УДК 342.5

doi.org/10.30970/jcl.4.2021.6

Тетяна Слінько
кандидатка юридичних наук, професорка,
завідувачка кафедри конституційного права України
Національного юридичного університету імені Ярослава Мудрого,
Харків, Україна
t.m.slinko@nlu.edu.ua

СУЧАСНІ ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ КРАЇНИ Й ШЛЯХИ ЇХ ПОДОЛАННЯ

CURRENT THREATS TO THE COUNTRY'S INFORMATION SECURITY AND WAYS TO ADDRESS THEM

Tetiana Slinko
Candidate of Juridical Sciences, professor, head of Department of Constitutional Law of Ukraine,
Yaroslav Mudryi National Law University, Kharkiv, Ukraine

Abstract | The essential characteristics of information security are investigated in the article. Modern threats to the information security of Ukraine are analyzed. The necessity of developing a logically complete from the legal and organizational point of view system of management, formation, development, using, protection of information resources, ensuring national security is substantiated. The issues that are currently a priority for the proper functioning of the national information security system are pointed out. It is proved in the article that from the point of view of information security today Ukraine is at risk, as this area has not been given due attention, which, in the end, was one of the reasons for increasing internal contradictions inspired by external ones with the assistance of information and communication tools.
The need to ensure information security and protection of the information sovereignty is caused by the construction of the information space and the necessity to guarantee the national security of Ukraine as a whole. In conditions of the current Russian aggressive policy towards Ukraine, only such a thing could influence the positive course of events and help reduce the impact of both domestic and external factors.

Keywords: information security, territorial integrity, information security threats, constitutional order, information sovereignty.

Анотація | У статті досліджено сутнісні характеристики інформаційної безпеки. Проаналізовано сучасні загрози інформаційній безпеці України. Обґрунтовано необхідність розробки логічно завершеної з правової й організаційної точок зору системи управління, формування,

розвитку, використання, захисту інформаційних ресурсів, забезпечення національної безпеки. Виокремлено питання, вирішення яких наразі є першочерговим для належного функціонування національної системи інформаційної безпеки.

Встановлено, що з точки зору інформаційної безпеки на сьогодні Україна перебуває в зоні ризику, оскільки цій сфері не приділялося належної уваги, що, урешті-решт, і стало однією з причин посилення внутрішніх протирічь і конфліктів, інспірованих ззовні за допомогою в першу чергу інформаційно-комунікаційних засобів.

Необхідність забезпечення інформаційної безпеки й захисту інформаційного суверенітету, як нами доведено, зумовлена формуванням інформаційного простору, необхідністю забезпечення національної безпеки України в цілому.

В умовах ведення сучасним російським керівництвом агресивної політики щодо України лише така могла б вплинути на позитивний хід подій і сприяти зменшенню впливу як внутрішньо- політичних, так і зовнішніх факторів.

Ключові слова: інформаційна безпека, територіальна цілісність, інформаційні загрози, конституційний лад, інформаційний суверенітет.

У сучасних умовах, коли майже у всі сфери життя впроваджуються надсучасні інформаційні технології, стрімко розвиваються телекомунікаційні системи, з'являються нові глобальні мережі, засновані на використанні інтерактивних засобів поширення інформації, стає можливим задоволення власних інтересів, отримання (майже миттєво) потрібних відомостей. Нині кожна людина має змогу дізнатися про останні події у будь-якому куточку світу. У той же час існує й інший бік прогресу: влада, громадяни будь-якої держави без застосування воєнного інструментарію, а лише завдяки Інтернету, соцмережам, каналам передавання інформації у змозі послабити або навіть зруйнувати конкуруючу державу, наприклад, вивести з ладу банківську систему чи якийсь сайт, як-от надання держпослуг, втрутитися у роботу електронної пошти окремо взятого відомства (як це було з поштою ФБР) тощо. На жаль, досить часто нині доводиться чути про хакерські атаки, від яких ніхто, як виявилося, не захищений. Красномовними і показовими у цьому контексті, на наш погляд, є дані, наведені у звіті компанії Microsoft щодо хакерських атак протягом 2020–2021 років, зробленому на підставі інформації, що зібрали її системи безпеки. Так, згідно з даними Microsoft до здійснення 58 % атак причетна Росія. «Більшість хакерських атак була спрямована проти Сполучених Штатів – 46%. Україна у цьому рейтингу посідає друге місце (19%), на третьому – Велика Британія, зі значним відривом (9%). Також частина атак припала на Бельгію, Японію, Німеччину (3%) та інші країни»[1].

На наше переконання, викликає занепокоєння той факт, що «найчастіше хакерські атаки були спрямовані на галузь держуправління (48%), на неурядові організації та аналітичні центри (31%)»[2]. Звісно, за такої ситуації навіть найрозвиненіша країна (і цьому є підтвердження) виявиться незахищеною, якщо не усвідомить реальних і потенційних загроз, які несуть інформаційні технології, за допомогою яких чи завдяки яким працюють телекомунікаційні системи, не зможе оцінити масштабів і наслідків негативного впливу. Чого тільки варті «злом водоочисної станції у Флориді й спроба отруїти воду для 15 тисяч жителів. Кібератака на Австралійський канал 9News Australia, що призвела до зриву ефірів. Атака з метою викупу, яка стала причиною зупинки найбільшого в США паливопроводу і коштувала 5 млн доларів. І це лише частина сумних новин»[3]. Єдиним виходом за цих умов є створення дієвої системи захисту й протидії цим загрозам.

Таким чином, в епоху побудови глобального інформаційного суспільства, в якому майже щодня з'являються нові чи оновлені інформаційні технології, використовуються надсучасні засоби

[1] Країни-жертви та країни-агресори у хакерських війнах. URL: https://www.slovoidilo.ua/2021/10/22/infografika/svit/krayiny-zhertvy-ta-krayiny-ahresory-xakerskyx-vijnax

[2] Там же.

[3] Там же.

зв'язку й передачі інформації тощо, українській державі необхідно передусім визначити сукупність зовнішніх загроз (тобто систематизувати і структурувати), встановити, яким із них треба приділити більшу увагу як потенційно найнебезпечнішим, виявити, так би мовити, найслабкіші місця.

Наведене набуває особливої актуальності з огляду на те, що, і ми наводили статистику, нині більшість держав зіткнулася з тим, що їх система забезпечення інформаційної безпеки й захисту інформаційного суверенітету виявилася уразливою, а це негативно впливає на можливості держави ефективно здійснювати захист її національних інтересів в інформаційній сфері. Так, на думку фахівців, одним з найбільш небезпечних зовнішніх чинників сміливо можна визнати процес глобалізації, що супроводжується підривом традиційних і нав'язуванням країнам і народам інших цінностей, зокрема, за допомогою нових інформаційно-телекомунікаційних систем і технологій. Обсяги світової інформаційної індустрії на початку 90-х років минулого століття досягли 2 трлн доларів США, а на початку XXI століття зросли на порядок. Як справедливо зауважує В. Р. Сіденко: «Зростає усвідомлення необхідності дотримуватися певних глобальних принципів поведінки, оскільки альтернативою може бути неконтрольоване зростання глобальних ризиків, від яких не зможе сховатися ніхто. Звідси ми спостерігаємо небачений раніше темп поширення нових міжнародних та навіть глобальних угод щодо регулювання тих чи інших складових людської діяльності»[4].

У контексті сказаного окремо увагу варто звернути на те, що в умовах глобалізації інформаційних процесів, формування світового інформаційного простору, швидкого зростання світового ринку інформації жодна держава, звісно ж, не може функціонувати в інформаційній ізоляції. Саме це й насторожує, бо в цьому разі інформаційні джерела і потоки на території будь-якої країни майже неможливо повністю убезпечити від втручань, нападів, зовнішнього інформаційного впливу й витоку внутрішньої інформації. Вбачається, що саме цим пояснюється важливість для України (як, до речі, і для будь-якої іншої держави) вирішення проблем у сфері інформаційної безпеки, запобігання поширенню негативних тенденцій і подолання наслідків, які настали через спроби хакерів втрутитися чи провести кібератаку. Більш того, і це головне, приходить усвідомлення того, що необхідно розробити логічно завершену з правової й організаційної точок зору систему формування, розвитку, використання, управління, захисту інформаційних ресурсів, забезпечення національної безпеки, складовою якої є інформаційна безпека. Додамо, що йдеться як про можновладців, так і про пересічних громадян, право яких на недоторканність особистого життя, закріпленого ст. 31, 32 Конституції України[5], захищається державою. Підтвердженням вказаного є рішення Конституційного Суду України *від 20 січня 2012 року № 2-рп/2012*, в якому, спираючись на результати системного аналізу положень частин першої, другої статті 24, частини першої статті 32 Конституції України, Суд констатував, що «реалізація права на недоторканність особистого і сімейного життя гарантується кожній особі незалежно від статі, політичних, майнових, соціальних, мовних чи інших ознак»[6].

Наведене набуває неабиякої ваги з огляду на ситуацію, що склалася: зовнішня агресія з боку Росії, анексія Криму, поширення країною-агресором фейків тощо. Звісно, за таких умов для України питання забезпечення інформаційної безпеки як невід'ємної складової національної безпеки стоять особливо гостро. До цього додається й ціла низка інших проблем, які лише на перший погляд є суто технічними. Мова йде про внутрішнє життя української держави, яке сьогодні супроводжується вкрай складними відносинами столичного центру зі східними регіонами, хворобливою соці-

[4] Сіденко В.Р. Нові глобальні виклики та їх вплив на формування суспільних цінностей. Український соціум. 2014. №1(48). С. 11.

[5] Конституція України. URL : https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

[6] Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20 січня 2012 року № 2-рп/2012. URL: https://zakon.rada.gov.ua/laws/show/v002p710-12#Text

альною модернізацією, внутрішньою нестабільністю і політичною невпорядкованістю, політичним і соціальним розшаруванням, що інколи доходить до рівня протистояння, кризою економіки та фінансовою дестабілізацією. Як бачимо, саме збройний конфлікт, політична напруженість, інформаційна агресія з боку Росії є тим важелем, який підштовхує Україну до рішучих дій, спрямованих на захист свого суверенітету й незалежності. Зупинимося на цьому трохи детальніше.

Ні для кого не секрет, що російська військова агресія, анексія Криму і Севастополя становлять реальну загрозу існуванню Української держави, її територіальній цілісності, забезпеченню інформаційної безпеки й захисту інформаційного суверенітету, що, як, до речі, і в більшості демократичних суспільств, захищається національним законодавством. Здавалося б все є: і нормативна база, і бажання, і прагнення.

Однак реалії протилежні. Як іронічно зауважує О. Білорус, досліджуючи глобалізацію і національну стратегію України: «Законодавче поле у нас взірцеве, завдяки йому в інформаційній сфері працює будь-хто і як захоче. Ми фактично втратили інформаційний суверенітет, бо маємо всього 10% державної частки, коли Франція, Польща, Німеччина – до 40 %, а деякі наші сусіди й 60%. Вони мають по 3–5 державних радіо-, 2–3 телеканали, а у нас особливо в кабельних мережах фактично сидить інша держава»[7]. Проте, як відомо, проблема забезпечення інформаційної безпеки як невід'ємної складової загальної національної системи безпеки держави й захисту засад конституційного ладу безпосередньо має вирішуватися державними структурами, до обов'язків яких віднесено забезпечення, додержання й захист Конституції України. Звісно, це логічно, бо з державно-правової точки зору в системі національної безпеки особливе місце повинні посідати охорона Конституції, забезпечення стабільності конституційного ладу України. Не випадково проф. Ю. М. Тодика вказану проблему розглядав як комплексну політико-правову, яка набуває особливого значення в період становлення державності, економічної, політичної і соціальної нестабільності, формування правової системи держави на концептуально новій основі[8].

На підтвердження правильності і виваженості думки науковця додамо, що конституційно-правові засади інформаційної безпеки закріплюються ст. 17 Конституції України, в якій в пріоритетному порядку встановлюється, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу[9]. Чи означає це, що інформаційну безпеку поставлено на один щабель з такими важливими компонентами системи національних інтересів, як суверенітет і територіальна цілісність, і цей статус питання інформаційної безпеки є законодавчо закріплений в Основному Законі? На нашу думку, відповідь має бути позитивною, враховуючи ступінь її важливості.

Більш того, результати дослідження сучасних підходів до вивчення і розуміння інформаційної безпеки свідчать, що окреслена проблема є багатоаспектною. Проте цій сфері тривалий час не приділялася належна увага, що стало однією з причин посилення внутрішніх протиріч і конфліктів, інспірованих ззовні за допомогою використання передусім інформаційно-комунікаційних засобів. Як показала історія (світові війни і революції), безпека більше не забезпечується раціональними домовленостями і непорушними державними інститутами[10]. Очевидно, що загрози безпеці сьогодні можуть бути як зовнішніми, так і внутрішніми, саме тому її забезпечення набуває особливої ваги.

Продовжуючи висвітлення питання, не можна оминути того, що правові основи регулювання державної політики з питань національної безпеки закладені в Законі України «Про основи державної політики національної безпеки України», де вперше дано офіційну оцінку значущості й системній сутності інформаційної безпеки як невід'ємної складової національної безпеки України.

---

[7] Білорус О.Г. Глобалізація і національна стратегія України. Київ: ВО «Батьківщина»; Броди: Просвіта, 2001. С. 47.

[8] Тодика Ю. М. Народовладдя на трансформаційному етапі розвитку держави і суспільства : монографія. Харків : Право, 2007. 480 с.

[9] Конституція України. URL : https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

[10] Національна безпека: світоглядні та теоретико-методологічні засади: монографія /за заг. ред. О.П. Дзьобаня. Харків : Право, 2021. С. 55.

Крім того, сукупність ідей та концепцій, що визначають національні інтереси України в інформаційній сфері, загрози їх задоволення, напрями і пріоритети державної політики в інформаційній сфері й механізми регулювання суспільних відносин набули нормативного закріплення у Доктрині інформаційної безпеки України, затвердженій і введеній в дію Указом Президента України від 25 лютого 2017 року[11].

Враховуючи все це, можемо сміливо стверджувати, що нині важливого політичного і практичного значення при удосконаленні правового забезпечення інформаційної безпеки й інформаційного суверенітету набуває Концепція національної безпеки України, у якій визначаються можливі загрози, що стосуються інформаційної сфери.

Варто зауважити, що, незважаючи на те, що сама Доктрина не є нормативно-правовим актом, в якому передбачені конкретні правові механізми, вона визнається базовим актом, в якому відображені цілі, «вектори» діяльності української держави у даній сфері. Як зазначено в тексті Доктрини, метою її прийняття є «уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни»[12]. У Доктрині також визначено, що «Російською Федерацією застосовуються проти України найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України»[13].

Вказане зайвий раз підтверджує тезу про те, що вітчизняний інформаційний простір протягом всього існування незалежної України був і залишається об'єктом постійних зовнішніх атак, а впродовж останніх 6 років інформаційні атаки проти нашої держави лише посилилися. Крім того, як зазначають експерти в «Аналізі державної політики у сфері національної безпеки і оборони України»: «Дії суб'єктів забезпечення національної безпеки України на початку загострення воєнно-політичної ситуації були не ефективними. Оперативність прийняття управлінських рішень у сфері національної безпеки була низькою, що не забезпечувало своєчасного реагування на нові загрози. Відсутність постійно діючого механізму моделювання і прогнозування як основи для прийняття рішень не дозволяло діяти на упередження[14]. У зв'язку з цим, на наше глибоке переконання, інформаційні загрози нашій державі потребують ретельного аналізу, а технології їх нівелювання і протистояння їм – осучаснення, оскільки, як, сподіваємося, нами доведено, інформаційна безпека – один із фундаментальних чинників існування й розвитку будь-якої держави у XXI столітті.

Висвітлюючи питання, не можна також не зупинитися на наслідках інформаційних війн. Як нами вже було раніше вказано, одним із них є деформація духовних цінностей суспільства й особистості, що негативно впливає на інші сфери життєдіяльності держави, зокрема, на політичну, правову, моральну тощо. У сучасних умовах, коли стрімко поширюються інформаційні технології, створюються віртуальні світи, користуються популярністю різноманітні соціальні мережі, проблема інформаційної безпеки набула нових форм й вимірів. Як нами відмічалося, розвиток інформаційно-комунікаційних технологій, з одного боку, значно розширює можливості людини й суспільства (і це, звісно, добре), а з другого – несе в собі низку загроз інформаційному суверенітету держави, повага до якого виступає одним із основних закріплених у Статуті ООН та інших міжнародних актах принципів сучасного міжнародного права. Наведене пояснюється тим, що світова спільнота обстоює ідею, що в ідеалі всі держави мають бути рівноправними щодо власного інформаційного су-

[11] Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25.02.17 р. № 47/2017. Дата оновлення: 25.02.2017 р. URL: https://zakon.rada. gov.ua/ laws/show/47/2017#Text (дата звернення : 08.09. 2020).

[12] Там же.

[13] Там же.

[14] Аналіз державної політики у сфері національної безпеки і оборони України. 2015 рік. URL: https://rpr.org.ua/wp-content/uploads/2018/02/Analiz-polityky-NB-pravl-final.pdf

веренітету. Однак, і про це вже йшлося, реальність є дещо іншою. Більшість країн світу, які формально незалежні, зазнають відкритого або прихованого впливу з боку потужних інформаційних гігантів, якими є як окремі держави (США, Китай, РФ, Японія, Ізраїль тощо), так і транснаціональні корпорації (Apple, Amazon, Facebook, Google, Microsoft, IBM тощо), що мають статус технологічних флагманів, розуміються на сучасному обладнанні й програмному забезпеченні, нейронних мережах, штучному інтелекті, хмарних обчисленнях тощо. Крім того, як показує досвід гібридної війни, що ведеться Росією проти нашої країни, постійно робляться спроби маніпулювати свідомістю місцевого населення, політичних або економічних еліт, інколи держави вдаються до відвертого диктату, інформаційної дискримінації, неповаги до права вільно обирати й розвивати власну інформаційну систему, встановлювати власні правила суверенного інформаційного середовища тощо. Інколи держава змушена поступитися своєю суверенністю на користь олігополії, що керує глобальними телекомунікаційними мережами, включаючи Інтернет та інформаційні соціальні майданчики.

Усе наведене вище дозволяє зробити висновок про те, що з точки зору інформаційної безпеки на сьогодні Україна перебуває в зоні ризику, оскільки цій сфері не приділялося належної уваги, що, урешті-решт, і стало однією з причин посилення внутрішніх протирічь і конфліктів, інспірованих ззовні за допомогою в першу чергу інформаційно-комунікаційних засобів.

Повернемося до того, що, як нами відзначалося вище, аби протистояти загрозам, передусім слід зрозуміти природу інформаційної безпеки. Як показує аналіз різноманітних підходів до розкриття суті інформаційної безпеки, можна виокремити наступні її сутнісні характеристики: по-перше, це стан захищеності інформаційного простору; по-друге, це стан захищеності національних інтересів України в інформаційному середовищі; по-третє, це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі; по-четверте, це суспільні відносини, пов'язані із захистом життєво важливих інтересів людини і громадянина, суспільства і держави від реальних та потенційних загроз в інформаційному просторі; по-п'яте, це невід'ємна частина політичної, економічної, оборонної та інших складових національної безпеки[15].

Додамо, що за традиційного підходу до визначення загроз інформаційній безпеці суспільства, як зауважує проф. О. Дзьобань, можна виокремити такі основні їх групи. Перша група загроз пов'язана з бурхливим розвитком нового класу зброї – інформаційної, яка здатна ефективно впливати і на психіку, свідомість людей, і на інформаційно-технічну інфраструктуру суспільства й армії. Друга група інформаційно-технічних загроз для особистості, суспільства і держави – це новий клас соціальних злочинів, заснованих на використанні сучасної інформаційної технології (махінації з електронними грошима, комп'ютерне хуліганство та ін.). Третя – електронний контроль за життям, настроями, планами громадян, політичних організацій. Четверта – використання нової інформаційної технології у політичних цілях[16].

До наведеного варто додати те, що на думку вітчизняних експертів із проблем інформаційної безпеки, які аналізували іноземний вплив на інформаційний медіа- і кіберпростір України, на сьогодні наявні ознаки реальних загроз для нашої держави. Про це свідчать такі основні тенденції:

- цілеспрямоване формування окремими іноземними державами негативного міжнародного іміджу України;
- активізація критики вищого державного керівництва України;
- здійснення низкою зарубіжних країн потужного інформаційного тиску на Україну з метою спонукання українського керівництва до прийняття вигідних для цих країн рішень у внутрішньо- й зовнішньополітичній сферах;

[15] Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: навч. посібник. Київ :КНТ, 2006. С. 36.

[16] Дзьобань О. П. Інформаційна безпека у проблемному полі соціокультурної реальності: монографія. Харків : Майдан, 2010. С. 232.

- посилення інформаційних заходів із перешкоджання реалізації Україною її зовнішньополітичного курсу і спонукання до участі в проєктах, які в сучасних умовах не вигідні нашій державі;
- дискредитація нашої держави як конкурента у сфері міжнародного військово-технічного співробітництва;
- зростання для України загроз кібернетичних атак, що зумовлено появою нових, більш досконалих зразків кібернетичної зброї[17].

Вказане, звісно, загрожує існуванню держави як цілісного інституційного утворення. У той же час не менш потужними є загрози суспільній інформаційній безпеці країни, які мають дещо інші вектори впливу, їх руйнівний характер щодо функціонування держави є поліспрямованим і до певної міри латентним, а отже, вкрай небезпечним[18].

Підсумовуючи, можемо вказати, що «інформаційна війна» з Росією багато чому нас навчила, але й призвела до негативних наслідків. Так, в Україні заборонені російські ЗМІ і соціальні мережі, відомі випадки кіберпереслідування і судових процесів за обвинуваченням у державній зраді. Як не прикро, до цього додалося ще й те, що пандемія Covid-19 як загальнолюдське лихо не сприяла зменшенню загроз і припиненню нападів на журналістів, а інколи використовувалася місцевою владою як привід для ще більшого обмеження доступу до інформації. Як і раніше, стурбованість викликають і маніпуляції з новинами, порушення конфіденційності джерел, кібератаки і ексцеси в боротьбі з фейковими новинами. Крім того, контрольований сепаратистами схід країни перетворився на закриту зону без критично налаштованих журналістів та іноземних спостерігачів.

Отже, необхідність забезпечення інформаційної безпеки й захисту інформаційного суверенітету, як нами доведено, зумовлена формуванням інформаційного простору, необхідністю забезпечення національної безпеки України в цілому й існуванням загроз в інформаційній сфері держави, які можуть завдавати значної шкоди загальним національним інтересам. Як показує досвід провідних країн, розроблення виваженої і чіткої національної інформаційної стратегії сприятиме успішному вирішенню завдань у політичній, економічній, соціальній та інших сферах життя. Більш того, в умовах ведення сучасним російським керівництвом агресивної політики щодо України лише така могла б вплинути на позитивний хід подій і сприяти зменшенню впливу як внутрішньополітичних, так і зовнішніх факторів. Для своєчасного вирішення цих завдань у правовому, організаційному й організаційно-технічному аспектах Україні ще багато треба зробити. Зокрема, щоб захистити інформаційний простір треба створити системи управління національними інформаційними ресурсами, надійного захисту каналів державного управління, протидії інформаційним загрозам.

Список використаних джерел

Бібліографія:

1. Аналіз державної політики у сфері національної безпеки і оборони України. 2015 рік. URL: https://rpr.org.ua/wp-content/uploads/2018/02/Analiz-polityky-NB-pravl-final.pdf
2. Білорус О.Г. Глобалізація і національна стратегія України. Київ: ВО «Батьківщина»; Броди: Просвіта, 2001. 301 с.
3. Дзьобань О. П. Інформаційна безпека у проблемному полі соціокультурної реальності: монографія. Харків : Майдан, 2010. 260 с.
4. Косогов О.М. Пріоритетні напрями державної політики щодо забезпечення безпеки національного кібер-про-стору. Збірник наукових праць Харківського університету Повітряних Сил. 2014. Вип. 3. С.127–130.

[17] Косогов О.М. Пріоритетні напрями державної політики щодо забезпечення безпеки національного кіберпростору. Збірник наукових праць Харківського університету Повітряних Сил. 2014. Вип. 3. С.127–130.

[18] Мануйлов Є.М., Калиновський Ю.Ю. Роль і місце інформаційної безпеки у розбудові сучасної української держави. Вісник Національного юридичного університету «Юридична академія імені Ярослава Мудрого», Серія: Політологія. 2016. № 2(29). С. 145.

5. Країни-жертви та країни-агресори у хакерських війнах. URL: https://www.slovoidilo.ua/2021/10/22/infografika/svit/krayiny-zhertvy-ta-krayiny-ahresory-xakerskyx-vijnax
6. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: навч. посібник. Київ:КНТ, 2006. 280 с. С. 36
7. Мануйлов Є.М., Калиновський Ю.Ю. Роль і місце інформаційної безпеки у розбудові сучасної української держави. Вісник Національного юридичного університету «Юридична академія імені Ярослава Мудрого», Серія: Політологія. 2016. № 2(29). 330 с.
8. Національна безпека: світоглядні та теоретико-методологічні засади: монографія / за заг. ред. О.П. Дзьобаня. Харків: Право, 2021. 776 с.
9. Сіденко В.Р. Нові глобальні виклики та їх вплив на формування суспільних цінностей. Український соціум. 2014. №1(48). С. 7-22.
10. Тодика Ю.М. Народовладдя на трансформаційному етапі розвитку держави і суспільства : монографія. Харків : Право, 2007. 480 с.

Перелік юридичних документів:

11. Конституція України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text
12. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25.02.17 р. № 47/2017. Дата оновлення: 25.02.2017 р. URL: https://zakon.rada. gov.ua/laws/show/47/2017#Text (дата звернення : 08.09. 2020).
13. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20 січня 2012 року № 2-рп/2012. URL: https://zakon.rada.gov.ua/laws/show/v002p710-12#Text

References

Bibliography:

1. Analiz derzhavnoi polityky u sferi natsionalnoi bezpeky i oborony Ukrainy. 2015 rik. URL: https://rpr.org.ua/wp-content/uploads/2018/02/Analiz-polityky-NB-pravl-final.pdf
2. Bilorus O.H. Hlobalizatsiia i natsionalna stratehiia Ukrainy. Kyiv: VO «Batkivshchyna»; Brody: Prosvita, 2001. 301 s.
3. Dzoban O. P. Informatsiina bezpeka u problemnomu poli sotsiokulturnoi realnosti: monohrafiia. Kharkiv : Maidan, 2010. 260 s.
4. Kosohov O.M. Priorytetni napriamy derzhavnoi polityky shchodo zabezpechennia bezpeky natsionalnoho kiberprostoru. Zbirnyk naukovykh prats Kharkivskoho universytetu Povitrianykh Syl. 2014. Vyp. 3. S.127–130.
5. Krainy-zhertvy ta krainy-ahresory u khakerskykh viinakh. URL: https://www.slovoidilo.ua/2021/10/22/infografika/svit/krayiny-zhertvy-ta-krayiny-ahresory-xakerskyx-vijnax
6. Lipkan V. A., Maksymenko YU. YE., Zhelikhovskyi V. M. Informatsiina bezpeka Ukrainy v umovakh yevrointehratsii: navch. posibnyk. Kyiv:KNT, 2006. 280 s. S. 36
7. Manuilov YE.M., Kalynovskyi YU.YU. Rol i mistse informatsiinoi bezpeky u rozbudovi suchasnoi ukrainskoi derzhavy. Visnyk Natsionalnoho yurydychnoho universytetu «Yurydychna akademiia imeni Yaroslava Mudroho», Seriia: Politolohiia. 2016. № 2(29). 330 s.
8. Natsionalna bezpeka: svitohliadni ta teoretyko-metodolohichni zasady: monohrafiia / za zah. red. O.P. Dzobania. Kharkiv: Pravo, 2021. 776 s.
9. Sidenko V.R. Novi hlobalni vyklyky ta yikh vplyv na formuvannia suspilnykh tsinnostei. Ukrainskyi sotsium. 2014. №1(48). S. 7-22.
10. Todyka YU.M. Narodovladdia na transformatsiinomu etapi rozvytku derzhavy i suspilstva : monohrafiia. Kharkiv : Pravo, 2007. 480 s.

List of legal documents:

11. Konstytutsiia Ukrainy. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text
12. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku «Pro Doktrynu informatsiinoi bezpeky Ukrainy»: Ukaz Prezydenta Ukrainy vid 25.02.17 r. № 47/2017. Data onovlennia: 25.02.2017 r. URL: https://zakon.rada. gov.ua/ laws/show/47/2017#Text (data zvernennia : 08.09. 2020).
13. Rishennia Konstytutsiinoho Sudu Ukrainy u spravi za konstytutsiinym podanniam Zhashkivskoi raionnoi rady Cherkaskoi oblasti shchodo ofitsiinoho tlumachennia polozhen chastyn pershoi, druhoi statti 32, chastyn druhoi, tretoi statti 34 Konstytutsii Ukrainy vid 20 sichnia 2012 roku № 2-rp/2012. URL: https://zakon.rada.gov.ua/laws/show/v002p710-12#Text