УДК 340.12:316.352. 004.9
DOI: 10.31359/1993-0909-2023-30-1-91

Євген Анатолійович Гетьман
Національна академія правових наук України
Харків, Україна

Кафедра міжнародного приватного права та порівняльного правознавства
Національний юридичний університет імені Ярослава Мудрого
Харків, Україна

В'ячеслав Станіславович Політанський
Відділ науково-організаційного забезпечення діяльності президії, відділень та наукових установ
Національна академія правових наук України
Харків, Україна

Сектор теоретико-методологічних проблем організації державної влади
Науково-дослідний інститут державного будівництва та місцевого самоврядування
Національна академія правових наук України
Харків, Україна

Катерина Олегівна Гетьман
Відділення правознавство
Харківський фаховий автомобільно-дорожній коледж
Харків, Україна

ДО ПИТАННЯ ПРАКТИКИ СТАНОВЛЕННЯ ТА РОЗВИТКУ МІЖНАРОДНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ЯК ПРАВОВОГО МЕХАНІЗМУ ЗДІЙСНЕННЯ ЕЛЕКТРОННОГО УРЯДУВАННЯ

Анотація. *У статті досліджуються особливості становлення, розвитку та функціонування міжнародної інформаційної безпеки в практиці провідних країн світу, як одного з ключових правових механізмів здійснення електронного урядування. Досліджено міжнародну інформаційну безпеку разом із її основними елементами та моделями системи глобальної інформаційної безпеки. Проаналізован сучасні концепції міжнародної інформаційної безпеки. Встановлено, що в основу проблематики міжнародної інформаційної безпеки в широкому розумінні мають бути покладені принципи неподільності безпеки та відповідальності держав за свій інформаційний простір. Вивчено основні елементи та два основних підходи щодо змісту міжнародної інформаційної безпеки. За результатами досліджень аналітики визначено та проаналізовано загальні моделі системи глобальної інформаційної безпеки. Проаналізовано практику становлення та розвитку ін-*

формаційної безпеки в США та в країнах Європейського Союзу де ключовими напрямами розвитку інформаційної безпеки, стало забезпечення національної безпеки. Досліджено практику співробітництва України в галузі інформаційної безпеки з найбільш впливовими міжнародними організаціями. Відзначино, що транскордонний характер загроз інформаційній безпеці обумовлює необхідність вироблення і реалізації комплексних зусиль для ефективної протидії їм у взаємодії з міжнародними організаціями. Зроблено висновок про те, що внутрішні і зовнішні аспекти міжнародної інформаційної безпека, покликані надійно захищати культурне надбання кожної окремої країни світу, її інтелектуальну власність господарюючих суб'єктів і громадян, а також спеціальні відомості, що становлять державну і професійну таємницю. А також те, що інформаційна безпека, як сфера правового регулювання, апріорі не може розвиватись без врахування міжнародного правового поля та досвіду зарубіжних країн.

Ключові слова: *інформаційна безпека, електронне урядування, інформаційно-комунікаційні технології, система, досвід, захист.*

Yevhen A. Hetman
National Academy of Legal Sciences of Ukraine,
Kharkiv, Ukraine

Department of Private International Law and Comparative Law
Yaroslav Mudryi National Law University
Kharkiv, Ukraine

Viacheslav S. Politanskyi
Department of Scientific and Organizational Support of Presidium Activities,
Departments and Scientific Institutions
National Academy of Legal Sciences of Ukraine,
Kharkiv, Ukraine

Sector of Theoretical and Methodological Problems of the Organization of State Power
Scientific Research Institute of State Building AND Local Government
National Academy of Legal Sciences of Ukraine
Kharkiv, Ukraine

Kateryna O. Hetman
Department of jurisprudence
Kharkiv Vocational Automobile and Road College
Kharkiv, Ukraine

ON THE QUESTION OF THE PRACTICE OF ESTABLISHMENT AND DEVELOPMENT OF INTERNATIONAL INFORMATION SECURITY AS A LEGAL MECHANISM FOR THE IMPLEMENTATION OF ELECTRONIC GOVERNMENT

Abstract. *The article examines the peculiarities of the formation, development and functioning of information security in the practice of the leading countries of the world, as one of the key*

legal mechanisms for the implementation of e-government. International information security is studied as one of the key aspects of the international security system, along with its main elements and models of the global information security system. Modern concepts of international information security are analyzed. It was established that the principles of the indivisibility of security and the responsibility of states for their information space should be the basis of the problems of international information security in a broad sense. The main elements and two main approaches to the content of international information security have been studied. Based on the results of analytics research, general models of the global information security system have been defined and analyzed. The practice of formation and development of information security in the USA and in the countries of the European Union, where national security has become the key direction of information security development, has been analyzed. The practice of cooperation of Ukraine in the field of information security with the most influential international organizations was studied. It should be noted that the cross-border nature of threats to information security necessitates the development and implementation of complex efforts to effectively counter them in cooperation with international organizations. It was concluded that the internal and external aspects of international information security are designed to reliably protect the cultural heritage of each individual country of the world, its intellectual property of business entities and citizens, as well as special information constituting state and professional secrets. And also the fact that information security, as a field of legal regulation, a priori cannot develop without taking into account the international legal field and the experience of foreign countries.

Keywords*: informational security, electronic governance, information and communication technologies, system, experience, protection.*

ВСТУП

Сучасний етап розвитку суспільства характеризується зростаючою роллю інформаційної сфери, що представляє собою сукупність інформації, інформаційної інфраструктури, суб'єктів, здійснюють збір, формування, поширення і використання інформації, а також системи регулювання що виникає при таких суспільних відносинах.

Зміни, що відбулися в результаті комп'ютеризації за останні 30 років, виявилися такими глибокими й масштабними, що вони торкнулися серцевини соціального буття, способу життя людей, їх безпеки. Ці соціальні зміни знайшли теоретичне висвітлення у низці нових концепцій суспільного розвитку, що з'явилися наприкінці XX століття [1, с. 131].

Сьогодні назріла об'єктивна потреба у державно-правовому регулюванні науково-технологічної та інформаційної діяльності, що відповідала б реаліям сучасного світу та рівню розвитку інформаційних технологій, нормам міжнародного права, але водночас ефективно захищала б власні українські національні інтереси [2, с. 71]. Відносини, пов'язані із забезпеченням міжнародної інформаційної безпеки, як найважливіші на сьогодні для суспільства та держави вимагають найшвидшого дослідження та законодавчого регулювання. Крім того, у вітчизняній науці це питання є малодослідженим, а велика кількість вчених й досі не дійшли згоди з багатьох ключових питань представленої проблематики [3, с. 71].

Інформаційна безпека з одного боку виступає частиною концепції електронного урядуваня, з іншого є значно ширшим поняттям, яке з'явилося значно раніше досліджуваного нам явища. Питання інформаційної безпеки, що тим чи іншим чином стосуються легітимації політичної влади можуть бути розподілені на чотири великі групи. Електронне урядуваня, як вже неодноразово наголошувалося, тут виступає у своїх інструменталістських проявах, як модель організації взаємодії держави, громадян та бізнесу на основі використання можливостей ІКТ [4, с. 93].

Загальноприйнятним вважається той факт, що на сьогодні у світі сформувалося два основних підходи щодо змісту міжнародної інформаційної безпеки. Перша група країн демонструє підхід до проблематики міжнародної інформаційної безпеки в широкому розумінні, в основу якої мають бути покладені принципи неподільності безпеки та відповідальності держав за свій інформаційний простір. Друга група країн звужує питання міжнародної інформаційної безпеки до міжнародної кібербезпеки і такий підхід зосереджується на боротьбі із злочинами у сфері інформаційно-комунікаційних технологій, у т.ч. боротьбу із кібертероризмом. Як наслідок, при цих підходах простежується різне розуміння місця інформаційної безпеки людни в складній системі інформаційної безпеки як на міжнародному, так і на національному рівнях. Перший підхід, на нашу думку, передбачає узаконення значного простору для обмеження інформаційних прав і свобод людини на користь гарантування інформаційного безпеки міжнародної спільноти і окремих держав. При цьому прихильниками такого розвитку міжнародної політики виступають здебільшого держави, що мають значні проблеми щодо реалізації конституційних засад демократії, або ж взагалі не визнають демократичних цінностей.

Другий підхід визначається значно більшим соціальним і економічним спрямуванням, передбачає встановлення міжнародних стандартів для інформаційних прав та свобод людини (особливо пов'язаних з використанням мережі) на достатньо високому рівні. При цьому не передбачає втручання в питання інформаційного суверенітету, ведення інформаційних воєн та деякі інші аспекти політичної і військової сфери [5, с. 382–383].

Досліджуються практики становлення, розвитку та функціонування міжнародної інформаційної безпеки в практиці провідних країн світу, як одного з ключових правових механізмів здійснення електронного урядування є непростим, що пояснює його наукову малодослідженість. Окремі аспекти цього питання, у той чи інший спосіб досліджували такі закордоні і вітчизняні учені, як: V. Akhramovych [2], B. Cathy [4], T. Damian [4], T. Muzhanova [2], Y. Pepa [2], G. Shuklin [2], R. Tsagarousianou [4], S. Zozulia [2], О. Бусол [11], О. Г. Данильян [1], О. П. Дзьобань [1], О. Д. Довгань [13], І. М. Доронін [13], С. Б. Жданенко [1], І. М. Забара [6], О. О. Золотар [5], В. А. Ліпкан [16], Т. В. Попова [16], А. Федоров [8], І. Г. Ханін [7], В. Г. Щепанківський [10].

Мета статті полягає в дослідженні практики становлення й розвитку міжнародної інформаційної безпеки в практиці провідних країн світу й узагальнення існуючого масиву напрацювань з цієї проблематики відомих, вітчизняних і закордонних науковців й вчених, а також у надані авторських висновків.

1. МАТЕРІАЛИ ТА МЕТОДИ

Для досягнення сформульованих мети і завдань у дослідженні застосовуються загальнонаукові та спеціальні для правознавства методи та способи наукового пізнання. Це дозволило якнайретельніше проаналізувати всі питання стосовно особливостей практики становлення й розвитку міжнародної інформаційної безпеки в практиці провідних країн світу та можливої її рецепції для України. Так, історичний метод дав змогу встановити, що ідея міжнародної інформаційної безпеки зародилася ще у 50-ті роки XX ст., де головною метою її формування було забезпечення національної безпеки кожної країни світу. Де ще на початку XXI ст. в рамках Ради Європи була прийнята Конвенція про злочинність у сфері комп'ютерної інформації «Конвенція про кіберзлочинність» будучи фактично єдиним міжнародним документом у сфері захисту міжнародної інформаційної безпеки.

Діалектичний метод дав змогу дослідити й отримати нові знання про зміст та ідеї системи міжнародної інформаційної безпеки в США та країнах Європейського Союзу, яка є одними із ключових правових механізмів здійснення електронного урядування, тобто створення і підтримка відповідних інженерно-технічних потужностей та інформаційної організації, що відповідають реальним і потенційним загрозам, а також демографічному й економічному становищу країни.

Порівняльно-правовий метод використовувався для дослідження й порівняння систем інформаційної безпеки в США та країнах Європейського Союзу, що дало можливість встановити той факт, що інформаційна безпека більшості країн світу характеризується високим ступенем захищеності, стійкістю основних сфер життєдіяльності по відношенню до небезпечних інформаційних впливів.

Метод синтезу допоміг отримати нові знання про те, що міжнародна інформаційна безпека людини має на меті не стільки забезпечення збереження цілісності особи та її здатності до розвитку, а скільки збереження її інформації й даних про неї, при цьому враховуючи реалії становлення сучасного інформаційного суспільства.

Крім того, цей метод допоміг встановити, що сьогодні цілий ряд міжнародних організацій займаються питаннями розробки міжнародних стандартів і рекомендацій щодо посилення рівня міжнародної інформаційної безпеки.

Метод аналізу допоміг встановити, що в сучасних умовах рівень розвитку та безпека інформаційного простору країни є системоутворюючими факторами у забезпеченні безпеки, що активно впливають на стан політичної, економічної, воєнної, інформаційної та інших складових національної безпеки держави. Крім

того, інформаційна безпека є складним, системним, багаторівневим явищем, на стан і перспективи розвитку якого мають безпосередній вплив зовнішні і внутрішні чинники, найважливішими з яких є: 1) політична обстановка у світі; 2) наявність потенційних зовнішніх і внутрішніх загроз; 3) стан і рівень інформаційно-комунікаційного розвитку країни; 4) внутрішньополітична обстановка в державі.

Більш того, за допомогою методу аналізу явним стало те, що міжнародна інформаційна безпека в XXI столітті виходить на перше місце в системі національної безпеки держави, тому лише та держава може розраховувати на лідерство в економічній, військово-політичній та інших сферах, мати стратегічну і тактичну перевагу, гнучкіше регулювати економічні витрати на розвиток озброєнь і військової техніки, підтримувати перевагу з ряду передових технологій, яка має перевагу в засобах інформації та інформаційної боротьби. Крім того, ефективність системи забезпечення інформаційної безпеки будь якої держави стає вирішальним чинником в політиці будь-якого суб'єкта геополітичної конкуренції. Неефективність системи інформаційної безпеки може стати чинником, здатним привести до великомасштабних аварій і катастроф, наслідки яких можуть викликати, зокрема, дезорганізацію державного управління, крах національної фінансової системи тощо.

Метод узагальнення допоміг зробити висновок про те, що забезпечення інформаційної безпеки людини, суспільства і держави, на рівні національного законодавства і зусиллями виключно однієї держави, в сучасних умовах вбачається неефективним; оскільки загрози інформаційній безпеці набувають глобального виміру, отже вимагають спільних зусиль на міжнародному рівні.

2. РЕЗУЛЬТАТИ ТА ОБГОВОРЕННЯ

2.1 Місце інформаційної безпеки у системі міжнародної безпеки.

Загальновідомим є той факт, що інформаційна безпека людини є складовою частиною міжнародної інформаційної безпеки. Під міжнародною інформаційною безпекою в термінології ООН розуміється захищеність глобальної інформаційної системи від т.зв. «тріади загроз» – терористичних, злочинних і військово-політичних.

З цього приводу правильною є думка Золотар О. О., стосовно того, що інформаційна безпека людини у глобалізованому суспільстві належить до предметної сфери міжнародного публічного права. Тому серед джерел слід звернути увагу на 1) міжнародні договори, 2) міжнародно-правові звичаї і 3) загальні принципи права, а також 4) судові рішення і 5) доктрини найбільш кваліфікованих фахівців з публічного права різних націй як допоміжний засіб для визначення правових норм, що закріплені у пункті 1 статті 38 Статуту Міжнародного суду ООН в якості застосовуваних джерел міжнародного права, крім згаданих трьох основних джерел. До джерел міжнародного права також відносяться рішення (акти) міжнародних міжурядових організацій. Хоча вони і не застосовуються при розгляді

спорів Міжнародним судом ООН, в той же час виконують регуляторну функцію, визначаючи поведінку держав як основних суб'єктів міжнародного права [5, с. 299–300].

Тоді як на думку Забари І. М., сучасні концепції міжнародної інформаційної безпеки характеризуються однаковим усвідомленням і розумінням: 1) місця і значення інформаційних технологій, їх взаємозв'язку в рамках інформаційного простору (кіберпростору), ролі в реалізації загальної концепції інформаційного суспільства; 2) необхідності захисту найважливіших національних інфраструктур, глобальних інформаційно-комунікаційних мереж і систем, а також цілісності накопиченої інформації; 3) складності, серйозності та чисельності загроз для інформаційно-комунікаційних технологій (далі – ІКТ), пов'язаних як з процесами природнього і антропогенного характеру, так і діяльністю людини; 4) неефективності традиційних стратегій (таких, як заходи, що аналогічно застосовуються в процесі контролю за озброєнням або їх стримування); 5) державних завдань, що постають на національному і міжнародному рівнях; 6) необхідності об'єднання зусиль з метою збереження і розширення внеску, який ІКТ роблять у забезпечення безпеки і цілісності держав; 7) необхідності міжнародної взаємодії в питанні розробки стратегій зменшення ризиків для ІКТ [2].

Поруч із цим існує думка про те, що міжнародну інформаційну безпеку необхідно розглядати в якості одного з ключових аспектів системи міжнародної безпеки, що безумовно потребує міжнародно-правового регулювання. В основу проблематики міжнародної інформаційної безпеки в широкому розумінні мають бути покладені принципи неподільності безпеки та відповідальності держав за свій інформаційний простір. Таким чином, протидія загрозам військового (військово-політичного), терористичного і кримінального характеру з використанням ІКТ, повинна здійснюватись системно і узгоджено. Відповідно, міжнародно-правове регулювання повинно бути поширено на всі зазначені структурні елементи, і задля досягнення цього запропоновано прийняття міжнародної угоди на універсальному рівні. Прикладом реалізації такого поєднання виступає Угода між урядами держав-членів ШОС про співробітництво в області забезпечення міжнародної інформаційної безпеки від 16.06.2009, в якій знайшли відображення відповідні положення цієї концепції [5, с. 316].

При цьому до основних елементів міжнародної системи інформаційної безпеки, що формується, на думку І. Ханіна, слід відносити: 1) міжнародні доктринальні документи універсального характеру, присвячені інформатизації, інформаційному суспільству та інформаційній безпеці; 2) міжнародні стандарти у галузі інформаційної безпеки; 3) міжнародні професійні (спеціалізовані) установи, які займаються питаннями інформаційної безпеки у різних галузях; 4) міжнародно-регіональні інститути та структури, які створюються інтеграційними об'єднаннями (на прикладі, ЄС); 5) інститути, що створюються військово-політичними організаціями (на прикладі НАТО); 6) національні доктрини, концепції та стратегії [7].

Ще у серпні 2000 р. Всесвітня організація учених на своїй 25-й сесії у переліку загроз людству на перше місце поставила загрозу міжнародній інформаційній безпеці. Декілька разів Генеральна Асамблея ООН закликала світову спільноту обговорити проблему і прийняти рішення по усуненню можливості використання інформації в цілях не сумісних із забезпеченням безпеки людства. Прийняття таких рішень блокувалося державами, що домінують в інформаційній сфері і здійснюють активну розробку інформаційної зброї [8, с. 91].

Тому участь України в двосторонніх і багатосторонніх міжнародних структурах забезпечення як регіональної, так і власної інформаційної безпеки, є актуальним напрямом державної політики у цій галузі.

Важливо відзначити, що на початку XXI ст. у рамках Ради Європи була прийнята Конвенція про злочинність у сфері комп'ютерної інформації «Конвенція про кіберзлочинність» будучи фактично єдиним міжнародним договором, учасники якого не тільки члени Ради Європи, а й деякі інші країни. Україна підписала цю концепція 23.11.2001, ратифікувала її 10.03.2006, а вступила в силу вона аж 01.07.2006, згідно якої головною метою Ради Європи є досягнення більшої єдності між її членами [9].

Проблематика міжнародної інформаційної безпеки стабільно займає одне з центальной місць в порядку денному ШОС. Учасники організації ще в 2006-му на саміті в Шанхаї прийняли Заяву глав держав-членів ШОС по міжнародній інформаційній безпеці. У документі висловлювалася стурбованість «Використанням ІКТ з метою, що завдають шкоди безпеці людини, суспільства і держави ». Пріоритетною метою виражався намір держав скоординовано вживати заходів для реагування на загрози безпеки в інформаційній сфері. В ході подальших заходів ШОС приймалися нові документи, що регулюють поведінку держав у інформаційному просторі і відповідальне використання ІКТ, що базувався на єдиному баченні і довірі між країнами об'єднання. У 2009 році був підписаний основоположний документ, який визначив формат, цілі та принципи співробітництва країн Організації в галузі міжнародної інформаційної безпеки – Угода між урядами держав-членів Шанхайської організації співробітництва про співпрацю в області забезпечення міжнародної інформаційної безпеки [5, с. 323].

Слід підкреслити, що стратегії глобального інформаційного протиборства лежать в основі аналітичних розробок дослідницьких інституцій різних країн, метою яких є саме забезпечення інформаційного лідерства у сфері міжнародної безпеки. За результатами досліджень аналітики виділяють такі моделі системи глобальної інформаційної безпеки:

1) Модель А – створення абсолютної системи захисту країни – інформаційного лідера проти будь-якого виду наступальної інформаційної зброї, що обумовлює об'єктивні переваги в потенційній інформаційній війні, змушує інші країни шукати альянсу у військово-інформаційних діях з країною-інфолідером. При цьому може бути використано систему жорсткого контролю над інформаційним озбро-

єнням противника на підставі потенційних міжнародних документів з інформаційної безпеки;

2) Модель B – створення значної переваги держави – потенційного ініціатора інформаційної війни в наступальних видах озброєнь, у знешкодженні систем захисту держави-противника засобами інформаційного впливу, координація дій із союзними державами з використаннями визначених засобів інформаційної зброї для ідентифікації джерел і типів інформаційних загроз;

3) Модель C – наявність кількох країн – інфолідерів та потенційного протиборства між ними, визначення фактору стримування експансії інформаційних загроз, забезпечення в перспективі домінування однієї з держав у сфері міжнародної інформаційної безпеки з можливостями значного впливу на глобальну інфосферу та переважного права вирішення проблем глобального світового порядку;

4) Модель D – всі конфліктуючі сторони використовують транспарентність інформації для формування ситуативних альянсів, для досягнення переваг локальних рішень, які спроможні заблокувати технологічне лідерство, для використання можливостей інфоінфраструктури на окремих територіях з метою організації внутрішнього конфлікту між опозиційними силами (політичні, сепаратистські, міжнаціональні конфлікти) для проведення міжнародних антитерористичних інформаційних операцій;

5) Модель E – протиборство світової спільноти та міжнародної організованої злочинності, здатної контролювати перебіг політичних, економічних, суспільних і, зрештою, цивілізаційних процесів. Можливість такої моделі передбачена в дослідженні Національної ради розвідки США «Mapping the global future» – 2020 у версії «Коло страху» («Cycle of fear»), яка є найбільш песимістичним сценарієм майбутнього світової спільноти [9, с. 222–224].

Феномен міжнародної інформаційної безпеки обумовлюється стратегічною спрямованістю інформаційних озброєнь проти критично важливих структур життєдіяльності і функціонування міжнародного співтовариства, визнання інформаційної зброї як нового глобального виду зброї масового ураження, катастрофічного за наслідками свого застосування (деякі дослідники називають інформаційні озброєння «інформаційним апокаліпсисом»).

Тому, питання міжнародної інформаційної безпеки є вагомою складовою геополітичного образу країни у сфері міжнародних відносин і проявом тенденцій нових глобальних викликів і глибинних процесів [10, с. 228].

2.2 Практика становлення та розвитку інформаційної безпеки в США

Що стосується практики становлення та розвитку інформаційної безпеки в США, то з цього приводу існує декілька варіантів. Так на думку Бусола О., державна політика США у сфері інформаційної безпеки пройшла тривалий еволюційний шлях, який складається з чотирьох етапів: виникнення – 1939–1947 рр.; станов-

лення – 1947–1982 рр.; активний розвиток – 1983–2001 рр.; докорінне вдосконалення – 2001 р. – дотепер [11].

Її історичні корені сягають початку значно глибше, ніж утворення у 1957-му році військового агентства передових досліджень ARPA (Advanced Research Projects Agency), мережевий проект якої ARPANET і став першим кроком до повстання інтернету.

Очевидно, що ключовим напрямом розвитку інформаційної безпеки, стало забезпечення національної безпеки. Початки нормативно-правого регулювання сфері інформаційної безпеки сягають початку XX століття.

Зокрема, перший закон у сфері інформаційної безпеки держави – «Про захист інформації» був прийнятий у США ще в 1906 р. Проте інтенсивний розвиток законодавства щодо інформаційної безпеки розпочався після винайдення комп'ютерів та створення мережі ARPANET, в основу якої були покладені ідеї,спрямовані на: – цілковиту приватизацію і лібералізацію ринку інформаційних технологій, зокрема, підкреслювалась непотрібність громадського контролю за розвитком мереж і їх контенту; – первинну роль побудови мереж, на базі яких і розвиваються послуги (на відміну від європейської моделі, де відзначається пріоритетний розвиток сектора послуг, а вже потім – його технічного, мережевого забезпечення); – універсалізацію телекомунікаційного обслуговування для всіх [5, с. 331].

Важливою складовою системи правового забезпечення інформаційної безпеки США стало встановлення на федеральному рівні кримінальної відповідальності за злочини у сфері комп'ютерної інформації в Акті про підробку засобів доступу, комп'ютерне шахрайство та зловживання (Counterfeit Access Device and Computer Fraud and Abuse Act).

Важливою ознакою американської моделі правового забезпечення іфномраційної безпеки є пріоритет національних інтересів при вирішенні питань безпеки інформації (у тому числі і приватної). Зокрема, вже згадуваний Computer Security Act декларує, що вимоги державних органів щодо забезпечення необхідного рівня захисту інформації можуть бути поширені на будь-яку «важливу інформацію» [5, с. 333–334].

А початком сучасної цілеспрямованої систематичної організаційної діяльності у сфері інформаційної безпеки на національному рівні можна вважати директиви адміністрації Президента Білла Клінтона Presidential Decision Directive 63 (PDD 63) «Захист критично важливої інфраструктури» 1998 року, та підписаний на його основі «Загальнонаціональний план захисту інформаційних систем» у 2000 р., який визначив основні напрями діяльності держави та суспільства у сфері забезпечення інформаційної безпеки.

Суттєвих змін зазнала система інформаційної безпеки США після подій 11 вересня 2001 року. Актом про посилення повноважень спецслужб було визначено як одна з форм тероризму, несанкціоноване проникнення в державні комп'ютерні мережі з метою отримання вигоди чи нанесення шкоди, а також

суттєво збільшено повноваження ФБР США щодо моніторингу інтернету [5, с. 334–335].

Виходячи із цього, склалася думка про те, що практика формування політики США в сфері інформаційної безпеки поєднує в собі такі аспекти: зміцнення системи забезпечення інформаційної безпеки США; домінування США в глобальному інформаційному просторі; намагання поєднати ринкові інструменти в регулюванні інформаційної сфери з широкими повноваженнями держави в особі уповноважених органів по контролю над інформаційними ресурсами.

2.3 Практика становлення та розвитку інформаційної безпеки країн Європейського Союзу.

У свою чергу, що стосується практики впровадження інформаційної безпеки в країнах ЄС, то позиція, яка відображала її спільну європейську політику була окреслена Європейською Комісією в документі під назвою «Мережева та інформаційна безпека: європейський політичний підхід» у 2001 р. [12]. Під «мережевою та інформаційною безпекою» розумілись здатність мережі або інформаційної системи чинити опір випадковим подіям або зловмисним діям, які становлять загрозу доступності, аутентичності, цілісності та конфіденційності даних, що зберігаються або передаються, а також послуг, що надаються через ці мережі і системи. Більш широкий підхід до розуміння змісту поняття «інформаційна безпека» був висловлений представником Швеції при обговоренні питань міжнародної інформаційної безпеки на 56-й сесії Генеральної Асамблеї ООН, згідно з якою інформаційна та мережева безпека означає захист особистої інформації про відправників і одержувачів, захист інформації від несанкціонованих змін, захист від несанкціонованого доступу до інформації і створення надійного джерела постачання обладнання, послуг та інформації, а також охоплює захист інформації, що стосується військового потенціалу та інших аспектів національної безпеки. При цьому недостатній захист життєво важливих інформаційних ресурсів та інформаційних і телекомунікаційних систем, може створити загрозу міжнародній безпеці.

Також заслуговує на увагу Резолюція Ради ЄС № 2003/С 48/01 від 18.02.2003 про Європейський підхід до культури мережі та інформаційної безпеки, якою запропоновано державам-членам сприяти забезпеченню безпеки, як суттєвому аспекту в управлінні як на державному так і приватному рівні [5, с. 341].

Окрім того, у 2004 р. було створено європейське агентство по мережевій і інформаційній безпеці (ENISA) з метою підвищення ефективності функціонування внутрішнього ринку. Агентство виступає в ролі консультанта і центру передових технології у сфері мережевої і інформаційної безпеки для країн-членів і інститутів Євросоюзу. Крім того, агентство сприяє розвитку зв'язків між країнами-членами Євросоюзу, інститутами Євросоюзу, господарюючими суб'єктами і приватним бізнесом [13, с. 16].

У програмі «е-Європа 2005» констатувалось, що забезпечення інформаційної безпеки не є суто технологічною проблемою, вона стосується значною мірою людської поведінки, знання та передбачення погроз і засобів захисту [14].

У 2016 році Європейський парламент прийняв Директиву ЄС щодо мережевої та інформаційної безпеки, метою якої є встановлення загальних стандартів кібербезпеки та покращення співпраці між країнами ЄС [15]. Її положення мають допомогти компаніям більш ефективно боротися з хакерами та запобігати нападам на цифрову інфраструктуру, над якою мережа охоплює багато країн або весь Європейський Союз.

У свою чергу неможливо не відмітити доволі цікаву та правильну думку Т. В. Попової, В. А. Ліпкана, які у своїй спільній праці під інформаційною безпекою Європейського Союзу вважають захист особистої інформації про відправників і одержувачів, захист інформації від несанкціонованих змін, захист від несанкціонованого доступу до інформації і створення надійного джерела постачання обладнання, послуг та інформації. Інформаційна безпека Європейського Союзу також охоплює захист інформації, що стосується військового потенціалу та інших аспектів національної безпеки. Недостатній захист життєво важливий інформаційних ресурсів та інформаційних і телекомунікаційних систем може створити загрозу міжнародній безпеці. Позиція Європейського Союзу з приводу інформаційної безпеки відзначається раціоналізмом, адже предметом безпеки називаються конкретні поияття різних видів інформації. Крім того простежується доволі чітке чітке розмежування особливостей інформаційної безпеки людини і суспільства (особиста інформація, інформаційне забезпечення життя суспільства) та інформаційної безпеки держави (інформаційне забезпечення національної безпеки) [16, с. 138].

2.4 Питання забезпечення інформаційної безпеки в Україні

Варто зазначити, що на сьогодні законодавець постійно акцентує увагу на проблемі інформаційної безпеки в електронному урядуванні. Більш того, прагнення України бути повноцінним членом Європейського Союзу обумовлюють необхідність слідування європейським принципам, нормам і стандартам і у сфері управління інформаційним суспільством та захисту інформації.

Для України, яка зіткнулася з гібридом інформаційної війни, питання забезпечення інформаційної безпеки останнім часом набули важливого значення. Зважаючи на це, розроблення та вдосконалення основ забезпечення інформаційної безпеки України є одним із найважливіших та особливо актуальних завдань держави.

У межах нашого дослідження важливо відзначити, що транскордонний характер загроз інформаційній безпеці обумовлює необхідність вироблення і реалізації комплексних зусиль для ефективної протидії їм у взаємодії з міжнародними організаціями. Так, найбільш активне співробітництво України в галузі інформаційної безпеки спостерігається з НАТО в рамках програми «Безпека через науку».

Ця програма використовує такі механізми підтримки в галузі інформаційної безпеки: гранти на налагодження та укріплення зв'язків, які існують;візити експертів та трансфер технологій; створення дослідницьких центрів; підтримку проектів досліджень.

У цілому співробітництво між НАТО і країнами-партнерами, одним з яких є Україна, в рамках Ради євроатлантичного партнерства (РЄАП) та програми «Партнерство заради миру» (ПЗМ) передбачає певні зобов'язання сторін щодо обміну та захисту інформації. Для збільшення транспарентності військового планування й оборонних бюджетів, забезпечення демократичного контролю над збройними силами сторони можуть брати участь у взаємному обміні інформацією про виконання певних заходів. Перед обміном будь-якою таємною інформацією між країною-учасницею ПЗМ і НАТО, органи з безпеки інформації мають бути взаємно впевненими, що сторона, яка приймає інформацію, готова забезпечити захист інформації.

Приєднання України до програми ПЗМ передбачало підписання і ратифікацію у 2002 р. Угоди про безпеку між Урядом України і Організацією Північноатлантичного Договору [17]. Пізніше 27.04.2015 Україною була підписана і ратифікована Угода про співробітництво у сфері підтримки між Кабінетом Міністрів України та Організацією НАТО з підтримки та постачання (ОНПП) [18]. Згідно з цими угодами сторони погоджуються консультуватися в політичних питаннях і питаннях безпеки, розширювати й інтенсифікувати політичне і військове співробітництво в Європі, усвідомлюючи, що ефективність співробітництва в цих сферах має на увазі обмін таємною інформацією та/або інформацією обмеженого доступу.

Необхідно відмітити, що Угода про безпеку між Урядом України і Організацією Північноатлантичного Договору й Угода про співробітництво у сфері підтримки між Кабінетом Міністрів України та Організацією НАТО з підтримки та постачання (ОНПП) стали значними досягненнями України в галузі інформаційної безпеки і визначають основні вимоги щодо обміну таємною або конфіденційною інформацією між Україною та НАТО та її захисту і можуть стати основою прийняття відповідних документів у процесі подальшого співробітництва чи повної інтеграції України в Альянс.

ВИСНОВКИ

У сучасних умовах рівень розвитку та безпека інформаційного простору країни є системоутворюючими факторами у забезпеченні безпеки, що активно впливають на стан політичної, економічної, воєнної, інформаційної та інших складових національної безпеки держави. Тенденція забезпечення національної безпеки та її складових враховується провідними державами світу та оборонними блоками при модернізації власних стратегій, але назва документів, що розкривають зміст концепції національної безпеки, у державах різний. Зокрема, в США – це «Стратегія національної безпеки», Канаді – «Політика національної безпеки»,

Італії – «Стратегічна концепція національної оборони», Великобританії, Китаї та низці інших країн подібними документами є так звані «Білі книги». В Україні – «Біла книга», нова редакція від 8 червня 2012 року № 389/2012 «Стратегія національної безпеки України «Україна у світі, що змінюється» [19] і № 390/2012 «Військова доктрина України» [20] .

Саме тому, внутрішні і зовнішні аспекти міжнародної інформаційної безпека, покликані надійно захищати культурне надбання кожної окремої країни світу, її інтелектуальну власність господарюючих суб'єктів і громадян, а також спеціальні відомості, що становлять державну і професійну таємницю.

Підсумовуючи, зазначимо, що забезпечення інформаційної безпеки людини, суспільства і держави, на рівні національного законодавства і зусиллями виключно однієї держави, в сучасних умовах вбачається неефективним; оскільки загрози інформаційній безпеці набувають глобального виміру, отже вимагають спільних зусиль на міжнародному рівні.

Отже, склалася думка про те, що інформаційна безпека, як сфера правового регулювання, апріорі не може розвиватись без врахування міжнародного правового поля та досвіду зарубіжних країн. Це обумовлено самою істотою інформаційної сфери, яку складно обмежити національними кордонами в демократичній державі. При цьому важливо, що правове регулювання має відповідати не лише обраному політичному курсу, а й базуватись на існуючій суспільній практиці, відповідати нагальним інтересам громадян і запитам суспільства. Становлення правового забезпечення інформаційної безпеки людини відбувається в конкретних історичних умовах та невіддільне від правового статусу людини в державі, ступеня розвитку демократичних процесів та правової культури суспільства.

РЕКОМЕНДАЦІЇ

Цінність теми дослідження проявляється в тому, що серйозне занепокоєння викликає поширення фактів протизаконного збору і використання інформації, несанкціонованого доступу до інформаційних ресурсів, незаконного копіювання інформації в електронних системах, порушення технологій обробки інформації, запуску програм-вірусів, знищення та модифікації даних в інформаційних системах, маніпулювання суспільною та індивідуальною свідомістю тощо. Багато держав украй стурбовані станом інформаційної безпеки, залежність від якої зростатиме у процесі технічного прогресу. Вони розробляють і впроваджують комплекс правових, організаційно-технічних та економічних заходів забезпечення інформаційної безпеки. Тому актуальним постає питання захисту інформації за допомогою формування міцної інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

[1] Сучасне суспільство: філософсько-правове дослідження актуальних проблем : монографія / О. Г. Данильян, О. П. Дзьобань, С. Б. Жданенко та ін.; за ред. О. Г. Данильяна. Харків : Право, 2016. 488 с.

[2] Akhramovych V., Shuklin G., Pepa Y., Muzhanova T., Zozulia S. Devising a procedure to determine the level of informational space security in social networks considering interrelations among users. *Eastern-European Journal of Enterprise Technologies.* 2022. N 1(9-115). P. 63–74.
[3] Quezada-Tavárez K. Impact of the right of access on the balance between security and fundamental rights: Informational power as a tool to watch the watchers. *European Data Protection Law Review.* 2021. N 7(1). P. 59–73.
[4] Tsagarousianou R., Damian T., Cathy B. Cyberdemocracy: Technology, Cities, and Civic Networks. London and New York : Routledge, 1998. 324 p.
[5] Золотар О. О. Інформаційна безпека людини: теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018 446 с.
[6] Забара І. М. Міжнародна інформаційна безпека: сучасні концепції в міжнародному праві. *Теорія і практика правознавства*. 2013. Вип. 2. URL: http://nbuv.gov.ua/UJRN/tipp_2013_2_77 (дата звернення: 03.01.2023).
[7] Ханін І. Г. Формування міжнародної системи інформаційної безпеки: економічні орієнтири для України. URL: http://www.m.nayka.com.ua/?op=1&j=%20efektyvnaekonomika&s=ua&z=4457 (дата звернення: 03.01.2023).
[8] Федоров А. Семь тезисов противников «Международной информационной безопасности». *Международная жизнь*. 2001. №12. С. 89–92.
[9] Конвенція про кіберзлочинність. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text. (дата звернення: 03.01.2023).
[10] Щепанківський В. Г. Інформаційна безпека як складова сучасного образу країни. *Актуальні проблеми міжнародних відносин*. 2011. Вип. 102(1). С. 219–228.
[11] Бусол О. Інформаційна безпека США: законодавче регулювання та перспективи співпраці для України. URL: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2988:informatsijna-bezpeka-ssha-akonodavche-regulyuvannyata-perspektivi-spivpratsi-dlya-ukrajini&catid=8&Itemid=350 (дата звернення: 03.01.2023).
[12] Communication from the European Commission: «Network and Information Security: Proposal for a European Policy Approach». 2001, June 6. URL: http://ec.europa.eu/information_society/eeurope/2002/news_library/pdf_files/netsec_en (дата звернення: 03.01.2023).
[13] Довгань О. Д., Доронін І. М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту : монографія; НАПрН України, НДІІП Київ : Вид. дім «АртЕк». 2017. 107 с.
[14] EU: eEurope 2005 – An Information Society For All. Action Plan. URL: http://ec.europa.eu/information_society/eeurope/2005/all_about/action_plan/index_en.htm (дата звернення: 03.01.2023).
[15] The Directive on security of network and information systems (NIS Directive) URL:https://ec.europa.eu/digital-single-market/en/network-and-information-security-nisdirective (дата звернення: 03.01.2023).
[16] Попова Т. В., Ліпкан В. А. Стратегічні комунікації : словник / за заг. ред. В. А. Ліпкана. Київ : ФОП О. С. Яіпкан, 2016. 416 с.
[17] Угода про безпеку між Урядом України і Організацією Північноатлантичного Договору від 13.03.1995. URL: https://zakon.rada.gov.ua/laws/show/%20950_002#Text (дата звернення: 03.01.2023).
[18] Угода про співробітництво у сфері підтримки між Кабінетом Міністрів України та Організацією НАТО з підтримки та постачання (ОНПП) від 27.04.2015. URL: http://zakon.rada.gov.ua/laws/show/950_029 (дата звернення: 03.01.2023).

[19] Стратегія національної безпеки України «Україна у світі, що змінюється» : Указ Президента України від 08.06.2012 № 389/2012. URL: https://zakon.rada.gov.ua/laws/show/105/2007 (дата звернення: 03.01.2023).
[20] Воєнна доктрина України : Указ Президента України від 08.06.2012 № 390/2012. URL: http://zakon2.rada.gov.ua/laws/show/648/2004 (дата звернення: 03.01.2023).

REFERENCES

[1] Danylian, O. H., Dzoban, O. P., Zhdanenko. S. B. & and oth. (2016). *Modern society: a philosophical and legal study of current problems*. In O. H. Danyliana (Ed.). Kharkiv: Pravo.
[2] Akhramovych, V., Shuklin, G., Pepa, Y., Muzhanova, T., & Zozulia, S. (2022). Devising a procedure to determine the level of informational space security in social networks considering interrelations among users. *Eastern-European Journal of Enterprise Technologies,* 1(9-115), 63–74.
[3] Quezada Tavárez, K. (2021). Impact of the right of access on the balance between security and fundamental rights: Informational power as a tool to watch the watchers. *European Data Protection Law Review,* 7(1), 59–73.
[4] Tsagarousianou, R., Damian, T., Cathy, B. (1998). *Cyberdemocracy: Technology, Cities, and Civic Networks*. London; New York: Routledge, 1998.
[5] Zolotar, O. O. (2018). *Human information security: theory and practice*. Kyiv: LLC «Publishing house»ArtEk.
[6] Zabara, I. M. (2013). International information security: modern concepts in international law. *Theory and practice of jurisprudence*, 2. Retrieved from http://nbuv.gov.ua/UJRN/tipp_2013_2_77.
[7] Khanin, I. H. *Formation of the international system of information security: economic guidelines for Ukraine*. Retrieved from http://www.m.nayka.com.ua/?op=1&j=%20efektyvnaekonomika&s=ua&z=4457
[8] Fedorov, A. (2001). Seven theses of opponents of «International Information Security». *International life*, 12, 89–92.
[9] Cybercrime Convention. Retrieved from https://zakon.rada.gov.ua/laws/show/994_575#Text
[10] Shchepankivskyi, V. H. (2011). Information security as a component of the modern image of the country. *Actual problems of international relations*, 102(1), 219–228.
[11] Busol, O. Information security of the USA: legislative regulation and prospects for cooperation for Ukraine. Retrieved from http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2988:informatsijna-bezpeka-ssha-akonodavche-regulyuvannyata-perspektivi-spivpratsi-dlya-ukrajini&catid=8&Itemid=350
[12] Communication from the European Commission: «Network and Information Security: Proposal for a European Policy Approach» (2001, June). Retrieved from http://ec.europa.eu/information_society/eeurope/2002/news_library/pdf_files/netsec_en
[13] Dovgan, O. D., Doronin, I. M. (2017). *Escalation of cyber threats to the national interests of Ukraine and legal aspects of cyber protection*. Kyiv: Publishing house «ArtEk».
[14] EU: eEurope 2005 – An Information Society For All. Action Plan. Retrieved from http://ec.europa.eu/information_society/eeurope/2005/all_about/action_plan/index_en.htm
[15] The Directive on security of network and information systems (NIS Directive). Retrieved from https://ec.europa.eu/digital-single-market/en/network-and-information-security-nisdirective

[16] Popova, T. V., & Lipkan, V. A. (2016). Strategic communications: a dictionary. In V. A. Lipkan (Ed.). Kyiv: FOP OS Yaipkan.
[17] Security Agreement between the Government of Ukraine and the North Atlantic Treaty Organization (1995, March). Retrieved from https://zakon.rada.gov.ua/laws/show/%20950_002#Text
[18] Agreement on cooperation in the field of support between the Cabinet of Ministers of Ukraine and the NATO Support and Supply Organization (SSO) (2015, April). Retrieved from http://zakon.rada.gov.ua/laws/show/950_029
[19] National Security Strategy of Ukraine «Ukraine in a Changing World»: Decree of the President of Ukraine (2012, June). Retrieved from https://zakon.rada.gov.ua/laws/show/105/2007
[20] Military doctrine of Ukraine: Decree of the President of Ukraine (2012, June). Retrieved from http://zakon2.rada.gov.ua/laws/show/648/2004 (data zvernennia: 03.01.2023).

Євген Анатолійович Гетьман
Доктор юридичних наук, професор
Головний учений секретар
Член-кореспондент Національної академії правових наук України
Національна академія правових наук України
61024, вул. Пушкінська, 70, Харків, Україна

Кафедра міжнародного приватного права та порівняльного правознавства
Національний юридичний університет імені Ярослава Мудрого
61024, вул. Пушкінська, 77, Харків, Україна

В'ячеслав Станіславович Політанський
Кандидат юридичних наук
Начальник відділу науково-організаційного забезпечення діяльності президії відділень та наукових установ
Національна академія правових наук України
61024, вул. Пушкінська, 70, Харків, Україна

Провідний науковий співробітник
Науково-дослідний інститут державного будівництва
та місцевого самоврядування
Національної академія правових наук України
61002, вул. Чернишевська, 80, Харків, Україна

Катерина Олегівна Гетьман
Кандидат юридичних наук
Відділення правознавство
Харківський фаховий автомобільно-дорожній коледж
610201, вул. Котельниковська, 3 Харків, Україна

Yevhen A. Hetman
Doctor of Legal Science, Professor
Chief Scientific Secretary
Corresponding Member National Academy of Legal Sciences of Ukraine
National Academy of Legal Sciences of Ukraine
61024, 70 Pushkinska Str., Kharkiv, Ukraine

Department of Private International Law and Comparative Law
Yaroslav Mudryi National Law University
61024, 77 Pushkinska Str., Kharkiv, Ukraine

Viacheslav S. Politanskyi
Candidate of Legal Sciences
Head of the Department scientific and organizational support
for the activities of the presidium, departments and scientific institutions
National Academy of Legal Sciences of Ukraine
61024, 70 Pushkinska Str., Kharkiv, Ukraine

Leading Researcher
Research Institute of State Construction and local self-government
National Academy of Legal Sciences of Ukraine
61002, 80 Chernyshevska Str., Kharkiv, Ukraine

Kateryna O. Hetman
Candidate of Legal Sciences
Department of jurisprudence
Kharkiv Vocational Automobile and Road College
610201, 3 Kotelnikovska Str. Kharkiv, Ukraine

Рекомендоване цитування: Гетьман Є. А., Політанський В. С., Гетьман К. О. До питання практики становлення та розвитку міжнародної інформаційної безпеки, як правового механізму здійснення електронного урядування. *Вісник Національної академії правових наук України*. 2023. Т. 30. № 1. С. 91–108.

Suggested Citation: Hetman, Ye.A., Politanskyi V. S., & Hetman K. O. (2023). To the question of the practice of establishing and developing international information security as a legal mechanism for implementing electronic governance. *Journal of the National Academy of Legal Sciences of Ukraine*, 30(1), 91–108.

Стаття надійшла / Submitted: 02/02/2023
Доопрацьовано / Revised: 02/03/2023
Схвалено до друку / Accepted: 24/03/2023