прав, свобод, законних інтересів людини і громадянина, окремих груп людей і громадянського суспільства в цілому, де держава і людина несуть взаємну відповідальність, згідно з правовим законодавством [6, с. 212].

На сьогодні питання правової держави є досить актуальним і особливу увагу привертає до себе з тієї причини, що існує багато різних неузгоджень та прогалин в діяльності української держави та її влади, і саме це змушує все частіше розмовляти юристів, політиків, науковців та взагалі громадян України щодо так званого «не правового характеру» нашої держави. Це пояснюється невиконанням чи неналежним виконанням, недотриманням тих принципів правової держави, на які яких зосереджена увага даної статті. Слід особливо підкреслити, що формування та функціонування правової держави в нашій та будь-якій іншій державі світу передбачають встановлення не тільки формального, а й реального панування закону, дотримання його основних принципів у всіх сферах життя суспільства, розширення сфери його прямого, безпосереднього впливу на суспільні відносини.

ЛІТЕРАТУРА:

1. *Шевчук С. Доктрина верховенства права та конституціоналізму: історична ґенеза і співвідношення. Право України. 2010. №3. с. 52.*
2. *Верховенство права. Законодавчий бюлетень. Київ, 2005. с. 5.*
3. *Ткачук П. Застосування принципу верховенства права судами конституційної та загальної юрисдикції. Вісник Конституційного Суду України. 2005. №5. с. 94.*
4. *Верховенство права. Законодавчий бюлетень. Київ, 2005. с.-5-6.*
5. *Правова система України: історія, стан та перспективи: у 5 т. Харків: Право, 2008. Т. 1. с. 151.*
6. *Юридична енциклопедія: в 6 т./ Редкол.: Ю.С. Шемчушенко та ін.. Київ, 2003. Т. 5. П-С. 736 с.*

УДК 351.746:007

Грубінко А.В.
д.і.н., професор, професор кафедри теорії та історії держави і права Західноукраїнського національного університету

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ПОЛІТИКИ КІБЕРБЕЗПЕКИ ЄВРОПЕЙСЬКОГО СОЮЗУ

Гарантування міжнародної інформаційної безпеки та кібербезпеки як її складової залишається одним із стратегічних завдань діяльності ЄС. Через

високого рівня популяризацію Інтернету і цифрових послуг в світі країни ЄС особливо схильні піддаватися загрозі кібератак.

Для Європейського Союзу політика кібербезпеки набула комплексного стратегічного виміру досить пізно. У 2001 р. Європейська комісія представила перший документ «Network and Information Security: Proposal for A European Policy Approach», в якому окреслено європейський підхід до проблеми інформаційної безпеки [1]. Атаки на інформаційні системи можуть мати серйозні наслідки у національному масштабі, наприклад, збої в роботі систем комунікацій, витік конфіденційної інформації тощо.

У лютому 2005 р. Рада ЄС прийняла Рамкове рішення 2005/222/JHA про напад на інформаційні системи, встановивши мінімальні правила щодо визначення кримінальних злочинів і санкцій. У травні 2007 р. Європейська комісія представила документ «Towards a general policy on the fight against cyber crime», в якому висвітлено основні напрями політики ЄС у протидії кіберзлочинності [2]. 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 «Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience», в якому визначено проблеми, що потребують негайного реагування ЄС [3].

Практичне формування автономної кіберполітики ЄС розпочалося лише після затвердження в лютому 2013 р. Стратегії кібербезпеки «Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace». 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 [4, p. 12].

Відомі резонансні події навколо і в середині ЄС, такі як втручання Росії у вибори в США у 2016 році та інших країнах, Brexit і невизначеність щодо майбутнього трансатлантичних відносин після обрання Дональда Трампа на пост президента Сполучених Штатів 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 року 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 [5]. У липні 2016 р. прийнята чергова Директива ЄС «Concerning measures for a high common level of security of network and information systems across the Union», яка сформувала єдині правила та вимоги в сфері кібербезпеки для всіх країн-членів.

Накопичення великих масивів інформації і оперування ними, надання електронних послуг, початкове підключення в Європейському Союзі у

найближчі роки понад 1 мілрд. пристроїв до електронних мереж надає не лише переваги, але й здійснює негативний вплив – зростає кількість кібернетичних загроз. Європейська Комісія у 2017 р. запропонувала своє бачення нової архітектури європейської кібернетичної безпеки – опублікований у вересні 2017 року документ «Resilience, Deterrence and Defence: Building strong cybersecurity for the EU». Запропоновано механізми посилення стійкості ЄС до кібератак шляхом утворення Європейської Агенції з кібербезпеки (у 2020 році замінила Європейську асоціацію мереж та інформаційної безпеки (ENISA), запровадження загальноєвропейської системи сертифікації кібербезпеки для продуктів та послуг ІКТ.

Виникнення 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 проекту нової Стратегії кібербезпеки ЄС, представленого публічно 16 грудня 2020 року. Символічно, що за тиждень до цієї події, 9 грудня 2020 року 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 військово 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 [6]. Таким чином, в ЄС намагаються діяти відповідно до вимог часу та адекватно відповідати на нові вклики і загрози у сфері кібербезпеки.

Отже, Європейський Союз в силу своїх економічних інтересів, глобальних амбіцій і видів загроз безпеці з певним успіхом намагається розробити і реалізувати надійну політику кібербезпеки, яка б грунтувалася на відповідних інструментах і функціональних інститутах.

Європа зацікавлена в комплексній розробці політики кібербезпеки ЄС. В Євросоюзі не зупиняються на досягнутому та постійно прагнуть розвивати можливості протистояння і попередження кіберзагрозам з метою досягнення стратегічної автономії організації. Прийняття запропонованої Європейською комісією нової Стратегії кібербезпеки ЄС значно підвищисть якість боротьби з кіберзагрозами в сучасних умовах диверсифікації зовнішніх і внутрішніх викликів безпеці об'єднання.

ЛІТЕРАТУРА:

1. *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: 08.02.2021).
2. *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: 08.02.2021).*
3. *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: 12.02.2021).*
4. *Challenges to effective EU cybersecurity policy Briefing Paper March 2019. European Union, 2019. 72 p.*
5. *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy. June 2016. Brussels. 56 p.*
6. *Shaping Europe's digital future. Policy. Cybersecurity. European Commission. URL: https://ec.europa.eu/digital-single-market/en/cybersecurity (дата звернення: 10.02.2021).*

УДК 340 (073)

Зварич Д. І.
к. психол. н., доцент кафедри теорії та історії держави і права Західноукраїнського національного університету

ПРАВОВІ ЗАСАДИ ПОПЕРЕДЖЕННЯ НАСИЛЬСТВА В СІМ'Ї

Насильство в сім'ї – будь-які умисні дії фізичного, сексуального, психологічного чи економічного спрямування одного члена сім'ї по відношенню до іншого члена сім'ї, якщо ці дії порушують конституційні права і свободи члена сім'ї як людини та громадянина і наносять йому моральну шкоду, шкоду його фізичному чи психічному здоров'ю. В Україні щороку фіксується понад 100 тис. звернень за фактами насильства в сім'ї. Світовий досвід говорить про те, що насильство в сім'ї має місце незалежно від релігійних переконань чи етнічного походження, соціального статусу чи сексуальної орієнтації.