УДК 316.774

Глушко Аліна Дмитрівна,
кандидат економічних наук, доцент
Перегінець Юлія Ярославівна, *магістрантка*
Національний університет «Полтавська політехніка імені Юрія Кондратюка» (Україна)

ІНСТИТУЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЄВРОПЕЙСЬКОГО СОЮЗУ

Дослідження інституційного забезпечення інформаційної безпеки доцільно розпочати з деталізації та систематизації категоріального апарату, зокрема понять «інститут», «інституції», «інституційне забезпечення».

Аналіз наукових підходів до визначення категорій «інститут» та «інституція» дає змогу зробити висновок про однорідність їх економічного змісту та відмінність ступеня системності. Інституцію правомірно розглядати як систему, тоді як інститут – базовий неділимий елемент інституції [1].

Один із основоположників інституціоналізму, Дж. Коммонс, характеризує інституції у вузькому значенні, як «систему законів чи природних прав, в межах яких індивіди діють як в'язні» та у широкому – як «колективну дію по контролю, лібералізації та розширенню індивідуальної діяльності». Згідно з підходом представника неоінституціоналізму Д. Норта, поняття «інституції» охоплює будь-які види обмежень, створені для спрямування людської взаємодії в певному напрямі. Призначення інституцій у суспільстві полягає в тому, щоб зменшити невизначеність через встановлення постійної структури людської взаємодії. Зазначений підхід підтримав Е. Остром, який визначає інституції як сукупність правил прийняття рішень у певних сферах діяльності.

Формою прояву інституцій є інститути. Сутнісними

характеристиками цієї категорії можуть виступати як юридичні норми, так і порядок встановлення зв'язків між ними, «що надає можливість упорядкувати (регламентувати) стосунки між суб'єктами права з метою надання їм стійкого характеру, для чого і створюються відповідні організаційні структури та органи контролю» [2, 3]. Поняття «інститут» є базовим для теорії інституціоналізму і позначає певний звичай, порядок, прийнятий у суспільстві, а також закріплення їх у вигляді закону або організації.

У сфері інформаційної безпеки напрацьовано великий масив спеціальних регламентів, директив і рішень, які забезпечують проведення відповідних спільних заходів у внутрішньому і зовнішньому вимірі та дії країн-членів [4]. Особлива увага інформаційній безпеці приділяється у контексті розвитку електронної торгівлі у межах єдиного внутрішнього ринку ЄС, а також у контексті реалізації європейської концепції інформаційного суспільства.

Європейська стратегія безпеки передбачає прямі заходи щодо досягнення і підтримки високого рівня інформаційної безпеки у всіх її вимірах. Єврокомісія реалізує цілісну стратегію кібербезпеки, постійно посилюючи компетенції ЄС та централізацію управління у цій сфері. У ЄС передбачається створення єдиної бази даних про кіберзагрози і системи постійного обміну інформацією. Велика увага у ЄС приділяється питанням безпеки у мережі Інтернет, удосконаленню технічних стандартів і правил, підтримці НДДКР у сфері інформаційної безпеки, розвитку і регулюванню цифрового ринку товарів, захисту інтелектуальної власності [5]. У структурі ЄС створено Європейське агентство з питань мережевої та інформаційної безпеки (ENISA), яке виступає хабом для обміну інформацією, досвідом і знаннями у сфері інформаційної безпеки [6].

Велика кількість заходів щодо інформаційної безпеки (особливо у військовій сфері) ЄС здійснює у співробітництві з

НАТО, об'єднуючи досвід, повноваження і зусилля цих організацій. У результаті взаємодія ЄС-НАТО стає основою євроатлантичної кібербезпеки, що також пов'язано з управлінням кризами та миротворчістю [7], сферами людської безпеки та внутрішніх справ.

Виступаючи організацією колективної безпеки, діяльність НАТО безпосередньо включає протистояння кіберзагрозам та захист інформаційних систем, що поєднано в окремий напрям політики (з 2008 р.). Також НАТО розробляє вимоги до своїх країн-членів щодо інформаційної безпеки та здійснює відповідну підтримку, зокрема у сфері професійної підготовки. У структурі НАТО діє декілька спеціалізованих структур (Cooperative Cyber Defence Centre of Excellence, Communications and Information Systems School, Industry Cyber Partnership тощо), а також Центр стратегічних комунікацій НАТО, який забезпечує підготовку інформаційних операцій. НАТО посилює співробітництво зі своїми країнами-партнерами у реалізації спільних заходів обороноздатності, охоплюючи інформаційний сегмент [8].

Наступним елементом МСІБ є національні доктрини, концепції та законодавчі акти. Найбільший вплив на створення нових трендів мають документи, наприклад, країн, що лідирують у сфері ІКТ, наприклад США (наприклад, National Information Infrastructure Protection Act, International strategy for cyberspace) та Індії (National Cyber Security Policy). Для України великий інтерес викликає досвід і стратегії лідерів ЄС (Франції, Великої Британії, Нідерландів), постсоціалістичних країн Європи (Естонії, Словаччини, Чехії, Литви та ін.), Канади, Японії тощо. Урахування цих стратегій дозволяє координувати національну політику України та визначити пріоритети співробітництва з окремими країнами, ЄС та НАТО.

Література

1. Glushko A., Marchyshynets O. (2018). Institutional provision of the state regulatory policy in Ukraine. *Journal of Advanced Research in Law and Economics* . ASERS Publishing House. Volume 9, Issue 3. P. 941–948.

2. Варналій З.С., Буркальцева Д.Д., Саєнко О.С. (2011). Економічна безпека України: проблеми та пріоритети зміцнення. К.: Знання України. 299 с.

3. Онищенко С.В. (2016). Інституційне забезпечення бюджетної безпеки України. *Вісник Київського національного університету імені Тараса Шевченка.* Економіка. том. 5. С. 31-38.

4. Onyshchenko S., Yanko A., Hlushko A., Sivitska S. Conceptual principles of providing the information security of the national economy of Ukraine in the conditions of digitalization. *International Journal of Management*. 2020. № 11(12). P. 1709-1726. https://doi.org/10.34218/IJM.11.12.2020.157

5. Глушко А.Д. Маслій О.А. Вплив інформаційної політики на рівень фінансової безпеки України. *Науковий вісник Херсонського державного університету. Серія «Економічні науки».* 2022. № 46. С. 39-46.

6. European Commission. URL: http://ec.europa.eu.

7. Onyshchenko S., Yehorycheva S., Furmanchuk O., Maslii O. Ukraine Construction Complex Innovation-Oriented Development Management. Proceedings of the 2nd International Conference on Building Innovations, 2019, pp. 687-700. https://doi.org/10.1007/978-3-030- 42939-3_68

8. NATO. URL: http://www.nato.int.

9. Danylyshyn B. M., Onyshchenko S. V., Maslii O. A. (2019). Socio-economic security: modern approach to ensuring the socio-economic development of the region. Ekonomika i rehion, vol. 4 (75), pp. 6–13.

10. Onyshchenko S., Hlushko A., Yanko A. Role and importance of information security in a pandemic environment. Economics and Region. 2020. №2 (77). P.103–108.