СЕКЦІЯ 2

ГЛОБАЛЬНІ ВИКЛИКИ ТА СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ МІЖНАРОДНОГО ПРАВА

SECTION 2

GLOBAL CHALLENGES AND MODERN TRENDS IN THE DEVELOPMENT OF INTERNATIONAL LAW

УДК 341.1:004.056

Фліссак К. А.
д.е.н., професор, професор кафедри
міжнародного та європейського права,
Західноукраїнський національний університет

МІЖНАРОДНО-ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сучасний стан глобалізованої світогосподарської системи в умовах динамічного розвитку інформаційного суспільства, а також невпинного впровадження і широкого використання інформаційних технологій актуалізує проблематику інформаційного забезпечення у всіх сферах та галузях діяльності на різних рівнях – як всередині держави, так і в міжнародних відносинах між країнами і регіональними наднаціональними об'єднаннями. При цьому з порядку денного в системі міжнародних відносин не сходить необхідність формування системи забезпечення міжнародної інформаційної безпеки, що, у свою чергу, зумовлює необхідність формування узгоджених міжнародно-правових підходів до регулювання інформаційної безпеки.

Зазначена проблематика є актуальною і в межах національних держав: чим більше розвиваються інформаційні технології і чим більше використовуються модернізовані форми і методи роботи з інформацією, тим більше ризиків і загроз виникає для інформаційного забезпечення.

Інформаційна безпека увійшла у категорію невід'ємної складової національної, економічної, технологічної, продовольчої, енергетичної, воєнної безпеки [1, с.582]. У системі міжнародних відносин забезпечення безпеки у сфері використання інформаційно-комунікаційних технологій стає передумовою попередження і врегулювання міждержавних конфліктів у глобальному інформаційному просторі.

Ефективність інформаційної безпеки в значній мірі залежить від необхідного нормативно-правового забезпечення і правового регулювання. Оскільки інформаційні технології, як і рух інформаційних ресурсів, не

замикаються в межах окремих країн, то цілком оправданим і доцільним є пріоритет визначення рамкових правових умов регулювання інформаційної безпеки на міжнародному рівні. Головна роль в даній ситуації безперечно належить ООН та її відповідним структурам. Одним із основних нормативних документів щодо формування засад інформаційної безпеки є Резолюція ГА ООН від 20 грудня 2002 р. 57/239 «Створення глобальної культури кібербезпеки» [2].

Даний документ поставив вимогу до всіх учасників розробки, впровадження і використання інформаційних систем враховувати 9 взаємодоповнюючих елементів: 1) поінформованість (обізнаність) щодо необхідності безпеки вказаних систем; 2) відповідальність за безпеку; 3) реагування (вжиття в повній мірі своєчасних заходів у випадках інцидентів); 4) етика (враховувати і визнавати законні інтереси інших суб'єктів); 5) демократія (вільний потік інформації, її конфіденційність, захист інформації особистого характеру, відкритість і гласність); 6) оцінка ризиків (виявлення загроз і факторів вразливості, вибір належних інструментів контролю); 7) проектування і впровадження засобів забезпечення безпеки); 8) управління забезпеченням безпеки; 9) переоцінка (вносити належні зміни політику, практику, заходи і процедури забезпечення безпеки). Зазначені елементи фактично формують універсальну модель поведінки суб'єктів у сфері інформаційної безпеки на глобальному рівні.

Оперативна робота з питань правового регулювання інформаційної безпеки в ООН здійснюється Робочою групою відкритого складу з питань безпеки у сфері інформаційно-комунікаційних технологій, доповіді якої регулюють питання безпеки у даній сфері та сприяють зміцненню довіри між державами. Водночас важливу роль у формуванні норм відповідальної поведінки держав у кіберпросторі відіграє Група урядових експертів.

Конкретизація правових норм регулювання інформаційної безпеки для рівня міжнародних та регіональних наднаціональних об'єднань, а також окремих країн здійснюється відповідними структурами таких формувань і органами законодавчої влади держав.

З метою правового регулювання інформаційної безпеки в Європейському Союзі діє ціла система законів і рекомендацій, що регламентують застосування відповідних стандартів та норм [3]. Зокрема існує низка важливих стандартів та норм інформаційної безпеки, дотримання яких сприяє впровадженню структурованої та ефективної системи управління інформаційною безпекою.

Зазначені стандарти формують комплексну систему управління інформаційною безпекою, що охоплює організаційні, технічні та ризик-орієнтовані аспекти. Міжнародний стандарт ISO/IEC 27001 визначає вимоги до Системи управління інформаційною безпекою, є одним із найбільш використовуваних стандартів у сфері інформаційної безпеки, формує основу для впровадження та управління. Стандарт ISO/IEC 27002 надає рекомендації щодо впровадження заходів інформаційної безпеки. Стандарт ISO/IEC 27005 надає рекомендації щодо управління ризиками інформаційної безпеки, допомагає організаціям у виявленні, оцінці та усуненні ризиків інформаційної безпеки. Стандарт ISO/IEC 27701 розширює ISO/IEC 27001 та ISO/IEC 27002 вимогами та рекомендаціями щодо управління інформацією про

конфіденційність. Він допомагає організаціям створити систему управління інформацією про конфіденційність. Важливим щодо регулювання інформаційної безпеки в межах Євросоюзу є стандарт ISO/IEC 22301, який регламентує вимоги до системи управління безперервністю бізнесу і стосується інформаційної безпеки, оскільки охоплює планування та впровадження заходів для підтримки та відновлення бізнес-функцій у разі виникнення інцидентів.

Загальний регламент про захист даних має на меті стандартизувати та посилити захист персональних даних у Європейському Союзі [4]. Регламент передбачає суворі санкції у разі порушень та наголошує на відповідальності винних осіб. Директива про мережеву та інформаційну безпеку [5] спрямована на забезпечення високого загального рівня безпеки мережевих та інформаційних систем у межах Європейського Союзу, має на меті сприяти зміцненню стійкості критичної інфраструктури до кіберзагроз та покращити транскордонну співпрацю у разі інцидентів безпеки [6].

Аналіз практики правового регулювання інформаційної безпеки ЄС свідчить, що в ряді випадків має місце переплетення національного законодавства країн-членів об'єднання і законодавчих норм Євросоюзу. Є нормативні документи щодо юрисдикції у сфері інформаційного забезпечення, використання інформаційних ресурсів та інформаційної безпеки, які поширюються на всі країни ЄС, а є такі, якими керуються в окремих країнах. Зокрема, у ФРН для регулювання інформаційної безпеки сформовано цілісний пакет нормативно-правових актів, які приймались у різні періоди на національному рівні відповідно до регламенту Євросоюзу, у міру необхідності з врахуванням розвитку інформаційних технологій, появи нових форм і методів роботи в інформаційному середовищі та виникненням нових ризиків і загроз для інформаційної безпеки. Так, Федеральний закон про захист даних, прийнятий 30.06.2017 р. [7] має на меті гарантувати захист персональних даних у Німеччині та захистити інформаційне самовизначення громадян, регулює умови, за яких дані можуть збиратися, оброблятися та використовуватися, ставлячи принцип мінімізації даних в основу його діяльності. Закон про цифрові послуги [8] імплементує нормативні акти ЄС до німецького законодавства та набув чинності 14.05.2024 р., прийнятий з метою створення безпечного та відповідального цифрового середовища. Закон про IT-безпеку має на меті підняти IT-безпеку у ФРН на новий рівень та краще захистити цифрову інфраструктуру від кібератак, а особлива увага приділяється операторам критичної інфраструктури, чий збій може мати значні негативні наслідки для суспільства. Такий підхід демонструє імплементацію міжнародних та регіональних норм у національне законодавство, що забезпечує їх практичну ефективність.

Таким чином, на нашу думку, міжнародно-правове регулювання інформаційної безпеки набуває ознак складної багаторівневої системи, в якій взаємодіють універсальні, регіональні та національні правові механізми. Узгодженість цих рівнів є ключовою передумовою ефективного функціонування глобального інформаційного простору та забезпечення стійкості держав до сучасних кіберзагроз. У зв'язку з цим подальший розвиток міжнародно-правових інструментів у сфері інформаційної безпеки має здійснюватися з урахуванням зростаючої ролі цифрових технологій і

транснаціонального характеру інформаційних процесів.

ЛІТЕРАТУРА:

1. Фліссак К.А. Економічна дипломатія у системі забезпечення національних інтересів України: моногр. Тернопіль. Новий колір. 2016. 812 с.

2. Resolution adopted by the General Assembly [*on the report of the Second Committee (A/57/529/Add.3)*] 57/239. Creation of a global culture of cybersecurity.

3. EU-weite Gesetze und Richtlinien. URL: https://cybersecurityportal.de/uebersicht/gesetze-richtlinien-standards-normen/#gesetze-verordnungen

4. Verordnung (EU) 2016/679 Des Europäischen Parlament und des Rates vom 27 April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). URL: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679

5. Richtlinie (EU) 2016/1148 des Europäischen Parlament un des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union. URL: eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:02016L1148-20160719

6. Flissak C., Burdin V., Kasianchuk M., Kolomiiets V., Tychna B., Mazuryk S. International Legal Instruments and Counteraction Mechanisms Against Information Violations and Cybercrime. 2021 11th International Conference on Advanced Computer Information Technologies (ACIT). IEEE. P. 489-493. URL: doi.org/10.1109/ACIT52158.2021.9548431

7. Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), das zuletzt durch Artikel 7 des Gesetzes vom 6.Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist. URL: https://www.gesetze-im-internet.de/bdsg_2018/BDSG.pdf

8. Digitale-Dienste-Gesetz vom 6. Mai 2024 (BGBl. 2024 I Nr. 149), das durch Artikel 26 Absatz 2 des Gesetzes vom 25. März 2026 (BGBl. 2026 I Nr. 81) geändert worden ist. URL: https://www.gesetze-im-internet.de/ddg/BJNR0950B0024.htm

УДК 347.44:342.7:004(4-6ЄС)

Гера В. О.
аспірантка першого курсу юридичного факультету
Західноукраїнський національний університет

ЗАХИСТ ПРАВ СУБ'ЄКТІВ ДАНИХ У ДОГОВІРНОМУ ПРАВІ:ВИКЛИКИ ЦИФРОВІЗАЦІЇ ТА ДОСВІД ЄС

У сучасних умовах цифровізації використання мережі Інтернет стало невід'ємною частиною повсякденного життя. Зокрема, користувачі здійснюють онлайн-покупки,використовують різноманітні застосунки, зберігають персональні даніта укладаютьелектронні договори. У зв'язку із цим особисті данінабувають ознак цінного нематеріального активу, що зумовлює