НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В КОНТЕКСТІ НАБУТТЯ ЧЛЕНСТВА В ЄВРОПЕЙСЬКОМУ СОЮЗІ

КАВИН Святослав - аспірант Львівського університету імені Івана Франка кафедра європейського права, факультет міжнародних відносин
ORCID: 0000-0002-6189-3848
УДК 314
DOI 10.32782/NP.2023.3.21

Стаття присвячена вивченню формування нормативно-правового поля України у сфері забезпечення інформаційної безпеки. Проведено аналіз законодавчих та нормативно-правових актів України у сфері інформаційної безпеки. Виокремлені тенденції розвитку правового захисту інформаційного простору України в контексті набуття членства в Європейському Союзі. Також визначені проблеми впровадження сучасних європейських стандартів інформаційної безпеки в умовах становлення національної системи кібербезпеки України. Представлено суб'єктний склад функціонування системи забезпечення інформаційної безпеки держави, а також функціональний зміст суб'єктів забезпечення інформаційної безпеки.

Ключові слова: Конституція України, інформаційна безпека України, кібербезпека, національна безпека України, міжнародна інформаційна безпека, інформаційні загрози, нормативно-правові акти, правові засади інформаційних відносин.

Вступ

На сьогодні в Україні закладена основа правового регулювання забезпечення національної безпеки й інформаційної безпеки, зокрема, завдяки чому одержали своє законодавче закріплення основні поняття, що стосуються інфораційної безпеки, а також правове обґрунтування системи її забезпечення.

Водночас, основні нормативно-правові акти у сфері інформаційної безпеки потребують доопрацювання, зокрема щодо визначення й законодавчого закріплення поняття та змісту категорії «система інформаційної безпеки». Разом з тим важливою залишається також проблема неузгодженості термінології в інформаційному законодавстві. Варто зауважити, що в нормативно-правовому полі України відсутні поняття «державної інформаційної політики» та «національного інформаційного простору». Також існує потреба чіткого визначення на законодавчому рівні таких категорій, як «предмет інформаційних правовідносин», «об'єкт інформаційного права».

Важливою проблемою в цьому напрямку залишається також певна несистемність вітчизняної правової політики в інформаційній сфері. Тобто інколи законодавчі акти ухвалюються з метою вирішення суто тактичних завдань, без урахування стратегічних орієнтирів та об'єктивних українських умов. Окрім того, частина інформаційних відносин регулюється підзаконними, а подекуди й відомчими нормативними актами. Відповідно значна кількість питань функціонування інформаційної сфери в Україні залишається досі недостатньо врегульованою на законодавчому рівні, зокрема це стосується проблем у сфері створення, поширення та використання інформації.

Існує також необхідність розробки теоретичних і правових засад забезпечення інформаційної безпеки України. Зокрема, наразі немає усталеного підходу до визначення системи інформаційної безпеки як на доктринальному, так і на нормативному рівнях.

Актуальність вирішення окреслених проблем є очевидною і відповідно потребує детального дослідження.

Мета дослідження

Дослідження формування нормативно-правового поля України у сфері інформаційної безпеки на основі права Європейського Союзу в умовах глобальної інформатизації в контексті набуття членства України в Європейському Союзі.

Аналіз досліджень і публікацій

Твердий і незмінний курс України на Європейську інтеграцію активізував процеси цифрової трансформації держави.- У цьому контексті, враховуючи виклики та загрози, що постали перед Україною в інформаційному просторі зумовили виникнення наукового інтересу до проблем правового забезпечення інформаційної безпеки України, систематизації її законодавства в цій сфері, оцінці ефективності чинного юридичного інструментарію, який використовується з метою регулювання захисту інформації, вироблення певної спільної концепції регулювання правовідносини, пов'язаних із забезпеченням інформаційної безпеки в системі національного права.

Цій проблематиці присвятили свої дослідження відомі вітчизняні науковці-правознавці, зокрема О.А. Баранов [13],- Н.Р. Нижник [17], Г.П. Ситник [17], В.Т Білоус [17], В.М. Брижка [14], Є. Захаров [28], Р. Тополевський [28], В. Пилипчук [22], П.М. Сніцаренко [26], Ю.О. Сарачив [26], В.М. Семененко [26], В.А. Ткаченко [26], О.Г. Ярема [30], Довгань О.Д. [16], Перун Т.Ю. [21], Нашинець – Наумова А.Ю. [19], Ткачук Т.Ю. [16], [27], Шемчук В.В. [29], Гаврильців М.Т. [15], Бокалінська О. [20], Малашко О.Є. [18]. Акцент у роботах був сконцентрований на аналізі правового інструментарію інформаційних та кіберзагроз для системи національної безпеки України. Зокрема, досліджувались механізми правового регулювання забезпечення інформаційної безпеки, а також інституційні засади інформаційної безпеки України. Особлива увага була приділена міжнародному нормативно-правовому співробітництву щодо інформаційної безпеки в контексті євроатлантичної інтеграції України.

Виклад основного матеріалу

Відповідно до ст. 17 Конституції України, захист інформаційної безпеки, нарівні із захистом суверенітету та територіальної цілісності України, є найважливішою функцією держави та справою всього українського народу [1]. Тож інформаційна безпека, безперечно, є однією з найважливіших складових національної безпеки України.

Правовою основою національної програми забезпечення інформаційної безпеки є: Закон України «Про інформацію» [2], Закон України «Про Концепцію Національної програми інформатизації» [3], Закон України «Про основні засади забезпечення кібербезпеки України» [4], Закон України «Про захист інформації в інформаційно-комунікаційних системах» [5], «Стратегія інформаційної безпеки України» [8], «Стратегія кібербезпеки України» [6], «Доктрина інформаційної безпеки України» [9], а також міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

Законом України «Про інформацію» від 02.10.1992 р. визначено основні напрямами державної інформаційної політики, серед яких особливого значення набуває нормативно-правове забезпечення інформаційної безпеки України [2]. У цьому контексті в Концепції Національної програми інформатизації серед основних напрямків інформатизації виділено організаційно-правове забезпечення процесу інформатизації, що передбачає розроблення пакету нормативно-правових актів з питань організації та правового регулювання відносин у сфері інформатизації, зокрема: розроблення системи державних стандартів у галузі інформатизації; сертифікація технічного і програмного забезпечення; захист авторського права та інтелектуальної власності. [3]

Але особливості розвитку інформаційної сфери свідчать про те, що існують об'єктивні передумови для зниження ефективності стратегічного планування та реалізації національної програми забезпечення інформаційної безпеки. До числа таких передумов, насамперед, належить суперечливість роз-

витку національного права внаслідок нерівномірної адаптації правової бази інформаційної безпеки до вимог Європейського Союзу та НАТО [16]. У цьому контексті, з урахуванням глобального проникнення інформаційних технологій у найважливіші сфери життя суспільства, нашій державі необхідно передбачити комплекс правових норм за допомогою яких ефективно забезпечувався б захист інформаційного простору, насамперед враховуючи відповідні міжнародно-правові механізми в цій сфері [24].

Доктрина інформаційної безпеки України, яка затверджена Указом Президента України «Про рішення Ради національної безпеки і оборони України № 47 від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» [9], покладає функції щодо забезпечення інформаційної безпеки на такі органи: Рада національної безпеки і оборони України; Кабінет Міністрів України; Міністерство інформаційної політики України; Міністерство закордонних справ України; Міністерство оборони України; Служба безпеки України; Державна служба спеціального зв'язку та захисту інформації України; розвідувальні органи України; Національна поліція України. Доктрина також передбачає, що Національний інститут стратегічних досліджень забезпечує науково-аналітичне та експертне супроводження процесу формування й реалізації державної інформаційної політики [9].

А в загальному кожна державна організація в межах своєї діяльності, реалізуючи функції держави, тією чи іншою мірою виступає суб'єктом державного забезпечення інформаційної безпеки. Існує також система державних органів, для яких окремі напрями забезпечення інформаційної безпеки є безпосередньою функцією. До таких структур в Україні можна віднести: Державну службу спеціального зв'язку та захисту інформації України, Національну комісію з питань регулювання зв'язку України, Державну службу України з питань захисту персональних даних, Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України, Національну раду України з питань телебачення і радіомовлення; Державний комітет України по стандартизації, метрології та сертифікації; а також Головне управління з питань безпекової та оборонної політики, Головне управління забезпечення доступу до публічної інформації.

Важливою складовою правової основи захисту інформаційної безпеки України є Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017, метою якого є врегулювання відносин, пов'язаних із забезпеченням кібербезпеки, як складової національної безпеки України, провадженням діяльності із захисту національних інтересів та національних інформресурсів у кіберпросторі, кіберзахистом систем електронних комунікацій. [4] У законі визначено принципи забезпечення кібербезпеки України, які грунтуються на верховенстві права, гарантій захисту інформації та міжнародному співробітництві. Це дає правову основу для зміцнення взаємної довіри на міждержавному рівні у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, а також консолідації зусиль у розслідуванні та запобіганні кіберзлочинам.

Прийняття Закону стало важливим етапом інституалізації національної системи кібербезпеки, який визначив правові та організаційні основи забезпечення захисту національних інтересів України у кіберпросторі. Окрім того, Закон визначив основні цілі, напрями та принципи державної політики у сфері кібербезпеки, а також основні засади координації їхньої діяльності із забезпечення кібербезпеки. Необхідно відмітити, що в рамках Закону було: удосконалено нормативне забезпечення з питань кіберзахисту об'єктів критичної інформаційної інфраструктури, а також ухвалено порядок її визначення та загальні вимоги до її кіберзахисту; утворено центри забезпечення кіберзахисту в ключових державних інституціях, зокрема: у Державній службі спеціального зв'язку та захисту інформації України, Службі безпеки України, Національному банку України, Міністерстві інфраструктури України, Міністерстві оборони України, Збройних Силах України; створена та діє урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA; а також утво-

рений Національний центр резервування державних інформаційних ресурсів.

Разом з тим у Законі відмічено, що функціонування національної системи кібербезпеки забезпечується шляхом «досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО», а також з урахуванням «кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту». [4] Ці принципи і склали основу для розроблення відповідних нормативно-правових актів, створення єдиної (універсальної) системи індикаторів кіберзагроз і запровадження національної системи аудиту інформаційної безпеки на критично важливих об'єктах кіберзахисту.

Тут також важливо відзначити вимоги для об'єктів критичної інформаційної інфраструктури (КІІ), затверджені Постановою КМУ «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» № 518 від 19.06.2019 [12]. Загальні Вимоги інформаційної безпеки встановлені, з урахуванням міжнародних стандартів та специфіки галузі, до якої належать відповідні об'єкти критичної інформаційної інфраструктури, окрім того, встановлено обов'язковий незалежний аудит інформаційної безпеки, порядок та вимоги до якого також централізовано затверджуються Кабінетом Міністрів України.

Разом з тим, актуальним залишається комплекс питань, пов'язаних з формуванням основи національної КІІ, зокрема методів захисту її обєктів, а також питань щодо реалізації та впровадження системи аудиту інформаційної безпеки в Україні У цьому контексті особливої уваги набуло питання методології та критеріїв формування реєстру об'єктів національної КІІ, а також питання функціонування системи аудиту інформаційної безпеки (ІБ) в Україні. Так, Постановою № 943 КМУ «Деякі питання об'єктів критичної інформаційної інфраструктури» від 9 жовтня 2020 року затверджено «Порядок формування переліку об'єктів критичної інформаційної інфраструктури», а також «Порядок внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування.» [11]

Указом Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про невідкладні заходи з кібероборони держави» від 26 серпня 2021 р. № 446/2021 ухвалено створення у системі Міністерства оборони України кібервійськ, мета яких – реагувати на загрози у кіберпросторі. [7] Оскільки в українському законодавстів терміна «кібервійська» немає, немає також відповідної нормативно-правової бази для їх діяльності, то Національним координаційним центром кібербезпеки здійснюється розробка законодавчих нормативних актів, що, зокрема, визначатимуть структуру кібервійськ та їх функції. На сьогодні за кібербезпеку України відповідають підрозділи дев'яти органів, зокрема: СБУ, Держспецзв'язку, Кіберполіція, РНБО, НБУ, Мінцифри, Міністерство оборони, Збройні сили та розвідувальні органи. Разом з тим у Міністерстві оборони запропонували назвати цей новий підрозділ Силами кібероборони, оскільки це дасть ширші юридичні можливості в майбутньому.

У цьому контексті необхідно зауважити, що діяльність суб'єктів національної системи кібербезпеки залишається недостатньо скоординованою і такою, що спрямована на виконання лише поточних завдань. Невирішеними залишаються, зокрема, питання оперативного обміну інформацією про кіберзагрози. А з метою покращення координації діяльності суб'єктів сектору безпеки й оборони, які забезпечують кібербезпеку, утворено робочий орган Ради національної безпеки і оборони України – Національний координаційний центр кібербезпеки, рішення якого сприяють вирішенню найбільш складних проблем у цій сфері.

Відповідно, Нова Стратегія кібербезпеки України, затверджена Указом Президента України № 447 від 26.08.2021 [6], враховує зазначені проблеми, відповідний стан кібербезпекового середовища на національному та міжнародному рівні, а також положення Стратегії кібербезпеки ЄС на цифрове десятиліття, стратегій кібербезпеки окремих держав ЄС та держав НАТО.

У Новій Стратегії кібербезпеки України визначено виклики для України у сфері кібербезпеки, зокрема, це мілітаризація кіберпростору та розвиток кіберзброї, що дає можливість приховано проводити кібератаки для підтримки бойових дій і розвідувально-підривної діяльності у кіберпросторі; та впровадження нових технологій, цифрових послуг та механізмів електронної взаємодії, що здійснюється безсистемно в частині заходів з кібербезпеки та без належної оцінки ризиків. [6]

Також у Стратегії визначені загрози кібербезпеці України, зокрема, це кібератаки, які спрямовані, насамперед, на інформаційно-комунікаційні системи державних органів України та об'єкти критичної інформаційної інфраструктури з метою виведення їх з ладу (кібердиверсія). Разом з тим набуває поширення використання кіберпростору для вчинення злочинів проти основ національної безпеки України, а також кримінальних правопорушень, у т.ч. викраденням чутливої інформації (кібершпигунство). [6]

Враховуючи виклики та загрози, що постали перед Україною у кіберпросторі, критично зростає роль кібербезпеки в процесах цифрової трансформації держави. В цьому контексті в Стратегії визначено передумови та чинники, які формують окреслені загрози, зокрема, це: [6]

- недосконаліть нормативно-правової бази у сфері кібербезпеки, а також її застарілість у сфері захисту інформації, повільна імплементація положень європейського законодавства, недостатня врегульованість цифрової складової розслідування кримінальних правопорушень, а також низький рівень правової відповідальності за порушення вимог законодавства у цій сфері;
- відсутність системи незалежного аудиту інформаційної безпеки та механізмів розкриття інформації про вразливості в умовах динамічної цифровізації всіх сфер державного управління та життєдіяльності держави;
- відсутність законодавчого акта про критичну інфраструктуру України та її захист, що значно ускладнює формування системи кіберзахисту такої інфраструктури;

Важливе значення для ефективного функціонування системи забезпечення інформаційної безпеки держави має її суб'єктний склад, компетенція суб'єктів забезпечення інформаційної безпеки та належна організація взаємодії між ними.

Указом Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» від 28 грудня 2021 р. № 685/2021 була затверджена Стратегія інформаційної безпеки України, яка визначає актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам. Метою Стратегії є посилення спроможностей щодо забезпечення інформаційної безпеки держави та її інформаційного простору. Досягнення мети здійснюватиметься шляхом ужиття заходів щодо стримування та протидії загрозам інформаційній безпеці України та нейтралізації інформаційної агресії, а також шляхом розвитку міжнародної співпраці у сфері інформаційної безпеки на засадах партнерства та взаємної підтримки. [8]

У Стратегії визнчено національні виклики та загрози, серед яких відмічено несформованість системи стратегічних комунікацій та недосконаліть регулювання відносин у сфері інформаційної діяльності.

Щодо несформованості системи стратегічних комунікацій, зазначено наступне - в Україні триває процес становлення системи стратегічних комунікацій, однак ще не створено дієвого механізму координації і взаємодії між усіма органами державної влади, залученими до здійснення заходів із протидії загрозам в інформаційній сфері. Зазначене послаблює можливості до розбудови комплексного стратегічного планування інформаційного потоку, здійснення системної комунікативної діяльності Кабінету Міністрів України, об'єднання всіх ключових суб'єктів у сфері інформаційних відносин, суб'єктів формування і реалізації державної політики щодо ефективного захисту національного інформаційного простору, утвердження позитивного іміджу України, реалізації цілей захисту національної безпеки України в інформаційній сфері. [8]

Щодо недосконалості регулювання відносин у сфері інформаційної діяльності, за-

значено наступне - регулювання відносин у сфері інформаційної діяльності не відповідає сучасним викликам та загрозам. Це перешкоджає розвитку українського медіаринку, ускладнює ведення бізнесу у цій сфері, зберігає залежність засобів масової інформації від їх власників, а також не забезпечує додержання професійних стандартів діяльності журналістів.

У Стратегії також визначено механізми реалізації зазначеної мети та завдань, зокрема з розподілом функцій між суб'єктами, в безпосередню компетенцію яких входять забезпечення інформаційної безпеки. Зокрема, відзначено: [8]

Важливим акцентом є те, що до реалізації Стратегії відповідальними державними органами можуть залучатися наукові та науково-дослідні установи, які забезпечують науково-аналітичне та експертне супроводження процесу формування та реалізації державної інформаційної політики.

Нормативно-правове забезпечення реалізації Стратегії здійснюватиметься шляхом системного перегляду та внесення змін до відповідних законодавчих та інших нормативно-правових актів в інформаційній сфері.

Цікавою з правової точки зору, є ідея «створення інформаційно-аналітичної системи формування національних індикаторів ІБ», яка відповідала б нинішнім європейським стандартам і практикам. Ідея була закладена ще в 2017 році Державною службою спеціального зв'язку та захисту інформації України (ДССЗЗІ) в «Концепції впровадження системи аудиту інформаційної безпеки («Дорожня карта»)» і знайшла своє відображення в Постанові Кабінет Міністрів України «Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури» № 257 від 24 березня 2023 р., якою визначено основні засади щодо реалізації та впровадження системи аудиту інформаційної безпеки в Україні та затверджено порядок організації та проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури держави», якою затвердив Порядок проведення такого аудиту [10].

У цьому контексті були визначені ключові задачі, зокрема: 1) розроблення системи національних індикаторів ІБ, з метою «впровадження єдиної (універсальної) системи індикаторів кіберзагроз з урахуванням міжнародних стандартів з питань кібербезпеки та кіберзахисту» 2) організація аудиту ІБ в Україні, зокрема, «впровадження системи аудиту ІБ на національному рівні та використання послуг аудиту ІБ, що можуть надаватися національними державними аудиторами.

Одним із найважливіших питань у сфері розбудови забезпечення інформаційної безпеки в Україні є впровадження системи стратегічного управління. Його основні складники – це система інформаційно-аналітичного забезпечення, система обґрунтування рішень, система ухвалення рішень, система забезпечення реалізації рішень. Ці процедури мають бути чітко регламентовані та нормативно закріплені. Аналіз визначеної чинним законодавством України компетенції державних органів, на які покладаються завдання щодо забезпечення інформаційної безпеки, дозволяє дійти висновку, що, з погляду функціональних завдань суб'єктів, система забезпечення інформаційної безпеки держави оптимально забезпечується силовими структурами.

У цьому контексті Ткачук Т.Ю. зауважує, що доцільно вибудувати єдину систему суб'єктів забезпечення інформаційної безпеки, на які безпосередньо покладається виконання заходів у сфері забезпечення інформаційної безпеки, ранжувавши їх за основними сферами відповідальності. Відповідно, таким чином, можна вести мову про те, що, з погляду функціональних завдань суб'єктів, система забезпечення інформаційної безпеки держави складається з таких підсистем: підсистема інформаційної розвідки; підсистема інформаційного захисту, яка включає в себе підсистему захисту інформації та підсистему захисту від інформаційних впливів; підсистема інформаційного впливу. [27]

Тут важливим є досвід Європейського Союзу у сфері забезпечення інформаційної безпеки і відповідно адаптація правових стандартів, що мають місце в державах Європейського Союзу. Тут основу складають ***Стратегія Єдиного Цифрового Ринку (Digital Single Market Strategy)*** та ***Європейський Поря-***

док денний з питань безпеки (European Agenda on Security). І це є пріоритетним напрямком нашої держави в контексті розбудови національної системи інформаційної безпеки. [25]

У зв'язку з актуальністю безпеки інформаційного простору, в інститутах Європейського Союзу сформувалось концептуальне бачення майбутнього міжнародно-правового регулювання забезпечення інформаційної безпеки, яке полягає в попередженні злочинів, пов'язаних із використанням інформаційно-комунікаційних технологій. Зокрема, у січні 2023 р. набула чинності Директива (ЄС) 2022/2555 Європейського Парламенту та Ради від 14 грудня 2022 року про заходи щодо високого спільного рівня кібербезпеки в Союзі, яка вносить зміни до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972, та скасування Директиви (ЄС) 2016/1148 (Директива NIS 2) (***Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)),*** *яка* закріплює єдині правила та вимоги у сфері кібербезпеки для всіх держав ЄС, але разом з тим залишила за кожною країною ЄС право вживати власних заходів щодо імплементації норм цієї Директиви в національне законодавство з урахуванням національних інтересів. У цьому контексті важливим для України є формування в рамках правової платформи ЄС концепції міжнародної інформаційної безпеки, яка передбачала б комплексне вирішення проблеми, зокрема прийняття нормативно-правових актів про забезпечення інформаційної безпеки, у яких необхідно закріпити: основні загрози безпеці в інформаційному просторі; основні засади забезпечення інформаційної безпеки; детально прописати принципи міжнародного співробітництва в боротьбі із злочинами в інформаційній сфері, зокрема кіберзлочини; визначити ефективні та дієві механізми правової відповідальності в інформаційному просторі аж до створення спеціального національного органу щодо розслідування злочинів в інформаційній сфері.

Враховуючи сучасні реалії цифровізації суспільства, Україна формує свою політику безпеки на основі міжнародній співпраці з ЄС, у т. ч. з Єврпейськими інституціями, у рамках євроінтеграційних процесів України щодо набуття членства в ЄС, інтегруючи свої національні ресурси кіберзахисту в межах вимог права Європейського Союзу. Тут важливо відмітити Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій, а також про скасування Регламенту (ЄС) № 526/2013 (Акт про кібербезпеку) ***/Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)/***, яким визначається створення європейських схем сертифікації кібербезпеки з метою забезпечення адекватного рівня кібербезпеки продуктів і послуг ІКТ у ЄС, а також створює нові механізми для розвитку європейської стратегічної автономії, що має важливе значення для підвищення безпеки Європейського єдиного цифрового простору. Але співпраця із спеціальними інституціями Європейського Союзу, зокрема щодо забезпечення інформаційної безпеки критично-важливих інфраструктур носить обмежений характер, оскільки інформація щодо національних критичних структур має статус секретної й охороняється національним законодавством. Відповідно це є основною проблемою під час створення дієвих і ефективних механізмів забезпечення національної безпеки так як у ЄС відсутня уніфікована правова платформа щодо забезпечення інформаційної безпеки, зокрема захисту критично-важливої інфраструктури від кібератак. Таке відношення власне диктує застосування насамперед силових механізмів щодо протидії кіберзлочинності, як найбільш ефективних в умовах трансформації сучасної системи міжнародної безпеки

Разом з тим Україна активно модернізує власні сектори безпеки в кіберпросторі

відповідно до права ЄС, зокрема шляхом упорядкування нормативної бази для забезпечення цілісності державної політики у вказаній сфері, а також вироблення єдиних принципів щодо забезпечення стійкості і стабільності інформаційного простору.- У цьому контексті Україна є активним учасником усіх безпекових процесів у Європі, а також активно забезпечує процес створення власних сил швидкого реагування на кіберзагрози, зокрема CERT та кібервійськ. Це власне і є національною платформою формування організаційно-правової основи забезпечення національної кібербезпеки України в контексті адаптації вітчизняного законодавства до стандартів права ЄС у цій сфері.

У відповідності з правом Європейського Союзу в Україні тривають процеси гармонізації та введення в дію сучасних міжнародних стандартів інформаційної безпеки, насамперед – серії міжнародних стандартів ISO/IEC 27000, розроблених Міжнародною організацією з стандартизації (ISO) спільно з Міжнародною електротехнічною комісією (IEC). Впровадження системи управління інформаційною безпекою (СУІБ) відповідно до ISO/IEC 27000 дозволяє оптимізувати процес захисту і дає можливість максимально забезпечити захист інформації і мінімізувати ризики інформаційної безпеки в сукупності з оцінками ефективності інвестицій у забезпеченні безпеки і захисту інформації.

У перспективних планах гармонізації національної правової системи інформаційної безпеки з правом Європейського Союзу є необхідність продовження і розширення діяльність зі створення умов для формування системи міжнародної інформаційної безпеки на основі загальновизнаних принципів і норм міжнародного права. Зокрема, необхідність у підготовці й ухваленні нормативно-правових актів, що регламентують застосування принципів і норм міжнародного права у сфері використання інформаційних та комунікаційних технологій.

Таким чином, необхідно активно охороняти свій інформаційний простір і приділяти першочергову увагу захисту критично важливої інфраструктури як ключової умови національної безпеки.

Висновки

Україна отримала статус держави-кандидата на членство в ЄС, відповідно це зумовлює необхідність імплементації підходів актів права ЄС у національне законодавство України із впровадженням відповідних стандартів, зокрема у сфері інформаційної безпеки.

Разом з тим аналіз законодавчої бази України в галузі інформаційної безпеки в контексті набуття членства в ЄС, виявив ряд проблем щодо гармонізації відповідного законодавства України з правом Європейського Союзу. Зокрема, по-перше, відсутність єдиного трактування базових понять у сфері інформаційної безпеки відповідно до стандартів визначеним правом ЄС; по-друге, неоднозначне тлумачення в Українському законодавстві та відповідно, застосування на практиці норм права у сфері інформаційної безпеки; по-третє, невизначеність на законодавчому рівні щодо реалізації функції забезпечення інформаційної безпеки та механізмів протидії інформаційним загрозам; по-четверте, обмеженість відповідних інформаційно-комунікаційних зв'язків між силовими суб'єктам України та ЄС щодо інформаційної безпеки критичної інфраструктури.

Для комплексного вирішення виявлених проблем у процесі набуття участі в ЄС, необхідно імплементувати законодавчі ініціативи ЄС в Українське законодавство, зокрема:

затвердити в українському законодавстві єдине трактування базових понять у сфері інформаційної безпеки відповідно до стандартів, визначених правом ЄС;

кодифікувати українське законодавство у сфері інформаційної безпеки згідно зі стандартами встановленими ЄС, що дасть можливість єдиного розуміння норм права в процесі реалізації функції забезпечення інформаційної безпеки;

закріпити в українському законодавстві механізми протидії інформаційним загрозам, що базуються на принципах управління ризиками, визначених правилами встановленими ЄС;

забезпечити структурну систематизацію українського законодавства у сфері інформа-

ційної безпеки згідно зі стандартами та правилами закріплених правом ЄС;

затвердити в українському законодавстві перелік злочинів в ІТ-сфері, а також кримінальну відповідальність за злочини в ІТ-сфері, встановлені нормативно-правовими актами ЄС;

затвердити в українському законодавстві регламент міжнародних інформаційно-комунікаційних зв'язків між силовими суб'єктами України та ЄС у сфері забезпечення інформаційної безпеки, зокрема критичної інфраструктури як ключової умови національної безпеки.

З огляду на глобальний розвиток інформаційного суспільства та динаміку суспільних інформаційних відносин, Національне законодавство України потребує подальшого узгодження з чинними міжнародно-правовими актами у сфері інформаційної безпеки та імплементації існуючих міжнародно-правових стандартів. Ефективність реалізації цього процесу досягається на основі активного розвитку правотворчої діяльності України у цій сфері. Це посилить вплив нашої держави як суб'єкта міжнародного права та сприятиме удосконаленню правового регулювання забезпечення інформаційної безпеки.

Література

1. Конституція України: Основний Закон України від 28.06.1996 № 254к/96-ВР.

2. Закон України «Про інформацію»
URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
(дата звернення: 27.04.2023).

3. Закон України «Про Концепцію Національної програми інформатизації» URL: https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80#Text
(дата звернення: 27.04.2023).

4. Закон України «Про основні засади забезпечення кібербезпеки України» URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
(дата звернення: 27.04.2023).

5. Закон України «Про захист інформації в інформаційно-комунікаційних системах»
URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
(дата звернення: 27.04.2023).

6. Указ Президента України Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» від 26.08.2021 р. № 447/2021
URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text
(дата звернення: 27.04.2023).

7. Указ Президента України Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про невідкладні заходи з кібероборони держави» від 26 серпня 2021 р. № 446/2021
URL: https://zakon.rada.gov.ua/laws/show/446/2021#Text
(дата звернення: 27.04.2023).

8. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» від 28 грудня 2021 р. № 685/2021
URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text
(дата звернення: 27.04.2023).

9. Указ Президента України Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» від 25.02.2017 № 47/2017
URL: www.president.gov.ua/documents/472017-21374
(дата звернення: 27.04.2023).

10. Постанова Кабінету Міністрів України № 257 від 24 березня 2023 «Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури»
URL: https://zakon.rada.gov.ua/laws/show/257-2023-%D0%BF#Text
(дата звернення: 27.04.2023).

11. Постанова Кабінету Міністрів України № 943 від 9 жовтня 2020 «Деякі питання об'єктів критичної інформаційної інфраструктури»
URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text
(дата звернення: 27.04.2023).

12. Постанова Кабінету Міністрів України № 518 від 19.06.2019 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури»
URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text
(дата звернення: 27.04.2023).

13. Баранов О.А. Базовий принцип інформаційного права – забезпечення інформаційної безпеки. Запобігання новим викликам та загрозам інформаційній безпеці України: правові аспекти: матеріали наук.-практ. конф. м. Київ, 6 жовт. 2016 р. / упоряд. В.М. Фурашев. Київ: Вид-во "Політехніка". 2016. С. 29-35.

14. Брижко В.М. Основи систематизації інформаційного законодавства: теоретичні та правові засади: монографія. Київ: ТОВ "Пан-Тот", 2012. 304 с

15. Гаврильців М.Т. Інформаційна безпека держави в системі національної безпеки україни Юридичний науковий електронний журнал № 2/2020 с. 200-203

16. Довгань О.Д., Ткачук Т.Ю. Концептуальні засади законодавчого забезпечення інформаційної безпеки україни ІНФОРМАЦІЯ І ПРАВО. № 1(28)/2019 с.86-99

17. Нижник Н.Р., Ситник Г.П., Білоус В.Т. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): навчальний посібник. Ірпінь : Акад. ДПС України, 2000. 304 с.

18. Малашко Олександр Євгенійович Адміністративно-правові засади забезпечення інформаційної безпеки в Україні у контексті європейської інтеграції Кваліфікаційна наукова праця (ДИСЕРТАЦІЯ) на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.07 - адміністративне право і процес; фінансове право; інформаційне право, 2020

19. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія / А.Ю. Нашинець-Наумова. – Київ: Видавничий дім «Гельветика», 2017. – 168 с

20. Ольга Бакалінська, Олександр Бакалинський Правове забезпечення кібербезпеки в Україні Підприємництво господарство і право 9/2019 с.100-108

21. Перун Тарас Степанович Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні УДК 342.6:342.922(477) Кваліфікаційна наукова праця (ДИСЕРТАЦІЯ) на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.07 - адміністративне право і процес; фінансове право; інформаційне право, 2019

22. Пилипчук В.Г. Актуальні питання захисту прав, свобод і безпеки людини в сучасному інформаційному суспільстві. Проблеми захисту прав людини в інформаційному суспільстві: збірник матеріалів наук.-практ. конф. / упорядн. Фурашев В.М., Петряев С.Ю. (НДІІП НАПрН України, НІСД, Секретаріат Уповноваженого Верховної Ради України з прав людини, НТУУ "КПІ"). Київ: Вид-во "Політехніка". 2016. С. 6-8.

23. Попова Т. Безпека інформаційного простору України. Координувати чи ні? URL: http://www.radiosvoboda.org/a/28337376.html (дата звернення: 28.08.2018)

24. С.Я.Кавин До питання поняття інформаційної безпеки в національному та міжнародному праві // Juris Europensis Scientia – 2022 № 4 – С.95-101

25. С.Кавин, І.Брацук Нормативно-правові механізми забезпечення кібербезпеки в нових державах – членах ЄС // Вісник Київського національного університету імені Тараса Шевченка. Юридичні науки. – 2021 -- № 2 (117) – С.30-38

26. Сніцаренко П.М., Саричев Ю.О., Семененко В.М., Ткаченко В.А. Удосконалення чинного інформаційного законодавства України як необхідна умова адекватності заходів щодо забезпечення інформаційної безпеки держави. Збірник наукових праць Центру воєнностратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2018. № 2(63). С. 68-74.

27. Ткачук Тарас Юрійович Правове забезпечення інформаційної безпеки в умовах євроінтеграції України УДК 336.7:340.5:347.7 Кваліфікаційна наукова праця (ДИСЕРТАЦІЯ) на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.07 — адміністративне

право і процес; фінансове право; інформаційне право (081 — Право) 2019

28. Тополевський Р., Захаров Є. Коментарі до проекту Закону України "Про інформаційну безпеку України" від 22.09.04 р. № 5732. URL: http://khpg.org/index.php?id=1105737155 (дата звернення: 05.03.2019).

29. Шемчук В.В. Конституційно-правове забезпечення інформаційної безпеки сучасних держав: порівняльно-правовий аналіз УДК 342.5: 351.862.4 Кваліфікаційна наукова праця (ДИСЕРТАЦІЯ) на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.02 — конституційне право; муніципальне право (081 — Право) 2020

30. Ярема О.Г. Предмет правового забезпечення інформаційної безпеки в інформаційному праві. Науковий вісник Львівського державного університету внутрішніх справ. Серія Право. 2016. № 2. С. 244-252.

Sviatoslav Kavyn
ORCID: https://orcid.org/0000-0002-6189-3848
Ivan Franko University of Lviv
1 University Street, Lviv, Ukraine, 79000
Postgraduate student, Department of European Law
Faculty of International Relations
Phone: + 380631756263
Email: kavinsviatoslav@gmail.com

УДК 314

REGULATORY AND LEGAL PROVISION OF INFORMATION SECURITY OF UKRAINE IN THE CONTEXT OF ACQUIRING MEMBERSHIP IN THE EUROPEAN UNION

The article is devoted to the analysis of the formation of the regulatory and legal field of Ukraine based on the experience of the European Union in the context of the European integration of Ukraine. There was carried out an analysis of legislative and regulatory acts of Ukraine in the field of information security, in particular cyber security and countering cyber sabotage, cyber espionage and cyber crime in the information space. In this context, there were investigated the conceptual principles of legislative provision of information security of Ukraine in accordance with the legislation of Ukraine on provision of information security, as a component of national security of Ukraine. There are highlighted the tendencies in the development of the protection of the information space of Ukraine in the modern information society. There are determined the main problems of the information legislation of Ukraine in the field of creation, distribution and use of information and the ways to solve them. There are also identified the problems of implementing modern information security standards in the conditions of the formation of the national cyber security system of Ukraine. The subject composition of the functioning of the state information security system is presented, as well as the functional content of the subjects of information security.

Ukraine received the status of a candidate state for membership in the EU, accordingly, this necessitates the implementation of the approaches of EU legal acts into the national legislation of Ukraine with the implementation of relevant standards, particularly in the field of information security. In the plans for harmonization of the national legal system of information security with the law of the European Union, there is a need to continue and expand activities to create conditions for the formation of an international information security system based on generally recognized principles and norms of international law. In particular, the need for the preparation and adoption of normative legal acts regulating the application of the principles and norms of international law in the field of the use of information and communication technologies.

In this manner, it is necessary to actively protect the information space and pay primary attention to the protection of critical infrastructure as a key condition of national security.

Keywords: Constitution of Ukraine, information security of Ukraine, cyber security, national security of Ukraine, international information security, information threats, regulatory and legal acts, legal foundations of information relations.