УДК 351.746:316.77-049.5](4-6ЄС+73)
DOI https://doi.org/10.30970/2307-1664.2019.25.23

ПОЛІТИКА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У США ТА ЄС: ДОСВІД ДЛЯ УКРАЇНИ

Євгеній Таран
Національна академія державного управління при Президентові України,
кафедра суспільного розвитку і суспільно-владних відносин
вул. А. Цедіка, 20, 03057, м. Київ, Україна

У статті розглянуто державну інформаційну політику провідних світових акторів, зокрема Сполучених Штатів Америки та Європейського Союзу.

Оскільки проведення ефективної інформаційної політики стоїть на порядку денному в сучасних умовах розвитку інформаційного суспільства в усіх країнах, які дбають про свою інформаційну безпеку, існує необхідність розкрити її зміст, сутність та особливості її проведення провідними країнами світу й об'єднаннями країн задля вивчення кращих підходів і вироблення ефективних механізмів забезпечення інформаційної безпеки України.

При цьому варто зазначити, що підходи до політики забезпечення інформаційної безпеки США та ЄС відрізняються між собою. Мета США полягає не лише в інформаційному захисті всередині країни, а й у проведенні ефективної інформаційної політики, яка б поширювалася на інші країни світу, з метою досягнення інформаційної переваги над будь-якою країною. Метою США є розширення свого впливу на інші країни світу через надання їм усілякої інформаційної підтримки, захист їхніх національних інтересів та отримання підтримки цих країн у різних міжнародних організаціях, наприклад, ООН, МВФ тощо. Такий підхід забезпечує лідерство США не лише в інформаційній, а й у глобальній системі міжнародних відносин.

Активну роль у сфері інформаційної політики проводить і Європейський Союз. Оскільки до ЄС входять розвинені країни, вони можуть здійснювати потужний вплив на міжнародні відносини, встановлюючи стандарти поведінки в інформаційній, економічній, соціальній та інших сферах.

В умовах потужного інформаційного тиску з боку Російської Федерації політика забезпечення інформаційної безпеки є одним зі стратегічних завдань ЄС. Водночас ЄС проводить заходи із захисту свого внутрішнього інформаційного простору від російських негативних втручань.

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

Сучасна цивілізація характеризується формуванням і розповсюдженням інформаційного суспільства по всьому світу. Роль, що зростає, нових інформаційно-комунікаційних технологій призвела до інформаційно-комунікаційної революції, де інформаційна політка держави посідає ключове місце в забезпеченні її інформаційної безпеки, а також може розповсюджуватися на інформаційну безпеку інших країн, які є інформаційно-залежними від світових лідерів.

Рівень інтеграції інформаційно-комунікаційних технологій у процеси державотворення визначає конкурентоздатність сучасної держави та її соціальний прогрес у XXI ст.

Результати функціонування інформаційного суспільства призводять до значної нерівності в розвитку, рівні життя й доходів громадян різних країн. Швидка адаптація до інформаційних змін дає змогу країнам і їх населенню займати лідируючі позиції порівняно з іншими країнами й отримувати відповідні вигоди.

Через це інформаційна політика країни та забезпечення її інформаційної безпеки є важливим показником успішності країни або групи країн.

Метою дослідження є вивчення проведення державної політики забезпечення інформаційної безпеки в ЄС і США для визначення кращих здобутків у цій сфері з метою їх реалізації в українській державній політиці.

Швидкі темпи інформатизації вивели питання забезпечення інформаційної безпеки на порядок денний різних країн. Особливої актуальності вони набувають у країнах, які акцентують свій розвиток на побудову інформаційного суспільства. Для успішного функціонування інформаційного суспільства держава повинна проводити відповідну політику, яка б забезпечувала всебічний розвиток і впровадження інформаційних технологій у життя суспільства, а також 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 із 1974 р. [1, с. 89].

Сполучені Штати Америки є першою країною, яка почала розбудову інформаційного суспільства та зосередила свій розвиток на розбудові новітніх інформаційних технологій, що дало їй змогу зайняти лідируючі позиції в їх упровадженні серед інших кран світу, перетворивши інформаційну галузь на стратегічний ресурс. Оскільки інформаційна інфраструктура у США та питання інформаційної безпеки тісно пов'язані між собою, інформаційна політка в цій державі є пріоритетною для забезпечення національної безпеки.

Незважаючи на те що США мають наймогутнішу армію у світі з найновішою зброєю й технікою, уряд Сполучених Штатів Америки виділяє великі кошти, які спрямовуються на забезпечення інформаційної безпеки.

Мета інформаційної політики США полягає в розширенні світового впливу по всьому світу, а особливо в країнах Центральної та Східної Європи, Латинської Америки, країнах Близького Сходу й Азійсько-Тихоокеанського регіону.

Після закінчення Холодної війни США запровадили доктрину «інформаційної парасольки», яка прийшла на зміну «ядерній парасольці», що існувала під час Холодної війни. Особливістю доктрини «інформаційної парасольки» є те, що США зацікавлені надавати менш розвиненим країнам різнобічну інформаційну підтримку та захищати їхні національні інтереси, а в обмін на це ці країни будуть підтримувати США в різних міжнародних організаціях – ООН, НАТО тощо. Така ситуація дає США змогу утримувати позиції лідера в 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 в технологічному стосунку від США [4, с. 85].

Мета американської політики інформаційної безпеки полягає в досягненні домінування США в глобальному просторі. Інформаційна перевага США перетворилася на важливий аспект технологічного, економічного, військового й політичного домінування Сполучених Штатів Америки над іншими державами. В інформаційній політиці США поєднує інструменти лібералізації та регулювання інформаційної сфери, а також намагається встановити прямий державний контроль над інформаційними ресурсами в національних і міжнародних масштабах.

Хоча американська армія вважається найсильнішою у світі й жодна інша держава не наважиться почати проти неї війну, в сучасному світі існують інші небезпеки, наприклад, терористичні атаки, які можуть бути здійснені особами, що мають комп'ютери та вихід до інформаційних мереж. Для контролю подібних загроз і запобігання їм США

використовують космічні технології, за допомогою яких можуть отримувати інформацію про своїх можливих супротивників і застосувати превентивні дії в разі підозр.

Інформаційні технології разом із 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.

Дещо іншим шляхом у забезпеченні своєї інформаційної безпеки пішов ЄС. Незважаючи на те що із самого початку утворення цього об'єднання приділялася належна увага забезпеченню інформаційної безпеки, однією з найбільших загроз сучасності стала російська пропаганда, яка активізувала свої агресивні дії у 20014 р.

Попри це, 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 представлено перший документ під назвою «Мережева та інформаційна безпека: європейський політичний підхід», у якому окреслено європейський підхід до 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, що становлять загрозу доступності, автентичності, цілісності й конфіденційності даних, що зберігаються або передаються, а також послуг, що надаються через ці мережі та системи [10].

Відповідно до заяв керівних осіб ЄС, ключовим фактором у розвитку інформаційного суспільства є інформаційна безпека, оскільки інформаційні системи містять конфіденційні економічні дані, на які здійснюються атаки першочергово.

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

У 1996 р. Єврокомісія прийняла Резолюція про запобігання поширенню в мережі Інтернет інформації незаконного змісту, яка шкодить моральному здоров'ю суспільства. Відповідно до цієї Резолюції, поняття шкідливого змісту залежить від культурних традицій, а поняття «незаконного змісту» – від чинного законодавства [7].

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

1) забезпечення свободи комунікації он-лайн;
2) визначення обов'язків постачальників послуг;
3) запровадження захисту інтелектуальної інформації в режимі он-лайн;
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. створено Європейське агентство з питань мережевої та інформаційної безпеки (ENISA), яке є єдиним агентством у ЄС, якому визначено конкретний термін завершення його дії у 2020 р. Це агентство функціонує з 1 вересня 2005 р., знаходиться в м. Іракліон, Крит, Греція. Метою ENISA є вдосконалення інформаційної та мережевої безпеки в ЄС. Воно допомагатиме Єврокомісії, державам-членам ЄС і приватному сектору забезпечувати виконання вимог інформаційної безпеки, контролювати дотримання чинного та майбутнього законодавства ЄС. ENISA надає консультації як для держав-членів, так і для інституцій ЄС із питань, пов'язаних з інформаційною безпекою [5].

ENISA здійснює процес управління загальноєвропейською програмою "Cyber Europe", яка є серією навчань із кіберінцидентів та управління кризовими ситуаціями на рівні ЄС для державного і приватного секторів. Вправи, які розробляє та практикує "Cyber Europe", – це симуляція великомасштабних інцидентів, пов'язаних із кібербезпекою, що, посилюючись, можуть стати кіберкризами. Вправи пропонують можливості для аналізу передових технічних заходів із 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 терміну «кіберзлочинність» та висвітлено основні напрямки політики ЄС у протидії кіберзлочинності [12].

У цьому документі кіберзлочинність характеризується як кримінальні дії, які скоєні під час використання інформаційних систем та електронних комунікаційних мереж. Це поняття включає такі категорії злочинів:

– традиційні форми злочину, до яких належать шахрайство й 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 р. видано Повідомлення Європейської комісії «Захист Європи від широкомасштабних кібератак і руйнувань: посилення рівня підготовленості, безпеки та стійкості» [6], де визначено основні виклики, які потребували негайного прийняття рішень ЄС, а також основні заходи, необхідні для підвищення рівня безпеки та спроможності європейської інформаційної інфраструктури в протистоянні із зовнішніми впливами.

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 р. Європейською комісією представлено новий документ «Стійкість, стримування та захист: створення сильної кібербезпеки для ЄС» [11], де 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.

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

Інтегруючись до ЄС, Україна має вивчити досвід цього об'єднання у виробленні інформаційної політики. При цьому Україна повинна стати основним учасником безпекових процесів. Це позитивно сприятиме євроінтеграційним прагненням нашої держави та підвищить рівень інформаційної безпеки України.

Як показує вищевикладене дослідження, ЄС, на відміну від США, не має бажання бути світовим гегемоном і не намагається забезпечити собі інформаційне лідерство серед інших країн. Він не має на меті взяти під свій контроль різні країни або групи країн, які можуть бути його потенційними супротивниками.

Так як США є лідером у розробленні, виробництві й упровадженні інформаційної продукції, країни Європейського Союзу не можуть скласти їм гідну конкуренцію. При цьому, даючи змогу широко використовувати в країнах ЄС американські продукти, вони не можуть захисти себе від американських технологій, що може негативно вплинути на рівень інформаційної безпеки.

ЄС головне своє завдання в забезпеченні інформаційної безпеки вбачає в запровадженні заходів, які дадуть змогу запобігати наслідкам і змінювати наслідки від зовнішніх інформаційних впливів. Розуміючи важливість єдиної системи інформаційної захисту, Європейський Союз намагається організувати колективний і широкомасштабний підхід до забезпечення інформаційної безпеки як окремих держав-членів ЄС, так й об'єднання загалом.

Щодо досвіду ЄС і США, який Україна може використати у сфері забезпечення інформаційної безпеки, то, будучи одним із лідерів з підготовки ІТ спеціалістів, Україна повинна спрямувати свої зусилля на створення власних конкурентних ІТ технологій і створення необхідних умов для ІТ спеціалістів, які натепер у великій кількості їдуть за кордон, зокрема в країни ЄС і США, де для них створюються достойні умови.

Досвід США з упровадження інформаційних технологій у роботу державних органів є важливими для України в період воєнних дій, оскільки це дає можливість ефективніше використовувати інформаційні технології 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. ... докт. політ. наук : 23.00.04 / Націон. ун-т ім. Т. Шевченка. Київ, 2003. 475 с.
4. США в меняющемся мире / под общ. ред. В.И. Кривохижи. *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.

POLICY OF PROVIDING INFORMATION SECURITY IN THE US AND EU: EXPERIENCE FOR UKRAINE

Yevhenii Taran
National Academy for Public Administration under the President of Ukraine,
Social Development and Public-Power Relations Department
A. Tsedika str., 20, 03057, Kyiv, Ukraine

The article looks at the state information policy of the leading world actors, in particular the United States of America and the European Union. Since efficient information policy is on the agenda in the current conditions of information society development in all countries that care about their information security, there is a need to disclose its content, essence and features of its leading countries and associations of countries to study the best approaches and development of effective mechanisms for ensuring information security of Ukraine.

However, it should be mentioned that approaches to the US and the EU information security policies differ. The goal of the United States is not only to protect information domestically, but also to pursue an effective information policy that spreads to other countries of the world, in order to achieve information superiority over any other country. The goal of the US is to expand its influenice on other countries around the world by providing them with all kinds of information support, protecting their national interests while obtaining these countries' support in various international organizations, such as the UN, the IMF, etc. This approach ensures US leadership not only in the information but also in the global system of international relations.

The European Union also plays an active role in the area of information policy. Since the EU consists of developed country, they can have a strong influence on international relations by setting standards of behaviour in the information, economic, social and other areas.

In the face of intense information pressure from the Russian Federation, information security policy is one of the EU's strategic objectives. At the same time, the EU is taking measures to protect its internal information environment from negative Russian interference.

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