2. *Дацків І. Б. Дипломатія українських національних урядів у захисті державності (1917-1923 рр.): дис. ... д-ра. іст. наук: 07.00.02. Київ. 2010. 474с.*
3. *Дорошенко Д. І. Історія України, 1917-1923 рр. : в 2-х т. : документально-наукове видання. Київ: Темпора, 2002. 320 с.*
4. *Осташко Т. В'ячеслав Липинський – історик, політик, дипломат. Україна дипломатична: науковий щорічник. 2002. № 3. С. 656-659.*
5. *Скоропадський П. Спогади: кінець 1917 – грудень 1918 рр. Київ, Філадельфія. 1995. 494 с.*

УДК 343.32

Подковенко Т.О.
к.ю.н., доцент, доцент кафедри теорії та історії держави і права Західноукраїнського національного університету

СТРАТЕГІЯ ЄС З КІБЕРБЕЗПЕКИ: ВІДКРИТИЙ, НАДІЙНИЙ І БЕЗПЕЧНИЙ КІБЕРПРОСТІР

Суспільство XXI століття визначається як інформаційне суспільство. Високі темпи розвитку технологій в ІТ-секторі, розвиток електронного адміністрування та електронних послуг ставлять перед світовою спільнотою цілий ряд нових викликів. За останні десятиліття Інтернет, а в ширшому розумінні кіберпростір здійснює величезний вплив на усі сфери життєдіяльності суспільства. Наше повсякденне життя, основоположні права, соціальна взаємодія та економіка залежать від добре функціонуючих інформаційно-комунікаційних технологій. З однієї сторони, відкритий та вільний кіберпростір сприяє політичній та соціальній інтеграції у всьому світі, усуває існуючі бар'єри між державами, спільнотами та громадянами, забезпечує взаємодію та обмін інформацією та ідеями в глобальному масштабі, з іншої – може породжувати серйозні загрози, пов'язані з кіберзлочинністю. Щоб зберегти віртуальний простір відкритим та вільним, в Інтернет-середовищі повинні застосовуватися ті самі стандарти, принципи та цінності, які ЄС підтримує в реальному світі.

Ще у 2003 році Дан Вертон зазначив, що у високорозвинутих державах безперешкодне функціонування кіберпростору є основою не тільки для нормального функціонування економіки, але й для безпеки держави [1, с. 76]. На нашу думку, дане твердження стосується як зовнішньої безпеки, так і внутрішньої, а в контексті розвитку інформаційно-комунікаційних технологій є як ніколи актуальним.

Сучасні інформаційні загрози підкреслюють нагальну потребу у співпраці між державами для попередження постійних загроз в інтернеті, забезпечення кращого розслідування, затримання і переслідування зловмисників, подолання проблем кібербезпеки, адже сучасні суспільства глобально взаємопов'язані, а кібератаки можуть призвести до значних економічних і соціальних збитків. Саме тому міжнародні зусилля у посиленні кібербезпеки та захисту критично важливих інформаційних інфраструктур мають бути узгоджені та діяти у відповідь на ці нові тенденції в глобальному русі до цифрової економіки та інформаційного суспільства [2, с. 154].

Важливим кроком у визначенні пріоритетів щодо захисту кіберпростору стала Стратегія ЄС з кібербезпеки: відкритий, надійний і безпечний кіберпростір (Cybersecurity Strategy of the European Union: An Open, Safe and Security Cyberspace), яка є першим стратегічним документом ЄС щодо кібербезпеки. Він був опублікований 7 лютого 2013 року Європейською комісією [3]. Стратегія кібербезпеки ЄС стала першим всеохоплюючим документом ЄС у даній сфері. Документ стосується усіх аспектів кіберпростору: внутрішній ринок, правосуддя, внутрішня та зовнішня політика. Разом із Стратегією була розроблена та прийнята законодавча пропозиція щодо посилення безпеки інформаційних систем ЄС.

У Стратегії підкреслюється, що інформаційно-комунікаційні технології є основою економічного зростання і мають визначальне значення, оскільки лежать в основі складних систем, що керують економікою в таких секторах, як фінанси, охорона здоров'я, енергетика та транспорт. З цієї причини надзвичайно важливо побудувати тривалу співпрацю в галузі кібербезпеки між адміністрацією та ключовими галузями економіки.

Стратегією визначено п'ять стратегічних пріоритетів щодо гармонізації підходів до кібербезпеки в усіх державах-членах ЄС:

1) досягнення кіберстійкості;
2) суттєве зменшення кіберзлочинності;
3) розробка політики кібероборони та нарощування потенціалу у сфері кібербезпеки, пов'язаної зі Спільною політикою безпеки і оборони (CSDP);
4) розвиток виробничих і технологічних ресурсів для кібербезпеки;
5) створення узгодженої та послідовної міжнародної політики кіберпростору для ЄС і просування основних цінностей ЄС [3].

Стратегія закріплює основні напрямки міжнародної політики ЄС у кіберпросторі, а саме:

– свобода та відкритість: стратегія визначає принципи користування основоположними правами людини та громадянина у кіберпросторі;

– застосування законодавства ЄС у кіберпросторі у тій самій мірі, як і у фізичному світі. Відповідальність за безпеку кіберпростору лежить на усьому глобальному суспільстві: від пересічних громадян до держав;

– розвиток потенціалу кібербезпеки через співробітництво з міжнародними партнерами та організаціями, приватним сектором та громадянським суспільством [4, с. 30].

Варто зазначити, що попри зроблені акценти на безпеці кіберпростору, у документі проводиться ідея збереження та подальшого розвитку європейських цінностей. Рівень кібербезпеки буде високим та ефективним лише в тому випадку, якщо вона ґрунтується на основних правах і свободах, закріплених в Хартії основних прав Європейського Союзу, та на фундаментальних цінностях ЄС. У той же час захистити права людей та фундаментальні цінності демократії без захищених мереж та систем неможливо. Через масштаби впливу цифрового світу на суспільство, обмежений доступ до Інтернету чи відсутність та неможливість використання цифрових технологій ставлять громадян у невигідне становище. Кожен повинен мати доступ до Інтернету та безперебійне отримання необхідної інформації. Одночасно, щоб забезпечити безпечний доступ для всіх, має бути гарантована цілісність та безпека Інтернету.

Загрози, інциденти та злочини, вчинені в кіберпросторі, не мають кордонів. Тому всі учасники – від органів мережевої та інформаційної безпеки, правоохоронних органів та представників інформаційно-комунікаційної галузі повинні брати на себе спільну відповідальність за забезпечення кібербезпеки як на національному рівні, так і на рівні Європейського Союзу.

Таким чином, стрімкі інновації в інформаційних технологіях постійно визначають тенденції до створення та гарантування різноманітних систем кібербезпеки. Разом із розвитком технологій національні правові норми слід поступово адаптувати до міжнародних нормативних актів, зокрема до законодавства ЄС у сфері боротьби з кіберзлочинністю та забезпечення належного рівня кібербезпеки. Європейський Союз створив загальну основу для скоординованих дій щодо посилення кібербезпеки, оскільки кібербезпека визнана елементом національної безпеки.

ЛІТЕРАТУРА:

1. *Verton D. Black Ice: niewidzialna groźba cyberterroryzmu. Warszawa. 2004. 336s.*
2. *Трофименко О, Прокоп Ю., Логінова Н., Задарейко О. Кібербезпека України: аналіз сучасного стану. Захист інформації. 2019. Том 21. № 3. Липень-вересень. С. 150-157.*
3. *Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń. Wspólny komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu ekonomiczno-społecznego i Komitetu regionów 7.02.2013 r. URL: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52013JC0001 (дата звернення: 30.03.2021)*
4. *Законодавство та стратегії у сфері кібербезпеки країн Європейського Союзу США, Канади та інших. Інформаційна довідка, підготовлена Європейським інформаційно-дослідницьким центром на запит народного депутата України. URL: euinfocenter.rada.gov.ua/uploads/documents/28982.pdf (дата звернення: 29.03.2021)*