1. ТЕОРІЯ ТА ІСТОРІЯ ДЕРЖАВИ І ПРАВА. ІСТОРІЯ ПОЛІТИЧНИХ І ПРАВОВИХ ВЧЕНЬ. ФІЛОСОФІЯ ПРАВА

DOI:10.35774/app2021.01.005
УДК 351.746:007

Андрій Грубінко,
доктор історичних наук, професор, професор кафедри теорії та історії держави і права, директор Центру стратегічної аналітики та міжнародних студій Західноукраїнського національного університету
ORCID: http://orcid.org/0000-0002-4856-5831

ОСОБЛИВОСТІ ФОРМУВАННЯ ПОЛІТИКИ КІБЕРБЕЗПЕКИ ЄВРОПЕЙСЬКОГО СОЮЗУ: ПРАВОВІ АСПЕКТИ

Розглянуто сучасні правові та організаційні засади кібербезпеки Європейського Союзу (ЄС) проблеми й перспективи розвитку відповідного механізму ЄС в умовах сучасних кіберзагроз. Проаналізовано еволюцію і якісну динаміку кіберполітики ЄС – від прийняття перших правових актів на початку 2000-х років до оприлюднення проєкту другої Стратегії безпеки ЄС в грудні 2020 р. За результатами дослідження виявлено, що ЄС має можливості досягти стратегічної автономії у сфері кіберполітики. Однак для цього йому необхідна більш узгоджена політика координації дій, подальше збільшення фінансування та розбудова інституційної спроможності ЄС, вирівнювання можливостей держав-членів.

Ключові слова: *кібербезпека, політика кібербезпеки, Європейський Союз, кіберпростір, кіберзлочинність,*

Hrubinko A.

The article deals with the current legal and organizational principles of the European Union`s cybersecurity, *the problems and prospects for the development of the relevant EU mechanism in the context of modern cyber threats. The evolution and qualitative dynamics of the EU cyber policy from the adoption of the first legal acts in the early 2000s to the publication of the second EU Security Strategy draft in December 2020 are analyzed. The study found that the European Union has the potential to achieve strategic autonomy in cyberpolitics. However, it needs a more coherent policy of coordination, further increase of funding and building of institutional capacity of the EU, equalization of member states possibilities.*

The conclusions state that Europe is interested in the comprehensive development of EU cybersecurity policy. The cross-border nature of cyber threats means that the EU's resilience in this matter directly affects its security. The current direction of the EU's capacity building and especially close cooperation with NATO provide a chance to avoid

difficult political dilemmas. Official data from the European Union's Cyber Security Agency show that the number of violations of privacy is growing among the types of cyber attacks. This puts on the agenda the activities of EU structures and Member States the need to develop a system of human rights protection in the field of cybersecurity. One of its basic elements should be updated legislation, in particular, the new EU Cyber Security Strategy.

The European Union does not stop there and constantly strives to develop opportunities to counter and prevent cyber threats in order to achieve strategic autonomy of the organization. The EU needs to overcome its excessive bureaucratization and imbalance in the funding of cyber policy management programs and the practical development of cyber attack protection, prevention and repulsion systems. The EU's place in the future global cybersecurity system will depend on the real strengthening of this second segment of programs.

Keywords: *Cybersecurity Policy, European Union, cyberspace, cybercrime, cyber threats, cyber protection.*

Постановка проблеми. Стрімке поширення Інтернету на рубежі XX – XXI ст. привело до значного збільшення користувачів глобальної мережі. Їхня кількість уже перевищила 50% світового населення. Кіберпростір є важливою сферою діяльності, співробітництва і конкуренції, в якій беруть участь як держави, так і недержавні суб'єкти. Поряд з позитивними моментами протягом останнього десятиліття виявлялися негативні аспекти користування Інтернетом, такі як кіберзлочинність. У глобальній мережі люди працюють, отримують знання, спілкуються один з одним або просто розважаються, але водночас вони піддаються різним загрозам. Зазнають нападів особисті комп'ютери, сервери установ, акаунти, електронна пошта та інші засоби комунікацій. Метою таких нападів (кібератак) є отримання інформації або нанесення різного виду шкоди – фінансової, матеріальної, моральної або політичної. Кібератаки часто є частиною сценаріїв політичних і військових криз та конфліктів.

Масштаби кібератак є проблемою для національної безпеки держав та їхньої внутрішньої стабільності. За даними Pew Research Center, у 2018 р. кібератаки на міжнародному рівні посіли третє місце серед глобальних загроз [1]. Масштаби проблеми засвідчує динаміка заражень шкідливим програмним забезпеченням, що є найбільш поширеним видом кіберзлочинів [2].

Розвиток ІКТ (інформаційно-комунікаційних техногій) та Інтернету привів до виникнення абсолютно нових концепцій у галузі міжнародної безпеки, таких як «кіберзлочинність» і «кібертероризм». Водночас усе більшого значення у виробленні єдиних підходів до забезпечення кібернетичної безпеки як складової національної безпеки європейських країн та на глобальному рівні відіграє політика кібербезпеки ЄС.

Аналіз останніх досліджень і публікацій. Процес становлення політики кібербезпеки ЄС став предметом розгляду дослідників А. Балери, Д. Біго, М. Герке, М. Грокса, М. Дюмонтье, В. Кіютіна, А. Новікова, М. Рижкова, Д. Робинсона, В. Сомерса та інших. Серед проблем, які вони розглядають, – загальна правова політика ЄС щодо боротьби з кіберзлочинністю, міжнародне співробітництво у сфері кібернетичної та інформаційної безпеки, боротьба з кіберзлочинністю в ЄС, окремі кіберзлочини. Однак, незважаючи на велику кількість досліджень, динамічний розвиток інфраструктури в мережевій та інформаційній сфері, поширення кіберзлочинності зумовлює потребу в нових наукових дослідженнях.

Мета дослідження – проаналізувати концептуальні підходи до гарантування безпеки в європейському кіберпросторі, сучасні правові та організаційні засади кібербезпеки Європейського Союзу, з'ясувати проблеми і перспективи розвитку відповідного механізму ЄС в умовах сучасних кіберзагроз.

Виклад основного матеріалу дослідження. Для Європейського Союзу політика кібербезпеки набула комплексного стратегічного виміру доволі пізно. У 2001 р. Європейська комісія представила перший документ «Мережева та інформаційна безпека: пропозиція щодо підходу до європейської політики», в якому окреслено європейський підхід до проблеми інформаційної безпеки [3]. Атаки на інформаційні системи можуть мати серйозні наслідки у національному масштабі, наприклад відбуватись збої в роботі систем комунікацій, витік конфіденційної інформації тощо. У березні 2004 р. створено Агентство Європейського Союзу з мережевої та інформаційної безпеки (ENISA), яке активно співпрацює з Європолом, Європейським центром кіберзлочинності, іншими спеціалізованими структурами ЄС.

У лютому 2005 р. Рада ЄС прийняла Рамкове рішення 2005/222/ЈНА про напад на інформаційні системи, встановивши мінімальні правила щодо визначення кримінальних злочинів і санкцій. У травні 2007 р. Європейська комісія представила документ «На шляху до загальної політики щодо боротьби з кіберзлочинністю», в якому відображено основні напрями політики ЄС у протидії кіберзлочинності [4]. До кіберзлочинності було включено три категорії злочинів: а) традиційні форми злочину (шахрайство і підробки в електронних комунікаційних мережах та інформаційних системах); б) публікація протизаконного контенту в електронних медіа (дитяча порнографія, матеріали із закликами до расової ненависті тощо); в)

специфічні злочини в електронних мережах (атаки на інформаційні системи, хакерство тощо). У березні 2009 р. опубліковано повідомлення Європейської комісії «Захист Європи від широкомасштабних кібератак та зривів: підвищення готовності, безпеки та стійкості», в якому визначено проблеми, що потребують негайного реагування ЄС [5].

Практичне формування автономної кіберполітики ЄС розпочалося лише після затвердження в лютому 2013 р. Стратегії кібербезпеки «Стратегія кібербезпеки Європейського Союзу: відкритий та безпечний кіберпростір». З тих пір розпочався інтенсивний розвиток політики ЄС щодо кіберпростору в усіх його вимірах: цифрова економіка; мережева та інформаційна безпека; боротьба з кіберзлочинністю; спільна зовнішня політика і політика безпеки; кіберзахист [6, p. 12]. Це стосується співпраці ЄС з іншими суб'єктами безпеки, насамперед з НАТО.

Відомі резонансні події навколо і в середині ЄС, зокрема втручання Росії у вибори в США у 2016 р. та інших країнах, Brexit і невизначеність щодо майбутнього трансатлантичних відносин після обрання Дональда Трампа на пост президента США посилили дебати про зміцнення незалежності ЄС у сфері безпеки і оборони, розширення його стратегічної автономії. Тому прийнята Глобальна стратегія зовнішньої політики і політики безпеки Європейського Союзу 2016 р. відобразила еволюцію підходу об'єднання до кібербезпеки. Визнаючи, що інформаційні технології стали основою для функціонування і добробуту європейських суспільств, ЄС зробив кібербезпеку одним із своїх основних пріоритетів у сфері безпеки [7]. У липні 2016 р. прийнята чергова Директива ЄС «Щодо заходів щодо високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі», яка сформувала єдині правила та вимоги в сфері кібербезпеки для країн-членів.

Серед основних загроз національним кіберпросторам країн-членів ЄС передбачено: а) кібершпигунство за підтримки або з відома держави щодо інших держав та корпорацій, яке має на меті заволодіння державними або промисловими таємницями, персональними даними або іншою цінною інформацією; б) використання Інтернету у терористичних цілях (з метою пропаганди, збору коштів і вербування прихильників); в) кіберзлочинність (викрадення персональних даних та відмивання коштів, отриманих незаконним шляхом).

Агенція ЄС з кібербезпеки за підсумками аналізу даних за 2019 – 2020 рр., подала перелік 15 основних видів кібератак (у порядку за кількістю виявів) [8, с. 6]. Серед суб'єктів кібератак Агенція ЄС з кібербезпеки виокремила представників організованої злочинності (60% кількості кібератак), держави (14%), інсайдерів (10%), системних адміністраторів (8%), користувачів (4%), інших (2%) [9, p. 11]. Такі дані свідчать про системний характер організації і здійснення кіберзлочинності на міжнародному рівні.

Національне законодавство країн, як правило, регулює питання: захисту персональних даних (Нідерланди, Естонія, Швеція, Фінляндія, Іспанія); захисту електронної комерції та безпеки електронних транзакцій та платіжних інструментів (Польща, Естонія, Італія); безпеки важливих об'єктів інфраструктури та інформаційних систем (Франція) [10, p. 3]. Кіберстратегія багатьох європейських держав допускає не тільки оборонні, а й наступальні дії в кіберпросторі.

Політика ЄС у сфері кібербезпеки, незважаючи на очевидний прогрес, досягнутий за останні роки, все ще має проблеми функціонування. Насамперед їй не вистачає необхідного узгодження. Це виявляється як на регулятивному, так і на інституційному рівнях. ЄС зустрівся з проблемою нестачі кваліфікованих фахівців у сфері ІКТ, особливо експертів у сфері кібербезпеки. У традиційному вимірі (так звана «жорстка сила») повна стратегічна автономія ЄС, пов'язана з наявністю власних можливостей кіберзахисту, все ще не нереалізована. Держави-члени визнають необхідність зміцнення своїх ресурсів, але не хочуть ділитися своїми можливостями. До того ж потенціал окремих держав дуже різноманітний. У сфері можливостей кіберзахисту європейські держави надають перевагу співпраці і поділу завдань між ЄС і НАТО, в той час як дії ЄС розглядаються значною мірою як доповнювальні.

ЄС все ще суттєво відстає за обсягом фінансування кібербезпеки насамперед від світового лідера США. Загальні витрати на кібербезпеку в ЄС у відсотках до ВВП становлять близько 0,1%. У США цей показник у 2019 р. становив 0,35% (у т. ч. з приватним сектором) [6, p. 22]. Витрати на кібербезпеку нелегко виокремити із загальних витрат державного бюджету, але попередні дослідження показують, що їхній рівень (у перерахунку на відсоток ВВП) в Європі є низьким та неоптимальним, порівняно з іншими світовими гравцями, насамперед США.

На рівні ЄС інвестиції в кібербезпеку спрямовуються через різні програми спільного бюджету: у період 2014–2020 рр. близько 600 млн євро було інвестовано в проєкти з кібербезпеки та кіберзлочинності в рамках програми «Горизонт 2020»; Європейські структурні та інвестиційні фонди (ESI) передбачають

внесок до 400 млн євро для інвестицій у довірчу діяльність та кібербезпеку; за період 2014–2017 рр. від Connecting Europe Facility було інвестовано близько 30 млн. євро. Для порівняння в США уряд лише в рамках бюджету 2017 р. виділив понад 19 млрд дол. на забезпечення політики кібербезпеки [11].

Водночас, як зазначає Й. Голслах, головна проблема полягає не в тому, що Європа не здатна здійснювати інновації або не має інфраструктури, а в тому, що головну слабкість і далі становить створення великих брендів. Серед десяти найбільших у світі інтернет-компаній, виробників комп'ютерної техніки, ІКТ немає жодної європейської [12, с. 445–446].

Основна увага в структурах ЄС приділяється питанням організаційно-управлінського забезпечення кібербезпеки і значно менше – практичним аспектам розробки систем захисту та протидії кібератакам. Такий дисбаланс у системі фінансування конкретних напрямів кіберполітики становить одну з головних причин слабкості позицій ЄС у міжнародній системі кібербезпеки, де домінують США та Китай.

Співпраця НАТО-ЄС у сфері кіберзахисту розвивається практично без перерви та позбавлена політизації. Реалізація Спільної декларації НАТО-ЄС, підписаної в червні 2016 р. під час саміту Альянсу у Варшаві у сфері кібербезпеки відбувається гармонійно. ЄС спрямований більшою мірою на так звану «м'яку безпеку», тому надає пріоритет таким напрямам діяльності: а) посилення зовнішнього виміру політики ЄС у сфері кібербезпеки; б) підвищення стійкості мереж і систем ІКТ до кіберзагроз; в) розробка можливостей та інструментів для реагування на кібератаки; ефективна співпраця у боротьбі з кіберзлочинністю; г) просування стандартів та цінностей в кіберпросторі. Прогрес у цих галузях визначатиме потенціал ЄС у сфері кібербезпеки та його становище на світовій арені. Однак у найближчі роки держави об'єднання мають зробити усвідомлені і скоординовані дії, підтримані відповідним рівнем фінансування.

Виникнення згаданих нових кіберзагроз національній та міжнародній політиці, потреба розширення сфер дії правил кібербезпеки в рамках самого ЄС стали причинами подальшого вдосконалення нормативної бази кіберполітики ЄС, зокрема розробки проєкту нової Стратегії кібербезпеки ЄС, представленого публічно 16 грудня 2020 р. Символічно, що за тиждень до цієї події, 9 грудня 2020 р. зазнало кібератаки Європейське агентство лікарських засобів, яке в тому числі займається сертифікацією вакцин від COVID-19. Документ передбачає режим санкцій проти окремих країн, які загрожують кібербезпеці ЄС (визнані такими, зокрема, Росія, Китай, Північна Корея), посилення кіберрозвідки, створення спільних структур енергетичної та військової кібербезпеки у рамках постійної структурної співпраці в ЄС (PESCO), проєктів у боротьбі з кіберзлочинами на Західних Балканах, у країнах Східного партнерства та Південного сусідства ЄС. Окрім раніше затверджених сфер дії внутрішніх правил кібербезпеки ЄС (охорона здоров'я, банківська справа, питне водопостачання та енергетична інфраструктура), Європейська Комісія пропонує додати держуправління, харчовий сектор і фармацевтичне виробництво [13]. Таким чином, в ЄС намагаються діяти відповідно до вимог часу та адекватно відповідати на нові виклики і загрози у сфері кібербезпеки.

Прикладом розвитку згаданого механізму PESCO в рамках політики кібербезпеки є ініціатива уряду Литви щодо заснування Кібернетичних сил ЄС швидкого реагування (Cyber Rapid Response Team, CRRT), створених у березні 2020 р. за участю представників шести європейських держав [14]. Міжнародна команда швидкого реагування перебуває в режимі очікування на декількох фізичних сайтах і готова негайно відреагувати на кібератаку в разі її виникнення. Результати цього пілотного міжнародного проєкту мають бути поширені на весь Європейський Союз і становити основу багатонаціональних Кібернетичний сил ЄС.

Висновки. Європа зацікавлена в комплексній розробці політики кібербезпеки ЄС. Транскордонний характер кіберзагроз призводить до того, що стійкість ЄС у цьому питанні прямо впливає на його безпеку. Поточний напрям розвитку потенціалу ЄС та особливо тісна співпраця з НАТО дають шанси уникнути складних політичних дилем. Євроатлантичне співтовариство зацікавлене в тому, щоб не допустити фрагментації кіберпростору і зберегти його відкритий, вільний та універсальний характер в умовах сучасних комплексних викликів міжнародній безпеці, зокрема поширенню кіберзлочинності в усіх її різновидах.

Офіційні дані Агенції Європейського Союзу з кібербезпеки засвідчують, що серед переліку видів кібератак зростає кількість порушень недоторканості приватної сфери. Це ставить на порядок денний діяльності структур ЄС і держав-членів необхідність розробки системи захисту прав людини у сфері кібербезпеки. Одним з її базових елементів має бути оновлене законодавство, зокрема нова Стратегія кібербезпеки ЄС.

В Євросоюзі не зупиняються на досягнутому та постійно прагнуть розвивати можливості протистояння і попередження кіберзагрозам з метою досягнення стратегічної автономії організації. Головним фактором подальшого підвищення якісних показників виконання програм ЄС з кібербезпеки буде досягнення більшої згуртованості та взаємосумісності ресурсів і дій окремих держав-членів об'єднання. Також ЄС має подолати надмірну схильність до бюрократизації і дисбаланс у фінансуванні програм організаційно-управлінського забезпечення кіберполітики та практичної розробки систем захисту, попередження і подолання кібератак. Від реального посилення вказаного другого сегмента програм буде залежати місце ЄС у майбутній системі світової кібербезпеки.

Список використаних джерел

1. Globally, People Point to ISIS and Climate Change as Leading Security Threats. August 1, 2017. By Jacob Poushter and Dorothy Manevich. URL: http://www.pewglobal.org/2017/08/01/globally-people-point-to--isis-and-climate-change-as-leading-security-threats (дата звернення: 28.01.2021).
2. 2020 Cyber Security Statistics. The Ultimate List Of Stats, Data & Trends. URL: https://purplesec.us/resources/cyber-security-statistics/ (дата звернення: 28.01.2021).
3. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. Network and Information Security: Proposal for a European Policy Approach. COM(2001)298 final. Brussels, 6.6.2001. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0298:FIN:EN:PDF (дата звернення: 03.02.2021).
4. Communication from the Commission to the European Parliament, the Council and the Committee of the Regions. Towards a general policy on the fight against cyber crime. COM(2007) 267 final. Brussels, 22.5.2007. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF (дата звернення: 03.02.2021).
5. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection «Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience». COM(2009) 149 final. Brussels, 30.3.2009. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF (дата звернення: 05.02.2021).
6. Challenges to effective EU cybersecurity policy Briefing Paper March 2019. European Union, 2019. 72 p.
7. Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy. June 2016. Brussels, 2016. 56 p.
8. The year in review. From January 2019 to April 2020. ENISA Threat Landscape. 2020. 24 p.
9. Main incidents in the EU and worldwide. From January 2019 to April 2020. ENISA Threat Landscape. 2020. 25 p.
10. Zakonodavstvo ta strategii y sferi kiberbezpeky krayin Yevropeyskogo Soyuzu, SSHA, Kanady ta inshyh. Informatsiyina dovidka, pidgotovlena Yevropeyskym informatsiyino-doslidnytskym tsentrom na zapyt narodnogo deputata Ukrayiny. Kyiv: Infotsentr, Yevropeyskyy informatsiyno-doslidnytskyy tsentr, Laboratoriya zakonodavchyh initsiatyvs, 2016. 37 p.
11. Cybersecurity. State of federal it report. Public release version 1.0. Policy Papers. URL: https://www.cio.gov/assets/resources/sofit/02.05. cybersecurity.pdf (дата звернення: 03.02.2021).
12. Holslag J. The Power of Paradise. How Europe Can Lead the Asian Century. 2014. 606 p.
13. Joint communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. Brussels, 13.9.2017. JOIN(2017) 450 final. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450 (дата звернення: 03.02.2021).
14. Shaping Europe's digital future. Policy. Cybersecurity. European Commission. URL: https://ec.europa.eu/digital-single-market/en/cybersecurity (дата звернення: 05.02.2021).

References

1. Globally, People Point to ISIS and Climate Change as Leading Security Threats. August 1, 2017. By Jacob Poushter and Dorothy Manevich. Retrieved from http://www.pewglobal.org/2017/08/01/globally-people-point-to--isis-and-climate-change-as-leading-security-threats [in English].
2. 2020 Cyber Security Statistics. The Ultimate List Of Stats, Data & Trends. Retrieved from https://purplesec.us/resources/cyber-security-statistics/ [in English].
3. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. Network and Information Security: Proposal for a European Policy Approach. COM(2001)298 final. Brussels, 6.6.2001. Retrieved from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0298:FIN:EN:PDF [in English].

4. Communication from the Commission to the European Parliament, the Council and the Committee of the Regions. Towards a general policy on the fight against cyber crime. COM(2007) 267 final. Brussels, 22.5.2007. Retrieved from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267: FIN:EN:PDF [in English].
5. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection «Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience». COM(2009) 149 final. Brussels, 30.3.2009. Retrieved from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149: FIN:EN:PDF[in English].
6. Challenges to effective EU cybersecurity policy Briefing Paper March 2019 (2019). European Union [in English].
7. Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy. June 2016 (2016). Brussels [in English].
8. The year in review. From January 2019 to April 2020 (2020). ENISA Threat Landscape [in English].
9. Main incidents in the EU and worldwide. From January 2019 to April 2020 (2020). ENISA Threat Landscape [in English].
10. Zakonodavstvo ta strategii y sferi kiberbezpeky krayin Yevropeyskogo Soyuzu, SSHA, Kanady та inshyh. Informatsiyina dovidka, pidgotovlena Yevropeyskym informatsiyino-doslidnytskym tsentrom na zapyt narodnogo deputata Ukrayiny (2016). Kyiv: Infotsentr, Yevropeyskyy informatsiyno-doslidnytskyy tsentr, Laboratoriya zakonodavchyh initsiatyvs [in English].
11. Cybersecurity. State of federal it report. Public release version 1.0. Policy Papers. Retrieved from https://www.cio.gov/assets/resources/sofit/02.05. cybersecurity.pdf [in English].
12. Holslag, J. (2014). The Power of Paradise. How Europe Can Lead the Asian Century [in English].
13. Joint communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. Brussels, 13.9.2017. JOIN(2017) 450 final. Retrieved from https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450 [in English].
14. Shaping Europe's digital future. Policy. Cybersecurity. European Commission. Retrieved from https://ec.europa.eu/digital-single-market/en/cybersecurity [in English].

Стаття надійшла до редакції 12.02.2021.

DOI:10.35774/app2021.01.011
УДК 343.971 (477)

Тетяна Подковенко,
кандидат юридичних наук, доцент кафедри теорії та історії держави і права Західноукраїнського національного університету
ORCID: https://orcid.org/0000-0001-6027-16IX

НАЦІОНАЛЬНА БЕЗПЕКА УКРАЇНИ: АКСІОЛОГІЧНИЙ ТА ПРАВОВИЙ АСПЕКТИ

У статті представлений філософсько-правовий аналіз поняття національної безпеки. Розкрито підходи вітчизняних та зарубіжних науковців до поняття національної безпеки. Визначено, що у сучасних умовах проблема якісного забезпечення національної безпеки, розробка системної державної політики захисту національних інтересів та належних механізмів її реалізації є надзвичайно актуальною. Національна безпека є одним із ключових елементів функціонування держави, що забезпечує не просто можливості існування, а також належний розвиток та свободу реалізації національних інтересів та цінностей. У статті проаналізовано законодавство України про національну безпеку в аспекті відображення та захисту загальнолюдських цінностей.

Ключові слова: *безпека, національна безпека, забезпечення національної безпеки, національні інтереси, загальнолюдські цінності, політика національної безпеки.*

Подковенко Т.
Национальная безопасность Украины: аксиологический и правовой аспекты

В статье представлен философско-правовой анализ понятия национальной безопасности. Раскрыто подходы отечественных и зарубежных ученых к понятию национальной безопасности. Определено, что в современных условиях проблема качественного обеспечения национальной безопасности, разработка системной государственной политики защиты интересов и надлежащих механизмов ее реализации является чрезвычайно актуальной. Национальная безопасность является одним из ключевых элементов функционирования государства, обеспечивает не просто возможности существования, а также надлежащее развитие и свободу реализации национальных интересов и ценностей. В статье проанализировано законодательство Украины о национальной безопасности в аспекте отражения и защиты общечеловеческих ценностей.

Ключевые слова: *безопасность, национальная безопасность, обеспечение национальной безопасности, национальные интересы, общечеловечиские ценности, политика национальной безопасности.*

Podkovenko T.
National security of Ukraine: axiological and legal aspects

The article presents a philosophical and legal analysis of the concept of national security. The approaches of domestic and foreign scientists to the concept of national security are revealed. It is determined that in modern conditions the problem of quality national security, the development of a systematic state policy to protect national interests and appropriate mechanisms for its implementation is extremely relevant. National security is one of the key elements of the functioning of the state, which provides not only the possibility of existence, but also the proper development and freedom to realize national interests and values. The article analyzes the legislation of Ukraine on national security in terms of reflection and protection of universal values.

The approaches to understanding national security analyzed in the article only confirm the fact that the universality of the content of national security determines the universality of the values it reflects and the protection of which should be aimed at public policy. This is a special state of protection of the individual, society and state from internal and external threats, which ensures the realization of constitutional rights and freedoms of citizens, decent quality and standard of living, sovereignty, independence, state and territorial integrity, sustainable socio-economic development. The complexity and systematization of state policy, its focus on the protection of universal values of modern civilization should be the key to further development of our society.

Keywords: *security, national security, ensuring national security, national interests, universal values, national security policy.*

Постановка проблеми. У сучасному світі поняття безпеки займає особливе місце у всіх процесах життєдіяльності людини: політичних, економічних, соціальних, технічних, біологічних та інших. Про