УДК 341.232

DOI: 10.26565/2075-1834-2020-29-38

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА СИСТЕМИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ (МІЖНАРОДНИЙ І ЗАРУБІЖНИЙ ДОСВІД)

Войціховський А. В.,
кандидат юридичних наук, доцент,
професор кафедри конституційного
і міжнародного права факультету № 4
Харківського національного університету
внутрішніх справ,
Харків, проспект Льва Ландау, 27,
e-mail: voitsihovsky@gmail.com
orcid: https://orcid.org/0000-0001-5629-8852

АНОТАЦІЯ: стаття присвячена дослідженню правових і організаційних засад забезпечення інформаційної безпеки держав у сучасних умовах розвитку інформаційного суспільства. Проаналізовано теоретичні підходи до визначення сутності «інформаційна безпека» і «національна безпека», а також доведено їх взаємозв'язок.

Актуальність обраної теми наукового дослідження обумовлена тим, що протистояння в інформаційній сфері стає принципово новою сферою суперництва між державами. Швидкі темпи розвитку інформаційно-комунікаційних технологій, створення глобального інформаційного простору призвело до виникнення багатьох кібернетичних загроз у важливих сферах політичного, економічного, соціального, культурного життя суспільства. В роботі наведено результати аналізу інформаційної безпеки держави як чинника впливу на національну безпеку держави в цілому і, тим самим визначено інформаційну безпеку як складову частину національної безпеки.

З урахуванням масштабів глобального інформаційного виклику, неможливість вирішення зазначених проблем зусиллями окремих держав, у статті досліджується питання міжнародного співробітництва забезпечення міжнародної інформаційної безпеки у межах Організації Об'єднаних Націй. Розкривається зміст основних міжнародно-правових актів, прийнятих Генеральною Асамблеєю ООН, які вказують на загрози міжнародній безпеці інформаційного простору і необхідність прийняття державами спільних дієвих заходів у протидії викликам у зазначеній сфері.

Окрема увага в статті приділяється особливостям регіонального співробітництва держав у забезпеченні інформаційної безпеки в межах Європейського Союзу. Визначається, що цей напрям діяльності ЄС є одним із пріоритетних на сьогодні. Проаналізовані основні нормативно-правові акти ЄС, у яких представлений європейський підхід до проблеми забезпечення інформаційної безпеки. Дається загальна характеристика діяльності спеціалізованих органів ЄС (Європейське агентство з питань мережевої та інформаційної безпеки – ENISA, Європейський центр боротьби з кіберзлочинністю), діяльність яких направлена на забезпечення інформаційної безпеки.

У статті досліджуються питання гарантування інформаційної безпеки України та захисту національного інформаційного простору. Розкриваються види реальних і потенційних інформаційних загроз для інформаційного простору України, а також надано практичні рекомендації щодо вдосконалення державної інформаційної політики та створення ефективної системи протидії загрозам кіберпростору.

Акцентується увага на тім, що державна інформаційна політика повинна відбивати нагальні питання, що склалися у міжнародній інформаційній сфері та сфері забезпечення інформаційної безпеки. Ефективна реалізація стратегічних пріоритетів, основних принципів і завдань державної політики інформаційної безпеки потребує вдосконалення правових та організаційних механізмів управління інформаційною безпекою.

КЛЮЧОВІ СЛОВА: інформаційна безпека, національна безпека, кібербезпека, інформаційний простір, кіберпростір, інформаційне суспільство, об'єкти критичної інфраструктури, Організація Об'єднаний Націй, Європейський Союз.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК СОСТАВЛЯЮЩАЯ СИСТЕМЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ (МЕЖДУНАРОДНЫЙ И ЗАРУБЕЖНЫЙ ОПЫТ)

Войциховский А. В.,
кандидат юридических наук, доцент,
профессор кафедры конституционного
и международного права факультета № 4
Харьковского национального университета
внутренних дел,
Харьков, проспект Льва Ландау, 27,
e-mail: voitsihovsky@gmail.com
orcid: https://orcid.org/0000-0001-5629-8852

АННОТАЦИЯ: статья посвящена исследованию правовых и организационных основ обеспечения информационной безопасности государств в современных условиях развития информационного общества.

Проанализированы теоретические подходы к определению сущности «информационная безопасность» и «национальная безопасность». Приведены их связь и определено влияние информационной безопасности на национальную безопасность государства. Информационная безопасность рассматривается как составляющая национальной безопасности страны, а также как глобальная проблема защиты устойчивости международного информационного пространства.

Значительное внимание в статье уделяется анализу особенностей сотрудничества государств в обеспечении информационной безопасности в рамках ООН и ЕС. Раскрывается содержание основных международно-правовых актов, принятых этими организациями в сфере обеспечения международной информационной безопасности. Дается общая характеристика специальных органов ООН и ЕС, деятельность которых направлена на противодействие угрозам киберпространства.

Исследуются вопросы обеспечения информационной безопасности Украины и защиты национального информационного пространства. Раскрываются виды реальных и потенциальных информационных угроз информационного пространства Украины, а также даны практические рекомендации по совершенствованию государственной информационной политики и создания эффективной системы противодействия угрозам киберпространства.

КЛЮЧЕВЫЕ СЛОВА: информационная безопасность, национальная безопасность, кибербезопасность, информационное пространство, киберпространство, информационное общество, объекты критической инфраструктуры, Организация Объединенный Наций, Европейский Союз.

INFORMATION SECURITY AS COMPONENT NATIONAL SECURITY SYSTEMS (INTERNATIONAL AND FOREIGN EXPERIENCE)

Andrii Voitsikhovskyi,
Ph.D. in Law,
Associate Professor of the Department
of Constitutional and International Law
of Faculty 4 of Kharkiv National University
of Internal Affairs,
Kharkiv, Lev Landau avenue, 27,
e-mail: voitsihovsky@gmail.com
orcid: https://orcid.org/0000-0001-5629-8852

ANNOTATION: the article is devoted to the research of legal and organizational principles of ensuring information security of states in the modern conditions of development of information society. Theoretical approaches to the definition of the essence of «information security» and «national security» are analyzed and their interrelation is proved.

The urgency of the chosen topic of scientific research is caused by the fact that confrontation in the information sphere becomes a fundamentally new sphere of competition between the states. The rapid pace of development of information and communication technologies, creation of a global information space has led to many cybernetic threats in important spheres of political, economic, social and cultural life of society. The paper presents the results of the analysis of information security of the state as a factor of influence on the national security of the state as a whole, and thus defines information security as an integral part of national security.

Given the magnitude of the global information challenge, the inability to address these issues through the efforts of individual states, the article explores the issue of international cooperation in providing international information security within the United Nations. The contents of the basic international legal acts adopted by the UN General Assembly, which indicate the threats to the international security of the information space and the need for the states to take joint action to counter the challenges in the field.

Particular attention is paid to the peculiarities of regional cooperation of states in providing information security within the European Union. It is determined that this area of EU activity is one of the priorities for today. The main EU normative acts are analyzed, which present the European approach to the problem of information security. The general characteristics of the activities of the special bodies of the EU (European Union Agency for Network and Information Security - ENISA, European Cybercrime Centre), whose activities are aimed at providing information security, are given.

The article explores the issues of guaranteeing information security of Ukraine and protection of the national information space. The types of real and potential information threats to the information space of Ukraine are revealed, as well as practical recommendations are given on improving the state information policy and creating an effective system of counteracting cyberspace threats.

Emphasis is placed on the fact that state information policy should reflect urgent issues that have arisen in the international information and information security sphere. Effective implementation of strategic priorities, basic principles and tasks of the state information security policy requires improvement of legal and organizational mechanisms of information security management.

KEY WORDS: information security, national security, cybersecurity, information space, cyberspace, information society, critical infrastructure, United Nations, European Union.

Постановка проблеми. У сучасному світі кіберпростір, який не знає державних кордонів, стає найважливішим полем політичної, економічної, інформаційної та культурної конкуренції. По суті, кіберпростір завдяки швидким темпам розвитку інформаційно-комунікаційних технологій став простором нового «віртуального» типу, в якому стикаються інтереси різних політичних сил і різних

держав. Окрім того, багато протистоянь між розвідувальними відомствами різних країн, їх військовими структурами, а також економічні та інформаційні битви, включаючи економічне шпигунство і фінансові диверсії, розгортаються саме в кіберпросторі. Ця обставина визначає високу значимість процесів, що протікають в інформаційному просторі, для сучасного політичного аналізу, теорії і практики політичної науки і визнання інформаційної безпеки як елементу системи національної безпеки держави.

Актуальність. Актуальність обраної теми наукового дослідження обумовлена тим, що протистояння в інформаційній сфері стає принципово новою сферою протиборства між державами. Терміни та визначення з приставкою «кібер...» стали широко використовуватися як в міжнародних, так і у внутрішньодержавних дискусіях і документах, а також знайшли своє відображення в стратегічних доктринах окремих держав і міжнародних організацій (Організація Об'єднаних Націй, Європейський Союз, Рада Європи, Організація Північноатлантичного договору тощо).

Для України, яка зіткнулася із інформаційною війною, питання забезпечення інформаційної безпеки набули більш важливого значення. Зважаючи на це, розробка та вдосконалення основ забезпечення інформаційної безпеки є одним із найважливіших завдань держави.

Мета статті. Метою наукової статті є здійснення політико-правового аналізу сучасних загроз інформаційній безпеці та основних напрямів державної інформаційної політики в контексті забезпечення національної безпеки.

Завдання. Мета наукової статті досягається через виконання таких завдань: проаналізувати теоретичні підходи до визначення сутності «інформаційна безпека» і «національна безпека»; визначити вплив інформаційної безпеки на національну безпеку держави; дати загальну характеристику організаційно-правової основи міжнародного співробітництва держав у забезпеченні інформаційної безпеки в межах ООН і ЄС; дослідити питання забезпечення інформаційної безпеки України, з'ясувати види реальних і потенційних інформаційних загроз для інформаційного простору України, а також розробити практичні рекомендації щодо вдосконалення державної інформаційної політики.

Огляд праць з даної проблематики. Дослідження сучасних загроз інформаційній безпеці держави ґрунтується на наукових здобутках відомих дослідників у сфері міжнародного права, безпекознавства, політології, соціології, теорії управління тощо, таких як О. Бандурка, І. Боднар, О. Волеводз, В. Горбулін, І. Забара, О. Запорожець, І. Івченко, У. Ільницька, Р. Калюжний, А. Качинський, В. Конах, В. Ліпкан, А. Марущак, Г. Новицький, В. Пилипчук, Є. Скулиш, М. Стрельбицький, О. Тихомиров, Т. Ткачук та інші науковці, які присвятили свої праці питанням забезпечення національної безпеки. Серед зазначених авторами тем значне місце посідають теоретичні питання з окремих аспектів міжнародно-правових проблем забезпечення інформаційної безпеки, а також питання співробітництва в рамках окремих міжнародних організацій. Водночас, оскільки загрози інформаційній безпеці держави в сучасних умовах розвитку інформаційного суспільства є динамічними та постійно змінюються, відповідна проблематика наукових досліджень не втрачає своєї актуальності і донині.

Виклад основного матеріалу. У сучасній світоглядно-філософській думці існують два основні підходи до розуміння поняття «національна безпека». Фундатором першого, *реалістичного підходу* до розуміння даного поняття, є американський фахівець у галузі політичних наук Г. Моргентау, який визначив національну безпеку як недоторканність території та інститутів держави, зробивши наголос на воєнну і політичну безпеку, що складає традиційне розуміння. Другий підхід – *Human Security* – розвивався в межах ідеалістичної теорії міжнародних відносин і позначався аналізом воєнних, політичних, економічних, соціальних, гуманітарних, екологічних проблем [10].

Український законодавець, виходячи з другого підходу, за роки державної незалежності сформував потужну правову базу політики національної безпеки, основою для якої є чинна Конституція України. Зокрема, в ч. 1 ст. 3 Конституції України сформульовано концептуальні засади забезпечення безпеки людини: «людина, її життя і здоров'я, честь і гідність, недоторканість і безпека визначаються в Україні найвищою цінністю» [14]. У ч. 1 ст. 17 Конституції України чітко передбачено, що: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» [14].

Правові засади національної безпеки України регламентуються Законом України «Про національну безпеку України» від 21 червня 2018 р. [13], в якому визначено понятійний апарат у сфері національної безпеки. До основних категорій, які становлять зміст національної безпеки України віднесено: «національна безпека України», «національні інтереси України», «державна безпека», «громадська безпека і порядок», «воєнна безпека» тощо.

Відповідно до п. 9 ч. 1 ст. 1 Закону України «Про національну безпеку України» під національною безпекою України розуміється: «захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз» [13]. При цьому в п. 6 ч. 1 ст. 1 даного Закону дається визначення загрозам національної безпеки України, а саме: «явища, тенденції і чинники, що унеможливлюють чи

ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України» [13].

Виходячи з цих положень до об'єктів національної безпеки України слід віднести: *людина і громадянин* – їхні конституційні права і свободи та обов'язки; *суспільство* – його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності, інформаційне і навколишнє природне середовище і природні ресурси; *держава* – її конституційний лад, суверенітет, територіальна цілісність і недоторканність.

Оскільки національна безпека є комплексною системою, то вона має свої чисельні підсистеми, елементи, складові. До основних елементів національної безпеки можна віднести політичну, економічну, воєнну, соціальну, екологічну, інноваційну, науково-технологічну безпеку [17, с. 48].

Зважаючи на стрімкий розвиток інформаційно-комунікаційних технологій, тотальну комп'ютеризацію, створення глобального інформаційного простору були сформовані принципово нові субстанції – інформаційне суспільство, кіберпростір, що мають безмежний потенціал і значний вплив на політичний, економічний, соціальний і культурний розвиток держави. Саме створення інформаційного суспільства призвело до виникнення багатьох кіберзагроз у важливих сферах життєдіяльності суспільства (банківська, воєнна, критична інфраструктура тощо), тому до національної безпеки держави цілком виправдано відносять інформаційну безпеку як самостійний елемент національної безпеки.

Інформаційна безпека визнається правовим поняттям. Під ним розуміється стан захищеності національних інтересів України в інформаційній сфері, що визначається сукупністю збалансованих інтересів особистості, суспільства і держави [16, с. 4].

Глобалізація сучасного інформаційного простору призводить до послаблення інформаційного суверенітету держави, а рівень розвитку та безпека інформаційного простору впливають на стан безпеки будь-якої держави взагалі. Саме тому, одним із напрямів міжнародної діяльності в інформаційній сфері є формування та удосконалення системи заходів міжнародної інформаційної безпеки.

Враховуючи масштаби глобального інформаційного виклику, неможливість вирішення зазначених проблем зусиллями однієї або навіть декількох держав, слід усвідомити необхідність розвитку міждержавного співробітництва в сфері забезпечення міжнародної інформаційної безпеки в межах *Організації Об'єднаних Націй*, здатної комплексно вирішувати будь-які політичні проблеми, при найширшому представництві і максимально враховуючи інтереси всієї світової спільноти.

Ідея забезпечення міжнародної інформаційної безпеки вперше отримала практичну реалізацію в Резолюції Генеральної Асамблеї ООН A/RES/53/70 «Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки» від 4 грудня 1998 р. Цей документ започаткував спільне обговорення питань створення абсолютно нового міжнародно-правового режиму, структурним елементом якого в перспективі стали інформація, інформаційна технологія і методи її використання [19].

Резолюція Генеральної Асамблеї ООН A/RES/54/49 «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки» від 1 грудня 1999 р. вперше вказала на загрози міжнародній безпеці інформаційного простору стосовно не лише до цивільної, а також до військової сфери [20].

У виконання цієї Резолюції в 2000 р. в Секретаріаті ООН були представлені «Принципи, що стосуються міжнародної інформаційної безпеки», які були опубліковані в доповіді Генерального секретаря ООН від 10 червня 2000 р. для їх подальшого спільного обговорення. Принципи визначають правила поведінки держав в інформаційному просторі, створюючи для них відповідні моральні зобов'язання, а також закладають основу для міжнародних переговорів під егідою ООН та інших міжнародних організацій з проблем інформаційної безпеки. Вперше були наведені такі визначення понятійного апарату системи міжнародної інформаційної безпеки, як: «інформаційний простір», «інформаційний ресурс», «інформаційна війна», «інформаційна зброя», «інформаційна безпека», «загроза інформаційної безпеки», «міжнародна інформаційна безпека», «неправомірне використання інформаційно-телекомунікаційних систем», «несанкціоноване втручання в інформаційно-телекомунікаційні системи та інформаційні ресурси», «критично важливі структури», «міжнародний інформаційний тероризм» і «міжнародна інформаційна злочинність» [23].

Подальші сесії Генеральної Асамблеї ООН продовжували розпочату дискусію та пошук шляхів вирішення проблем, які знайшли своє закріплення у наступних резолюціях та доповідях. Питання, пов'язані з міжнародною інформаційною безпекою були предметом розгляду багатьох сесій Генеральної Асамблеї ООН, про що свідчать ухвалені резолюції: A/RES/55/63 від 4 грудня 2000 р. і A/RES/56/121 від 19 грудня 2001 р. про боротьбу зі злочинним використанням інформаційних технологій, A/RES/57/239 від 20 грудня 2002 р. про створення глобальної культури кібербезпеки, A/RES/58/199 від 23 грудня 2003 р. і A/RES/64/211 від 21 грудня 2009 р. про створення глобальної культури кібербезпеки і захисту найважливіших інформаційних інфраструктур, A/RES/62/17 від 5 грудня 2007 р. про сприяння розгляду на багатосторонньому рівні існуючих та потенційних загроз у сфері інформаційної безпеки, A/RES/71/28 від 5 грудня 2016 р. про досягнення в сфері інформатизації та телекомунікацій в контексті міжнародної

безпеки тощо.

Активну політику щодо забезпечення інформаційної безпеки проводить й *Європейський Союз*. Гарантування міжнародної інформаційної безпеки та її складової – кібербезпеки стало одним із пріоритетних напрямів діяльності ЄС.

У 2001 р. Комісією ЄС було представлено перший документ під назвою «Мережева та інформаційна безпека: європейський політичний підхід», в якому була представлена концепція вирішення проблеми інформаційної безпеки. У документі використовується термін «мережева та інформаційна безпека», який трактується як здатність мережі або інформаційної системи чинити опір випадковим подіям або зловмисним діям, які становлять загрозу доступності, автентичності, цілісності та конфіденційності даних, що зберігаються або передаються, а також послуг, що надаються через ці мережі і системи [6].

У наступні роки органами ЄС було прийнято велику кількість нормативно-правових документів, які передбачають різноманітні підходи забезпечення інформаційної безпеки в державах-членів ЄС. Серед них можна назвати такі: Рамкове рішення Ради ЄС 2005/222/ЈНА щодо нападу на інформаційні системи від 24 лютого 2005 р., яка встановила мінімальні правила визначення кримінальних злочинів та санкцій у сфері неправомірного впливу на інформаційні системи [3]; Повідомлення Комісії ЄС «На шляху до загальної політики в сфері боротьби з кіберзлочинністю» від 22 травня 2007 р., в якому даються визначення терміну «кіберзлочинність» та основні напрями політики ЄС щодо інформаційної безпеки [8]; Повідомлення Комісії ЄС «Захист Європи від широкомасштабних кібератак та руйнувань: посилення рівня підготовленості, безпеки та стійкості» від 30 березня 2009 р., в якому визначено основні заходи для посилення безпеки та здатності європейської критичної інформаційної інфраструктури протистояти зовнішнім впливам [1]; Стратегія кібербезпеки ЄС «Відкритий, надійний та безпечний кіберпростір» від 07 лютого 2013 р., яка рекомендує державам-членам ЄС розвивати міждержавне співробітництво у протидії кіберзагрозам [4]; Директива Європейського парламенту і Ради ЄС щодо заходів по забезпеченню високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі від 6 липня 2016 р., яка закріпила єдині правила та вимоги в сфері кібербезпеки для всіх держав-членів ЄС (підвищення спроможності системи кібербезпеки на національному рівні, підвищення рівня європейського співробітництва і запровадження управління ризиками та зобов'язання сповіщати про кіберінциденти операторів базових послуг та провайдерів цифрових послуг тощо) [2]; Повідомлення Комісії ЄС «Стійкість, стримування та захист: створення сильної кібербезпеки для ЄС» від 13 вересня 2017 р., в якому визначається важливість кібербезпеки для процвітання та безпеки держав-членів ЄС і необхідність колективного та широкомасштабного підходу у протидії кіберзагрозам [7] тощо.

Задля вдосконалення системи інформаційної безпеки в рамках ЄС був сформований спеціалізований організаційний механізм. Важливу роль у ньому відіграє Європейське агентство з питань мережевої та інформаційної безпеки (ENISA), яке було створено 10 березня 2004 р. До завдань ENISA відноситься вдосконалення мережевої та інформаційної безпеки в ЄС, сприяння розвитку культури мережевої та інформаційної безпеки на користь громадян, споживачів, підприємств та громадських організацій ЄС, а також сприяння безперебійному функціонуванню внутрішнього ринку ЄС [5].

Усвідомлюючи той факт, що ефективність забезпечення інформаційної безпеки в європейському кіберпросторі також залежить від розвитку співпраці держав у рамках міжнародних органів у 2013 р. в структурі Європейського поліцейського офісу (Європол) був утворений *Європейський центр боротьби з кіберзлочинністю*. До пріоритетних напрямів діяльності Центру відноситься розслідування шахрайства через інтернет-мережі, а також розслідування злочинів, що посягають на безпеку критично важливої інфраструктури та інформаційних систем ЄС [12].

Слід відзначити, що ЄС сьогодні активно модернізує власні сектори безпеки у кіберпросторі у відповідності до викликів сучасності. Цей процес відбувається шляхом: впорядкування нормативної бази, що має забезпечити цілісність державної політики в даній сфері; вироблення європейських керівних принципів щодо забезпечення інформаційної безпеки; збільшення чисельності підрозділів, що забезпечують інформаційну безпеку; посилення контролю за національним інформаційним простором; зміцнення захисних механізмів для критичної інформаційної інфраструктури ЄС тощо.

Розуміючи актуальність проблеми забезпечення інформаційної безпеки як складової системи національної безпеки, більшість держав світу почали здійснювати внутрішньодержавні комплексні заходи з безпеки в кіберпросторі. Ці заходи пов'язані, перш за все, з розробкою і вдосконаленням національного законодавства в даній галузі і створенням спеціалізованих структур, що відповідають за безпеку в кіберпросторі.

Кібербезпека, на сьогодні, є стратегічною проблемою державного значення, яка зачіпає всі верстви населення. Державна політика з кібербезпеки служить засобом посилення національної безпеки і надійності інформаційних систем держави. Стратегії з кібербезпеки були прийняті такими державами як США, Швеція, Естонія, Фінляндія, Чехія, Франція, Німеччина, Литва, Великобританія, Канада, Японія, Індія, Австралія, Нова Зеландія, Колумбія тощо. Список країн наочно показує, що проблема кібербезпеки визнається актуальною в усьому світі [11, с. 3]. Не залишилась осторонь цієї проблеми й Україна, яка 15

березня 2016 р. схвалила Стратегію кібербезпеки України [22]. Цей документ визначає пріоритети та напрямки кібербезпеки і є важливим структурним елементом для формування політики інформаційної безпеки, яка відповідатиме світовому рівню.

Останнім часом для багатьох країн світу стало актуальним питанням захисту об'єктів критичної інфраструктури. Під *захистом об'єктів критичної інфраструктури* розуміються заходи щодо забезпечення безпеки взаємозалежних систем, мереж і активів, що лежать в основі служб, життєво необхідних для функціонування суспільства. Об'єкти критичної інфраструктури можуть бути військовими і цивільними, а також мати подвійне призначення. Як приклади життєво важливими об'єктами матеріальної інфраструктури можна назвати дороги, мости, аеропорти, споруди зв'язку, електростанції, банківська сфера, виробництво і розподіл електроенергії, медичні послуги, державні аварійно-рятувальні служби, а також повітряні і наземні перевезення тощо. З цього приводу, в Резолюції Ради Безпеки ООН S/RES/2341 (2017) «Про захист критичної інфраструктури» від 13 лютого 2017 р. зазначається, що «кожна держава сама визначає, які об'єкти його інфраструктури є критично важливими і, як забезпечити їх ефективний захист…» [21]. Таким чином, сегменти інфраструктури, визначені в різних країнах, можуть різнитися від звичайного усвідомлення «стратегічних об'єктів». Наприклад, у США ця сфера, поряд з об'єктами, що забезпечують життєдіяльність суспільства, також включає в себе «Національні пам'ятники (статуї) і історичні площі», «Виборчу систему», дипломатичні місії, які також можуть стати об'єктом кібератак.

У сучасних умовах розвитку інформаційного суспільства об'єкти критичної інфраструктури не можуть існувати без інформаційної інфраструктури, тобто без комп'ютерів і мереж, представлених, в першу чергу, системами диспетчерського управління та збору даних, взаємозалежність яких дозволяє обмінюватися інформацією та здійснювати аналіз відповідно до всіх критично важливих функцій. Здійснення далекого доступу до управління такими об'єктами на користь підвищення ефективності та скорочення витрат відкрило критичну інфраструктуру для кіберзагроз. Нинішня геополітична арена перетворила кібератаки на критичну інфраструктуру в «кібервійну», оскільки потенціал для порушення критичної інфраструктури країни шляхом вимкнення електростанцій, руйнування нафтопроводів, навіть припинення постачання води та опалення комунальних підприємств може надати значну військову перевагу. Безперечно, що саме ці обставини в значній мірі можуть підірвати основи національної безпеки будь-якої країни світу.

Увага до проблеми забезпечення інформаційної безпеки не обійшла й Україну, яка останнім часом потерпає від антиукраїнського впливу, що пропагує ідею сепаратизму, насильства, національної ворожнечі і є спробами руйнування національної ідентичності України, знищення міжнаціональної злагоди, посягання на конституційний лад України, територіальну цілісність держави тощо. Проблема забезпечення інформаційної безпеки України актуалізувалася в умовах війни на Сході, коли з боку Російської Федерації відбувається інформаційна експансія, упереджене та тенденційне висвітлення фактів та явищ, а технології російських інформаційно-психологічних операцій спрямовані на забезпечення домінування в українському (а також у глобальному) інформаційному просторі та на утримання медійної переваги. Через російські пропагандистські інформаційно-психологічні кампанії, акції, медіазаходи відбувається вплив не лише на суспільну свідомість громадян України, а й на світову громадськість.

Окрім того, Україна одночасно з іншими державами 27 червня 2017 р. зазнала найбільшої хакерської атаки, яка поширила вірус Petya.A, що блокує роботу комп'ютерних систем. Кібератаки зазнали українські державні установи (Кабінет Міністрів України, Національна поліція України тощо), аеропорт «Бориспіль», Чорнобильська атомна електростанція, українські банки, енергетичні компанії, державні інтернет-ресурси і локальні мережі, українські медіа і ряд інших великих підприємств. Ця кібератака призвела до зараження комп'ютерів по всьому світу (США, Великобританія, Німеччина, Польща, Індія, Литва та ін.), і завдала збитків приблизно на 8 млрд. доларів США [9, с.143].

З урахуванням зазначених загроз заходи щодо забезпечення інформаційної безпеки України повинні здійснюватися шляхом: забезпечення інформаційного суверенітету України; удосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції; вживання комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України тощо.

Необхідно відзначити, що Україною вже були зроблені деякі практичні кроки у сфері забезпечення інформаційної безпеки. Так, з метою створення державної системи захисту об'єктів критичної

інфраструктури, порушення роботи яких може завдати шкоди національним інтересам України 6 грудня 2017 р. Розпорядженням Кабінету Міністрів України була схвалена Концепція створення державної системи захисту критичної інфраструктури [15]. У документі визначаються основні напрямки, механізми і строки комплексного правового врегулювання питання захисту критичної інфраструктури та створення системи державного управління в цій сфер.

Завдання практичної реалізації нових підходів у протидії загрозам критичної інфраструктури було визначено Законом України «Про національну безпеку України» від 21 червня 2018 р. [13]. Крім того, здійснюється підготовка проекту Закону «Про критичну інфраструктуру та її захист», який дозволить забезпечити створення необхідної для цього законодавчої бази. У разі прийняття цей Закон закріпить принципи та напрями розбудови державної системи захисту критичної інфраструктури, визначить правові та організаційні засади забезпечення її діяльності і стане складовою частиною законодавства України у сфері національної безпеки [18].

Висновки. Підсумовуючи викладений матеріал, потрібно зауважити, що в умовах сучасного розвитку інформаційного суспільства, захист національного інформаційного простору та забезпечення інформаційної безпеки вже стали пріоритетними стратегічними завданнями багатьох держав світу. Інформаційна безпека визнається невід'ємним елементом системи національної безпеки. При цьому, інформаційна безпека як складова національної безпеки держави може розглядатися як самостійна частина.

Міжнародний характер загроз інформаційної безпеки зумовлює необхідність вироблення спільної стратегії інформаційної безпеки і розвиток міждержавного співробітництва в рамках міжнародних організацій у зазначеній сфері.

Питання забезпечення інформаційної безпеки є вкрай важливими для української держави на сучасному етапі, що, насамперед, обумовлено необхідністю протистояти протиправним посяганням на інформаційний простір України. Зважаючи на те, що стратегічно визнаним пріоритетом зовнішньої політики України є європейська інтеграція, то завданням для української влади повинно стати розвиток ефективного діалогу з ЄС у питаннях забезпечення інформаційної безпеки. Окрім того, потрібно детально вивчати практичний досвід зарубіжних країн, які вже мають організаційно-правову основу щодо забезпечення інформаційної безпеки та максимально використати їхній досвід у національній законотворчості та здійсненні дієвих заходів у зазначеній сфері.

ЛІТЕРАТУРА

1. Communication from the Commission on Critical Information Infrastructure Protection «Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience» [Електронний ресурс]. – Режим доступу : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52009DC0149.
2. Concerning measures for a high common level of security of network and information systems across the Union [Електронний ресурс]. – Режим доступу : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.
3. Council framework decision 2005/222/JHA on attacks against information systems [Електронний ресурс]. – Режим доступу : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32005F0222.
4. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [Електронний ресурс]. – Режим доступу: https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.
5. European Union Agency for Network and Information Security [Електронний ресурс]. – Режим доступу : https://www.enisa.europa.eu/about-enisa.
6. Network and information security: proposal for a european policy approach [Електронний ресурс]. – Режим доступу : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52001DC0298&from=EN.
7. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU [Електронний ресурс]. – Режим доступу : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN.
8. Towards a general policy on the fight against cyber crime [Електронний ресурс]. – Режим доступу : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14560.
9. Voitsikhovskyi A., Bakumov O., Ustymenko O., Marchuk M. The Legal Mechanisms of Ensuring Regional Cooperation in Combatting Crime Within the Framework of the Council of Europe: Experience of Ukraine [Електронний ресурс]. – Режим доступу : http://www.cejiss.org/issue-detail/the-legal-mechanisms-of-ensuring-regional-cooperation-in-combatting-crime-within-the-framework-of-the-council-of-europe-experience-of-ukraine?fbclid=IwAR2el_dNrQwU_U5YpDji0GJcS7iVdch4mX1j_nesgmMWgAIN9uopNjJsEhk.
10. Блюменау Д.И. Информация: миф или реальность? (О состоянии понятий «знание» и «социальная информация»). [Текст] / Д. Блюменау // Научно-техническая информация. – 1985. - № 2. Сер. 2. - С. 1–4.
11. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века [Електронний ресурс]. – Режим доступу : https://cyberleninka.ru/article/n/kiberbezopasnost-kak-osnovnoy-faktor-natsionalnoy-i-mezhdunarodnoy-bezopasnosti-hh-veka-chast-1/viewer.
12. Гассельбах К., Завгородня І. Європейський центр боротьби з кіберзлочинністю починає роботу [Електронний ресурс]. – Режим доступу : http://p.dw.com/p/17HRW.
13. Закон України «Про національну безпеку України» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19#n355.
14. Конституція України [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/254к/96-вр.
15. Концепція створення державної системи захисту критичної інфраструктури [Електронний ресурс]. – Режим доступу : https://www.kmu.gov.ua/ua/npas/pro-shvalennya-koncepciyi-stvorennya-derzhavnoyi-sistemi-zahistu-kritichnoyi-infrastrukturi.
16. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання [Текст] : монографія / А.Ю. Нашинець-Наумова. – Київ: «Гельветика», 2017. – 168 с.

17. Правові засади інформаційної безпеки України [Текст] : монографія / Біленчук П.Д. [та ін.] ; за ред. П.Д. Біленчука. Харків, 2018. - 289 с.
18. Про критичну інфраструктуру та її захист [Електронний ресурс]. – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996.
19. Резолюция A/RES/53/70 ГА ООН «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности» [Електронний ресурс]. – Режим доступу : https://undocs.org/ru/A/RES/53/70.
20. Резолюция A/RES/54/49 ГА ООН «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности» [Електронний ресурс]. – Режим доступу : https://undocs.org/ru/A/RES/54/49.
21. Резолюція Ради Безпеки ООН S/RES/2341 (2017) «Про захист критичної інфраструктури» [Електронний ресурс]. – Режим доступу : https://undocs.org/ru/S/RES/2341(2017).
22. Стратегія кібербезпеки України [Електронний ресурс]. – Режим доступу : https://zakon5.rada.gov.ua/laws/show/96/2016.
23. Фролова О.М. Роль ООН в системі міжнародної інформаційної безпеки [Електронний ресурс]. – Режим доступу : http://journals.iir.kiev.ua/index.php/pol_n/article/viewFile/3468/3140.

REFERENCES

1. Communication from the Commission on Critical Information Infrastructure Protection «Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience» [Elektronnij resurs]. – Rezhim dostupu : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52009DC0149.
2. Concerning measures for a high common level of security of network and information systems across the Union [Elektronnij resurs]. – Rezhim dostupu : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.
3. Council framework decision 2005/222/JHA on attacks against information systems [Elektronnij resurs]. – Rezhim dostupu : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32005F0222.
4. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [Elektronnij resurs]. – Rezhim dostupu : https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.
5. European Union Agency for Network and Information Security [Elektronnij resurs]. – Rezhim dostupu : https://www.enisa.europa.eu/about-enisa.
6. Network and information security: proposal for a european policy approach [Elektronnij resurs]. – Rezhim dostupu : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52001DC0298&from=EN.
7. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU [Elektronnij resurs]. – Rezhim dostupu : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN.
8. Towards a general policy on the fight against cyber crime [Elektronnij resurs]. – Rezhim dostupu : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14560.
9. Voitsikhovskyi A., Bakumov O., Ustymenko O., Marchuk M. The Legal Mechanisms of Ensuring Regional Cooperation in Combatting Crime Within the Framework of the Council of Europe: Experience of Ukraine [Elektronnij resurs]. – Rezhim dostupu : http://www.cejiss.org/issue-detail/the-legal-mechanisms-of-ensuring-regional-cooperation-in-combatting-crime-within-the-framework-of-the-council-of-europe-experience-of-ukraine?fbclid=IwAR2el_dNrQwU_U5YpDji0GJcS7iVdch4mX1j_nesgmMWgAIN9uopNjJsEhk.
10. Bljumenau D.I. Informacija: mif ili real'nost'? (O sostojanii ponjatij «znanie» i «social'naja informacija»). [Tekst] / D. Bljumenau // Nauchno-tehnicheskaja informacija. – 1985. - № 2. Ser. 2. - S. 1–4.
11. Borodakij Ju.V., Dobrodeev A.Ju., Butusov I.V. Kiberbezopasnost' kak osnovnoj faktor nacional'noj i mezhdunarodnoj bezopasnosti HHI veka [Elektronnij resurs]. – Rezhim dostupu : https://cyberleninka.ru/article/n/kiberbezopasnost-kak-osnovnoy-faktor-natsionalnoy-i-mezhdunarodnoy-bezopasnosti-hh-veka-chast-1/viewer.
12. Gassel'bah K., Zavgorodnja I. Євropejs'kij centr borot'bi z kiberzlochinnistju pochinaє robotu [Elektronnij resurs]. – Rezhim dostupu : http://p.dw.com/p/17HRW.
13. Zakon Ukraïni «Pro nacional'nu bezpeku Ukraïni» [Elektronnij resurs]. – Rezhim dostupu: https://zakon.rada.gov.ua/laws/show/2469-19#n355.
14. Konstitucija Ukraïni [Elektronnij resurs]. – Rezhim dostupu: http://zakon.rada.gov.ua/laws/show/254k/96-vr.
15. Koncepcija stvorennja derzhavnoї sistemi zahistu kritichnoї infrastrukturi [Elektronnij resurs]. – Rezhim dostupu : https://www.kmu.gov.ua/ua/npas/pro-shvalennya-koncepciyi-stvorennya-derzhavnoyi-sistemi-zahistu-kritichnoyi-infrastrukturi.
16. Nashinec'-Naumova A.Ju. Informacijna bezpeka: pitannja pravovogo reguljuvannja [Tekst] : monografija / A.Ju. Nashinec'-Naumova. – Kiїv: «Gel'vetika», 2017. – 168 s.
17. Pravovi zasadi informacijnoї bezpeki Ukraïni [Tekst] : monografija / Bilenchuk P.D. [ta in.] ; za red. P.D. Bilenchuka. Harkiv, 2018. - 289 s.
18. Pro kritichnu infrastrukturu ta її zahist [Elektronnij resurs]. – Rezhim dostupu : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996.
19. Rezoljucija A/RES/53/70 GA OON «Dostizhenija v sfere informatizacii i telekommunikacii v kontekste mezhdunarodnoj bezopasnosti» [Elektronnij resurs]. – Rezhim dostupu : https://undocs.org/ru/A/RES/53/70.
20. Rezoljucija A/RES/54/49 GA OON «Dostizhenija v sfere informatizacii i telekommunikacii v kontekste mezhdunarodnoj bezopasnosti» [Elektronnij resurs]. – Rezhim dostupu : https://undocs.org/ru/A/RES/54/49.
21. Rezoljucija Radi Bezpeki OON S/RES/2341 (2017) «Pro zahist kritichnoї infrastrukturi» [Elektronnij resurs]. – Rezhim dostupu : https://undocs.org/ru/S/RES/2341(2017).
22. Strategija kiberbezpeki Ukraïni [Elektronnij resurs]. – Rezhim dostupu : https://zakon5.rada.gov.ua/laws/show/96/2016.
23. Frolova O.M. Rol' OON v sistemi mizhnarodnoї informacijnoї bezpeki [Elektronnij resurs]. – Rezhim dostupu : http://journals.iir.kiev.ua/index.php/pol_n/article/viewFile/3468/3140.