УДК: 341:004.738

Мирослава СІРАНТ
Національний університет «Львівська політехніка»,
заступник директора
Навчально-наукового інституту права,
психології та інноваційної освіти,
д.ю.н., професор
myroslava.m.sirant@lpnu.ua
ORCID: 0000-0002-9393-2397

Сергій ЄСІМОВ
Львівський державний університет внутрішніх справ,
професор кафедр адміністративно-правових дисциплін
к.ю.н., професор
esimov_ss@ukr.net
ORCID 0000-0002-9327-0071

ПРАВОВИЙ СТАТУС СПЕЦІАЛІЗОВАНИХ ОРГАНІВ ЄВРОПЕЙСЬКОГО СОЮЗУ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

http://doi.org/10.23939/law2025.48.406

Стаття присвячена дослідженню правового статусу спеціалізованих органів Європейського Союзу у сфері забезпечення кібербезпеки. Актуальність дослідження обумовлена політикою європейської інтеграції визначеної Конституцією України. Об’єктом дослідження є суспільні відносини, які мають місце при забезпечення кібербезпеки в країнах-членах Європейського Союзу. Предметом дослідження є нормативні акти Європейського Союзу, які регламентують діяльність Агентство Європейського Союзу з кібербезпеки. Методологія дослідження базується на діалектиці. Серед загальнонаукових методів у дослідженні було застосовано: аналіз; синтез; системний метод; структурно-функціональний метод. До спеціальних наукових методів, використаних у дослідженні, належать: історико-правовий метод; порівняльно-правовий метод; метод системного аналізу права; формально юридичний метод; метод аналізу правозастосовної практики; метод правового моделювання. Термін «кібербезпека» офіційно з’явився в ЄС спочатку як політична категорія: вперше був використаний Європейською комісією у Стратегії кібербезпеки Європейського Союзу – Відкритий, безпечний та надійний кіберпростір 2013 р. Зазначено, що відмінною рисою європейського підходу є опора на екстериторіальний суверенітет і завдання підвищення міжнародного престижу Європейського Союзу шляхом реалізації глобальної ініціативи – Програми дій з просування відповідальної поведінки держав у кіберпросторі. Особлива увага в Європейському Союзі приділяється співробітництву на регіональному рівні, основною метою якого є формування системи забезпечення кібербезпеки в європейському регіоні з опорою на нормативну та інституційну

базу Європейського Союзу, а також інструменти співробітництва Ради Європи, Організація з безпеки і співробітництва в Європі (ОБСЄ) та Північноатлантичного договору (НАТО).

Ключові слова: європейська інтеграція, інформаційна безпека, кібератаки, нормативні акти, координаційний центр, центр компетенцій.

Постановка проблеми. Розвиток суспільства, держави, права протікає під впливом процесів цифровізації, в основі яких лежать інформаційно-комунікаційні технології та створювані завдяки їм інформаційні мережі, системи, бази даних. Нові можливості та переваги, одержувані від впровадження інформаційно-комунікаційних технологій у публічно-правові та приватноправові відносини, супроводжуються появою нових видів небезпек і злочинних посягань, які перетворилися на нову глобальну проблему. Серед регіональних міжнародних організацій та інтеграційних об'єднань найбільш вагомих результатів у розробленні правових стандартів забезпечення кібербезпеки досяг Європейський Союз. У законодавстві ЄС, спрямованому на забезпечення кібербезпеки, сфера кібербезпеки є самостійним напрямом правового регулювання.

Аналіз дослідження проблеми. Окремі аспекти правового статус спеціалізованих органів Європейського Союзу у сфері забезпечення кібербезпеки досліджувалися в роботах: А. В. Войціховського, С. В. Демедюка, І. М. Забари, О. Ю. Запорожця, В. К. Конаха, В. А. Ліпкана, С. В. Легомінова, Р. В. Лук'янчука, Т. М. Мужанової, Г. П. Нестеренко, А. М. Орлеана, Є. Б. Тіхомірова, Ю. В. Щавінський, Ю. М. Якименко та інші.

Метою статті є дослідження правового статусу спеціалізованих органів Європейського Союзу у сфері забезпечення кібербезпеки.

Виклад основного матеріалу Поряд із органами загальної та спеціальної компетенції ЄС, серед органів ЄС, виділяються органи, діяльність яких присвячена виключно кібербезпеці. Ключове місце серед них займає Агентство ЄС з кібербезпеки, яке раніше називалося Європейське агентство з мережевої та інформаційної безпеки (далі – Агентство). Правовою основою, ухвалення Регламенту (ЄС) 460/2004 Європейського парламенту та Ради про створення Європейського агентства з мережевої та інформаційної безпеки (далі – Регламенту (ЄС) 460/2004) стала ст. 95 Договору про заснування Європейського Співтовариства (нині ст. 114 Договору про функціонування ЄС), який дозволяє вживати органам ЄС заходів, що гармонізують національне законодавство держав-членів ЄС, присвячених створенню або функціонуванню внутрішнього ринку [1; 2].

У ст. 18 Регламенту (ЄС) 460/2004 встановлено, що Агентство є органом ЄС і має правосуб'єктність. Відповідно до законодавства ЄС агентства є окремими органами, відмінними від інститутів ЄС та окремими юридичними особами, які створюються для виконання конкретних завдань. Спочатку Агентство було створено 14 березня 2004 року. терміном на п'ять років, тобто Агентство мало обмежений мандат. Агентство, відповідно до своєї мети, має підвищувати рівень компетентності ЄС, держав-членів та представників бізнесу у питаннях запобігання, вирішення та реагування на проблеми. Для забезпечення виконання цілей, зазначених у Регламенті (ЄС) 460/2004, виділялося 11 завдань, які кореспондують цілям Агентства та полягають у наступному:

- збирання інформації про ризики, що можуть вплинути на стійкість і доступність мереж зв'язку, на справжність, цілісність та конфіденційність інформації у наданні результатів державам-членам та Європейській комісії;
- надання консультацій інститутам, органам та установам ЄС, державам членам;
- зміцнення співробітництва між різними суб'єктами, що діють у галузі мережевої та інформаційної безпеки;
- сприяння співпраці між Європейською комісією та державами-членами у розробці спільних методологій для запобігання, вирішення та реагування на питання мережевої та інформаційної безпеки;

− підвищення обізнаності та доступності своєчасної, об'єктивної та всеосяжної інформації з питань мережевої та інформаційної безпеки для всіх користувачів;

− надання допомоги Європейській комісії та членам діалогу з промисловістю для вирішення проблем, пов'язаних з безпекою, в апаратних та програмних продуктах;

− відстеження розробки стандартів для продуктів та послуг у галузі мережевої та інформаційної безпеки; консультування Європейської комісії з досліджень у галузі мережевої та інформаційної безпеки, щодо ефективного використання технологій запобігання ризикам;

− сприяння діяльності з оцінки ризиків, сумісним рішенням з управління ризиками та дослідженням щодо рішень з управління превентивної діяльності в організаціях державного та приватного сектору; сприяти зусиллям Співтовариства зі співробітництва з третіми країнами та з міжнародними організаціями, з метою сприяння глобальному підходу до питань мережної та інформаційної безпеки, сприяючи розвитку культури мережевої та інформаційної безпеки;

− самостійно висловлювати свої власні висновки, орієнтації та давати рекомендації з питань, що входять до сфери компетенції Агентства.

Робота Агентства зведена до незалежного консультаційного органу держав-членів та європейських підприємців, що забезпечує доступ до інформації та ресурсів, необхідних для функціонування у кіберпросторі.

З метою ефективного забезпечення виконання цілей та завдань організаційна структура Агентства в період першого мандату представляла ієрархію із трьох структур:

1. Правління, що складається з одного представника кожної держави-члена, трьох представників, що призначаються Європейською комісією, трьох представників, запропонованих Європейською комісією та призначених Радою ЄС без права голосу, кожен з яких представляє одну з наступних груп: індустрія інформаційно-комунікаційних технологій; групи споживачів; академічні експерти з мережевої та інформаційної безпеки.
2. Виконавчий директор, який призначався Правлінням на основі списку кандидатів, запропонованого Європейською комісією після відкритого конкурсу.
3. Групи зацікавлених сторін, що включає експертів, які представляють зацікавлені сторони.

Враховуючи позитивну оцінку діяльності Агентства, видану Європейською комісією у 2008 р., Європейський парламент та Рада ухвалили Регламент (ЄС) 1007/2008 від 24 вересня 2008 р., що змінює Регламент (ЄС) № 460/2004 про створення Європейського агентства продовжуючи мандат Агентства до 2012 р. [3].

Стратегія кібербезпеки для Європейського союзу 2013 року – Відкритий, безпечний та надійний кіберпростір (2013/2606(RSP)) визначило Агентство як необхідного суб'єкта, який здійснює нагляд за управлінням кібербезпекою, яка потребувала лише модернізованого мандату з додатковими повноваженнями [4, с. 30].

У результаті було прийнято новий Регламент про Агентство, який посилював мандат цієї організації. Новий мандат було затверджено Регламентом (ЄС) 526/2013 від 16 квітня 2013 р. та було встановлено на сім років. Для підвищення ефективності роботи новий Регламент заснував нову додаткову філію Агентства з оперативним персоналом в Афінах. [5].

Новий Регламент (ЄС) 526/2013 закріпив, що Агентство виконує завдання, покладені правовими актами Союзу. З прийняттям Директиви (ЄС) 2016/1148 про забезпечення безпеки мережевих та інформаційних систем, Агентству була відведена роль секретаріату Груп реагування на інциденти, пов'язані з комп'ютерною безпекою (далі – CSIRTs), яка була створена для сприяння швидкому та ефективному оперативному співробітництву між ЄС та державами щодо кібербезпеки та обміну інформацією про ризики [6, с. 61].

Як позитивні характеристики Агентства було виділено його роль у забезпеченні співробітництва між державами-членами, Групами реагування на інциденти, пов'язані з комп'ютерною безпекою. Недостатня здатність Агентства задовольняти потреби зацікавлених сторін, зокрема потреби галузевих компаній, а не тільки держав-членів, пояснюється недостатніми ресурсами Агентства.

У 2019 р. був прийнятий Акт про кібербезпеку, який наділив Агентство постійним мандатом з розширеними завданнями щодо створення та управління сертифікацією кібербезпеки ЄС. Оскільки основна роль у сфері сертифікації приділяється Агентству, положення, що закріплюють діяльність Агентства та сертифікації, зосереджені в одному акті. Положення про Агентство містяться у перших двох розділах Акту про кібербезпеку, а положення, що встановлюють європейську систему сертифікації, встановлені у 3 розділі Акту про кібербезпеку.

Завдання Агентства, закладені Регламентом (ЄС) 460/2004, зберегли чинність, до них були додані завдання, пов'язані з сертифікацією. Це підготовка європейських схем сертифікації кібербезпеки продуктів та послуг інформаційно-комунікаційних технологій; надання допомоги Європейській комісії у наданні Секретаріату Європейської групи сертифікації кібербезпеки; складання та публікація керівних принципів та розробка передової практики щодо вимог кібербезпеки продуктів та послуг інформаційно-комунікаційних технологій у співпраці з національними органами з нагляду за сертифікацією та промисловістю.

Ст. 12 Акту про кібербезпеку визначає повноваження Агентства у сфері міжнародного співробітництва: участь у якості спостерігача в організації міжнародних навчань з кібербезпеки; обмін досвідом з міжнародними організаціями; надання консультацій та підтримки Європейської комісії з питань, що стосуються угод про взаємне визнання сертифікатів кібербезпеки з третіми країнами [7]. У листопаді 2021 р. Агентством було прийнято Міжнародну стратегію Агентства з кібербезпеки. У ній закріплюються три підходи (обмежений, допоміжний та роз'яснювальний), які Агентство може використовувати під час здійснення міжнародного співробітництва. Встановлюється 10 принципів, які визначають підхід ЄС до цієї співпраці.

Згідно з єдиним програмним документом на 2023-2025 р. розмір фінансування Агентства у 2022 р. складає 24 мільйони євро, а у 2023 р. 25 мільйонів євро. У єдиному програмному документі зазначається, що поточні ресурси Агентства становлять на 3 мільйони євро менше, ніж його потреби.

У березні 2022 р. Агентство отримало додаткове фінансування від Європейської комісії у розмірі 15 мільйонів євро, виділених для підтримки здійснення Агентством регулярних завдань у зв'язку з збройною агресією російської федерації щодо України. Питання забезпечення Агентства кадровими ресурсами є складним, зважаючи на труднощі утримання висококваліфікованих фахівців.

Незважаючи на це, кадрова чисельність Агентства в період з 2019 р. до 2022 р. збільшилася з 59 до 82 посад, у зв'язку з появою нових завдань, які були передбачені відповідно до Акту про кібербезпеку.

Після ухвалення нової Директиви (ЄС) 2022/2555 про заходи щодо забезпечення кібербезпеки, яка скасувала Директиву (ЄС) 2016/1148 про забезпечення безпеки мережевих та інформаційних систем, роль Агентства була зміцнена [8; 9].

Ця Директива встановила додаткові зобов'язання Агентства. З прийняттям Директиви (ЄС) 2022/2555 про заходи щодо забезпечення кібербезпеки Агентству, крім підготовки технічного звіту, встановлено обов'язок щодо підготовки Звіту про стан кібербезпеки ЄС у спільній співпраці з Європейською комісією та Групою співробітництва.

Відповідно до ст. 16 Директиви (ЄС) 2022/2555 про заходи щодо забезпечення кібербезпеки Агентству необхідно забезпечити секретаріат Європейської мережі зв'язків з кібер кризами (далі – EU-CyCLONe), яка була заснована Директивою для підтримки скоординованого управління інцидентами кібербезпеки в масштабі державами-членами та інститутами, органами, установами та агентствами ЄС.

Враховуючи широке коло питань, якими займається Агентство, таке серйозне питання, як дослідження та інновації, потребує створення ефективних механізмів співпраці між державними та приватними компаніями щодо розвитку нових досліджень та інновацій у галузі кібербезпеки. У зв'язку з цим Рішенням Європейської комісії було ініційовано створення публічно-приватного партнерства з кібербезпеки, спрямованого на підтримку та розвиток науково-дослідного потенціалу. Метою партнерства є розвиток співпраці між державними та приватними суб'єктами на ранніх стадіях дослідницького та інноваційного процесу; стимулювання промисловості кібербезпеки; координувати промислові ресурси цифрової безпеки у Європі.

За оцінками Європейської комісії, Комісія інвестувала понад 63,5 мільйонів євро у чотири пілотні проєкти (CONCORDIA, ECHO, SPARTA216 та CyberSec4Europe) у рамках програми «Горизонт 2025-2027».

У 2018 р. Європейська Комісія виступила з пропозицією щодо створення Європейського центру промислової, технологічної та дослідницької компетенції у галузі кібербезпеки з Мережею національних координаційних центрів.

Функціонування вищезгаданого публічно-приватного партнерства створило добрий потенціал для майбутнього Європейського промислового, технологічного та дослідницького центру компетенцій у галузі кібербезпеки та Мережі національних координаційних центрів.

В результаті до організаційної структури ЄС Регламентом (ЄС) 2021/887 від 20 травня 2021 р. про створення Європейського центру компетенції в галузі промисловості, технологій та досліджень з кібербезпеки та мережі національних координаційних центрів були включені ще два структурні елементи: Європейський центр компетенцій Центр компетенції) та Мережа національних координаційних центрів (далі – Мережа) [10].

Роль Центру компетенцій та мережі полягає в тому, щоб допомогти Європейському Союзу у розвитку технологічного, академічного суспільного, дослідницького та промислового потенціалу кібербезпеки (ст. 3 Регламенту (ЄС) 2021/887 про створення Європейського центру компетенцій та мережі національних координаційних центрів). Основними завданнями Центру компетенцій та Мережі виступають такі: стимулювати розробку та впровадження технологій у галузі кібербезпеки та доповнювати зусилля щодо нарощування потенціалу в цій галузі на рівні ЄС та національному рівні. Як правову основу для створення Центру компетенцій було визначено ст. 173 та 188 Договору про функціонування ЄС.

Регламент (ЄС) 2021/887 про створення Європейського центру компетенцій та мережі національних координаційних центрів до завдань Центру компетенцій відносить підтримку сфери кібербезпеки, зокрема малих та середніх підприємств, з метою зміцнення передового досвіду, потенціалу та конкурентоспроможності Союзу в галузі кібербезпеки розгортання, залучення інвестицій.

Центр компетенцій є агентством ЄС. Структура Центру компетенцій складається з:

1. Правління, яке включає одного представника кожної держави-члена та двох представників Європейської комісії, які діють від імені Союзу. Представник Агентства ЄС з кібербезпеки є постійним спостерігачем у Правлінні.
2. Виконавчого директора, яким має бути особа, яка має досвід і репутацію у сферах, у яких працює Центр компетенцій. Виконавчий директор несе відповідальність за діяльність та повсякденне управління Центром компетенцій і є його законним представником.
3. Стратегічної консультативної групи, яка має складатися не більше ніж із 20 членів. Члени призначаються Керівною радою, яка діє за пропозицією Виконавчого директора, з числа представників членів товариства, за винятком представників інститутів, органів, установ та агенцій Союзу.

Стратегічна консультативна група повинна регулярно консультувати Центр компетенцій щодо виконання діяльності Центру компетенцій та забезпечувати зв'язок із спільнотою та іншими відповідними заінтересованими сторонами. Держави-члени повинні призначити національний координаційний центр з числа національних юридичних осіб, які мають необхідні можливості для управління засобами для виконання місії та цілей, викладених у Регламенті (ЄС) 2021/887 про створення Європейського центру компетенцій та мережі національних координаційних центрів.

Національні координаційні центри отримують фінансування на виконання завдань від держав-членів та бюджету ЄС. Завдання національних координаційних центрів полягають у підтримці Центру компетенції, у виконанні його місії та завдань; надання технічної допомоги заінтересованим сторонам шляхом надання їм підтримки на етапі подання заявок на проєкти, керовані Центром компетенції; здійснення конкретних дій, на які Центр компетенцій виділив гранти, зокрема шляхом надання фінансової підтримки третім сторонам; без шкоди для компетенції держав-членів у галузі освіти та з урахуванням відповідних завдань Агентства, взаємодія з національними органами влади щодо можливого вкладу у просування та розповсюдження освітніх програм з кібербезпеки та інші. Згідно з єдиним програмним документом на 2023-2025 р. планується, що Мережа функціонує з 2023 року.

Внесок у роботу Центру та Мережі вносить Співтовариство фахівців у галузі кібербезпеки, яке включає до складу представників промисловості (малі та середні підприємства), академічні та дослідницькі організації, інші відповідні асоціації громадянського суспільства, при необхідності відповідні європейські організації зі стандартизації, державні установи та інші організації, що займаються операційними та технічними питаннями.

Центр компетенцій у співпраці з мережею виступає основним органом з реалізації фінансових ресурсів ЄС, які виділяються на кібербезпеку в програмах «Цифрова Європа» та «Горизонт Європа» [11]. Фінансове забезпечення діяльності Центру та Мережі здійснюється за рахунок бюджету ЄС, але фінансування спільних дій відбувається за рахунок добровільних внесків держав-членів та Союзу.

У грудні 2022 р. Європейська комісія виділила 3 мільйони євро на фінансування проєкту під назвою «Європейська спільнота кібербезпеки», який очолює Європейська організація з кібербезпеки.

В ЄС було розроблено цілий організаційно-правовий механізм для забезпечення підвищення конкурентоспроможності ринку Європи в галузі кібербезпеки. На закінчення розгляду організаційної структури ЄС щодо забезпечення кібербезпеки, слід розглянути існуючі в ЄС механізми співробітництва між органами ЄС. Співпраця та обмін інформацією у вирішенні проблем кібербезпеки є важливими елементами для досягнення високого рівня захисту від кіберзагроз, тому створення узгодженого механізму взаємодії та співробітництва між органами, задіяними в галузі кібербезпеки, є пріоритетним завданням ЄС.

З метою встановлення співробітництва між Європолом та Агентством ЄС з кібербезпеки та надання підтримки державам-членам ЄС та його установам у запобіганні та боротьбі з кіберзлочинністю, між Агентством ЄС з кібербезпеки та Європолом було підписано Угоду про стратегічне партнерство, яка закладає основу для взаємодії та взаємодопомоги між цими організаціями.

Тим не менш, у правовому плані відправною точкою для встановлення співробітництва між органами, що займаються кібербезпекою, стала стаття ст. 7 Акту про кібербезпеку. У зазначеному Регламенті як зобов'язання визначено, що Агентство має співпрацювати на оперативному рівні та налагоджувати взаємодію з інститутами, органами, установами та агентствами Союзу, включаючи CERT-EU, органами, що займаються кіберзлочинністю, та органами, що займаються захистом конфіденційності та персональних даних.

Офіційно угоду про співробітництво між Агентством та Групою реагування на комп'ютерні надзвичайні ситуації для інститутів, органів та агентств ЄС (далі – CERT-EU) було встановлено після підписання у 2021 р. Меморандуму про взаєморозуміння, в якому визначено галузі співпраці (нарощування потенціалу, оперативне співробітництво, знання: CERT-EU відіграватиме провідну роль у наданні допомоги інститутам, органам та агентствам ЄС, а Агентство робитиме свій внесок в обсязі та межах, визначених його мандатом, і навпаки.

Для покращення співпраці між Європейським оборонним агентством, Агентством ЄС з кібербезпеки, Європейським центром боротьби з кіберзлочинністю та CERT-EU було також підписано Меморандум про взаєморозуміння.

Європейській комісії було зазначено, що цей Меморандум зміцнив співпрацю та синергію між цими організаціями відповідно до їхніх мандатів та сприяв подальшому розвитку надання експертних знань, оперативної та технічної підтримки ЄС та державам-членам у галузі кібербезпеки.

У червні 2021 р. Європейська комісія у Рекомендації оголосила про створення Спільного кіберпідрозділу. Раніше пропозиція щодо його створення була викладена у політичних керівних засадах голови Європейської комісії. Ця ініціатива є важливим кроком на шляху до завершення європейської системи управління ризиками у сфері кібербезпеки. Вона спрямована на забезпечення координації зусиль у ЄС щодо запобігання, виявлення, стримування, пом'якшення наслідків та реагування на великомасштабні кіберінциденти та кризи.

Об'єднаний кібер підрозділ виступатиме як платформа для забезпечення скоординованого реагування ЄС на великомасштабні кібер інциденти та кризи для надання допомоги у відновленні після цих атак. Об'єднаний кібер підрозділ забезпечує віртуальну та фізичну платформу та не вимагає створення додаткового автономного органу. Його створення впливає на компетенцію та повноваження національних органів з кібербезпеки та відповідних структур Союзу.

Воно об'єднує усі спільноти з кібербезпеки, тобто громадянське населення, правоохоронні органи, дипломатію та оборону. Учасники платформи мають грати або оперативну, або допоміжну роль.

Оперативні учасники повинні включати Європейську комісію, Агентство ЄС з кібербезпеки, Європол, Європейську службу зовнішньополітичної діяльності, CERT-EU, мережу CSIRTs та EU-CyCLONe. Допоміжні учасники повинні включати Європейське оборонне агентство, голову Горизонтальної робочої групи з кіберпитань Ради ЄС та одного представника з проєктів з кібербезпеки Постійного структурованого співробітництва.

У ЄС питанням забезпечення кібербезпеки опікується розгалужена система органів. Центральна роль приділяється спеціалізованому органу ЄС – Агентству ЄС з кібербезпеки. До основних недоліків організаційного механізму в галузі кібербезпеки необхідно віднести недостатнє чітке розмежування відповідальності між ними, великі фінансові витрати на підтримку функціонування.

У листопаді 2023 року Рада ЄС і Європарламент досягли попередньої угоди щодо Регламенту про кіберстійкість, а в березні 2024 року Європарламент схвалив його зі змінами, внесеними за результатами дебатів. Щоб набути чинності, Регламент має бути офіційно прийнятий Радою ЄС [12, с. 142]. Регламент про кіберстійкість стане першим у світі нормативним актом, який визначає вимоги безпеки для продуктів як перешкоду для входу на ринок. Обмеження почнуть діяти з 2027 року.

Висновки. Проблема кібербезпеки є об'єктивним наслідком цифрової трансформації суспільного життя. Зростання цифровізації у всіх сферах збільшує кількість кіберзагроз, кількість кібератак і проблем кібербезпеки. Наявність ризиків, що супроводжують формування цифрового суспільства, вимагає постійної уваги для запобігання та усунення загроз на рівні різних секторів економіки, державної діяльності та суспільства. У даний час Європейський Союз приділяє пріоритетну увагу розвитку та вдосконаленню правового регулювання кібербезпеки. Подальший розвиток правового регулювання Європейського Союзу буде пов'язаний із формуванням одноманітної судової практики щодо тлумачення та застосування нормативно-правових актів Європейського Союзу Судом Європейського Союзу, як це сталося в інших сферах суспільного життя.

Доцільно виділити недоліки у діяльності Європейського Союзу щодо правового регулювання забезпечення кібербезпеки, а саме повільний темп прийняття правових актів, тривалий термін їх імплементації до національного законодавства держав-членів Європейського Союзу.

У перспективі доцільно дослідити динаміку інституційного забезпечення як елемента розробки та впровадження політики кібербезпеки.

Подяки. Немає.

Фінансування. Автори заявляють про відсутність фінансової підтримки для проведення досліджень, написання або публікації цієї статті.

Внесок авторів: Сірант Мирослава – 50 %, Єсімов Сергій – 50 %. Автори схвалюють цю роботу і беруть на себе відповідальність за її цілісність.

Конфлікт інтересів. Автори заявляють про відсутність конфлікту інтересів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/reg/2004/460/oj/eng (Дата звернення: 03.07.2025).

2. CONSOLIDATED VERSION OF THE TREATY ON EUROPEAN UNION. URL: https://eur-lex.europa.-eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826 e6da6.0023.02/DOC_1&format=PDF (Дата звернення: 03.07.2025).

3. Regulation (EC) No 1007/2008 of the European Parliament and of the Council of 24 September 2008 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration (Text with EEA relevance). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex: 32008R1007 (Дата звернення: 03.07.2025).

4. Законодавство та стратегії у сфері кібербезпеки країн Європейського Союзу США, Канади та інших. Верховна Рада України. Європейський інформаційно-дослідницький центр. URL: https://infocenter.rada.gov. ua/uploads/documents/28982.pdf (Дата звернення: 03.07.2025).

5. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace: adopted by the European Commission on 7 February 2013. URL: https://www.europarl.europa.eu/doceo/document/TA-7-2013-03_EN.html (Дата звернення: 03.07.2025).

6. Бойко В. Д., Василенко М. Д., Кухаренко С. В. (2019). Кібербезпека в ЄС та країнах-членах: генезис та проблеми її підвищення. *Інформаційна безпека людини, суспільства, держави. №3. С. 57-69.*

7. Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 Text with EEA relevance/ URL: https://eur-lex.europa.eu/eli/reg/2013/526/oj/eng (Дата звернення: 03.07.2025).

8. 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) (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng (Дата звернення: 03.07.2025).

9. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj/eng (Дата звернення: 03.07.2025).

10. Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. URL: https://eur-lex.europa.eu/eli/reg/2021/887/oj/eng (Дата звернення: 03.07.2025).

11. Програма «Цифрова Європа». URL: https://eufordigital.eu/uk/discover-eu/the-digital-europe-program me/ (Дата звернення: 03.07.2025).

12. Мужанова Т.М., Легомінова С.В., Якименко Ю.М., Щавінський Ю.В., Нестеренко Г.П. (2024). Основні підходи й напрями розвитку політики кібербезпеки Європейського Союзу. *Кібербезпека: освіта, наука, техніка*. 2024. № 4. С. 133-149.

REFERENCES

1. ***Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance***). Retrieved from: https://eur-lex.europa.eu/eli/reg/2004/460/oj/eng (Accessed: 03.07.2025) [In English].

2. ***CONSOLIDATED VERSION OF THE TREATY ON EUROPEAN UNION.*** Retrieved from: https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF (Accessed: 03.07.2025) [In English].

3. ***Regulation (EC) No 1007/2008 of the European Parliament and of the Council of 24 September 2008 amending*** Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration (Text with EEA relevance). Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/ ?uri=celex: 32008R1007 (Accessed: 03.07.2025) [In English].

4. ***Zakonodavstvo ta stratehiyi u sferi kiberbezpeky krayin Yevropeys′koho Soyuzu SSHA, Kanady ta inshykh*** [Legislation and strategies in the field of cybersecurity in the European Union, the United States, Canada, and other countries.]. Verkhovna Rada Ukrayiny. Yevropeys′kyy informatsiyno-doslidnyts′kyy tsentr. [Legislation and strategies in the field of cybersecurity of the European Union countries, the USA, Canada and others. Verkhovna Rada of Ukraine. European Information and Research Center]. Retrieved from: https://infocenter.rada.gov.ua/uploads/ documents/28982.pdf (Accessed: 03.07.2025) [In Ukrainian].

5. ***Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace***: adopted by the European Commission on 7 February 2013. Retrieved from: https://www.europarl.europa.eu/doceo/document/TA-7-2013-03_EN.html (Accessed: 03.07.2025) [In English].

6. Boyko V. D., Vasylenko M. D., Kukharenko S. V. (2019). ***Kiberbezpeka v YES ta krayinakh-chlenakh: henezys ta problemy yiyi pidvyshchennya.*** [Cybersecurity in the EU and member states: genesis and problems of its improvement]. Informatsiyna bezpeka lyudyny, suspil′stva, derzhavy – Information security of man, society, state. 3. 57-69. (Accessed: 03.07.2025) [In English].

7. ***Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation*** (EC) No 460/2004 Text with EEA relevance/ Retrieved from: https://eur-lex.europa.eu/eli/reg/2013/526/oj/eng (Accessed: 03.07.2025) [In English].

8. ***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) (Text with EEA relevance). Retrieved from: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng (Accessed: 03.07.2025) [In English].

9. ***Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union***. Retrieved from: https://eur-lex.europa.eu/eli/dir/2016/1148/oj/eng (Accessed: 03.07.2025) [In English].

10. ***Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres***. Retrieved from: https://eur-lex.europa.eu/eli/reg/2021/887/oj/eng (Accessed: 03.07.2025) [In English].

11. ***Prohrama «Tsyfrova Yevropa».*** [Digital Europe Program]. Retrieved from: https://eufordigital.eu/uk/discover-eu/the-digital-europe-programme/ (Accessed: 03.07.2025) [In Ukrainian].

13. Muzhanova T.M., Lehominova S.V., Yakymenko YU.M., Shchavins′kyy YU.V., Nesterenko H.P. (2024). ***Osnovni pidkhody y napryamy rozvytku polityky kiberbezpeky Yevropeys′koho Soyuzu***. [Main approaches and directions of development of cybersecurity policy of the European Union]. Kiberbezpeka: osvita, nauka, tekhnika – Cybersecurity: Education, Science, Technology. 4.133-149. DOI: 10.28925/2663-4023.2024.24.133149 (Accessed: 03.07.2025) [In Ukrainian].

Отримано: 17.07.2025
Прорецензовано: 29.08.2025
Схвалено до друку: 29.09.2025
Опубліковано (онлайн): 12.12.2025
Надруковано: 26.12.2025

Myroslava SIRANT
Lviv Polytechnic National University,
Educational and Research Institute of Law,
Psychology and Innovative Education,
Deputy Director
Dr. Habil. (Law), Professor
myroslava.m.sirant@lpnu.ua
ORCID: 0000-0002-9393-2397

Serhiy YESIMOV,
Lviv State University of Internal Affairs,
Professor of the Department of Administrative and Legal Disciplines
Ph.D. in Law, Professor
esimov_ss@ukr.net
ORCID 0000-0002-9327-0071

LEGAL STATUS OF SPECIALIZED BODIES OF THE EUROPEAN UNION IN THE FIELD OF CYBERSECURITY

The article is devoted to the study of the legal status of specialized bodies of the European Union in the field of cybersecurity. The relevance of the study is due to the policy of European integration defined by the Constitution of Ukraine. The object of the study is the social relations that take place when ensuring cybersecurity in the member states of the European Union. The subject of the study is the regulatory acts

of the European Union that regulate the activities of the European Union Agency for Cybersecurity. The research methodology is based on dialectics. Among the general scientific methods used in the study were: analysis; synthesis; system method; structural-functional method. The special scientific methods used in the study include: historical-legal method; comparative-legal method; method of systemic analysis of law; formal legal method; method of analysis of law enforcement practice; method of legal modeling. The term «cybersecurity» officially appeared in the EU initially as a political category: it was first used by the European Commission in the Cybersecurity Strategy of the European Union - An Open, Safe and Secure Cyberspace in 2013. It is noted that a distinctive feature of the European approach is the reliance on extraterritorial sovereignty and the task of increasing the international prestige of the European Union through the implementation of a global initiative - the Action Program for Promoting Responsible Behavior of States in Cyberspace. The European Union pays special attention to cooperation at the regional level, the main goal of which is to form a system for ensuring cybersecurity in the European region based on the regulatory and institutional framework of the European Union, as well as cooperation instruments of the Council of Europe, the Organization for Security and Cooperation in Europe (OSCE) and the North Atlantic Treaty Organization (NATO).

Keywords: European integration, information security, cyberattacks, regulations, coordination center, center of competences.