4. Учебно-методический комплекс «Энергетическое право ЕС» (Текст учебника и методические указания). – М., 2008. – С. 218.
5. Energy Law in Europe / M. Roggenkamp, A. Ronne, C. Redgwell, I. Del Guayo (eds.) – Oxford: Oxford University Press, 2001, p.157.
6. Горшукова Ю.Д. Международно-правовые аспекты обеспечения европейской энерге-тической безопасности. Специальность: 12.00.10 – международное право; европейское право. Автореферат дисс. … кандидата юридических наук. – М., 2011. – С. 9.
7. Михайлов Е.Е. Сущность, основные положения и международно-правовое обеспечение меж-дународной энергетической безопасности как научной категории / Е.Е. Михайлов // Вестник Калининградского юридического института МВД России. – № 3. – 2011. – С. 38-43.
8. Regulation (EU) № 994/2010 of the European Parliament and of the Council of 20 October 2010 concerning measures to safeguard security of gas supply and repealing Council Directive 2004/67/ EC Text with EEA relevance // OJ. – L 295. – 12.11.2010. – P. 1–22.
9. European Commission Communication, The EU Energy Policy: Engaging with Partners be-yond Our Borders SEC (2011) 1022 final, [Електронний ресурс]. – Режим доступу: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri= SEC:2011:1022: FIN: EN: PDF.
10. Green Paper. Towards a European Strategy for the security of energy supply. – Luxembourg: Of-fice for Official Publications of the European Communities, 2001. – 15 p. P. 9.
11. Protecting Europe: Ensuring the security of energy and transport services across the European Un-ion, Brussels, European Commission, 2005. [Електронний ресурс]. – Режим доступу: http://ec.europa.eu/dgs/energy_transport/security/ energy/ index_en.htm.

СУЧАСНІ ПРІОРИТЕТИ ПРАВОВОГО РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ ЄВРОПЕЙСЬКОГО СОЮЗУ

Забара І.М.
кандидат юридичних наук, доцент,
доцент кафедри міжнародного права
Інститут міжнародних відносин
Київського національного університету імені Тараса Шевченка

Теперішній період розвитку правового регулювання інформаційної безпеки Європейського Союзу є послідовним продовженням попередніх чотирьох періодів (зокрема 1980–1998 рр., 1999–2004 рр., 2005–2008 рр. і 2009–2013 рр.). Він є послідовним і логічним продовженням і європейської політики в галузі впровадження і розвитку новітніх і перспективних

інформаційно-комунікаційних технологій. Його розвиток, що розпочався з 2014 р., пов'язаний із кількома чинниками і характеризується наступним.

Сучасний період – з 2014 р. до 2017 р. вирізняється від попередніх значними змінами, внесеними інформаційно-комунікаційними технологіями (далі – ІКТ), які вже стали невід'ємним елементом як європейської економіки, так і повсякденного життя. Реалізація інноваційних способів використання ІКТ стає сьогоденною реальністю і очікує на подальший масштабний розвиток.

Серед інших, зміни, що несуть нові явища – хмарні технології (Cloud Technology), Інтернет речей (Internet of Things), «великі дані» (Big Data), Social networking service, Mobile device – є одними із різноманітних і масштабних.

Накопичення великих масивів інформації і оперування ними, надання електронних послуг, і початкове підключення в Європейському Союзі, як очікується, у найближчі роки, більше мільярда пристроїв до електронних мереж надає значні переваги і зручності. У той же час, це здійснює і значний негативний вплив – зростає кількість, обсяг, розмах і різноманітність кібернетичних загроз.

Розуміючи суть загроз і враховуючи ситуацію, Європейська комісія у 2017 р. запропонувала своє бачення нової, викликаної часом, архітектури європейської кібербезпеки та її правового забезпечення.

Масштабний за задумом і доволі значний, запропонований проект спирається на існуючі правові засади і, разом з тим, запроваджує нові ініціативи, спрямовані на наступні цілі, що вдосконалюють систему кібербезпеки Європейського Союзу, зокрема:

– створення стійкості Європейського Союзу до кібератак та посилення його загальної спроможності до кібербезпеки;

– створення дієвої кримінальної відповідальності;

– зміцнення глобальної кібернетичної стабільності через міжнародне співробітництво.

Широке і загальне формулювання цілей знайшло доволі чіткі положення щодо їх реалізації в сучасних умовах, а також у можливій близькій і середньостроковій перспективах.

Задля реалізації цих цілей Європейською комісією запропоновано:

Досягнення першої мети – створення стійкості Європейського Союзу до кібератак та посилення його загальної спроможності до кібербезпеки передбачає наступні заходи.

а) *утворення Агенції Європейського Союзу з кібербезпеки*;

Утворення Агенції планується здійснити на базі чинної Європейської асоціації мереж та інформаційної безпеки (ENISA), мандат якої спливає у 2020 р. Європейська комісія пропонує надати більших повноважень Агенції з кібербезпеки, забезпечивши його постійним мандатом, значними операційними ресурсами та стабільною фінансовою основою.

Головною метою діяльності Агентства буде надання допомоги державам-членам. Головними напрямами роботи визначені оперативна співпраця і сертифікація безпеки ІКТ. Мандат, повноваження та завдання нової Агенції підлягатимуть постійному перегляду і розширенню.

b) *запровадження загальноєвропейської системи сертифікації кібербезпеки для продуктів та послуг ІКТ*;

Європейська комісія пропонує створити систему яка, як очікується, буде визначати і надавати численні індивідуальні європейські схеми сертифікації кібербезпеки ІКТ зокрема, у формі чітко визначених описів вимог безпеки, яким повинні будуть відповідати продукція, системи чи послуги ІКТ. Отримані сертифікати безпеки ІКТ, що підтверджують відповідність цим вимогам, визнаватимуться в усіх державах-членах ЄС.

Використання схем сертифікації буде на добровільній основі для учасників ринку. Високі стандарти кібербезпеки ІКТ, підтверджені і засвідчені за допомогою такої схеми сертифікації, можуть перетворитися на конкурентні переваги для компаній, які бажають забезпечити споживачів продуктами та послугами, що мають певний рівень кіберзахисту.

Сертифікація безпеки ІКТ відіграватиме важливу роль у підвищенні довіри та безпеки до продуктів та послуг ІКТ, що є ключовими для безперешкодного функціонування єдиного ринку цифрових технологій.

c) *прийняття акту щодо співпраці у реагуванні на масштабні інциденти та кризові ситуації в галузі кібербезпеки ЄС;*

Запропоновано прийняти «Керівництво щодо реагування на масштабні інциденти та кризові ситуації в галузі кібербезпеки».

Акт визначає цілі та способи співпраці між державами-членами та інституціями ЄС у відповідь на масштабні інциденти та кризові ситуації та пояснює, як існуючі механізми врегулювання кризи можуть взаємодіяти з існуючими органами кібербезпеки на рівні ЄС. Також пропонується державам-членам та інституціям ЄС створити *Рамкову програму критичного реагування в галузі кібербезпеки в ЄС*, задля дієвості цього проекту. Заплановано, що він буде регулярно проходити тестування в кібер-та інших програмах кризового менеджменту.

d) *створення мережі з кібербезпеки з центром досліджень у галузі кібербезпеки;*

На думку Європейської комісії, протидія кіберзагрозам з боку ЄС потребує масштабних інвестицій у технології кібербезпеки, продукти, процеси та експертизу для досягнення технологічної автономії кібербезпеки та захисту своєї цифрової економіки, суспільства та демократії. Ці можливості є також важливими для сприяння глобальним зусиллям, спрямованим на створення безпечного кіберпростору для всіх. На основі роботи держав-членів та державно-приватного партнерства, започаткованого в 2016 році, Комісія пропонує створення мережі з кібербезпеки з центром досліджень у галузі кібербезпеки в Європі.

Центр європейських досліджень та компетенції з кібербезпеки допоможе розробити та впровадити інструменти та технології, необхідні для усунення постійно змінюваних загроз. Він буде доповнювати зусилля з нарощування потенціалу в цій сфері на рівні ЄС та на національному рівні.

Досягнення другої мети – створення дієвої системи кримінальної відповідальності пов’язується із вдосконаленням законодавства ЄС.

Одним з кроків на шляху вдосконалення кримінального законодавства щодо реагування на кібератаки було прийняття у 2013 році *Директиви про напади на інформаційні системи*, яка встановила мінімальні правила щодо визначення кримінальних злочинів та санкцій у сфері нападів на інформаційні системи та забезпечила оперативні заходи.

Разом з цим, Комісія пропонує додатково посилити кіберзахист шляхом прийняття нової *Директиви з боротьби з шахрайством та підробкою безготівкових засобів платежу*. Відповідно до Стратегії кібербезпеки ЄС, а також Стратегії єдиного цифрового ринку, нова Директива посилить здатність держав-членів проводити кримінальне переслідування за шахрайство з безготівковими платежами.

Досягнення третьої мети – зміцнення глобальної кібернетичної стабільності через міжнародне співробітництво пропонується шляхом створення та підтримка надійних альянсів та партнерських відносин з третіми країнами задля запобігання та стримування кібератак.

ЄС вже співпрацює з США, Японією, Індією, Південною Кореєю та Китаєм. Також діють тісні консультації з міжнародними організаціями, такими як НАТО, регіональний форум АСЕАН, ОБСЄ, Рада Європи та ОЕСР.

У липні 2017 р. у ЄС визначені рамки для спільної дипломатичної протидії зловмисній кібер-активності (“Toolbox” для кібер-дипломатії).

Вперше у 2017 та 2018 роках НАТО та ЄС проведуть паралельні та скоординовані навчання у відповідь на можливий гібридний сценарій.

В умовах розробки Україною національного законодавства у сфері кібербезпеки дієвим може виступити врахування досвіду ЄС, перспективних майбутніх планів, програм і проектів, а також участь у спільних європейських проектах із забезпечення кібербезпеки.