УДК 342.951:316.776

ПРО ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ

ON THE THREATS TO INFORMATION SECURITY OF UKRAINE

Цьвок М.С., к.ю.н.,
асистент кафедри адміністративного та інформаційного права
Інститут права та психології
Національного університету «Львівська політехніка»

У статті характеризуються загрози інформаційній безпеці України. Аналізується чинне вітчизняне законодавство, яке визначає актуальні загрози інформаційній безпеці України. Розглядаються наукові підходи щодо визначення джерел загроз інформаційної безпеки нашої країни. Пропонується до законодавчих положень, які визначають засади внутрішньої та зовнішньої політики України, віднести інформаційну політику держави.

Ключові слова: інформаційна безпека, інформаційна загроза, інформаційна політика, інформаційний простір, національна безпека.

В статье характеризуются угрозы информационной безопасности Украины. Анализируется действующее отечественное законодательство, которое определяет актуальные угрозы информационной безопасности Украины. Рассматриваются научные подходы к определению источников угроз информационной безопасности нашей страны. Предлагается к законодательным положениям, которые определяют основы внутренней и внешней политики Украины, определить информационную политику государства.

Ключевые слова: информационная безопасность, информационная угроза, информационная политика, информационное пространство, национальная безопасность.

The article deals with the theoretical definition of the concept of "threat". It is noticed that in the legislative and scientific sources, the definition "threats to the national security in the information sphere" is often used with the definition "threats to the information security of Ukraine". In this research, these definitions are considered to be identical. The article also describes the threats to Ukraine's information security. Existing domestic legislation, which determines current threats to the information security of Ukraine, is analyzed. The external and internal sources of threats to the information security of our country are defined. It is emphasized that today information legislation is being improved at the international level to manage new potential threats. As an example, in Ukraine the Decision of the National Defense and Security Council of Ukraine, dated April 28, 2017 "On Introducing Special Economic and Other Restrictive Measures (Sanctions) of Personal Nature" is used. It defines the list of individuals and legal entities to which Ukraine applies special economic and other restrictive measures (sanctions) of personal nature. These restrictive measures (sanctions) include the restriction or termination of provision of telecommunication services and use of public telecommunications networks, as well as the prohibition for certain Internet providers to allow access to websites and services. It is offered to include the information policy of the state into the legislative provisions defining the principles of domestic and foreign policy of Ukraine. The author concludes that the issue of information security of Ukraine is open for discussion today as the threats, existing in the information space, are constantly changing and intensifying due to the development of modern information technologies, which expand opportunities for rapid and voluminous exchange of information both between individuals in Ukraine and abroad, and directly between countries of the world.

Key words: information security, information threat, information policy, information space, national security.

Сьогодні дедалі більшої актуальності набувають питання, що стосуються інформаційної безпеки нашої країни. Цьому неабияк сприяють як внутрішні, так і зовнішні чинники, які впливають на інформаційний простір України. Однак результат такого впливу не завжди є позитивним.

Хоча саме «стан захищеності інформаційного середовища суспільства, що забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави» вважається «інформаційною безпекою» [1].

Поняття «інформаційна безпека», яке формувалось протягом останніх п'ятдесяти років та знаходило відображення у таких назвах – комп'ютерна безпека, безпека даних – за сучасних умов набуває дедалі більшого значення і стає одним із найважливіших елементів забезпечення національної безпеки та складовою міжнародної інформаційної безпеки [2, с. 205].

Інформаційна безпека кожної країни залежить не тільки від злагодженого функціонування державних інституцій за умови верховенства права та поваги до свобод і прав людини, але й здатності громадян критично усвідомлювати та брати на себе відповідальність за власну поведінку під час конфлікту. В епоху поширення Інтернету та соціальних мереж, де кожен користувач стає виробником інформаційного потоку, відповідальність зумовлюється зростанням критичного мислення й медіаграмотності користувачів, щоб не допустити поширення неправдивої чи невірогідної інформації, вмінням розрізнити інформаційні атаки, поведінку ботів та тролів. Виклики цифрової епохи обумовлюють також необхідність для кожного користувача засвоювати технологічний складник інформаційного простору та посилювати навички у цифровій безпеці [3, с. 35].

Зокрема, на інформаційну безпеку держави впливають: а) політична обстановка у світі; б) внутрішньополітична обстановка у державі; в) стан і рівень інформаційно-комунікаційного розвитку країни тощо. Загрози інформаційній безпеці здебільшого супроводжують виникнення й реалізацію загроз в економічний і політичній сферах, у сфері виконання функцій держави тощо, і заподіяння шкоди в інформаційній сфері є передусім засобом досягнення інших цілей. Поряд із суто корисливою метою, у сучасних умовах інформаційні загрози пов'язані з розпалюванням міжнаціональної, міжконфесійної та іншої ворожнечі, дискредитацією правоохоронної системи й органів державної влади загалом, заподіянням шкоди честі, гідності та ділової репутації фізичних осіб, у тому числі публічних, формуванням «образу ворога», «зомбуванням» населення задля створення умов щодо управління масовою свідомістю [4, с. 185].

Метою статті є аналіз вітчизняного законодавства, а також узагальнення наукових підходів у частині визначення загроз інформаційній безпеці України.

Поняття «загроза» визначається у кількох значеннях, а саме як: 1) груба, зухвала обіцянка заподіяти яке-небудь зло, неприємність; нахваляння; 2) можливість або неминучість виникнення чогось небезпечного, прикрого, тяжкого для кого-, чого-небудь; 3) можливість небезпеки; 4) погрожування; небезпека [5, с. 277; 6, с. 249]. Як слушно зауважує В. Ліпкан, «необхідною умовою загрози є реальність, пов'язана з наявністю побоювань щодо приведення її до виконання. Мають існувати реальні побоювання втілення у життя такої загрози. Про реальність загрози можуть свідчити її конкретний зміст і супутні обставини (обстановка, місце, характер та інтенсивність тощо), а також

обставини, що випливають із попередніх відносин об'єктів. Крім цього реальність загрози може виявлятися як характеристика самого суб'єкта загрози (постійне вчинення ним актів тероризму, диверсій, проведення інформаційних війн, можливість порушення норм міжнародного права тощо). Водночас це не означає, що суб'єкт загрози має наміри обов'язково довести її до виконання». Тому, на його переконання, визначення реальності загрози є завданням складним і потребує відпрацювання цілої системи ідентифікації дестабілізуючих чинників як загроз. Крім реальності, загроза має характеризуватися дійсністю, тобто не бути уявною [7, с. 52].

Законодавчо термін «загроза» закріплюється в Інструкції з проведення аналізу ризиків у Державній прикордонній службі України, яка затверджена Наказом Міністерства внутрішніх справ України 11 грудня 2017 р. № 1007 й означає наявні та потенційно можливі явища і чинники, що негативно впливають на сферу безпеки державного кордону [8].

Загроза має завжди предметний характер, наповнена конкретним змістом і у випадку чітко вираженого небезпечного стану такого змісту надто часто набуває конкретну правову характеристику. Ця характеристика частіше за все і фіксується у законах, наприклад, у статтях КК України (дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або захоплення державної влади, посягання на територіальну цілісність і недоторканість України, терористичний акт, шпигунство, диверсія тощо) [7, с. 53].

Водночас явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України законодавцем визначаються як загрози національній безпеці України (п. 6 ч. 1 ст. 1 Закону України від 21 червня 2016 р. «Про національну безпеку України») [9].

Саме загрози національній безпеці України та відповідні пріоритети державної політики у сферах національної безпеки і оборони визначаються у Стратегії національної безпеки України, Стратегії воєнної безпеки України, Стратегії кібербезпеки України, інших документах з питань національної безпеки і оборони, які схвалюються Радою національної безпеки і оборони України і затверджуються указами Президента України (ч. 5 ст. 3 Закону України від 21 червня 2018 р. «Про національну безпеку України») [9].

Зокрема у Стратегії національної безпеки України, затвердженої Указом Президента України від 26 травня 2015 р. № 287/2015 визначено актуальні загрози національній безпеці України, серед яких виокремлюються наступні загрози інформаційній безпеці: а) ведення інформаційної війни проти України; б) відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства. (ч. 3.6 розділ 3) [10].

Слід зауважити, що часто у законодавчих та наукових джерелах нарівні з поняттям «загрози інформаційній безпеці України» використовується поняття «загрози національній безпеці в інформаційній сфері». У даному дослідженні ми не деталізуватимемо співвідношення цих понять та вживатимемо їх як тотожні за змістом.

Отже, загрози національній безпеці в інформаційній сфері визначаються як сукупність умов і факторів, які створюють небезпеку заподіяння шкоди об'єктам національних інтересів в інформаційній сфері й діяльності щодо реалізації цих інтересі. Їх поділяють на: а) загрози діяльності влади щодо реалізації національних інтересів в інформаційній сфері; б) загрози об'єктам національних інтересів в інформаційній сфері, які у свою чергу можна ділити на загрози інформації, інформаційній інфраструктурі та правовому статусу людини в інформаційній сфері [11, с. 323].

Водночас у Доктрині інформаційної безпеки України, затвердженої Указом Президента України від 25 лютого 2017 р. № 47/2017 йдеться про те, що «комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації», а також у розділі 4 визначаються актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері. Такими загрозами, на думку законодавця, є: 1) здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні; 2) проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі; 3) інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах; 4) інформаційне домінування держави-агресора на тимчасово окупованих територіях; 5) недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України; 6) неефективність державної інформаційної політики, недосконаліть законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіа-культури суспільства; 7) поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні [12].

О. Виговська зазначає, що загрози інформаційній безпеці України, з одного боку, є організаційним компонентом системи державного управління, а з другого – слугують індикатором ефективності функціонування останньої. На її думку, реалізація загроз свідчить про неефективність її діяльності, і навпаки. Серед загроз інформаційним ресурсам вона виділяє наступні: – розкриття інформаційних ресурсів (інформація і знання стають відомі тим, кому не слід цього знати); – порушення цілісності інформаційних ресурсів (умисний антропогенний вплив (модифікація, видалення, зниження) даних, які зберігаються в інформаційній системі суб'єкта управління, а також передаються від цієї інформаційної системи до інших); – збій роботи самого обладнання (може виникнути при блокуванні доступу до одного або декількох ресурсів інформаційної системи) [13, с. 53–54].

Об'єктами ураження і захисту від інформаційних загроз, як слушно зазначає В. Горбулін, можуть бути: – органи управління держави та її збройних сил; – інформаційні системи і ресурси цивільної інфраструктури (системи телекомунікації, засоби масової інформації, об'єкти транспортного й енергетичного комплексів, фінансового і промислового секторів); – лінії зв'язку й канали передачі даних; – інформаційні повідомлення і ресурси, що циркулюють або зберігаються у системах управління; – персонал інформаційно-аналітичних систем, що бере участь у процесах підготовки управлінських рішень; – соціальні групи й суспільство у цілому (цивільне населення і збройні сили), економічні й політичні інститути та ін. Відносно зазначених об'єктів за допомогою тих чи інших засобів реалізуються сучасні методи інформаційного протиборства: інформаційна експансія, інформаційна агресія, інформаційний тероризм, інформаційна війна [14, с. 71].

Розрізняють зовнішні та внутрішні джерела загроз інформаційній безпеці держави. До зовнішніх належать такі: –

діяльність іноземних політичних, військових, економічних та розвідувальних структур в інформаційній сфері; – діяльність міжнародних терористичних угрупувань; – політика домінування деяких країн в інформаційній сфері; – розробка та впровадження концепцій інформаційних війн будь-якими структурами; – культурна експансія щодо конкретної держави тощо [13, с. 52–53]. У контексті наявних на сьогодні політичних реалій потенційними загрозами інформаційній безпеці України у зовнішньополітичній сфері також є: – поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України; – проява комп'ютерної злочинності, комп'ютерного тероризму, що загрожують сталому та безпечному функціонуванню національних інформаційно-телекомунікаційних систем; – зовнішні негативні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також мережу Інтернет [2, с. 207–208].

Внутрішні джерела загроз інформаційній безпеці випливають із недостатнього політичного та соціального досвіду життя у правовій країні, що стосується процесу практичної реалізації конституційних прав та свобод громадян, у тому числі в інформаційній сфері [13, с. 52–53].

Сьогодні, на переконання І. Валюшко, сучасні технології створили умови для протистояння держав у новому середовищі – інформаційному. Воно є одним із найважливіших чинників розвитку людства, що відображає як потребу, так і специфіку сучасної цивілізації, пов'язаної як зі здобутками, так і з викликами для держав, суспільства та особистості. Такі явища, як: інформаційні війни, інформаційна зброя, інформаційний тероризм, дезінформація є основними загрозами інформаційній безпеці у нинішній час [15, с. 9].

Для управління новими потенційними загрозами Європейський Союз розробляє відповідні плани дій шляхом прийняття інформаційного законодавства, з увагою до національного та міжнародного досвіду регулювання інформаційних відносин, а також створення відповідного інституційного механізму, що складається із загальної системи органів (Європейська Рада, Європейська Комісія, Генеральний Директорат з освіти і культури), так і спеціально створеної (Генеральний Директорат з інформаційного суспільства, Форум інформаційного суспільства ЄС) [16, с. 10].

У свою чергу, в Україні Рішенням Ради Національної безпеки і оборони України від 28 квітня 2017 р. «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)», який набув чинності Указом Президента України від 15 травня 2017 р. № 133/2017, визначено перелік фізичних та юридичних осіб, до яких Україною застосовуються персональні спеціальні економічні та інші обмежувальні заходи (санкції). Серед цих обмежувальних заходів (санкцій) є заходи, які стосуються обмеження або припинення надання телекомунікаційних послуг і використання телекомунікаційних мереж загального користування, а також заборони певним Інтернет-провайдерам надання послуг з доступу користувачам мережі Інтернет до ресурсів/сервісів [17].

Важливим законодавчим актом, за допомогою якого визначаються засади внутрішньої політики України у сферах розбудови державності, розвитку місцевого самоврядування та стимулювання розвитку регіонів, формування інститутів громадянського суспільства, національної безпеки і оборони, в економічній, соціальній і гуманітарній сферах, в екологічній сфері та сфері техногенної безпеки, а також засади зовнішньої політики України є Закон України від 1 липня 2010 р. «Про засади внутрішньої і зовнішньої політики» [18]. Однак видається слушним доповнити даний законодавчий акт положеннями, які б визначали засади внутрішньої та зовнішньої інформаційної політики України, що б сприяло протидії загроз її інформаційній безпеці.

При цьому слід брати до уваги, що «інформаційна політика відповідає запитам трьох аспектів: держави, суспільства, окремої людини. Держава більше опікується захисними темами на кшталт інформаційної безпеки чи інформаційного суверенітету. Суспільство зацікавлене у тому, щоб інформаційний простір слугував модернізації, спрямовував країну на прогресивний розвиток. Окремого індивіда більше турбує доступ до інформації, він вимагає, щоби держава менше заважала йому у його інформаційних діях. Інформаційна політика працює з такими чутливими сферами, як: а) контент (стабілізаційний чи дестабілізаційний); б) суспільні цінності (традиційні чи руйнівні); в) характер суспільства (демократичний, інноваційний)» [19, с. 18].

На думку У. Ільницької, як протидія масштабним негативним інформаційно-психологічним впливам, операціям та війнам, пріоритетними напрямами державної інформаційної політики та важливими кроками з боку владних органів України мають бути: 1) інтеграція України до світового та регіонального європейського інформаційного просторів; 2) інтеграція у міжнародні інформаційні та інформаційно-телекомунікаційні системи та організації; 3) створення власної національної моделі інформаційного простору та забезпечення розвитку інформаційного суспільства; 4) модернізації усієї системи інформаційної безпеки держави та формування й реалізація ефективної інформаційної політики; 5) удосконалення законодавства з питань інформаційної безпеки, узгодження національного законодавства з міжнародними стандартами та дієве правове регулювання інформаційних процесів; 6) розвиток національної інформаційної інфраструктури; 7) підвищення конкурентоспроможності вітчизняної інформаційної продукції та інформаційних послуг; 8) впровадження сучасних інформаційно-комунікативних технологій у процеси державного управління; 9) ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації та коригуванні державної політики в інформаційній сфері [20, с. 30].

Вважаємо, що при формуванні засад інформаційної політики України до уваги доцільно також взяти положення проекту Закону України «Про інформаційний суверенітет та інформаційну безпеку України» № 1207-д від 12 серпня 1999 р., в якому зазначається, що основними напрямами державної інформаційної політики України у сфері інформаційної безпеки повинні бути: а) захист населення України від інформаційної продукції, яка загрожує його фізичному, інтелектуальному, морально-психологічному здоров'ю (пропаганда жорстокості, насильства, людиноненависності, порнографії, окультизму, вплив на підсвідомість тощо); б) посилення інформаційної безпеки України як невіддільної частини політичної, економічної, оборонної та інших складових національної безпеки; в) всебічне сприяння наданню інформаційних послуг (інформаційному забезпеченню) правоохоронним відомствам для виконання ними своїх функцій; г) охорона державної таємниці та іншої інформації з обмеженим доступом, що є об'єктом права власності держави або об'єктом лише володіння, користування чи розпорядження державою, а також здійснення державного контролю за режимом доступу до цієї інформації [21].

Підсумовуючи викладене, зауважимо, що сьогодні в Україні питання її інформаційної безпеки є відкритим для обговорення, адже наявні в інформаційному просторі загрози постійно змінюються та активізуються, в основному у зв'язку з розвитком сучасних інформаційних технологій, які розширюють можливості для швидкого та об'ємного обміну інформацією як між окремими особами в Україні та за її межами, так і безпосередньо поміж країнами світу. Загрози інформаційній безпеці України є перепоною для належного інформаційного обміну, тому вважаємо, що одним із важливих напрямів щодо цього є вдосконалення вітчизняного законодавства, яким врегульовуються як правові, так і організаційні засади забезпечення інформаційної безпеки України.

ЛІТЕРАТУРА

1. Угода про вільний доступ і порядок обміну відкритою науково-технічною інформацією держав – учасниць СНД: Міжнародний документ від 11 вересня 1998 р. № 997_889. URL: http://zakon.rada.gov.ua/laws/show/997_889/ed19990401/find?text=%C8%ED%F4%EE%F0%EC%E0%F6%E8%EE%ED%ED%E0%FF+%E1%E5%E7%EE%EF%E0%F1%ED%EE%F1%F2%FC (дата звернення: 23.09.2018).

2. Довгань О.Д. Забезпечення інформаційної безпеки в контексті глобалізації: теоретико-правові та організаційні аспекти: монографія. Київ, 2015. 388 с.

3. Як підсилити інформаційну безпеку в Інтернеті під час конфлікту: рекомендації для стейкхолдерів / В. Мороз, Т. Матичак, А. Бабак, В. Сазонов. Київ: К.І.С., 2017. 40 с.

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

5. Куньч З.Й. Універсальний словник української мови. Тернопіль: Навчальна книга – Богдан, 2007. 848 с.

6. Загнітко А.П., Щукіна І.А. Сучасний словник української мови. Донецьк: БАО, 2012. 960 с.

7. Ліпкан В. А. Теоретико-методологічні засади управління у сфері національної безпеки України: монографія. Київ, 2005. 350 с.

8. Інструкція з проведення аналізу ризиків у Державній прикордонній службі України, затверджено Наказом Міністерства внутрішніх справ України 11.12.2017 р .№ 1007, зареєстровано в Міністерстві юстиції України 22 січня 2018 р. за № 91/31543. URL: http://zakon.rada.gov.ua/laws/show/z0091-18/ed20171211#n20 (дата звернення: 23.09.2018).

9. Про національну безпеку України: Закон України від 21 червня 2018 р. № 2469-VIII / Верховна Рада України. Голос України. 2018. 07 липня. № 122.

10. Стратегія національної безпеки України, затверджено Указом Президента України від 26 травня 2015 р. № 287/2015 / Президент України. Офіційний вісник Президента України. 2015. 03 червня. № 13. Ст. 874.

11. Міжнародна інформаційна безпека: сучасні виклики та загрози. К.: Центр вільної преси, 2006. 916 с.

12. Доктрина інформаційної безпеки України, затверджено Указом Президента України від 25 лютого 2017 р. № 47/2017 / Президент України. Офіційний вісник Президента України. 2017. 03 березня. № 5. Ст. 102.

13. Виговська О.С. Інформаційна складова національної безпеки України: колективна монографія / О.С. Виговська, Н.Б. Бєлоусова. К.: Київ. ун-т ім. Б. Грінченка, 2017. 168 с.

14. Горбулін В.П. Проблеми інформаційного простору України: монографія / В.П. Горбулін, М.М. Биченюк; Ін-т пробл. нац. безпеки. К.: Інтертехнологія, 2009. 136 с.

15. Валюшко І.О. Інформаційна безпека України в контексті російсько-українського конфлікту: автореф. дис. … канд. юрид. наук: спец. 23.00.04 «Політичні проблеми міжнародних систем та глобального розвитку»; Чорноморський національний університет імені Петра Могили. Миколаїв, 2018. 17 с.

16. Максименко Ю.Є. Теоретико-правові засади забезпечення інформаційної безпеки України: автореф. дис. … канд. юрид. наук: спец. 2.00.01 «Теорія та історія держави і права, історія політичних і правових учень»; Київський національний університет внутрішніх справ. Київ, 2007. 20 с.

17. Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій): Рішення Ради Національної безпеки і оборони України від 28 квітня 2017 р., набув чинності Указом Президента України від 15 травня 2017 р. № 133/2017 / Президент України. Урядовий кур'єр. 2017. 05 травня. № 89.

18. Про засади внутрішньої і зовнішньої політики: Закон України від 01 липня 2010 р. № 2411-VI / Верховна Рада України. Відомості Верховної Ради України. 2010. № 40. Ст. 527.

19. Почепцов Г. Сучасні інформаційні війни. Вид. 2-ге, доповнене. К.: Вид. дім «Києво-Могилянська академія», 2016. 504 с.

20. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. Humanitarian Vision. 2016. Volume 2, number 1. P. 27–32.

21. Про інформаційний суверенітет та інформаційну безпеку України: проект Закону України № 1207-д від 12 серпня 1999 р. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=6670 (дата звернення: 23.09.2018).