Вісник Львівського університету. Серія філос.-політолог. студії. 2019. Випуск 26, с. 201-207
Visnuk of the Lviv University. Series Philos.-Political Studies. Issue 26, p. 201-207

УДК 351.746:316.77-049.5](4-6ЄС+73)
DOI https://doi.org/10.30970/2307-1664.2019.26.25

ДЕРЖАВНА ПОЛІТИКА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У США ТА ЄС

Євгеній Таран
Національна академія державного управління при Президентові України,
кафедра суспільного розвитку і суспільно-владних відносин,
вул. А. Цедіка, 20, 04112, м. Київ, Україна

Стаття розкриває державну політику забезпечення інформаційної безпеки у Сполучених Штатах Америки та Європейському Союзі.

Проведення ефективної інформаційної політики – важливе питання порядку денного у тих країнах світу, які дбають про свою інформаційну безпеку, особливо в умовах інформаційного суспільства.

Через це є необхідність проаналізувати особливості її проведення різними країнами світу та об'єднаннями країн, розкрити її зміст та сутність, вивчити кращі підходи до її вироблення та визначити ефективні механізми забезпечення інформаційної безпеки України.

Будучи двома потужними світовими акторами, ЄС та США мають різні підходи до політики забезпечення інформаційної безпеки. США поставили собі за мету здійснення інформаційного захисту як усередині країни, так і проведення ефективної інформаційної політики на світовій арені, яка б поширювалася на інші країни світу. Сполучені Штати Америки мають на меті розширення свого впливу на інші країни світу шляхом надання їм різносторонньої інформаційної підтримки та забезпечення захисту їх національних інтересів в обмін на підтримку позицій США цими країнами у різних міжнародних організаціях, наприклад ООН та МВФ. Це дає змогу забезпечити лідерство США не лише в інформаційній, але й у глобальній системі міжнародних відносин.

Європейський Союз також активно проводить свою інформаційну політику. Будучи об'єднанням розвинутих країн, Євросоюз може здійснювати потужний інформаційний вплив на міжнародні відносини та встановлювати стандарти поведінки в інформаційній, економічній, соціальній та інших сферах.

Перебуваючи в умовах потужного інформаційного тиску з боку Російської Федерації, політика забезпечення інформаційної безпеки стала одним зі стратегічних завдань ЄС. Європейський Союз розробляє заходи, які б дали змогу захистити свій внутрішній інформаційний простір від російських негативних втручань.

Надзвичайно актуальним це питання є для України, оскільки, перебуваючи в умовах гібридної війни та інформаційного протистояння з Російською Федерацією, наша країна має вивчати найкращий світовий досвід забезпечення інформаційної безпеки, брати на озброєння механізми захисту свого інформаційного простору від зовнішніх впливів та проводити інформаційну політику, яка б захищала її інформаційний суверенітет.

Ключові слова: інформаційна політика, інформаційна безпека, кібербезпека, ЄС, США.

Усе більше країн планети підпадають під процеси інформаційно-комунікаційної революції, яка визначає шлях розвитку сучасної цивілізації та характеризується формуванням і поширенням інформаційного суспільства по всьому світу. Оскільки основна роль у цих процесах відведена інформаційно-комунікаційним технологіям, ефективна інформаційна політика держав світу відіграє потужну роль у забезпеченні їхньої інформаційної безпеки, а здебільшого інформаційної безпеки інших, менш потужних країн.

Соціальний прогрес держави у XXI ст. та її конкурентоздатність залежать від рівня інтеграції інформаційно-комунікаційних технологій у процеси державотворення.

Аналізуючи результати функціонування інформаційного суспільства, видно, що різні країни, групи країн та їх населення мають неоднаковий рівень життя. Найуспішнішими є ті, хто спроможний адаптуватися до інформаційних змін, користується та впроваджує інформаційні технології у повсякденне життя.

Через це питання інформаційної безпеки та проведення ефективної інформаційної політики посідає важливе місце у системі забезпечення однієї окремо взятої країни, групи країн та світу загалом.

Метою дослідження є аналіз державної політики забезпечення інформаційної безпеки провідних світових акторів, виявлення закономірностей та характерних рис цього явища.

Під час дослідження такої проблематики використовувалися загальнонаукові методи дослідження. За допомогою методу дедукції, від загального до конкретного, було досліджено загальні підходи до явища інформаційної безпеки та відношення до неї провідних світових акторів. Цей метод дає змогу виявити загрози інформаційній безпеці, які виникають у різних країнах світу.

За допомогою проблемного підходу було зроблено аналіз основних проблем безпеки, які мають місце на фоні переходу від двополярної до однополярної моделі світу, що несе із собою збільшення протиріч у військовій, політичній та економічній сферах.

За допомогою формально-правового методу було проаналізовано законодавчо-нормативну базу, яка стосується інформаційної політики та інформаційної безпеки.

Поняття інформаційної безпеки почали все частіше стояти на порядку денному в різних кранах у зв'язку зі становленням інформаційного суспільства. Цьому сприяли швидкі темпи всезагальної інформатизації. Для успішного функціонування інформаційного суспільства держава має проводити відповідну політику, яка б забезпечувала всебічний розвиток і впровадження інформаційних технологій у життя суспільства, а також забезпечувала б інформаційну безпеку користувачів новітніх технологій.

Найбільш інформаційно розвиненою країною вважається США, оскільки вона першою зрозуміла вислів про володіння інформацією. Саме Сполучені Штати Америки запровадили систему захисту інформації на законодавчому рівні. У Сполучених Штатах Америки закони, що стосуються сфери захисту інформації, діють з 1974 року [1, с. 89].

США були першою країною, яка почала розбудову інформаційного суспільства. Починаючи з другої половини XX ст. Сполучені Штати Америки, зосередившись на створенні передових інформаційних технологій, спромоглися стати лідером у їх розробці і впровадженні, перетворивши їх на стратегічний ресурс. Оскільки інформаційна інфраструктура у США та питання інформаційної безпеки тісно пов'язані між собою, то інформаційна політка в цій державі є пріоритетною для забезпечення національної безпеки.

Хоча США і мають могутню армію з найновішою зброєю і технікою, уряд Сполучених Штатів Америки виділяє великі кошти, які спрямовуються на забезпечення інформаційної безпеки.

Інформаційна політика США полягає у розширенні свого впливу по всьому світу, а особливо в країнах Центральної та Східної Європи, Латинської Америки, країнах Близького Сходу та Азійсько-Тихоокеанського регіону. На зміну доктрині «ядерної парасольки», яка існувала в період холодної війни, прийшла доктрина «інформаційної парасольки». Її особливістю є те, що Сполучені Штати Америки надають іншим країнам різносторонню інформаційну підтримку, захищаючи їхні національні інтереси. В обмін ці країни підтри-

мують США у різних міжнародних організаціях – ООН, МВФ тощо. Це допомагає забезпечувати США позиції лідера у системі міжнародних відносин.

Натепер економічний розвиток багатьох кран світу забезпечується через використання американських інформаційних технологій. З одного боку, це говорить про потужність інформаційно-технологічного комплексу США, а з іншого – робить ці країни залежними у технологічному відношенні від США [4, с. 85].

Американська політика у сфері інформаційної безпеки спрямована на досягнення домінування США у глобальному просторі. Оскільки інформаційні ресурси використовуються практично в усіх сферах безпеки, інформаційне домінування перетворилося на важливий аспект технологічного, економічного, військового і політичного домінування США над іншими державами. Інформаційна політика США поєднує як інструменти лібералізації і регулювання інформаційної сфери, так і намагання встановити прямий державний контроль над інформаційними ресурсами в національних і міжнародних масштабах.

Хоча американська армія вважається найсильнішою у світі і жодна інша держава не наважиться почати проти неї війну, в сучасному світі є інші небезпеки, наприклад терористичні атаки, що можуть бути здійснені особами, які мають комп'ютери та вихід до інформаційних мереж. Для контролю і попередження подібних загроз США використовують космічні технології, за допомогою яких вони можуть отримувати інформацію про своїх можливих супротивників та застосувати превентивні дії у разі підозр.

Інформаційні технології разом з космічними засобами допомагають відслідковувати супротивника та знищувати його. Це значить, що США за допомогою інформаційних технологій можуть знешкоджувати засоби інформаційної зброї, руйнуючи їх інформаційні системи.

Європейський Союз пішов іншим шляхом у забезпеченні своєї інформаційної безпеки. Хоча заходи із забезпечення інформаційної безпеки почали реалізовуватися з часу створення цього об'єднання, однією з найбільших загроз стала російська пропаганда, яка активізувала свої агресивні дії у 2014 році. Гарантування міжнародної інформаційної безпеки залишається одним зі стратегічних завдань діяльності ЄС, оскільки більшість сучасних конфліктів як військового, так і політичного характеру відбуваються у віртуальному просторі.

У 2001 р. Європейською комісією було представлено перший документ під назвою «Мережева та інформаційна безпека: європейський політичний підхід». У цьому документі окреслено європейський підхід до проблеми інформаційної безпеки. У ньому 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 [10].

Як зазначають посадові особи ЄС, інформаційна безпека перетворюється на ключовий фактор у розвитку інформаційного суспільства. Інформаційні системи містять конфіденційні економічні дані, які першочергово підпадають під атаки.

Оскільки Інтернет має як позитивні, так і негативні сторони у становленні глобального та європейського суспільства, проблеми безпеки цієї мережі набувають особливої актуальності.

У 1996 році Єврокомісією була прийнята Резолюція про запобігання поширенню в мережі Інтернет інформації незаконного змісту, яка шкодить моральному здоров'ю суспільства. Відповідно до цієї Резолюції поняття «шкідливий зміст» залежить від культурних традицій, а поняття «незаконний зміст» – від чинного законодавства [7].

Відповідно до Резолюції основними заходами, які забезпечують безпеку інформації в мережі Інтернет, є [3, с. 232]:

1) забезпечення свободи комунікації онлайн;

2) визначення обов'язків постачальників послуг;

3) запровадження захисту інтелектуальної інформації в режимі онлайн;

4) забезпечення ефективного регулювання змісту інформації, що є в мережі Інтернет;

5) забезпечення захисту персональних даних;

6) забезпечення правового статусу документів;

7) забезпечення вільного доступу до інформації в мережі Інтернет для масового використання.

10 березня 2004 р. було створено Європейське агентство з питань мережевої та інформаційної безпеки (ENISA), яке є єдиним агентством у ЄС, якому було визначено конкретний термін завершення дії у 2020 р. Це агентство функціонує з 1 вересня 2005 р., знаходиться в Іракліоні (Крит, Греція). Метою ENISA є вдосконалення інформаційної та мережевої безпеки в ЄС. Воно допомагатиме Єврокомісії, державам-членам ЄС та приватному сектору забезпечувати виконання вимог інформаційної безпеки, контролювати дотримання чинного та майбутнього законодавства ЄС. ENISA надає консультації як державам-членам, так і інституціям ЄС з питань, пов'язаних з інформаційною безпекою [5].

ENISA здійснює процес управління загальноєвропейською програмою "Cyber Europe", яка є серією навчань з кіберінцидентів і управління кризовими ситуаціями на рівні ЄС для державного і приватного секторів. Вправи, які розробляє та практикує "Cyber Europe", – це симуляція великомасштабних інцидентів, пов'язаних з кібербезпекою, які, посилюючись, можуть стати кіберкризами. Вправи пропонують можливості для аналізу передових технічних заходів з кібербезпеки, вирішення проблем, пов'язаних із кризовими ситуаціями. Вони являють собою сценарії, насичені реальними подіями, розробленими європейськими експертами з кібербезпеки. Кожна з вправ надає навчальний досвід для учасників [8].

У зв'язку з високою оснащеністю суспільства комп'ютерними технологіями боротьба з кіберзлочинністю є дуже актуальною для країн ЄС.

У травні 2007 р. Європейською комісією представлено документ «На шляху до загальної політики в сфері боротьби з кіберзлочинністю», в якому дається визначення терміна «кіберзлочинність» та висвітлено основні напрями політики ЄС у протидії кіберзлочинності [12].

Відповідно до цього документа кіберзлочинність – це кримінальні дії, які скоєні із використанням електронних комунікаційних мереж та інформаційних систем. До цього поняття включено такі категорії злочинів:

– традиційні форми злочину, до яких належать шахрайство та підробки в електронних комунікаційних мережах та інформаційних системах;

– публікації незаконного контенту в електронних медіа (дитяча порнографія, матеріали із закликами до расової ненависті тощо);

– специфічні злочини в електронних мережах (атаки на електронні мережі, хакерство) [2, с. 39].

У березні 2009 року було видано Повідомлення Європейської комісії «Захист Європи від широкомасштабних кібератак і руйнувань: посилення рівня підготовленості, безпеки та стійкості», де було визначено основні виклики, які потребували негайного прийняття рішень ЄС, а також визначено основні заходи, які необхідні для підвищення рівня безпеки та спроможності європейської інформаційної інфраструктури у протистоянні із зовнішніми впливами [6].

Оскільки інформаційне суспільство надало кожному громадянинові країн-учасниць ЄС право доступу до даних відкритого характеру (закони, урядові рішення), культурної спадщини (літературні твори, наукові праці, програмне забезпечення), а також до інформації відкритого характеру в комп'ютерних мережах і системах, що потребують осмислення відповідальності за здійснення нової політики, серйозною проблемою для ЄС став захист персональних даних [9].

У 2017 році Європейською комісією було представлено новий документ «Стійкість, стримування та захист: створення спільної кібербезпеки для ЄС». У цьому документі зазначено, що кібербезпека має вирішальне значення для процвітання та безпеки країн-членів. Якщо заходи із забезпечення кібербезпеки не будуть прийматися, то ризик загроз збільшуватиметься відповідно до цифрових перетворень.

Політична напруга в суспільстві та недоліки військового кіберзахисту підвищують ризики у цій сфері. Хоча на країни-члени ЄС покладена відповідальність за національну безпеку, масштаби та транскордонний характер кіберзагроз створюють стимули для держав-членів щодо збільшення і підвищення рівня кібербезпеки ЄС загалом. Сильна кіберстійкість вимагає колективного і широкомасштабного підходу. Для цього необхідно створення більш надійних заходів, які б сприяли забезпеченню кібербезпеки та змогли б вчасно реагувати на кібератаки в країнах-членах ЄС, установах та організаціях [11].

Як вважає Єврокомісія, протидія інформаційним загрозам вимагає великих коштів для захисту своєї цифрової економіки.

Європейська комісія усвідомлює, що ефективність забезпечення інформаційної безпеки залежить від розвитку співпраці держав у рамках міжнародних органів, діяльність яких спрямована на протидію кіберзлочинності. Проводяться заходи зі створення європейської системи сповіщення про злочини у мережі Інтернет з метою кращої координації їх розкриття.

Зважаючи на значний досвід, який має ЄС у виробленні інформаційної політики, Україна має стати активним учасником цих безпекових процесів. Це підвищить рівень інформаційної безпеки України та позитивно сприятиме євроінтеграційним прагненням нашої держави.

На відміну від США, Європейський Союз не ставить собі за мету отримання інформаційної переваги серед усіх інших країн та не проводить політику світового гегемона. Він не намагається взяти під контроль різні країни та групи країн, які можуть бути потенційними супротивниками.

Оскільки США є безперечним лідером з виробництва інформаційної продукції, країни ЄС не можуть конкурувати з ними на рівних. Відкриваючи свої інформаційні кордони для продукції, яка виготовлена у США, країни ЄС не можуть захистити себе від американських технологій, що може негативно вплинути на виробників іноземної продукції в країнах ЄС та на рівень інформаційної безпеки.

Головне своє завдання у проведенні інформаційної політики та забезпеченні інформаційної безпеки ЄС вбачає у вжитті заходів, які дадуть змогу попереджувати та змінювати наслідки від зовнішніх інформаційних впливів. Розуміючи важливість єдиної системи інформаційного захисту, Європейський Союз намагається організувати колективний і широкомасштабний підхід до забезпечення інформаційної безпеки як окремих держав-членів ЄС, так і об'єднання загалом.

Щодо можливостей України у питаннях співпраці з ЄС та США у сфері забезпечення інформаційної безпеки, то можемо зазначити, що Україна є одним з лідерів з підготовки спеціалістів у ІТ-галузі, при цьому більшість цих спеціалістів від'їжджає за кордон. Укра-

їна є залежною від американського програмного продукту, як і практично будь-яка інша країна та окремі громадяни.

З огляду на це Україна має проводити свою державну політику у тому напрямі, щоб спрямувати зусилля на створення власних конкурентоздатних ІТ-технологій та створення умов для того, щоб ІТ-спеціалісти не їхали за кордон.

Разом із тим США мають величезний досвід впровадження інформаційних технологій у діяльність державних органів. Особливо важливим для України є військовий досвід використання інформаційних технологій для створення систем зв'язку, військового управління та високоточного озброєння.

Список використаної літератури

1. Беляков К. Інформація організаційно-правової сфери. *Право України*. 2004. № 6. С. 88–92.
2. Запорожець О.Ю. Політика Європейського Союзу в сфері інформаційної безпеки. *Актуальні проблеми міжнародних відносин.* 2009. Вип. 87, ч. ІІ. С. 36–45.
3. Макаренко Є.А. Міжнародна інформаційна політика: структура, тенденції, перспективи : дис... д-ра політич. наук : 23.00.04. Націон. ун-т ім. Т. Шевченка. Київ, 2003. 475 с.
4. США в меняющемся мире / под. общ. ред. Кривохижи В.И. РИСИМ, 1997. 85 с.
5. About ENISA / European Union Agency for Network and Information Security. URL: https://www.enisa.europa.eu/about-enisa.
6. Communication from the Commission on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience": adopted by the European Commission on 30 March 2009 / European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52009DC0149.
7. Convention on Cybercrime. Explanatory Report. Budapest, 23, November, 2001. Council of Europe. URL: www.europa.eu.
8. Cyber Europe / European Union Agency for Network and Information Security. URL: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.
9. Europe and Global Information Society. Recommendations of the High-Level Group on the Information Society to the Corfu European Council (Bangemann Group). European Commission, 1994.
10. Network and information security: proposal for a european policy approach: adopted by the European Commission on 6 June 2001 / European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52001DC0298.
11. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU: adopted by the European Commission on 13 September 2017 / European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:0450:FIN.
12. Towards a general policy on the fight against cyber crime: adopted by the European Commission on 22 May 2007 / European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14560.

NATIONAL INFORMATION SECURITY POLICY IN THE USA AND THE EU

Yevhenii Taran
National Academy for Public Administration under the President of Ukraine,
Social Development and Public-Power Relations Department,
A. Tsedika str., 20, 04112, Kyiv, Ukraine

The article describes the public policy of information security in the United States of America and the European Union.

Implementing an effective information policy raises an important agenda issue in those countries that care about their information security, especially in the context of the information society.

Therefore, there is a need to analyze the peculiarities of conducting it in different countries and associations of countries, to reveal its content and essence, study the best approaches to its development and identify effective mechanisms for ensuring information security of Ukraine.

Being two powerful global actors, the EU and the US take different approaches to their existing information security. The United States have demined their goal as conducting information defense both inside the country and carrying out information policy on the global arena, which would spread on other countries of the world. The United States has an aim of expanding its influence on other countries of the world by means of providing them with various information support and protection of their national interests in return for their support of the US positions in different international organizations, for instance the UN and the IMF. This allows to secure the US leadership not only in the information but also in the global system of international relations.

The European Union is also actively pursuing its information policy. Being a union of developed countries, the EU can carry out a powerful information influence on international relations and set standards for behavior in the information, economic, social and other areas.

In the face of intense information pressure from the Russian Federation, information security gossip has become one of the EU's strategic objectives. The European Union is developing measures to protect its internal information space from Russian negative interference.

This issue is extremely urgent for Ukraine, because under the circumstances of hybrid war and information confrontation with the Russian Federation, our country must study the best world experience in providing information security, adopt mechanisms for protecting its information environment from external influences and pursue the information policy that would protect its information sovereignty.

Key words: EU, US, information security, information policy, cybersecurity.