Савіцький В. В.,
кандидат економічних наук, доцент
Державний університет «Житомирська політехніка»

ЕТАПИ ФОРМУВАННЯ ЄВРОПЕЙСЬКОЇ ПОЛІТИКИ КІБЕРБЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Важливим елементом забезпечення комплексної безпеки об’єктів критичної енергетичної інфраструктури є протидія гібридним загрозам, а саме загрозам в інформаційному просторі. «Оскільки майбутні інфраструктури дедалі більше залежать від цифрових систем, їхня вразливість до кіберзагроз значно зросла. Складна та гіперпов'язана природа цих систем створює проблеми для підвищення кіберстійкості до несприятливих умов, стресів, атак або компрометації ресурсів кібербезпеки» [1].

Це обумовлено тим, що кіберзагрози можуть спричинити повне припинення енергопостачання і як наслідок вплинути на енергетичну, а в подальшому і національну безпеку держави. Безумовно, що в умовах війни для України питання забезпечення безперервного функціонування критичної енергетичної інфраструктури є вкрай важливим. «російська федерація залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, що ґрунтується на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у війні проти України» [2].

Складність забезпечення кібернетичної безпеки критичної енергетичної інфраструктури обумовлена ключовим фактором, а саме тим, що технології розвиваються швидше, ніж законодавство. Це призводить до того, що законодавство не завжди враховує ті зміни, які можуть відбуватися в техніко-технологічній сфері. На сьогодні система нормативно-правового регулювання забезпечення кібернетичної безпеки критичної енергетичної інфраструктури Європейського Союзу пройшла еволюцію за наступними етапами (табл. 1).

Таблиця 1. Еволюція системи нормативно-правового регулювання забезпечення кібернетичної безпеки критичної енергетичної інфраструктури Європейського Союзу

<table>
<tr><th colspan="4">Етап 1: ЗАРОДЖЕННЯ ПОЛІТИКИ ЄВРОПЕЙСЬКОГО СОЮЗУ ЩОДО ЗАБЕЗПЕЧЕННЯ МЕРЕЖЕВОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ</th></tr>
<tr><td>2001-2005 рр.</td><td colspan="3">Кіберзагрози почали розглядатися з позиції транскордонного впливу, що визначали потребу утворення спеціалізованих інституцій, що створили основу для регулювання цифрової безпеки критичної енергетичної інфраструктури</td></tr>
<tr><td colspan="4">ключові дати</td></tr>
<tr><td>2001 р. - Повідомлення Європейської Комісії COM(2001) 298 final «Мережева та інформаційна безпека: пропозиція європейського політичного підходу» [3];</td><td>2002 р. - Резолюція Ради ЄС про спільний підхід у сфері мережевої та інформаційної безпеки [4];</td><td>2004 р. - Регламент Європейського Парламенту та Ради (ЄС) № 460/2004 Про створення Європейського агентства з мережевої та інформаційної безпеки (ENISA) [5];</td><td>2005 р. - Рамкове рішення Ради 2005/222/ ЈНА Про атаки на інформаційні системи [6]</td></tr>
<tr><th colspan="4">Етап 2: ФОРМУВАННЯ ПОЛІТИКИ ЄВРОПЕЙСЬКОГО СОЮЗУ ЩОДО ЗАХИСТУ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ</th></tr>
<tr><td>2006-2012 рр.</td><td colspan="3">Управління кібербезпекою змінює акцент від загального захисту інформаційних мереж до безпеки критичної інфраструктури, зокрема енергетичної, яка стала першим сектором критичної інфраструктури Європейського Союзу</td></tr>
<tr><td colspan="4">ключові дати</td></tr>
<tr><td colspan="2">2006 р. - Повідомлення Європейської Комісії COM(2006) 251 final «Стратегія безпечного інформаційного суспільства - «Діалог, партнерство та розширення можливостей»» [7]</td><td>2008 р. - Директива Ради 2008/114/ЄС Про ідентифікацію і визначення європейських критичних інфраструктур та оцінку необхідності покращення їх захисту [8]</td><td>2009 р. - Повідомлення Європейської Комісії COM(2009) 149 final «Захист критичної інформаційної інфраструктури — «Захист Європи від масштабних кібератак та збоїв: підвищення готовності, безпеки та стійкості»» [9]</td></tr>
<tr><td>2010 р. - Повідомлення Європейської Комісії COM(2010) 245 final «Цифровий порядок денний для Європи» [10]</td><td>2011 р. - Повідомлення Європейської Комісії COM(2011) 163 final «Захист критичної інформаційної інфраструктури — «Досягнення та наступні кроки: на шляху до глобальної кібербезпеки»» [11]</td><td colspan="2">2012 р. - утворення Групи реагування на комп’ютерні надзвичайні події інституцій ЄС (CERT-EU) на постійній основі [12]</td></tr>
</table>

Проведений аналіз еволюції системи нормативно-правового регулювання управління кібербезпекою об’єктів критичної енергетичної інфраструктури в Європейському Союзі засвідчив її послідовну трансформацію, системний та

адаптивний характер становлення загальноєвропейської політики кібербезпеки в цілому та в енергетичному секторі зокрема. Запропонована періодизація засвідчує, що система нормативно-правового регулювання управління кібербезпекою критичної енергетичної інфраструктури Європейського Союзу формувалася понад двадцять років шляхом зміни об'єкта правового впливу від захисту мережі як технічної системи до забезпечення кіберстійкості критичного суб'єкта, безпеки цифрових продуктів та колективної спроможності Союзу загалом.

Список використаних джерел

1. Aghazadeh Ardebili A., Lezzi M., Pourmadadkar M. Risk Assessment for Cyber Resilience of Critical Infrastructures: Methods, Governance, and Standards. Applied Sciences. 2024. Vol. 14, No. 24. Art. 11807. DOI: 10.3390/app142411807.

2. Юдіна Д. Модель розрахунку рівня кіберзахисту об'єктів критичної інфраструктури. Кібербезпека: освіта, наука, техніка. 2025. Т. 4, № 28. DOI: 10.28925/2663-4023.2025.28.829.

3. Network and Information Security: Proposal for a European Policy Approach : Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, 6 June 2001. COM(2001) 298 final. Brussels, 2001. 32 p. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0298:FIN:EN:PDF.

4. Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security (2002/C 43/02). Official Journal of the European Communities. 2002. C 43. P. 2–4. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2002_043_R_0002_01.

5. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. Official Journal of the European Union. 2004. L 77. P. 1–11. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32004R0460.

6. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. Official Journal of the European Union. 2005. L 69. P.

67–71. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32005F0222.

7. A strategy for a Secure Information Society – “Dialogue, partnership and empowerment” : Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, 31 May 2006. COM(2006) 251 final. Brussels, 2006. 11 p. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52006DC0251.

8. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Official Journal of the European Union. 23.12.2008. L 345. P. 75–82. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008L0114

9. Critical Information Infrastructure Protection – “Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience” : Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, 30 March 2009. COM(2009) 149 final. Brussels, 2009. 12 p. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52009DC0149.

10. A Digital Agenda for Europe : Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 19 May 2010. COM(2010) 245 final. Brussels, 2010. 41 p. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52010DC0245.

11. On Critical Information Infrastructure Protection – “Achievements and next steps: towards global cyber-security” : Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 31 March 2011. COM(2011) 163 final. Brussels, 2011. 11 p. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52011DC0163.

12. Arrangement of 15 December 2017 between the European Parliament, the European Council, the Council of the European Union, the European Commission, the Court of Justice of the European Union, the European Central Bank, the European Court of Auditors, the European External Action Service, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank on the organisation and operation of a computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU). Official Journal of the European Union. 2018. C 12. P. 1–11. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018Q0113(01.