Забара І.М. Формування сучасних правових засад кібернетичної безпеки Європейського Союзу в умовах поширення нових інноваційних технологій

Забара Ігор Миколайович
кандидат юридичних наук, доцент,
доцент кафедри міжнародного права
Інституту міжнародних відносин
Київського національного університету імені Тараса Шевченка

ФОРМУВАННЯ СУЧАСНИХ ПРАВОВИХ ЗАСАД КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ЄВРОПЕЙСЬКОГО СОЮЗУ В УМОВАХ ПОШИРЕННЯ НОВИХ ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ

Стрімкий і масштабний розвиток інформаційно-комунікаційних технологій у Європейському Союзі і, як наслідок, поступовий рух до європейського та глобального інформаційного суспільства відкривають колосальні можливості для розвитку і добробуту. Проте, цей процес має й зворотний бік, що супроводжується новими і серйозними загрозами та наслідками.

Сучасне європейське бачення проблематики кібернетичної безпеки склалось не водночас і пройшло доволі тривалий шлях – від розуміння до комплексного бачення систем захисту. На нього значною мірою вплинуло кілька чинників, які визначили засади, пріоритети і сучасні горизонти. Зокрема, варто відмітити наступне:

по-перше, новизну, складність і чисельність викликів та загроз, що постали на початковому етапі при формування основоположних засад

кібернетичної безпеки ЄС;

по-друге, позитивне сприйняття ЄС орієнтирів щодо поточного і майбутнього розвитку правового забезпечення кібернетичної безпеки, окреслених низкою універсальних і регіональних міжнародних організацій;

по-третє, зосередженням правових питань, пов'язаних із кібернетичною і інформаційною безпекою, переважно на позиціях захисту загальновизнаних прав людини;

по-четверте, поступовим поширенням різноманітних злочинів, пов'язаних із використанням нових цифрових технологій з 70-х років XX сторіччя і, відповідно, необхідністю попередження злочинності та створення кримінального правосуддя у боротьбі із «високотехнологічною» та «комп'ютерною» злочинністю;

по-п'яте, наявністю переважно норм soft law («м'якого права») з питань кібернетичної і інформаційної безпеки, що містились у резолюціях міжнародних органів та організацій, у спільних заявах, деклараціях, комюніке.

Слід відмітити і й те, що притаманні початковому етапу розвитку законодавства ЄС спорадичність і епізодичність у правовому регулюванні боротьби із кібернетичною злочинністю, з часом були змінені на стійкі і тривалі відносини, що виокремили ці питання боротьби у самостійну область як соціальних, так і регіональних відносин. Це мало наслідком прийняття ЄС спеціальних актів, покликаних регулювати ці відносини. Саме вони були предметом розгляду А. Балери, Д. Биго, М. Герке, М. Грокса, М. Дюмонтье, В.Г. Кіютіна, А.П. Новікова, Д. Робинсона, В. Сомерса та багатьох інших. Серед розглянутих авторами були питання, пов'язані із загальною правовою політикою ЄС щодо боротьбі із кіберзлочинністю, міжнародним співробітництвом в сфері кібернетичної та інформаційної безпеки, загальними засадами боротьби із кіберзлочинністю в ЄС, окремими кібернетичними злочинами. Проте, на сьогодні поступово складаються нові

умови розвитку і використання інформаційно-комунікаційних технологій, що є інноваційними в сучасних умовах розвитку європейського інформаційного суспільства.

Метою статті є дослідження сучасних правових засад кібернетичної безпеки Європейського Союзу умовах поширення нових інноваційних технологій.

Питання забезпечення кібернетичної безпеки має у праві ЄС власну проблематику. Для розуміння сучасного періоду розвитку, вважаємо за потрібне здійснити стислий ретроспективний огляд, що надасть можливість поглянути на динаміку формування поглядів і становлення сучасної системи організації і правового забезпечення кібернетичної та інформаційної безпеки ЄС.

Перший період, 1980-1998 років, характеризується розробкою концептуальних теоретичних підходів до проблематики кібербезпеки у електронних мережах і прийняттям Директив спрямованих на захист персональних даних, а також захист права на невтручання в особисте життя осіб у телекомунікаційному секторі.

Початок другого періоду, 1999–2004 роки, пов'язують з прийняттям Європейським парламентом і Радою від 25 січня 1999 р. № 276/1999/ЕС Рішення про багаторічний план дій Співтовариства зі сприяння безпечному використанню Інтернету шляхом боротьби із незаконним і шкідливим змістом у глобальних мережах [1]. Програма Плану дій «Безпечний Інтернет», розрахована на період 1999–2004 років, мала на меті сприяти безпечному користуванню Інтернетом і формувати сприятливе середовище для розвитку європейської Інтернет-індустрії.

Третій період, 2005–2008 років, розпочався з прийняття Європейським парламентом і Радою від 11 травня 2005 року № 854/2005/ЄС Рішення про запровадження багаторічної програми Співтовариства зі сприяння безпечному використанню Інтернету і нових онлайнових технологій [2].

Програма «Безпечний Інтернет Плюс» була розрахована на 2005–2008 роки. Ґрунтуючись на попередній, нова програма мала розширені завдання, спрямовані переважно на боротьбу із поширенням небажаної інформації та розробку спільної політики у боротьбі з кіберзлочинністю.

Четвертий період, 2009–2013 років, передбачав реалізацію програми ЄС «Безпечний Інтернет 2009–2013 роки», — яку було розпочато відповідно до Рішення Європейського парламенту і Ради від 16 грудня 2008 р. №1351/2008/ЕС «Про встановлення багаторічної програми Співтовариства по захисту дітей, що користуються Інтернетом і іншими комунікаційними технологіями» [3]. Метою програми було підвищення навичок і знань дітей при користуванні новими технологіями, а також ідентифікація ризиків використання нових технологій і посилення боротьби з ними, розвиток співробітництва на національному, європейському та міжнародному рівнях; створення безпечного інформаційного середовища.

Зауважимо, що у зазначені періоди законодавство ЄС у сфері кібернетичної і інформаційної безпеки розвивалося у руслі міжнародних ініціатив Ради Європи, Організації економічного співробітництва і розвитку, Міжнародного Союзу Електрозв'язку, Організації Об'єднаних Націй.

Законодавчі заходи у боротьбі із кіберзлочинністю здійснювалися у рамках програм Європейського Союзу — «Безпечний Інтернет» (1999–2004 рр.), «Безпечний Інтернет Плюс» (2005–2008 рр.), «Безпечний Інтернет 2009–2013 рр.», прийнятих рішеннями Європейського Парламенту і Ради, і переважно були спрямовані на захист персональних даних, сприяння безпечному користуванню Інтернетом, формуванню сприятливого середовища для розвитку європейської Інтернет-індустрії, захист дітей, що користуються Інтернетом і новими інформаційними технологіями.

Найважливіші заходи у боротьбі із кіберзлочинністю здійснювалися у рамках програми ЄС «Попередження і боротьба із злочинністю» і передбачали співробітництво в протидії кіберзлочинності.

Складність та чисельність питань кібернетичної і інформаційної безпеки сформувала в законодавчих органах Європейського Союзу концептуальне бачення майбутнього міжнародно-правового регулювання виключно на рівні, спрямованому на вирішення кримінальних аспектів, пов'язаних із використанням інформаційно-комунікаційних технологій. В Європейському Союзі не було сприйнято концепцію міжнародної інформаційної безпеки, яка передбачала б комплексне вирішення проблеми на трьох рівнях міжнародно-правового регулювання – військово-політичному, терористичному і кримінальному.

Сучасний, п'ятий період розвитку правового регулювання інформаційної безпеки Європейського Союзу – 2013–2017 років – є послідовним продовженням попередніх періодів. Він є також логічним продовженням і європейської політики в галузі впровадження та розвитку новітніх і перспективних інформаційно-комунікаційних технологій. Його розвиток пов'язаний із кількома чинниками і характеризується наступним.

Теперішній період 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 кібернетичної безпеки 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 ЄС, зокрема:

створення стійкості ЄС 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 ЄС 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 кібернетичній 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 кібернетичної безпеки (з урахування умов Угоди про асоціацію між Україною, з однієї сторони, і Європейським Союзом і його державами-членами, з іншої сторони 2014 року [4]) дієвим може виступити врахування досвіду ЄС, перспективних майбутніх планів, програм і проектів, а також участь у спільних європейських проектах із забезпечення кібернетичної безпеки.

Список використаної літератури

1. Decision 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks [Электронный ресурс] – Режим доступу: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999D0276:EN:HTML

2. Decision №854/2005/EC of the European Parliament and of the Council of 11 May 2005 establishing a multiannual Community Programme on promoting safer use of the Internet and new online technologies [Электронный ресурс] –

Режим доступу: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:149:0001:0013:EN:PDF

3. Decision 1351/2008/EC of the European Parliament and of the Council of 16 December 2008 establishing a multiannual Community programme on protecting children using the Internet and other communication technologies [Электронный ресурс] – Режим доступу: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:348:0118:0127:EN:PDF

4. Угода про асоціацію між Україною, з однієї сторони, і Європейським Союзом і його державами-членами, з іншої сторони. – [Електронний ресурс]. – Режим доступу: http://www.kmu.gov.ua/kmu/docs/EA/00_Ukraine-EU_Association_Agreement_(body).pdf

Забара І.М. Формування сучасних правових засад кібернетичної безпеки Європейського Союзу в умовах поширення нових інноваційних технологій

У статті досліджуються правові аспекти кібернетичної безпеки Європейського Союзу в сучасних умовах широкомасштабного запровадження нових інноваційних технологій. Автор характеризує попередні періоди становлення і розвитку головних напрямків правового регулювання кібернетичної безпеки в Європейському Союзі і визначає особливості сучасного періоду розвитку. У статті досліджуються правові аспекти запропонованої ініціативи Європейської комісії, спрямовані на вдосконалення системи кібернетичної безпеки Європейського Союзу. Розглядаються ініціативи спрямовані на наступні цілі, що вдосконалюють систему кібернетичної безпеки Європейського Союзу зокрема, створення стійкості Європейського Союзу до кібератак та посилення його загальної спроможності до кібернетичної безпеки; створення дієвої кримінальної

відповідальності; зміцнення глобальної кібернетичної стабільності через міжнародне співробітництво.

Ключові слова: інноваційні технології, інформаційне суспільство, Європейський Союз, кібернетична безпека, правове регулювання.

Забара И.Н. Формирование современных правовых основ кибернетической безопасности Европейского Союза в условиях распространения новых инновационных технологий

В статье исследуются правовые аспекты кибернетической безопасности Европейского Союза в современных условиях широкомасштабного внедрения новых инновационных технологий. Автор характеризует предшествующие периоды становления и развития основных направлений правового регулирования кибернетической безопасности Европейского Союза и определяет особенности современного развития. В статье исследуются правовые аспекты, предложенные Европейской комиссией инициативы, направленной на усовершенствование системы кибернетической безопасности Европейского Союза. Рассматриваются инициативы. направленные на следующие цели, усовершенствующие систему кибернетической безопасности Европейского Союза в частности, создание стойкости Европейского Союза к кибернетическим атакам и усиление его общей способности к кибернетической безопасности; создание действенной криминальной ответственности; укрепление глобальной кибернетической стабильности через международное сотрудничество.

Ключевые слова: инновационные технологии, информационное общество, Европейский Союз, кибернетическая безопасность, правовое регулирование.

Zabara Igor. Formation of modern legal principles of cybernetic security of the European Union in the conditions of the spread of new innovative technologies

The article investigates the legal aspects of cybernetic security of the European Union in the current conditions of large-scale introduction of new innovative technologies. The author describes the previous periods of formation and development of the main directions of legal regulation of cybernetic security in the European Union and defines the features of the modern period of development. The article examines the legal aspects of the proposed European Commission initiative aimed at improving the European Union's cybernetic security system. The initiatives are aimed at the following goals, which improve the system of cybernetic security of the European Union, in particular, the creation of the European Union's resilience to cyberattacks and strengthening its overall capacity for cybernetic security; creation of effective criminal liability; strengthening global cybernetic stability through international cooperation.

Key words: innovation technologies, information society, European Union, cybernetic security, legal regulation.