УДК 32
DOI https://doi.org/10.32689/2523-4625-2022-3(63)-6

Анатолій КЛОЧКО
аспірант кафедри публічного адміністрування, ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», вул. Фрометівська, 2, Київ, Україна, 03039
ORCID: 0000-0002-2624-5386

Anatolii KLOCHKO
Postgraduated Student at the Department of Public Administration, Interregional Academy of Personnel Management, Frometivska str., 2, Kyiv, Ukraine, 03039
ORCID: 0000-0002-2624-5386

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ СУЧАСНОГО СУСПІЛЬСТВА

ENSURING INFORMATION SECURITY IN THE CONDITIONS OF MODERN SOCIETY

У статті особливу увагу приділено інформаційній війні з країнами, які намагаються нав'язати Україні свої цінності, зруйнувати традиційні морально-етичні засади українського суспільства. Автор зазначає, що інформація в усі періоди людства відігравала роль глобального чинника загальносистемної рівноваги. Першочерговими завданнями захисту інформації в автоматизованій системі в процесі електронної взаємодії є запобігання, поширення, модифікація, знищення, копіювання, блокування та неправомірне тиражування інформації обмеженого доступу.

Мета роботи. *Метою статті є аналіз системи забезпечення інформаційної безпеки в сучасному суспільстві.*

Методологія. *У статті акцентовано увагу на основні кіберзагрози національній безпеці України. У цьому контексті особливе значення мають створення єдиної національної системи кібербезпеки для подолання цих кіберзагроз.*

Наукова новизна. *Доведено, що національні інтереси України у сфері інформаційної безпеки повинні полягати у розвитку сучасних телекомунікаційних технологій, у захисті державних інформаційних ресурсів від несанкціонованого доступу.*

Висновки. *Наголошено на тому, що необхідно зробити в країні для подальшої розбудови ефективної та дієвої системи кібернетичної безпеки. Констатовано, що механізми захисту інформаційної безпеки України поділяються на два рівні (законодавчий та адміністративний). Зазначено, що запорукою створення надійної системи охорони інформації сьогодні може бути тільки зміцнення самої української держави та її державних органів, відповідальних за забезпечення інформаційної безпеки в країні. Доведено, що для посилення протидії інформаційній війні Росії проти України важливим є вивчення досвіду інших країн.*

Ключові слова: *інформація, національна безпека, інформаційна безпека, інформаційна війна, кіберзагрози.*

The article pays special attention to the information war with countries that are trying to impose their values on Ukraine, to destroy the traditional moral and ethical foundations of Ukrainian society. The author notes that information in all periods of mankind played the role of a global factor of system-wide balance. The primary tasks of information protection in an automated system in the process of electronic interaction are the prevention, distribution, modification, destruction, copying, blocking, and unlawful duplication of restricted access information.

The purpose of the work. *The purpose of the article is to analyze the information security system in modern society.*

Methodology. *The article focuses on the main cyber threats to the national security of Ukraine. In this context, the creation of a unified national cyber security system to overcome these cyber threats is of particular importance.*

Scientific novelty. *It has been proven that the national interests of Ukraine in the field of information security should consist in the development of modern telecommunication technologies, in the protection of state information resources from unauthorized access.*

Conclusions. *It is emphasized that what needs to be done in the country for the further development of an effective and efficient system of cyber security. It was established that the mechanisms for protecting information security of Ukraine are divided into two levels (legislative and administrative). It is noted that the key to creating a reliable information security system today can only be the strengthening of the Ukrainian state itself and its state bodies responsible for ensuring information security in the country. It has been proven that in order to strengthen countermeasures against Russia's information war against Ukraine, it is important to study the experience of other countries.*

Key words: *information, national security, information security, information warfare, cyber threats.*

Постановка проблеми. Ефективність здійснення влади в будь-якій державі, в тому числі і в Україні, в чималому залежить від його інформаційного забезпечення. Збалансована державна інформаційна політика України формується як складова частина її соціально- економічної політики, виходячи з пріоритетності національних інтересів та загроз національній безпеці країни.

Державна політика у сфері інформаційної безпеки має бути спрямована на накопичення та захист національних інформаційних ресурсів, розробку та впровадження сучасних безпечних інформаційних технологій, побудову захищеної національної інформаційної інфраструктури, формування і розвиток інформаційних стосунків та реалізовуватися шляхом створення і забезпечення ефективного функціонування в Україні цілісної системи інформаційної безпеки.

На сьогодні Україна опинилася у стані інформаційної війни з країнами, які намагаються нав'язати нашій країні свої цінності, зруйнувати традиційні морально-етичні засади українського суспільства. Сучасна інформаційна революція розгортається на фоні інформаційних війн, які своєю головною метою ставлять підрив національної безпеки держав. З урахуванням таких підходів безпекова інформаційна функція держави в усіх регіонах світу набуває особливої важливості.

Аналіз останніх досліджень та публікацій. В усі періоди розвитку людства інформація була невід'ємною сутністю основної трудової діяльності, виживання і самовдосконалення людей, відігравала роль глобального чинника загальносистемної рівноваги в економіко-екологічному комплексі [10].

В постіндустріальному суспільстві змінилася роль інформації. На думку О.Л. Гуровського, інформація набуває властивості потужного засобу впливу на громадсько-політичні, ідеологічні та соціально-економічні процеси, стає свого роду зброєю, яка вимагає створення системи протидії, захисту інформаційних ресурсів, які належать державним органам, що становлять державну, професійну, особисту таємницю [2].

Яхно О. М. зазначає, що рівень розвитку інформаційної складової тісно пов'язаний із безпекою держави: період становлення механізмів інформаційного суспільства є дуже небезпечним, оскільки країна може увійти у світові інфраструктури, не створивши при цьому механізмів захисту [12].

Розвиток суспільства, впровадження інноваційних технологій породив таке явище, як комп'ютерний тероризм, що є реальною загрозою функціонуванню інформаційно-телекомунікаційних систем держави за допомогою глобальної мережі Інтернет. Для всесвітньої мережі немає державних кордонів, атаку можна здійснити з будь-якої частини світу за допомогою гаджетів, які доступні кожному. Під кібертероризмом розуміють навмисну мотивовану атаку на інформацію, що обробляється комп'ютером, комп'ютерну систему або мережу; вона пов'язана з небезпекою для життя і здоров'я людей або настанням інших тяжких наслідків, якщо такі дії вчинені з метою порушення громадської безпеки, залякування населення, провокування воєнного конфлікту [11]. У Законі України «Про основні засади забезпечення кібернетичної безпеки України» кібертероризм визначено як терористичну діяльність, що здійснюється у кіберпросторі або з його використанням [7].

Першочерговими завданнями щодо захисту інформації в автоматизованій системі в процесі електронної взаємодії є: запобігання, поширення, модифікація, знищення, копіювання, блокування та неправомірне тиражування інформації обмеженого доступу.

Мета роботи. Метою статті є аналіз системи забезпечення інформаційної безпеки в сучасному суспільстві.

Виклад основного матеріалу. У прийнятій Стратегії Національної безпеки України [9] визначено пріоритети державної політики національної безпеки та основні напрями її забезпечення, а саме, посилення спроможностей національної системи кібербезпеки для ефективної протидії кіберзагрозам у сучасному безпековому середовищі. У п.63 Стратегії зазначається, що потрібно завершити створення національної системи кібербезпеки, сформувати сучасні спроможності суб'єктів забезпечення кібербезпеки і кібероборони та зміцнити систему їх координації. Підкреслено, що держава повинна визнавати кіберпростір, як простір суперництва, поряд із землею, водою та повітрям. Наявні загрози кіберскладової сьогодні існують починаючи від питань глобалізації та міжнародної конкуренції й закінчуючи інфраструктурою, інформаційними операціями та цифровою трансформацією.

Кіберпростір став на сьогоднішній день однією із найважливіших складових частин інформаційного простору та ареною ведення справжніх війн у віртуальному середовищі. Тому кібербезпека є основним елементом регулювання кіберопростору і водночас системи національної безпеки країни.

Глобальність і всеосяжність кіберпростору значно ускладнюють можливість виявлення кібербезпекових загроз та практичну реалізацію відповідних заходів реагування з боку держави. Вчений В.А. Ліпкан виводить основні кіберзагрози національній безпеці України, а саме:

– загроза гібридної війни з боку Російської Федерації;

– недостатній рівень кіберграмотності та медіа-культури населення;

– недостатній рівень проробленості на державному рівні комплексного цілісного підходу до комунікативної політики;

– вразливість до сучасних кіберзагроз ключових вітчизняних об'єктів інфраструктури й офіційних електронних ресурсів, особливо від кібератак хакерів;

– моральна застарілість і фізична зношеність матеріальної бази кіберпростору;

– застарілість і недосконаліть сучасних форм і методів боротьби з кіберзлочинністю;

– слабкість системи охорони державної таємниці в Україні тощо [5].

Саме для подолання цих кіберзагроз і необхідно створення єдиної національної системи кібербезпеки.

К.Л. Бугайчук і Г.М. Шорохова зазначають, що для подальшої розбудови ефективної та дієвої системи кібернетичної безпеки в Україні необхідно:

1) Чітко визначити спрямованість, зміст, форми та методи державної політики в сфері кібербезпеки.

2) Створити та впорядкувати відповідні організаційні структури, які будуть займатися дотриманням безпеки у кіберпросторі.

3) Налагодити ефективний процес управління безпекою у кіберпросторі та створити належні умови для реалізації запланованих заходів по кібербезпеці.

4) Налагодити чітку взаємодію між відповідними компетентними державними органами у сфері кібербезпеки та відповідну ефективну координацію їх діяльності.

5) Створити новітні механізми державного управління кібербезпекою через відкриття спеціалізованих наукових установ, центрів підготовки та експериментальних майданчиків.

6) Проводити активні дослідження у сфері інформаційних операцій, заохочувати дослідно-конструкторську та науково-технічну роботу в даній сфері [1].

М. Присяжнюк зазначає, лише та держава може розраховувати на лідерство в економічні, військово-політичній чи інших сферах, мати стртегічну й 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 [6].

Інформаційна безпека є не лише самостійною складовою національної безпеки, а й невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки, адже всі типи взаємовідносин між суб'єктами інформаційного суспільства ґрунтуються на споживанні й обміні інформацією. З цього приводу В.Ліпкан зазначає, що національні інтереси, загрози їм, управління цими загрозами в усіх галузях національної безпеки знаходять свій вираз, реалізуються через інформацію та інформаційну сферу [5].

Політика інформаційної безпеки реалізується системою інститутів публічної влади та інститутами громадянського суспільства.

Механізми захисту інформаційної безпеки України можна розділити на два рівні – законодавчий та адміністративний. Законодавчий рівень є найважливішим для забезпечення інформаційної безпеки.

Найважливіше на законодавчому рівні – створити механізм, що дозволяє узгодити процес розробки законів з реаліями і прогресом інформаційних технологій. Закони не можуть випереджати життя, але важливо, щоб відставання не було занадто великим, так як на практиці, крім інших негативних моментів, це веде до зниження інформаційної безпеки.

Адміністративний механізм забезпечення інформаційної безпеки охоплюють установи, діяльність яких спрямовано на формування та реалізацію інформаційної безпеки.

Головна мета заходів адміністративного рівня – сформувати програму робіт в галузі інформаційної безпеки та забезпечити її виконання, виділяючи необхідні ресурси і контролюючи стан справ.

Запорукою створення надійної системи охорони інформації сьогодні може бути тільки зміцнення самої української держави та її державних органів, відповідальних за забезпечення інформаційної безпеки в країні. У зв'язку з цим стоять масштабні завдання, пов'язані з виробленням системи забезпечення інформаційної безпеки, пошуку принципово нових, нестандартних форм організації, взаємодії, координації діяльності, удосконалення всіх засобів, спрямованих на забезпечення процесу управління загрозами та небезпеками.

Інформаційна безпека України має перед собою головне стратегічне завдання: створити потужний національний інформаційний простір як головний аспект, що засвідчує присут-

ність країни на світовій інформаційній арені. Також така ціль передбачає потребу створити систему протистояння будь-якій інформаційній загрозі та оборону власних інформаційних ресурсів, середовища та інфраструктурної складової країни.

Серед складових частин системи інформаційної безпеки важливе місце займає перелік її загроз.

Застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Саме проти України Російська Федерація використовує 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 [3].

Для посилення протидії інформаційній війні Росії проти України важливим є вивчення досвіду інших країн. США, Велика Британія, Ізраїль, ФРН, Російська Федерація, Китай постійно знаходяться під потужним зовнішнім інформаційним впливом, тому вимушені створювати національні системи інформаційного захисту. Системи інформаційної безпеки цих країн є найбільш розвинутими та мають достатню активну складову, завдяки чому існує можливість проведення інформаційно-психологічних заходів і кібернетичних атак проти країн-супротивників [4].

Відсутність достатніх державних інструментів для ведення інформаційної війни є актуальним питанням війни з Росією. Український учений М. Сенченко зазначає, що Україні для ефективного протистояння інформаційній війні з боку Росії потрібно мати хоча б: 1) ефективну систему ведення інформаційної війни; 2) ефективну концепцію інформаційної війни; 3) стратегію ведення інформаційної війни [8].

Основними заходами щодо забезпечення інформаційної безпеки України у зовнішньополітичній сфері є: розробка основних напрямів державної політики в галузі вдосконалення інформаційного забезпечення зовнішньополітичного курсу України; розробка та реалізація комплексу заходів щодо посилення інформаційної безпеки інформаційної інфраструктури органів виконавчої влади, що реалізують зовнішню політику України, українських представництв та організацій за кордоном, представництв України при міжнародних організаціях; створення українськими представництвами та організаціями за кордоном умов для роботи з нейтралізації поширюваної там дезінформації про зовнішню політику України; вдосконалення інформаційного забезпечення роботи з протидії порушенням прав і свобод українських громадян і юридичних осіб за кордоном; вдосконалення інформаційного забезпечення суб'єктів України з питань зовнішньополітичної діяльності, які входять до їхньої компетенції.

Висновки. Таким чином, національні інтереси України у сфері інформаційної безпеки повинні полягати у розвитку сучасних телекомунікаційних технологій, у захисті державних інформаційних ресурсів від несанкціонованого доступу. Сучасні інформаційні протистояння, засвідчили що інформаційний простір України потребує додаткового захисту від зовнішніх негативних інформаційно-психологічних впливів. Монополізація інформації призводить до того, що певне коло осіб керують свідомістю громадян для прийняття необхідного корисливого рішення для них. Такий розвиток подій є особливо загрозливим для України в контексті формування вищих органів державної влади.

З метою попередження і протидії існуючим та ймовірним загрозам інформаційній безпеці стратегічне завдання держави потягає у створенні та функціонуванні механізму забезпечення інформаційної безпеки. Він передбачає послідовну системну діяльність, сукупність заходів і державно-правових інституцій, що покликані гарантувати безперешкодну реалізацію національних інтересів держави в інформаційній сфері, відповідних інтересів людини і суспільства, попередження інформаційних конфліктів та оперативне їх подолання.

Література:

1. Бугайчук К. Л., Шорохова Г. М. Забезпечення кібербезпеки як умова протидії терористичній діяльності: нормативно-правові аспекти. *Протидія терористичній діяльності : міжнародний досвід і його актуальність для України : матеріали II Міжнародної науково-практичної конференції (15 грудня 2017 р.).* Київ : Національна академія прокуратури України, 2018. С. 135–138.

2. Гуровський В. О. Роль органів державної влади у сфері забезпечення інформаційної безпеки України. *Вісник Української академії державного управління при Президентові України*. Київ, 2014. № 3. С. 21–31.

3. Доктрина інформаційної безпеки України: уведена у дію Указом Президента України : від 25.02.2017 р. № 47/2017. URL: www.president.gov.ua

4. Левченко О. В. Проблеми і шляхи формування системи інформаційної безпеки держави. *Збірник наукових праць Харківського університету Повітряних Сил*. 2(39), 2014. С. 166–168.

5. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції : навчальний посібник. Київ : КНТ, 2006. 280 с.

6. Присяжнюк М. М. Інформаційна безпека України в сучасних умовах. *Вісник національного університету імені Тараса Шевченка. Військово-спеціальні науки*. 2013. Вип. 30. С.32–46.

7. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовт. 2017 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403. URL: http://zakon2. rada.gov.ua/laws/show/2163-19 21.Global Risks Report 2018"

8. Сенченко М. Запорука національної безпеки в умовах інформаційної війни. *Вісник Книжкової палати*. 2014. № 6. С.3–9.

9. Стратегія національної безпеки України : Указ Президента України від 14.09.2020 р. № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037

10. Сулима Є. М., Шепелев М. А. Глобалістика. Київ : Вища шк., 2010. С. 292.

11. Топчій В. В. Кібертероризм в Україні: поняття та запобігання кримінально-правовим та кримінологічними засобами. *Наукові вісник Херсонського університету. Сер. : Юридичні науки.* 2015. Вип. 6. Том 3. С. 65–68.

12. Яхно О. М. Україна в сучасному геополітичному просторі (політико-медійний аспект) : автореф. дис. … канд. політ. наук. Київ, 2006. 14 с.

References:

1.Buhaichuk K.L., Shorokhova H.M. Zabezpechennia kiberbezpeky yak umova protydii terorystychnii diialnosti: normatyvno-pravovi aspekty. *Protydiia terorystychnii diialnosti : mizhnarodnyi dosvid i yoho aktualnist dlia Ukrainy : materialy II Mizhnarodnoi naukovo-praktychnoi konferentsii (15 hrudnia 2017 r.).* Kyiv : Natsionalna akademiia prokuratury Ukrainy, 2018. S. 135–138.

2.Hurovskyi V. O. Rol orhaniv derzhavnoi vlady u sferi zabezpechennia informatsiinoi bezpeky Ukrainy. *Visnyk Ukrainskoi akademii derzhavnoho upravlinnia pry Prezydentovi Ukrainy.* Kyiv, 2014. № 3. S. 21–31.

3.Doktryna informatsiinoi bezpeky Ukrainy: uvedena u diiu Ukazom Prezydenta Ukrainy : vid 25.02.2017 r. № 47/2017. URL: www.president.gov.ua

4.Levchenko O.V. Problemy i shliakhy formuvannia systemy informatsiinoi bezpeky derzhavy. *Zbirnyk naukovykh prats Kharkivskoho universytetu Povitrianykh Syl*. 2(39), 2014. S. 166–168.

5.Lipkan V.A. Informatsiina bezpeka Ukrainy v umovakh yevrointehratsii: navchalnyi posibnyk. Kyiv : KNT, 2006. 280 s.

6.Prysiazhniuk M.M. Informatsiina bezpeka Ukrainy v suchasnykh umovakh. *Visnyk natsionalnoho universytetu imeni Tarasa Shevchenka. Viiskovo-spetsialni nauky*. 2013. Vyp. 30. S. 32–46.

7.Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy : Zakon Ukrainy vid 5 zhovt. 2017 r. № 2163-VIII. *Vidomosti Verkhovnoi Rady Ukrainy*. 2017. № 45. St. 403. URL: http://zakon2. rada.gov.ua /laws/show/2163-19 21.Global Risks Report 2018"

8.Senchenko M. Zaporuka natsionalnoi bezpeky v umovakh informatsiinoi viiny. *Visnyk Knyzhkovoi palaty.* 2014. № 6. S. 3–9.

9.Stratehiia natsionalnoi bezpeky Ukrainy : Ukaz Prezydenta Ukrainy vid 14.09.2020 r. № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037

10. Sulyma Ye.M., Shepelev M.A. Hlobalistyka. Kyiv : Vyshcha shk., 2010. S. 292.

11. Topchii V. V. Kiberteroryzm v Ukraini: poniattia ta zapobihannia kryminalno-pravovym ta kryminolohichnymy zasobamy. *Naukovi visnyk Khersonskoho universytetu. Ser. Yurydychni nauky.* 2015. Vyp. 6.Tom 3 S. 65–68.

12. Yakhno O. M. Ukraina v suchasnomu heopolitychnomu prostori (polityko-mediinyi aspekt) : avtoref. dys. … kand. polit. nauk. Kyiv, 2006. 14 s.