УДК 316.774

Глушко Аліна Дмитрівна,
кандидат економічних наук, доцент
Колінчук Дарія Володимирівна,
Ярмак Олександр Вікторович, *магістранти,*
Національний університет «Полтавська політехніка імені Юрія Кондратюка» (Україна)

СТРАТЕГІЧНІ НАПРЯМИ ЗМІЦНЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ДОСВІД ЄС

В сучасних умовах інформаційне середовище виступає полем взаємодії і, водночас, протистояння суб'єктів міжнародних відносин. Це вимагає впровадження ефективної державної політики в напрямі забезпечення безпеки усіх учасників. Досвід Європейського Союзу заслуговує на позитивну оцінку та детальне вивчення з метою використання в Україні.

Інформаційна політика ЄС на початку 1994 року була побудована у відповідності до рекомендацій звіту М. Бангемана «Європа і глобальне інформаційне суспільство». У цьому ж році Європейською Комісією ухвалено програмний документ «Шлях Європи до інформаційного суспільства», яким визначено вільний доступ до інформаційних систем, формування спільної європейської думки щодо інформаційного суспільства, розробку концепції інформаційної політики ЄС і підтримку національної ідентичності [1].

На сьогоднішній день Європейський Союз має ґрунтовну нормативно-правову та інституційну базу регулювання інформаційного простору та забезпечення інформаційної безпеки. У зв'язку зі зростанням дезінформаційних кампаній [2], зокрема з боку рф, удосконалення політики інформаційної безпеки та, в тому числі, кібербезпеки залишається актуальним питанням.

На рівні ЄС функціонує ряд інституцій, які проваджують політику захисту інформаційного та кіберпростору, розробляють інструменти для зміцнення інформаційної безпеки. Зокрема, Агентство Європейського Союзу з кібербезпеки (ENISA), засноване у 2004 році, сприяє формуванню високого рівня технічного і програмного забезпечення інформаційної та кібербезпеки країн-членів ЄС [3]. Агентство було створено з метою підвищення здатності ЄС запобігати загрозам інформаційної безпеки та своєчасно реагувати на інциденти в цифровому середовищі. Основними завданнями ENISA є: сприяння органам ЄС у формуванні політики щодо мережевої та інформаційної безпеки; сприяння органам та країнам – членам ЄС у проведенні політики, необхідної для відповідності вимогам до мережевої та інформаційної безпеки в рамках європейського законодавства; сприяння ЄС та країнам-членам у підвищенні здатності та готовності до запобігання, розпізнавання та відповіді на проблеми та інциденти, пов'язані з інформаційною безпекою; взаємодія з представниками громадського і приватного секторів [4]. На сьогоднішній день ENISA є центром забезпечення кібербезпеки в усій Європі.

Заслуговує на увагу діяльність Команди реагування на комп'ютерні надзвичайні ситуації для ЄС (CERT-EU), яка створена у 2011 році. CERT-EU є міжінституційним постачальником послуг, адміністративно розміщеним у Європейській Комісії [5]. Це одна з найрозвиненіших структур кіберзахисту в Європі та кібербезпеки ЄС. CERT-EU робить внесок у безпеку інфраструктури ІКТ шляхом запобігання, виявлення, пом'якшення кібератак та своєчасного реагування на них.

Щодо нормативно-правового забезпечення, доцільно відмітити прийняття у 2010 році стратегічно важливого документу – Стратегії кібербезпеки ЄС, яка закріплює основоположні дії щодо захисту громадян та бізнесу ЄС від

кіберзагроз, створення безпечних інформаційних систем та забезпечення відкритого, вільного та безпечного кіберпростору. Ключовими напрямами зміцнення інформаційної безпеки у відповідності до Стратегії визначено: створення мережі операційних центрів безпеки по всьому ЄС для моніторингу та прогнозування сигналів атак на мережі; створення єдиного органу з питань кібербезпеки, що здійснюватиме організовану діяльність з управління кризовими ситуаціями в ЄС; оперативне впровадження заходів та інструментарію функціонування 5G в ЄС та гарантування безпеки мереж 5G, а також розвиток наступних поколінь мереж; впровадження ключових стандартів безпеки в Інтернеті, оскільки вони мають важливе значення для підвищення загального рівня безпеки та відкритості глобальної мережі Інтернет при одночасному підвищенні конкурентоспроможності промисловості ЄС; підтримка надійного шифрування як засобу захисту основних прав та цифрової безпеки, водночас забезпечуючи здатність правоохоронних та судових органів здійснювати свої повноваження як в Інтернеті, так і в режимі офлайн; підвищення ефективності та результативності набору інструментів кібердипломатії, приділяючи особливу увагу запобіганню та протидії кібератакам, що можуть вплинути на ланцюги поставок, інфраструктуру та основні послуги, демократичні інститути та процеси та підірвати економічну безпеку; створення робочої групи з кіберрозвідки для зміцнення спеціального потенціалу ЄС INTCEN у цій галузі; важливість посилення співпраці з міжнародними організаціями та країнами-партнерами для просування спільного розуміння ландшафту кіберзагроз; розробка програми зовнішнього розвитку ЄС з метою підвищення кіберстійкості та спроможності у всьому світі [6]. Реалізація зазначених напрямів дозволить зміцнити інформаційну

безпеку ЄС та забезпечить формування безпекоорієнтованого інформаційного середовища [7].

Аналіз нормативно-правової бази реалізації державної регуляторної політики в Україні в напрямку забезпечення інформаційної безпеки дозволяє стверджувати про необхідність її удосконалення [8]. Це зумовлено, в першу чергу, стрімким розвитком цифрових технологій та модернізацією ризиків та загроз у інформаційному та кіберпросторі [9]. Таким чином, досвід ЄС щодо формування нормативно-правового та інституційного забезпечення інформаційної безпеки правомірно визначити базисом для удосконалення державної політики у сфері інформаційної безпеки в Україні.

Література

1. Балицька Ю.А. Формування нової стратегії публічності в інформаційній діяльності ЄС. URL: http://en.chnu.edu.ua/wp-content/uploads/2018/03/Balytska.pdf

2. Онищенко С. В., Маслій О.А. Ризики та загрози в умовах цифровізації: безпековий аспект. II International Scientific Conference Development of Socio-Economic Systems in a Global Competitive Environment: Conference Proceedings, May 24th, 2019. Le Mans, France. P.54-56.

3. Glushko A.D., Yanko A.S. Optimal reservation of data in the system of residual classes in the direction of ensuring information security of the national economy. Economics and Region. 2019. № 4 (75). P. 20–28. https://doi.org/10.26906/eip.2019.4(75).1814

4. Офіційний сайт European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/

5. Офіційний сайт Computer Emergency Response Team for the EU. URL: https://cert.europa.eu/

6. The EU Cybersecurity Strategy. URL: https://digital-strategy.ec.europa.eu/en/policies/ cybersecurity-strategy

7. Онищенко С., Білько С. Концепти синергетичного підходу до формування безпекоорієнтованого інформаційного середовища в Україні. Вісник Хмельницького національного університету. Економічні науки. 2023. № 1. С. 201–211.

8. Onyshchenko, S., Hlushko, A., Yanko, A. (2020). Role and importance of information security in a pandemic environment. Economics and Region, 2 (77), 103–108.

9. Onyshchenko, V., Yehorycheva, S., Maslii, O. & Yurkiv, N. (2020). Impact of Innovation and Digital Technologies on the Financial Security of the State. Lecture Notes in Civil Engineering. Volume 181. pp. 749–759. https://doi.org/10.1007/978%2D3%2D030%2D85043%2D2_69

УДК 338.24:339.1

Маслій Олександра Анатоліївна[7]**,**
кандидат економічних наук., доцент
Котелевець Марина Миколаївна, *аспірантка*,
Національний університет «Полтавська політехніка імені Юрія Кондратюка» (Україна)

БЕЗПЕКООРІЄНТОВАНИЙ ПІДХІД ДО ФОРМУВАННЯ ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА ЯК ОСНОВА ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ

В умовах становлення Індустрії 5.0 безпекоорієнтований підхід до формування інформаційного середовища національної економіки є основою економічної безпеки держави. Зростання кількості кібератак, витоків даних і кібершпигунства ставлять під загрозу не лише конфіденційність та безпеку громадян, але

[7] Тези підготовлено в межах виконання НДР молодих учених «Формування безпекоорієнтованого інформаційного середовища для підвищення економічної безпеки України у воєнний та повоєнний періоди», державний реєстраційний номер 0124U000615