематизованим й уніфікованим, містити коректно сформульовані визначення. Убачається за потрібне поряд з іншими визначити такі поняття, як: "інформаційна безпека держави", "захист інформації", "безпека інформації", "інформаційно-психологічна безпека", "стандарти інформаційної безпеки", "шкідливий (негативний) інформаційний вплив", "методи й засоби шкідливого інформаційного впливу" та інші. Чинником успішного виконання цього непростого наукового завдання є "проходження у професійній рефлексії юридичного явища від простого знакового заміщення до власне поняття як знаннєвої конструкції. Цей процес на початковому етапі збігається з юридичною діяльністю, юридичною практикою й відокремлюється від неї в результаті професійної рефлексії, дослідження права". Тому ретельний семантико-змістовий аналіз кожного терміна чи термінологічного сполучення, що включаються до понятійного апарату, специфіки їх уведення в науковий обіг та практики вживання в чинному законодавстві є обов'язковою умовою при розробці закону.

Об'єкт правового регулювання закону – відносини, які складаються у зв'язку з виникненням загроз і викликів правам і законним інтересам суб'єктів цих відносин в інформаційній сфері. Зокрема, це стосується й інформаційного впливу на психіку людини, людську й суспільну свідомість.

Суб'єкти правового регулювання закону – людина, суспільство, держава; органи державного управління, до компетенції яких входить забезпечення інформаційної безпеки; особа, права та/чи законні інтереси котрої в інформаційній сфері були в будь-який неправомірний спосіб порушені.

Щодо загальної структури законодавства, котре регулює сферу інформаційної безпеки, закріплення якої в даному законі вбачається вельми важливим. Системоутворювальним, базовим законодавчим актом має бути власне сам закон про інформаційну безпеку. Позаяк решта законів не повинні суперечити базовому, його прийняття означатиме потребу ретельного вивчення чинного законодавства й приведення його у відповідність.

Уважаємо, що засадничими положеннями побудови вказаного закону, як і діяльності із забезпечення інформаційної безпеки, мають стати такі принципи:

*пріоритет прав і свобод людини і громадянина (*цей закріплений у міжнародному праві принцип, що віддзеркалює сутність та межі діяльності із забезпечення інформаційної безпеки, є основоположним; у Доктрині інформаційної безпеки України

дотримання прав і свобод людини в інформаційній сфері віднесене до першорядних національних інтересів нашої країни);

збалансованість інтересів особи, суспільства та держави (цей принцип також передбачений Доктриною інформаційної безпеки України й випливає із першого, позаяк законність інтересів кожної людини простягається до меж прав і свобод інших людей, а також інтересів суспільства й держави, якраз і зумовлених потребою захисту від посягань на ці права і свободи. Адже саме цим урешті-решт спричинені обмеження, пов'язані, приміром, з охороною державної таємниці, захистом персональних даних тощо);

відповідність безпекових заходів ступеню загроз (також випливає із попереднього принципу. Для запобігання загрозам в інформаційній сфері та їх усунення належить застосовувати заходи, адекватні їх реальному рівню, з мінімально необхідним обмеженням прав і свобод громадян);

*монополія держави на розробку й виготовлення спеціальних засобів інформаційного, в тому числі інформаційно-психологічного, впливу (*в умовах агресії РФ це означає заборону в Україні певної шкідливої інформації, певних антигуманних інформаційно-психологічних технологій, які цілком слушно багатьма правниками називаються інформаційною зброєю);

прозорість, гласність і контроль громадянського суспільства у сфері забезпечення інформаційної безпеки (тобто, відповідно до Закону України "Про доступ до публічної інформації" будь-які відомості про діяльність органів державного управління, місцевого самоврядування щодо забезпечення інформаційної безпеки мають бути відкритими й доступними для ознайомлення громадян, якщо тільки вони не становлять державну чи іншу передбачену законом таємницю);

обов'язковість залучення до діяльності із забезпечення інформаційної безпеки громадських організацій (реалізація цього принципу, котрий випливає із попереднього та принципу збалансованості інтересів людини, суспільства й держави, дає змогу шляхом громадської оцінки законопроектів, пов'язаних з інформаційною сферою, значно повніше враховувати інтереси різних верств населення, підвищити якість відповідного законодавства).

Загрози інформаційній безпеці. Їх перелік наведено в Доктрині інформаційної безпеки України, й він цілком, на наш погляд, відповідає реаліям сьогодення. Якщо визначати їх у цілому, то це – сукупність чинників, котрі можуть призвести до порушення прав і свобод громадян, а також законних інтересів людини, суспільства й держави в інформаційній сфері.

Розділ 2. Загальні засади функціонування державної системи забезпечення інформаційної безпеки. Тут слід визначити пріоритетні завдання у цій сфері, головним із яких убачається створення й удосконалення відповідного законодавства. На його основі має бути сформована вказана система задля неухильного втілення уповноваженими державними органами законодавчих вимог у цій сфері. Функції координації цієї діяльності доцільно покласти на Службу безпеки України.

Окрім виконання охоронних завдань, діяльність державних органів у цій сфері має бути спрямована на збереження й розширення єдиного інформаційного, духовного, мовного простору України, традицій українського народу й суспільної моралі, розвиток правової свідомості й культури населення стосовно інформаційної безпеки, просвіту громадян з питань безпечного користування інформаційними технологіями, захисту від шкідливих інформаційних впливів тощо.

Основні функції державних органів у досліджуваній сфері випливають із наведених вище завдань. Це насамперед: захист інформаційних систем і ресурсів держави, таємних відомостей та іншої інформації з обмеженим доступом; виявлення фактів шкідливих інформаційних впливів та суб'єктів, що їх здійснюють, нейтралізація та припинення їх протиправної діяльності; розробка нових і вдосконалення існуючих методів і засобів запобігання та протидії загрозам інформаційній безпеці людини, суспільства, держави; організація чіткого функціонування дозвільної, експертної та контрольної систем у вказаній сфері; стандартизація галузі; технічна, правова та інша підготовка висококваліфікованих фахівців з питань забезпечення інформаційної безпеки; розвиток продуктивного міжнародного співробітництва з питань інформаційної безпеки, приведення вітчизняного законодавства у відповідність до міжнародно-правових актів у цій сфері тощо.

Задля реалізації державної політики у сфері забезпечення інформаційної безпеки відповідно до наведених вище принципів, завдань і функцій має бути створена ефективна державна система. Крім уповноважених державних органів, її мають складати науково-дослідницькі, науково-технічні установи, проектні, конструкторські та інші організації, котрі провадять наукові дослідження й розробляють технічні засоби, а також освітні заклади, які займаються підготовкою, перепідготовкою та підвищенням кваліфікації відповідних кадрів. Узгоджені дії вказаних суб'єктів забезпечуються шляхом ліцензійної, сертифікаційної, експертної та контрольної діяльності уповноважених на це органів у сфері забезпечення інформаційної безпеки, формування державних замовлень на відповідні наукові дослідження, освітні та інші послуги тощо.

Комплекс засобів, що їх застосовує державна система інформаційної безпеки, має гарантувати належний її рівень, у тому числі убезпечити суспільство від шкідливих інформаційно-психологічних впливів. Не останню роль у цьому має відіграти згадуване вище ліцензування, основні аспекти якого, зокрема умови отримання ліцензії, слід, на нашу думку, передбачити в базовому законі. Так, необхідною умовою отримання ліцензії вбачається сертифікація методів і засобів, які застосовуються під час проведення діяльності, пов'язаної з інформаційною безпекою.

Що стосується шкідливих інформаційних впливів, то достеменно виявити їх можна лише шляхом спеціальної експертизи. Остання проводиться для виявлення загроз інформаційній безпеці за державними стандартами й за дорученням відповідно уповноважених державних органів.

Допускається також заявний порядок проведення таких експертиз, тому варто, на нашу думку, закріпити окремий механізм розгляду вказаних запитів громадян. Зокрема, проведення подібної державної експертизи доцільно включити до необхідних заходів надання реабілітаційної допомоги людині, котра зазнала шкідливого інформаційно-психологічного впливу.

Необхідним елементом державної системи забезпечення інформаційної безпеки має також бути ефективний контроль за її достатністю та ефективністю, а також за дотриманням законності в усіх аспектах її функціонування.

***Розділ* 3.** Загальні питання забезпечення безпеки інформації з обмеженим доступом: підстави та принципи віднесення відомостей до категорії інформації з обмеженим доступом (таємна, службова інформація, конфіденційна,), види інформації з обмеженим доступом (державна, для службового користування, персональні дані, комерційна та ін. види інформації за змістом); загальні засади захисту інформації з обмеженим доступом.

Розділ 4. Загальні питання захисту відкритої (загальнодоступної) інформації від протиправних маніпуляцій з нею (викривлення, приховування, блокування тощо), зокрема: засади та вимоги до захисту інформації в загальнодоступних державних мережах; інформаційно-правові аспекти (на відміну від цивільно-правових) захисту об'єктів інтелектуальної власності (державна реєстрація, акредитація тощо) та ін.

Розділ 5. Загальні засади захисту від недостовірної та шкідливої інформації, негативного інформаційно-психологічного впливу. Тут варто, на наш погляд, зазначити загрози суб'єктам інформаційних відносин, спричинені застосуванням спеціальних методів і засобів інформаційно-психологічного впливу, зокрема: маніпулювання особистісною та суспільною свідомістю, навіювання хибних думок і провокування неправильних дій, завдання шкоди здоров'ю та життю людини тощо.

Виходячи із принципу монополії держави на застосування методів і засобів інформаційно-психологічного впливу, треба передбачити вичерпний перелік підстав, коли воно може бути правомірним, а саме:

1) без відома об'єктів інформаційно-психологічного впливу (у надзвичайних ситуаціях (*стихійні лиха, катастрофи техногенного чи іншого характеру тощо*) – для рятування людей, ліквідації наслідків та ін.; під час воєнних дій проти зовнішнього агресора, проведення антитерористичних, миротворчих операцій);

2) за згодою об'єктів інформаційно-психологічного впливу (з науковою метою *(психічні, психологічні дослідження тощо)*; під час підготовки фахівців (*які застосовують методи і засоби психологічного впливу; чия діяльність пов'язана з екстремальними та надзвичайними ситуаціями; які займаються антитерористичною діяльністю; з інформаційної безпеки)*).

Крім того, вбачається доцільним врегулювати питання захисту громадян, суспільства й держави від розповсюдження недостовірної інформації на шкоду їхнім законним інтересам (*наприклад, матеріали вітчизняних та зарубіжних засобів масової інформації, спрямовані на дискредитацію окремих осіб, підрив суспільної злагоди, дестабілізацію ситуації у країні і т.п.*). Слід передбачити право постраждалого суб'єкта на компенсацію завданої шкоди (*моральної та/чи матеріальної*) та публічне спростування недостовірних відомостей, а також порядок його реалізації.

Розділ 6. Загальні питання протидії інформаційному екстремізму. Необхідно визначити вичерпний перелік чітких критеріїв, за якими інформація визнається екстремістською (що загрожує конституційному ладу України), зокрема, умисел суб'єкта її розповсюдження, конкретні умови оприлюднення тощо. Підкреслимо важливість чіткого формулювання вказаних критеріїв, аби уникнути багатозначності їх тлумачення, що може призвести до фактичного запровадження цензури. Належність інформації до екстремістської має встановлюватися спеціальною експертизою, питання щодо організації та проведення якої теж мають бути врегульовані цим законом.

Розділ 7. Види відповідальності за правопорушення, пов'язані зі сферою інформаційної безпеки. Слід передбачити випадки застосування кожного з видів відповідальності – дисциплінарної, цивільно-правової, адміністративної, кримінальної.

Джерела та порядок фінансування діяльності із забезпечення інформаційної безпеки. Додамо, що обсяги бюджетного фінансування залежатимуть, зокрема, від того, чи буде створений спеціальний управлінський орган для керування державною системою забезпечення інформаційної безпеки або ж ці функції розподілятимуться між існуючими владними інститутами.

Висновки.

Підсумовуючи міркування стосовно запропонованої моделі закону, зазначимо, що прийняття базового Закону України "Про інформаційну безпеку України" вбачається необхідним задля консолідації, вдосконалення відповідного законодавства, чіткої структуризації системи нормативно-правових актів у цій галузі, усунення наявних суперечностей, лакун та інших вад.

Цей закон має, на наш погляд, закріпити найзагальніші положення, які поширюватимуться на решту нормативно-правових актів у цій галузі, а саме: принципи правового забезпечення, структуру відповідного законодавства, єдині параметри правового забезпечення інформаційної безпеки, єдину термінологію.

Крім того, вказаний закон, синтезувавши норми підгалузі правового забезпечення інформаційної безпеки, може стати одним із базових при кодифікації вітчизняного законодавства у сфері інформації та створенні Інформаційного кодексу України.

Зрозуміло, що подальша розробка вказаного закону потребує клопіткого теоретичного осягнення, вивчення великих масивів різногалузевих матеріалів, залучення до цієї роботи провідних правників, наукових установ, досвідчених практиків. На заключних етапах для створення якісного нормативно-правового акта законодавець має продемонструвати справжнє юридичне мистецтво, "завданням якого є відшліфування правового матеріалу" [13, с. 34]. Тому проведене вище дослідження правової природи феномену правового забезпечення інформаційної безпеки, місця у вітчизняній системі права цього утворення (підгалузі), норми котрого мають скласти основний зміст майбутнього закону про інформаційну безпеку, вбачається вельми актуальним і корисним.

У свою чергу, такий закон має стати основою для інших нормативних актів у сфері забезпечення інформаційної безпеки, а також керівних документів державної політики в інформаційній сфері та процесу стратегічного планування забезпечення інформаційної безпеки України.

Використана література

1. Баранов О.А. Базовий принцип інформаційного права – забезпечення інформаційної безпеки. *Запобігання новим викликам та загрозам інформаційній безпеці України: правові аспекти:* матеріали наук.-практ. конф. м. Київ, 6 жовт. 2016 р. / упоряд. В.М. Фурашев. Київ: Вид-во "Політехніка". 2016. С. 29-35.

2. Нижник Н.Р., Ситник Г.П., Білоус В.Т. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): навчальний посібник. Ірпінь : Акад. ДПС України, 2000. 304 с.

3. Брижко В.М. Основи систематизації інформаційного законодавства: теоретичні та правові засади: монографія. Київ: ТОВ "Пан-Тот", 2012. 304 с.

4. Тополевський Р., Захаров Є. Коментарі до проекту Закону України "Про інформаційну безпеку України" від 22.09.04 р. № 5732. URL: http://khpg.org/index.php?id=1105737155 (дата звернення: 05.03.2019).

5. Пилипчук В.Г. Актуальні питання захисту прав, свобод і безпеки людини в сучасному інформаційному суспільстві. *Проблеми захисту прав людини в інформаційному суспільстві*: збірник матеріалів наук.-практ. конф. / упорядн. Фурашев В.М., Петряев С.Ю. (НДІІП НАПрН України, НІСД, Секретаріат Уповноваженого Верховної Ради України з прав людини, НТУУ "КПІ"). Київ: Вид-во "Політехніка". 2016. С. 6-8.

6. Сніцаренко П.М., Саричев Ю.О., Семененко В.М., Ткаченко В.А. Удосконалення чинного інформаційного законодавства України як необхідна умова адекватності заходів щодо забезпечення інформаційної безпеки держави. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. 2018. № 2(63). С. 68-74.

7. Ярема О.Г. Предмет правового забезпечення інформаційної безпеки в інформаційному праві. *Науковий вісник Львівського державного університету внутрішніх справ. Серія Право.* 2016. № 2. С. 244-252.

8. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки: Закон України від 09.01.07 р. URL: http://zakon5.rada.gov.ua/laws/show/537-16 (дата звернення: 05.03.2019).

9. Про внесення змін до законів України щодо інформаційної безпеки: проект Закону України від 26.11.18 р. № 9340. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65011 (дата звернення: 05.03.2019).

10. Про засади інформаційної безпеки України: проект Закону України від 28.05.14 р., реєстр. № 4949. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=51123 (дата звернення: 05.03.2019).

11. Конвенція про кіберзлочинність. URL: http://zakon0.rada.gov.ua /laws/show/994_575 (дата звернення: 05.03.2019).

12. Про боротьбу з тероризмом: Закон України від 20.03.03 р. URL: http://zakon5.rada.gov.ua/laws/show/638-15 (дата звернення: 05.03.2019).

13. Рудольф фон Иеринг. Юридическая техника / сост. А.В. Поляков. Москва: Статут, 2008. 231 с.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~