УДК 342.951+34.096

ПРАВОВА ХАРАКТЕРИСТИКА ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ: ЗАГАЛЬНО-МЕТОДОЛОГІЧНИЙ АСПЕКТ

LEGAL DESCRIPTION OF INFORMATION SECURITY THREATS: GENERAL AND METHODOLOGICAL ASPECTS

Курбатова М.В.,
студентка
Київський національний університет імені Тараса Шевченка

Наукова стаття присвячена дослідженню правової природи загроз інформаційній безпеці. Розглядаються основні підходи до визначення поняття «загрози інформаційній безпеці». У межах статті також досліджується класифікація загроз інформаційній безпеці. Проаналізовано зарубіжний досвід протидії інформаційним загрозам та розроблено пропозиції до національного законодавства в частині вдосконалення забезпечення інформаційної безпеки.

Ключові слова: інформаційна безпека, загрози інформаційної безпеки, адміністративно-правове забезпечення, кібербезпека.

Научная статья посвящена исследованию правовой природы угроз информационной безопасности. Рассматриваются основные подходы к определению понятия «угрозы информационной безопасности». В рамках статьи также исследуется классификация угроз информационной безопасности. Проанализирован зарубежный опыт противодействия информационным угрозам и разработаны предложения в национальное законодательство в части совершенствования обеспечения информационной безопасности.

Ключевые слова: информационная безопасность, угрозы информационной безопасности, административно-правовое обеспечение, кибербезопасность.

The article addresses the issues of information security. The author presents different approaches to the concept of «information security threats». The article gives the description of the legal nature of information security threats and its importance for the national legal system.

Special attention is given to the classification of information security threats and its important role in this research. Also the article shows the concepts, which are enshrined in Ukrainian law, such as 'information security', 'threats to nation security', 'national interest'.

The author analyses international experience in countering information security threats. This issue has been brought to the discussion at the international level since 1995 because the increasing threats to information, pay great attention to the protection of critical infrastructure. In May 2000, in Paris, the conference of G8 dialogue between public authorities and the private sector on security and trust in the information world.

What is more, the article considers different Cyber Security Strategies of foreign countries, such as The USA and UK. The author focuses on international experience that will help public authorities to build an effective system to counter threats. One of the first steps to building an effective system is the adoption of cyber security strategy in Ukraine.

It is concluded that the Ukrainian law needs to be changed in terms of information security and introduce a number of regulatory and legal acts that can serve as the normative foundation for information security.

Key words: information security, information security threats, administrative and legal provision, cyber security.

Стрімкий розвиток інформаційних технологій і їх упровадження у повсякденне життя призвели до виникнення низки нових викликів світовому та національному інформаційному простору. Зважаючи на це, доцільним є підвищення рівня забезпечення інформаційної безпеки України саме у правовому аспекті, оскільки відповідно до Статті 17 Конституції України забезпечення інформаційної безпеки є однією з найважливіших функцій держави [1]. Таким чином, розвиток інформаційного суспільства та стан захищеності інформації у ньому багато в чому залежить від правового забезпечення інформаційної безпеки.

Інформаційна безпека характеризується стійкістю основних сфер життєдіяльності щодо небезпеки, тому поняття інформаційної безпеки стосується всіх аспектів захисту інформації. На законодавчому рівні 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 [3].

Виходячи з наведеного визначення, об'єктами інформаційної безпеки є життєво важливі інтереси людини, суспільства і держави. Забезпечення інформаційної безпеки потребує узгодження особистих, суспільних та державних інтересів з метою недопущення виникнення між ними конфліктів або ж нейтралізації їх наслідків у разі, якщо не можна досягти певного компромісу між ними.

Водночас у нормативному визначені інформаційної безпеки, закріпленому в Законі України «Про основні засади інформаційного суспільства в Україні на 2007–2015 роки», приділяється увага негативним інформаційним впливам, які можуть призвести до вкрай небезпечних соціальних, економічних, політичних та інших наслідків, тобто ці впливи представляють загрози інформаційній безпеці людини, суспільства та держави [7, с. 9-10].

Метою статті є дослідження поняття «загроза інформаційній безпеці» з погляду теорії та практики, її класифікація. Завданням є з'ясування нормативно-правової основи та зарубіжного досвіду щодо протидії інформаційним загрозам.

Для дослідження загроз інформаційній безпеці та протидії їм необхідно виходити зі змісту цього поняття. Важливо звернути увагу на те, що з точки зору термінології безпека буквально, у вузькому значенні, означає саме відсутність загрози. Необхідно звернутися до здобутків «загальної теорії безпеки як системи знань про захищеність людини від загроз», де категорія «загроза» визначається як можливість чи неминучість виникнення соціальних, природних або техногенних явищ із прогнозованими, але неконтрольованими небажаними подіями, що можуть статись у певний момент часу в межах даної території, спричинити смерть людей чи завдати шкоди їхньому здоров'ю, призвести до матеріальних і фінансових збитків, погіршити стан довкілля тощо [5, с. 35-40]. Виходячи з наведеного визначення, поняття «загроза інформаційної безпеки» можна визначити як можливість чи неминучість виникнення соціальних, політичних чи інших явищ із прогнозо-

ваними, але не контрольованими небажаними подіями, які можуть зашкодити інтересам людини, суспільства і держави; призвести до матеріальних збитків різних суб'єктів правовідносин; порушити доступність, цілісність та конфіденційність інформації. Водночас із погляду права дане визначення є недосконалим.

На нормативному рівні у законодавстві Україні відсутнє дане визначення, водночас у Законі України «Про основи національної безпеки України» наявне визначення поняття «загроза національній безпеці України», що являє собою наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України [2]. Дане визначення розкриває зміст загроз у широкому аспекті, оскільки національну безпеку пропонують визначати як результат управління реальними чи (та) потенційними загрозами з метою задоволення національних інтересів людини, суспільства та держави [8, с. 8-10].

У свою чергу, національний інтерес – сукупність потреб людини, суспільства та держави, реалізація яких забезпечує їх існування та розвиток через створення відповідних державно-правових та недержавних інституцій [8, с. 8-10]

Водночас на теоретичному рівні пропонують розглядати загрози інформаційній безпеці у контексті загроз національним інтересам в інформаційній сфері, які являють собою сукупність умов і факторів, які створюють небезпеку заподіяння шкоди об'єктам національних інтересів у інформаційній сфері й діяльності щодо реалізації цих інтересів. Їх поділяють на:

– загрози діяльності влади щодо реалізації національних інтересів в інформаційній сфері;

– загрози об'єктам національних інтересів в інформаційній сфері, які, у свою чергу, можна поділити на загрози інформації, інформаційній інфраструктурі та правовому статусу людини в інформаційній сфері [9, с. 323].

У теорії інформаційного права також існує підхід до розуміння загроз інформаційній безпеці, а саме: це одна з ланок структурного ряду безпекогенних чинників, таких як ризик – загроза – виклик – небезпека. На нашу думку, все ж таки більш доречним є використання саме категорії загроз, а інші наведені категорії розглядати як імовірні стадії реалізації загроз інформаційної безпеки. На думку І.Р. Березовської, в контексті нормативного підходу до розмежування понять «загроза» та «небезпека», оскільки Закон України «Про основи національної безпеки» оперує поняттями «загроза» та «небезпека», причому загроза передує небезпеці як співвідношення «можливість-дійсність», виокремлення ризиків, викликів, а також визначення пріоритетності загроз чи небезпек є недоцільним [6, с. 30-40].

Поряд із цим деякі науковці розглядають загрози інформаційній безпеці як сукупність факторів, що перешкоджають розвитку і використанню національного інформаційного середовища в інтересах громадян, суспільства і держави. Водночас науковці наводять й іншу дефініцію, розглядаючи загрози як юридичний факт, а саме дію чи подію, яка може призвести до руйнування, спотворення або несанкціонованого власником чи володільцем доступу до інформаційних ресурсів [9, с. 340].

Враховуючи вище наведені підходи до визначення даного поняття, можемо сформулювати власне визначення, а саме: загрози інформаційній безпеці – це сукупність організаційних, технічних і особистих факторів, програмних продуктів і систем, використання яких тягне за собою порушення прав та законних інтересів учасників інформаційних відносин, підриває основи національної безпеки або знищує програмне забезпечення різних інформаційно-телекомунікаційних систем як національного, так і локального рівня. Таким чином, загрози являють собою фактори реальної дійсності, які мають економічне, соціальне, політичне або природне підґрунтя; так і фактори життя суспільства (процеси, явища, дії або бездіяльність), які викликають певні інформаційні конфлікти, або створюють загрозу посягання на права особи, або ставлять під загрозу інформаційну інфраструктуру.

Важливу роль у дослідженні правової природи загроз інформаційній безпеці відіграє їх класифікація, яка дає змогу виявити різні сторони цього явища, а також виробити певні механізми протидії. У науковій літературі відсутній єдиний підхід до визначення критеріїв класифікації загроз інформаційній безпеці.

Загрози інформаційній безпеці можуть бути класифіковані за різними критеріями, зокрема:

1) залежно від сфери виникнення й існування:

– у сфері внутрішньої політики;

– у сфері зовнішньої політики;

2) за ймовірністю реалізації:

– імовірні – такі загрози, які за виконання певного комплексу умов обов'язково відбудуться. Прикладом може слугувати оголошення атаки інформаційних ресурсів суб'єкта забезпечення національної безпеки, яке передує самій атаці;

– неможливі – такі загрози, які за виконання певного комплексу умов ніколи не відбудуться;

– випадкові – такі загрози, які за виконання певного комплексу умов кожного разу протікають по-різному. Загрози даного рівня доцільно аналізувати за допомогою методів дослідження операцій, зокрема теорії ймовірностей і теорії ігор, які вивчають закономірності у випадкових явищах [7, с. 15].

3) за характером реалізації:

– реальні – активізація алгоритмів дестабілізації є неминучою і не обмежена часовим інтервалом і просторовою дією;

– потенційні – активізація алгоритмів дестабілізації можлива за певних умов середовища функціонування органу державного управління;

– здійснені – такі загрози, які втілені в життя;

– уявні – псевдоактивізація алгоритмів дестабілізації, або ж активізація таких алгоритмів, що за деякими ознаками схожі з алгоритмами дестабілізації, але такими не є [8, с. 120-130].

4) за ставленням до них:

– об'єктивні – такі загрози, які підтверджуються сукупністю обставин і фактів, що об'єктивно характеризують навколишнє середовище. При цьому ставлення до них суб'єкта управління не відіграє вирішальної ролі через те, що об'єктивні загрози існують незалежно від волі та свідомості суб'єкта. Так, наприклад, хоча український законодавець у Законі України «Про основи національної безпеки України» не визначив пріоритетність захисту від інформаційних загроз, приділивши їм найменшу увагу, насправді їх значення є непересічним, і акцентування уваги на інших загрозах призводить постійно до великих помилок у сфері саме інформаційній [8, с. 120-130];

– суб'єктивні – така сукупність чинників об'єктивної дійсності, яка вважається суб'єктом управління системою безпеки загрозою. У цьому разі визначальну роль у ідентифікації тих чи інших обставин та чинників відіграє воля суб'єкта управління, який і ухвалює безпосереднє рішення про надання статусу або ідентифікації тих чи інших подій як загроз безпеці.

5) за об'єктом впливу:

– на людину;

– на суспільство;

– на державу [8, с. 120-130].

Важливим критерієм для забезпечення з боку держави інформаційної безпеки і реалізації державної інформаційної політики у сфері безпеки є форма закріплення загроз:

– нормативні – ті, що офіційно визнані з боку органів державної влади і знайшли своє відображення у норматив-

них актах, наприклад у Законі України «Про основи національної безпеки»;

– ненормативні – ті, що існують об'єктивно, але не закріплені у нормативних актах.

У виробленні механізму протидії загрозам і вдосконаленні системи державної політики у цій галузі важливу роль відіграє такий критерій, як спосіб прояву загроз, зокрема:

– загрози, що проявляються шляхом блокування, знищення, пошкодження, видозміни програмного забезпечення;

– загрози, що проявляються шляхом незаконного збирання, поширення та знищення інформації;

– загрози, що проявляються через поширення шкідливої, забороненої чи неправдивої інформації;

– загрози, що проявляються через блокування роботи електронно-обчислювальних машин, інформаційно-телекомунікаційних мереж;

– загрози, що проявляються через електронне шахрайство, тощо.

Загрози інформаційній безпеці також можна класифікувати за критерієм тривалості, а саме, постійні або тимчасові загрози.

Як вже зазначалося вище, з огляду на розвиток інформаційних технологій та їх поширення у всіх сферах життєдіяльності, доречним буде такий критерій класифікації, як належність до галузей управління, де існують інформаційні загрози:

– в галузі економіки;
– в галузі промисловості;
– в галузі оборони;
– в галузі енергетики;
– в галузі науки та освіти;
– в галузі транспорту і зв'язку;
– в галузі інформатизації тощо.

Варто зазначити, що саме детальне вивчення загроз інформаційній безпеці дає змогу виробити такі адміністративно-правові засоби забезпечення інформаційної безпеки, які були б дієвими та динамічними.

На даному етапі у законодавстві Україні відсутні нормативно-правові акти, які б вирішували проблеми цієї сфери, тому доречним буде вивчення зарубіжного досвіду забезпечення інформаційної безпеки та протидії інформаційним загрозам.

Починаючи з 1995 року країни «Великої вісімки – G8» (з 2014 року – G7), зважаючи на збільшення інформаційних загроз, приділяли значну увагу захисту критичної інфраструктури. У травні 2000 року в Парижі відбулася конференція G8 з діалогу між суспільною владою та приватним сектором щодо безпеки та довіри в інформаційному світі [6, с. 55-59].

Науково-дослідні установи ООН активно займаються оцінкою світової безпеки в глобальному «цифровому» світі, аналізують можливість створення наступальних озброєнь для атак на інформаційні системи й мережі. У грудні 2003 року 57-ма Генеральна Асамблея ООН прийняла резолюцію 57/239 «Створення глобальної культури кібербезпеки», яка передбачає, що культура безпеки має формуватися у взаємодії державних і суспільних структур, включаючи розробників і користувачів ІТ, регуляторні та наглядові органи [6, с. 57].

Крім того, що дана проблематика обговорюється та врегульовується на міжнародному рівні, низка держав приймає й свої нормативно-правові акти у формі концепцій або стратегій. Так, наприклад, однією з перших країн, яка почала на законодавчому рівні приділяти увагу інформаційній безпеці, були США. У 2003 році було прийнято Національну стратегію безпеки у кіберпросторі, яка стала частиною більш загальної Стратегії забезпечення національної безпеки [11].

Великобританія, потенціал якої у сфері інформаційної безпеки вважається одним із найпотужніших у світі, продовжує нарощувати свої сили у забезпеченні захисту кіберпростору. У червні 2009 року вона випустила першу Стратегію кібербезпеки Сполученого Королівства, яка включала три основні напрями: зменшення ризику, розпізнання можливостей і вдосконалення відповіді на кібервипадки [12].

Вивчення досвіду зарубіжних країн у сфері реалізації адміністративно-правових засобів забезпечення інформаційної безпеки свідчить про те, що сьогодні однією з найбільших проблем «інформаційно розвинутих держав» є те, що впровадження інформаційних технологій відбувається швидше, ніж процеси правового регулювання пов'язаних із цим суспільних відносин [6, с. 58].

Отже, досліджуючи проблеми інформаційної безпеки, можемо дійти висновку, що на законодавчому рівні залишається багато неврегульованих питань. Так, відсутність визначення категорії «загрози інформаційної безпеки» і розкриття її змісту гальмують процес розроблення дієвих засобів забезпечення інформаційної безпеки і протидії загрозам. Водночас у теорії інформаційної безпеки також не вироблено єдиного підходу до визначення даної категорії, яке б можна було впровадити у законодавство України. Дослідження правової природи загроз інформаційній безпеці через їх зміст та класифікацію дає змогу покращити механізм державного забезпечення інформаційної безпеки; на законодавчому рівні розмежувати такі категорії, як «ризик», «загрози», «виклик», «небезпека», «вплив».

Враховуючи зарубіжний досвід, органи державної влади повинні взяти під регулюючий контроль побудову національної інформаційної інфраструктури. Так, 18 березня 2016 року набула чинності Стратегія кібербезпеки України, метою якої є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [4]. Відповідно, можна вважати це першим кроком для побудови дієвої системи протидії інформаційним загрозам.

З втратою чинності у 2014 році Доктрини інформаційної безпеки України (далі – Доктрина) постає потреба у прийняті відповідного нормативно-правового акта, який, враховуючи недоліки Доктрини, мав би сучасний понятійний апарат, у тому числі визначення категорії «загрози інформаційної безпеки», повністю розкривав би їх зміст. Нині у Міністерстві інформаційної політики України ведуться дискусії щодо розроблення Концепції інформаційної безпеки України.

Таким чином, дослідження цієї проблематики показало, що інформаційна безпека є невід'ємною частиною нашого суспільства і потребує докорінних змін з юридичної точки зору і покращення законодавчого підґрунтя забезпечення інформаційної безпеки.

ЛІТЕРАТУРА

1. Конституція України : Закон від 28.06.1996 № 254к/96-ВР (станом на 15 березня 2016 р.) // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.

2. Про основи національної безпеки : Закон України від 19.06.2003 № 964-IV // Голос України . –2003. – № 134.

3. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України від 09.01.2007 № 537-V // Голос України. – 2007. – № 21.

4. Про стратегію кібербезпеки України : Указ Президента України від 15.03.2016 № 96/2016 // Урядовий кур'єр. – 2016. – № 52.

5. Арістова І.В. Інформаційна безпека людини як споживача телекомунікаційних послуг : монографія / І.В. Арістова, Д.В. Сулацький ; НДІ інформатики і права Нац. акад. прав. наук України. – К.: Право України, 2013. – 184 с.

6. Березовська І.Р. Адміністративно-правові засоби забезпечення інформаційної безпеки України : монографія / І.Р. Березовська. – Львів : ЗУКЦ, 2014. – 173 с.
7. Горбулін В.П. Проблеми захисту інформаційного простору України : монографія / В.П. Горбулін ; Інститут проблем національної безпеки. – К.: Інтертехнологія, 2009. – 135 с.
8. Інформаційна безпека України в умовах Євроінтеграції : навчальний посібник / В.А. Ліпкан, Ю.Є. Максименко, В.М. Желіховський. – К.: КНТ, 2006. – 280 с.
9. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України : автореф. дис....канд. юрид. наук : спец. 12.00.01 «Теорія та історія держави і права; історія політичних і правових учень» / Ю. Є. Максименко ; Київський національний університет внутрішніх справ. – К, 2007. – 20 с.
10. Міжнародна інформаційна безпека: сучасні виклики та загрози / Є.А. Макаренко, М.М. Рижиков, М.А. Ожеван та ін. – К.: Центр вільної преси, 2006. – 916 с.
11. The National strategy to secure cyberspace, February 2003 [Електронний ресурс]. – Режим доступу : https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.
12. Cyber Security Strategy of United Kingdom: safety, security and resilience in cyber space. [Електронний ресурс]. – Режим доступу : https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf.

УДК 343.3/.7

АНТИКОРУПЦІЙНЕ ЗАКОНОДАВСТВО УКРАЇНИ: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

ANTI-CORRUPTION LEGISLATION OF UKRAINE: PROBLEMS AND PROSPECTS

Левченко А.О.,
студент кафедри права факультету менеджменту та права
Вінницький національний аграрний університет

У даній статті розглядається питання поетапного формування антикорупційного законодавства та державної політики у сфері запобігання корупції. Шляхом теоретичного аналізу чинного законодавства щодо запобігання корупції в Україні та останніх досліджень і публікацій із цього приводу визначено основні перспективні положення антикорупційного законодавства України. Виявлено проблемні питання впровадження та реалізації правових норм даного законодавства, що, безумовно, пов'язано з низкою недоліків, які існують у боротьбі з корупцією в умовах сьогодення.

Ключові слова: антикорупційне законодавство, нормативно-правові акти, корупція, нормативно-правове регулювання, запобігання корупції.

В данной статье рассматривается вопрос поэтапного формирования антикоррупционного законодательства и государственной политики в сфере предотвращения коррупции. Путем теоретического анализа действующего законодательства по предотвращению коррупции в Украине, последних исследований и публикаций по этому поводу определены основные перспективные положения антикоррупционного законодательства Украины. Выявлены проблемные вопросы внедрения и реализации правовых норм данного законодательства, что, безусловно, связано с рядом недостатков, которые существуют в борьбе с коррупцией в сегодняшних условиях.

Ключевые слова: антикоррупционное законодательство, нормативно-правовые акты, коррупция, нормативно-правовое регулирование, предотвращение коррупции.

This article discusses the gradual formation of anti-corruption legislation and public policy in the field of prevention of corruption. On the basis of which it is determined that the formation of this legislation was accompanied by significant changes and additions which are associated with the implementation of international standards in the field of combating corruption. However, it did not give significant results. Due to the fact that it was not created efficient data standards implementation mechanism in contemporary realities and to create the necessary system of special organs that could implement them.

By theoretical analysis of the current legislation on the prevention of corruption in Ukraine and the latest research and publications on the subject. The main long-term position of anti-corruption legislation of Ukraine, namely conflict of interest, limit the possibility of joint work of close persons, operation of special anti-corruption bodies, restrictions on persons released from posts or discontinued activities related to the implementation of the functions of the state or local self-government mechanism for disclosure of information, specified in the declarations of property, income, expenditure and financial liabilities, and the like. Despite the positive developments and the significant prospects of the current legislation on the prevention of corruption also identified problematic issues of introduction and implementation of legal norms of the legislation certainly involves a number of drawbacks that exist in the fight against corruption in the conditions.

Also it determined that the adoption of a brand new anti-corruption legislation to prevent corruption, accommodating the positive and forward-looking provisions of anti-corruption does not mean the end of its process of reform of the anti-corruption mechanism that will ensure the implementation of the declared goals and objectives that are of extreme importance for the national security of Ukraine and the combined international obligations to the EU.

Key words: anti-corruption legislation, regulations, corruption, legal regulation, prevention of corruption.

Сьогодні все більше стає зрозумілим, що питання протидії корупції – це питання майбутнього благополуччя українського народу. Це явище не дає можливості провести жодну реформу в нашій державі. Таким чином, боротьба з корупцією є проблемою загальнонаціонального значення. Сьогодні корупція в Україні перетворилась на одну з головних загроз національній безпеці та демократичному розвитку держави. Негативний вплив цього явища на всі аспекти політичного та соціально-економічного розвитку суспільства і держави в цілому має комплексний характер. Боротьба з корупцією потребує мобілізації всіх можливих ресурсів народу, в тому числі і правових.

Негативний стан справ у нашій державі підтверджується висновками вітчизняних та зарубіжних експертів, політичних та громадських діячів. За дослідженнями міжнародної організації «Transparency International», за минулий рік Україні вдалося заробити лише один додатковий бал за результатами світового індексу сприйняття корупції CPI 2015 року. На сьогоднішній день індекс CPI України складає 27 балів зі 100 можливих, що лише на один бал