Книга Є. Ю.,

студентка 2 курсу судово-адміністративного факультету,

Національний університет «Одеська юридична академія»

ЄВРОПЕЙСЬКИЙ СОЮЗ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Забезпечення кібербезпеки – це багатоетапний процес, що передбачає різні напрямки розвитку цифрового світу. Глобалізація інформаційного простору, а відповідно і тотальна модернізація суспільства сприяли отриманню якісно нових видів загроз, зокрема: інформаційного тероризму, кібератак та кіберзлочинності. Об'єктами цих загроз залишаються критично важливі інфраструктури, а відповідно – серйозна загроза національної безпеки держави. Хоча безпека національних інтересів держави належить безпосередньо до компетенції державних установ, єдиної міжнародно-правової платформи щодо забезпечення інформаційної безпеки ще не існує[4].

Сучасна концепція стратегічного управління економічною безпекою виникла у відповідь на виклики та загрози зовнішнього та внутрішнього середовища, спричинені тотальною діджиталізацією суспільства. Інформаційне суспільство характеризується постійним вдосконаленням інформаційних технологій та швидкими темпами їх впровадження в усі сфери суспільного життя. Результатом є віртуалізація значної частини зв'язків з громадськістю та зростання залежності країн від електронних мереж та інформаційних систем. Важливими тенденціями сучасного етапу є також активізація транскордонних інформаційних потоків, а також поширення різноманітних методів і засобів обміну інформацією, які є практично неконтрольованими [3]. Як наслідок, поширюються нові інформаційні загрози та виклики, які потребують негайного реагування та застосування нестандартних заходів та рішень з боку ЄС та кожної країни-члена зокрема - інформаційна безпека стає пріоритетним у формуванні економічної безпеки ЄС. У цьому контексті сформовано основні напрямки європейської політики інформаційної безпеки, зокрема: розвиток європейської системи попередження та інформування про нові погрози, надання технологічного супроводу (пріоритет

надається розвитку досліджень мережевої та інформаційної безпеки), підтримка ринково орієнтованої стандартизації та сертифікації, юридичний супровід, посилення безпеки на державному рівні, розвиток міжнародного співробітництва з питань інформаційної безпеки.

Основним завданням ЄС є зміцнення діалогу Європейської Комісії з міжнародними організаціями та партнерами з питань безпеки мереж і, зокрема, щодо зростаючої залежності від електронних мереж. У цьому контексті організація процесу стратегічного управління економічної безпеки ЄС передбачає таку послідовність: визначення стратегічних цілей, стратегічний аналіз, визначення переліку та пріоритетності загроз економічній безпеці, оцінка рівня економічної безпеки, моделювання сценаріїв як ЄС, так і окремих національних економік, стратегія і тактика забезпечення економічної безпеки Європейського Союзу та країн ЄС, розробка заходів, інструментів та механізмів реалізації стратегії економічної безпеки країни, моніторинг та контроль[3].

Сьогодні у більшості країн, у тому числі в країнах Європейського Союзу, активно розвивається законодавство з кібербезпеки. Формування правового забезпечення кіберзахисту базується на двох засадах: національних та на основі єдиної міжнародної платформи. У цьому контексті важливим чинником розвитку та формування нормативно-правового забезпечення кібербезпеки є те, що таке поняття охоплює різні галузі права.

Базовим міжнародним нормативно-правовим документом, що регулює суспільні відносини у сфері боротьби з кіберзлочинністю, є Конвенція Ради Європи «Про кіберзлочинність» від 23 листопада 2001 року.

Важливим є положення «Конвенції», що дозволяє вживати законодавчих та інших заходів, що уповноважують її компетентні органи конфісковувати або аналогічним чином захищати від знищення дані, які має провайдер і які необхідні для розслідування. Це дозволяє правоохоронним органам розслідувати такі злочини або вживати заходів для збереження даних, які можуть бути знижені через певний час[1].

Безсумнівно, з правової точки зору велике значення мають загальні принципи міжнародного співробітництва, які визначені в «Конвенції». Йдеться про

екстрадицію комп'ютерних злочинців та надання один одному всебічної взаємодопомоги у розслідуванні кримінальних справ, пов'язаних з комп'ютерними системами та даними, а також у збиранні електронних доказів.

Хоча в Конвенції детально і не прописаний механізм правового регулювання реалізації двох останніх способів збирання комп’ютерної інформації, наявний досвід і співвідношення з нормами законодавства України та інших країн дозволяють стверджувати, що вони, найімовірніше, в даний час підлягають використанню шляхом проведення оперативно-розшукових заходів, передбачених пп.9 і 10 ст.8 Закону України «Про оперативно-розшукову діяльність».

Варто зауважити, що оперативно-розшукова діяльність може здійснюватися тільки уповноваженими на те підрозділами державних органів (ст.5 вищевказаного Закону). У таких умовах безпосередня реалізація постачальниками послуг повноважень по збору і запису в режимі реального часу даних про рух інформації, перехопленню (збиранню і запису) даних про зміст повідомлень видається такою, що суперечить конституційним принципам законодавства[2].

Існує важлива відмінність і, отже, деякі значні протиріччя між вимогами внутрішньої безпеки, з одного боку, та інтересами національної безпеки з іншого. Перший стосується рівня безпеки, якого країна прагне досягти, але водночас є нейтральною щодо операторів інформаційних послуг, їх національності та громадянства. Другий тип заходів базується на інтересах національної безпеки та на тому, що логічно буде використано для усунення передбачуваних ризиків, пов’язаних з операторами з певних країн.

Отже, у контексті визначення інформаційної безпеки у відповідному міжнародному законодавстві можна зазначити, що в умовах глобалізації інформаційного простору акцент інформаційної безпеки припадає на сферу кібербезпеки, що потребує якісно нової нормативної платформи для відносин у сфері інформаційної безпеки в рамках захисту національної безпеки та механізмів усунення загроз правовими засобами.

Література

1. Конвенція Ради Європи про кіберзлочинність: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi? page=1&nreg=994_575.

2. Закон України Про оперативно-розшукову діяльність (Відомості Верховної Ради України (ВВР), 1992, № 22, ст.303), Редакція від 15.06.2022 - https://zakon.rada.gov.ua/laws/show/2135-12#Text.

3. Regulatory and Legal Enforcement of Cyber Security in Countries of the European Union: The Experience of Germany and France, Sviatoslav Kavyn, Ivan Bratsuk, AnatoliyLytvynenko,2021 https://www.journals.vu.lt/teise/article/view/25171/24464.

4. Sviatoslav Kavyn. Regulatory mechanisms for guaranteeing cybersecurity in the Baltic States, 2020 URL: http://pgp-journal.kiev.ua/archive/2020/12/56.pdf.