УДК 342.52

ПЕТРОВ С.Г., *кандидат юридичних наук.*
ORCID: https://orcid.org/0000-0001-7786-4657.

ОРГАНІЗАЦІЙНІ І ПРАВОВІ ОСНОВИ ВИРІШЕННЯ ПРОБЛЕМ ПРОТИДІЇ КІБЕРПОСЯГАННЯМ У ЄВРОПЕЙСЬКОМУ СОЮЗІ

Анотація. *У статті здійснено аналіз організаційних та правових підходів ЄС та окремих держав-членів щодо протидії кіберпосяганням. Запропоновано врахувати в Україні досвід Польщі щодо функціонування установи, яка поєднує наукові дослідження, освітні програми і практичну реалізації заходів протидії кіберпосяганням, Австрії – щодо існування національного CERTу Австрії для приватного сектору.*

Ключові слова: *кіберпосягання, організаційні та правові основи, Європейський Союз, кібербезпека, державно-приватне партнерство.*

Summary. *The article deals with the issues of organizational and legal approaches of the EU and individual Member States to address cyber-attacks. It is suggested for Ukraine to take into account the experience of Poland in the functioning of an institution that combines scientific research, educational programs and practical implementation of measures against cyberattacks, of Austria – regarding the existence of a national CERT of Austria for the private sector*

Keywords: *cyber attacks, organizational and legal framework, European Union, cybersecurity, public-private partnership.*

Аннотация. *В статье осуществлен анализ организационных и правовых подходов ЕС и отдельных государств-членов по противодействию киберпосягательствам. Предложено учесть в Украине опыт Польши по функционированию учреждения, которое сочетает научные исследования, образовательные программы и практическую реализацию мер противодействия киберпосягательствам, Австрии – относительно существования национального CERT для частного сектора.*

Ключевые слова: *киберпосягательства, организационные и правовые основы, Европейский Союз, кибербезопасность, государственно-частное партнерство.*

Постановка проблеми. Євроінтеграційний вектор України, закріплений в Угоді про асоціацію між Україною та Європейським Союзом, є незмінним зовнішньополітичним пріоритетом нашої держави. Угода про асоціацію визначила такий формат відносин між Україною та ЄС, який став стратегічним орієнтиром соціально-економічних реформ в Україні, зокрема і у безпековому напрямку.

Проблема захисту від кіберпосягань на інформаційні ресурси наразі є актуальною як для ЄС та його держав-членів, так і для України. Розбудова державних структур, поглиблення державно-приватного партнерства, удосконалення правових основ протидії кіберпосяганням вимагає усебічного аналізу позитивних практик провідних країн. Унікальність прикладів у цьому контексті полягає у дворівневому правовому регулюванні і відповідно управлінні: на рівні ЄС і на рівні держав-членів об'єднання.

Результати аналізу наукових публікацій свідчать про те, що питання забезпечення кібернетичної і інформаційної безпеки держави були предметом досліджень багатьох українських учених, а саме О.Д. Довганя, О.О. Климчука, А.І. Марущака, В.В. Остроухова, В.М. Панченко, В.Г. Пилипчука, В.І. Польового, О.Б. Розвадовського, В.Б. Хлевицького, О.М. Юрченка та інших.

Частково досвід країн-учасниць НАТО у сфері забезпечення кібернетичної безпеки розкривав Р.В.Лук'янчук, який акцентував увагу на етапах взаємодії між Україною та Альянсом у межах функціонування Трастового фонду НАТО з кібербезпеки, обґрунтував доцільність прискорення процесу приєднання України до НАТО з метою входження до системи колективної безпеки, у тому числі й у форматі забезпечення кібербезпеки [1].

Проблеми кібербезпеки останнім часом є предметом для обговорення на різноманітних науко-практичних форумах [2; 3]. Видаються підручники, які розкривають теоретичні та прикладні питання міжнародної інформаційної та кібербезпеки як складової міжнародної системи підтримання миру і стабільності [4].

На основі аналізу європейського досвіду з питань боротьби з правопорушеннями в інформаційній сфері дослідники обґрунтовують також часткові питання задля протидії кіберпосяганням, наприклад, необхідність підписання Меморандуму про взаєморозуміння між Інтернет-провайдерами та правоохоронними органами у межах державно-приватного партнерства [5].

Загалом, як бачимо, підходи Європейського Союзу і держав-членів до вирішення проблем протидії кіберпосяганням були предметом досліджень тільки частково.

Метою статті є розкриття організаційних і правових основ протидії кіберпосяганням у Європейському Союзі і формулювання прийнятних для України прикладів.

Виклад основного матеріалу. Розпочнемо з аналізу організаційних та правових підходів ЄС до спільної політики безпеки та оборони, які ґрунтуються на Глобальній стратегії щодо безпеки і оборони Європейського Союзу [6], Глобальній стратегії щодо зовнішніх відносин та безпеки Європейського Союзу [7] Плані реалізації Глобальної стратегії у сфері безпеки і оборони [8]. Зазначеними документами не тільки наголошується на важливості співробітництва ЄС і НАТО, а й на протидії гібридним загрозам, оперативному співробітництві з питань кібербезпеки.

Правову основу для протидії кіберпосяганням у Європейському Союзі безпосередньо визначає Будапештська Конвенція Ради Європи з кіберзлочинності (далі – Конвенція), прийнята ще у 2001 році [9], учасниками якої є не тільки країни Європи, а й інші (США, Аргентина, Австралія, Чилі, Японія та інші).

З метою розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання електронних доказів, які стосуються кримінальних правопорушень, Конвенція передбачає загальні принципи міжнародного співробітництва, зокрема цілодобову інформаційну мережу національних контактних пунктів "24/7" для боротьби зі злочинами у сфері комп'ютерних технологій [9, ст.ст. 23, 35]. Така мережа забезпечує надання оперативної міжнародної правової допомоги, а саме термінове збереження комп'ютерних даних, щодо яких є загроза їх втрати, знищення або модифікації; збирання і вилучення доказів в електронній формі у кримінальних справах про вчинення транснаціональних кіберзлочинів; отримання оперативної інформації щодо обставин вчинення транснаціональних кіберзлочинів; встановлення місцезнаходження осіб, підозрюваних у вчиненні транснаціональних кіберзлочинів; оперативний інформаційний обмін щодо збережених та отриманих даних між національними та іноземними правоохоронними органами.

Остання зустріч національних представників мережі контактних пунктів "24/7" у межах спільної програми Ради Європи і ЄС Глобальної протидії кіберзлочинності (Global Action on Cybercrime Extended, GLACY+) [10] відбулася 8 жовтня 2019 р. і стосувалася практичних аспектів взаємодії правоохоронних органів держав-підписантів Конвенції [11].

ЄС продовжує розбудовувати інституційну платформу для обговорення актуальних питань кібербезпеки, боротьби з кіберзлочинністю тощо. Зокрема, на напрацювання єдиної міжнародної політики у сфері протидії кіберзлочинності у контексті перетворення Конвенції на єдиний міжнародний механізм спрямовується робота Програмного офісу з протидії кіберзлочинності Ради Європи – Cybercrime Programme Office (C-PROC) [12]. Одним з важливих питань, на яке спрямовуються зусилля фахівців C-PROC, є підвищення ефективності процедур правової допомоги при здійсненні заходів з протидії кіберзлочинності та кібертероризму. Комітетом Конвенції ще у червні 2017 року прийнято рішення щодо доцільності укладання додаткового протоколу до Конвенції з метою закріплення правових та організаційних передумов для створення спільних слідчих робочих груп з розслідування кіберзлочинів, міждержавної взаємодії із провайдерами Інтернет-послуг тощо.

Задля створення організаційних передумов для проведення спільних розслідувань кіберзлочинів у 2013 році в ЄС у складі Європолу створено Європейський центр по боротьбі з кіберзлочинністю (European Cybercrime Centre (EC3) [13]. Основними завданнями EC3 передбачено: забезпечення обміну інформацією між підрозділами правоохоронних органів ЄС та третіми країнами; боротьба з розповсюдженням у мережі Інтернет дитячої порнографії; підготовка кваліфікованих кадрів у сфері боротьби з кіберзлочинністю; розробка методики виявлення і припинення злочинів у сфері інформаційних технологій тощо. Своєрідною "підслідністю" EC3 є кіберзлочини, які: скоєні міжнародними злочинними угрупованнями з метою отримання значних прибутків, або у результаті діяльності яких було задано значної шкоди; завдають значної шкоди потерпілим, зокрема, кібернасильство, сексуальна експлуатація дітей он-лайн, розповсюдження порнографії тощо; завдають шкоди критичній інфраструктурі країн-членів ЄС.

Вітчизняні дослідники інформаційно-правової науки, розкриваючи питання врахування європейського досвіду щодо питань боротьби з правопорушеннями в інформаційній сфері, обґрунтовують необхідність забезпечення доступу правоохоронних органів України їх до баз даних та аналітичних матеріалів Центру EC3 [5, с. 17]. Така позиція потребує підтримки з урахуванням того, що лише оперативний облік інформації є запорукою ефективності протидії кіберзлочинності. Відзначимо, що бажано забезпечувати доступ до зазначених ресурсів не лише Національної поліції України, а й інших правоохоронних органів, зокрема СБ України і Державного бюро розслідувань України.

Перейдемо до розгляду організаційних і правових основ для вирішення проблем протидії кіберпосяганням у окремих державах-членах ЄС. Розпочнемо з Федеративної Республіки Німеччини.

Оновлена Стратегія кібербезпеки ФРН від 9 листопада 2016 року удосконалює Стратегію кібербезпеки від 2011 року і передбачає понад 30 стратегічних цілей та заходів, зокрема спрямована на просвітницьку діяльність щодо роз'яснення важливості кібербезпеки для користувачів, розширення співпраці між державою та бізнесом, а також розширення мережі "команд швидкого реагування" на кіберзагрози [14].

У ФРН створено Національний центр кіберзахисту, який забезпечує ефективну співпрацю між усіма державними установами для координації захисних та контрзаходів щодо кіберінцидентів [15]. Зазначена платформа для співпраці об'єднує представників Федерального управління кримінальної поліції, Федерального управління з питань захисту Конституції, Федеральної служби розвідки, Федеральних Збройних Сил, Федерального управління з питань цивільного захисту та ліквідації наслідків

надзвичайних подій, Управління митної кримінальної поліції та контролюючий орган щодо операторів та критичних інформаційних інфраструктур – Федеральне відомство з питань інформаційної безпеки (далі – BSI).

Вітчизняні дослідники міжнародного права зазначають, що швидкий і вузьковідомчий обмін інформацією про вразливі місця ІТ-продуктів, форми нападу і злочинців надає можливість Національному центру кіберзахисту ФРН аналізувати кібератаки і давати узгоджені рекомендації щодо протидії [16].

У цьому контексті відзначимо, що в Україні продовжується робота щодо врахування провідного європейського досвіду у питаннях протидії кіберзагрозам. Зокрема, по аналогії з Національним центром кіберзахисту ФРН підвищено роль Національного координаційного центру кібербезпеки України (далі – НКЦК) відповідним Указом Президента України від 28 січня 2020 року [17]. На нашу думку, такі додаткові повноваження НКЦК, як здійснення координації та контролю за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, здійснення аналізу стану кіберзахисту критично важливих об'єктів інфраструктури, стану готовності суб'єктів забезпечення кібербезпеки до виконання завдань з питань протидії кіберзагрозам, здійснення превентивних заходів у боротьбі з кіберзлочинністю; розроблення концептуальних засад і пропозицій щодо створення та функціонування відповідно до уніфікованих технічних вимог центрів обробки даних та центрів забезпечення кібербезпеки державних органів, а також об'єктів критичної інформаційної інфраструктури, упровадження вітчизняних програмних та програмно-апаратних засобів для здійснення уповноваженими суб'єктами заходів із кіберрозвідки, кібероборони, контррозвідувального захисту кібербезпеки держави, розслідування кіберзлочинів тощо стануть важливою передумовою централізації державної політики у сфері кібербезпеки.

Метою BSI є сприяння безпеці інформаційних технологій в Німеччині. BSI насамперед забезпечує кібербезпеку федерального уряду Німеччини, однак також пропонує свої послуги приватним та комерційним користувачам та постачальникам інформаційних технологій і запроваджує дієві технології приватно-публічного партнерства [18].

Заслуговує на увагу також досвід Польщі у протидії кіберпосяганням, який свідчить про важливість стратегії, нормативних актів, впровадження їх в життя, ведення підготовки фахівців у сфері кібербезпеки, а також контролю окремих установ, підприємств і громадян, міжнародної співпраці, а також безперервного розвитку в цій сфері [19].

Польща бере активну участь у реалізації політики ООН, НАТО та ЄС, а також на оперативному рівні співпрацює з Чехією, Словаччиною, Угорщиною та Австрією у межах Центральноєвропейської платформи кібербезпеки [20].

Досвід Польщі цікавий тим, що у цій країні створено Урядовий центр безпеки (далі – RCB) задля створення ефективної та всебічної системи антикризового управління [21]. RCB – це надвідомча структура, спрямована на оптимізацію та стандартизацію сприйняття загроз окремими урядовими відомствами з метою підвищення їх здатності вирішувати складні ситуації.

Відповідно до Закону Польщі від 2007 року про управління кризовими ситуаціями, до критичної інфраструктури віднесено: системи постачання енергії, палива та енергії, системи зв'язку, телекомунікаційні мережі, фінансові системи, системи харчування, водопостачання, охорони здоров'я, транспортні системи, системи порятунку, системи, що забезпечують безперервність діяльності державного управління, системи виробництва, зберігання та використання хімічних і радіоактивних речовин, включаючи

трубопроводи для небезпечних речовин. Важливо для врахування у розбудові правової основи для захисту критичної інфраструктури в Україні враховувати, що під критичною інфраструктурою у Польщі розуміють як фізичну, так і кібернетичну системи (включаючи об'єкти, споруди чи установки), необхідні для мінімальної роботи економіки та держави [22].

Цікавим для врахування Україною є приклад функціонування Національного науково-дослідного інституту Польщі (далі – NASK), яким керує Міністерство цифрових справ Польщі і основна функція якого – це забезпечення безпеки Інтернету. NASK – це польський національний реєстратор імен Інтернету в домені.pl; NASK керує центром стратегічного аналізу щодо кібербезпеки; команда швидкого реагування CERT Polska також діє в структурі NASK; у цій установі створена платформа для державно-приватного партнерства.

Крім того, NASK здійснює науково-дослідну діяльність у галузі безпеки, надійності та ефективності мереж ІКТ, зокрема CyberSecIdent, Cyberpark ENIGMA – проекти, присвячені питанням кібербезпеки, які запроваджені в цій установі. Академія NASK проводить унікальні тренінги для компаній та установ з акцентом на безпеку ІКТ, а також модерує програму ЄС Безпечний Інтернет, сприяючи безпечному використанню нових технологій та Інтернету серед дітей та молоді [23]. Як бачимо, зазначена установа є не тільки адміністративним органом щодо регулювання доменних імен, реагування на кіберінциденти тощо, а й платформою для широкомасштабних наукових та освітніх проектів. Такий досвід є актуальним для нашої держави, оскільки передбачає поєднання наукових підходів, освітніх програм і практичної реалізації заходів протидії кіберпосяганням.

У Австрії система протидії кіберпосяганням грунтується на двох основних документах: Програмі захисту критичної інфраструктури (далі – APCIP) та Національній стратегії кіберзахисту.

Австрія має ефективну інфраструктуру і високий рівень безпеки постачання продовольства, транспорту, телекомунікацій, енергетичних та фінансових послуг, соціальних та медичних послуг. APCIP постійно доповнюється з метою забезпечення високої якості послуг і безпеки їх надання. Крім того, у Австрії Федеральною канцелярією започаткована "Платформа кібербезпеки" як основа для державно-приватного партнерства у сфері кібербезпеки та захисту критичної інфраструктури [24].

Національна стратегія з питань кібербезпеки передбачає, що забезпечення кібербезпеки в національному та міжнародному кіберпросторі є одним із головних пріоритетів Австрії та спільним викликом для держави, бізнесу та суспільства. З метою забезпечення регулярного обміну інформацією між зацікавленими сторонами в Австрії налагоджено постійний моніторинг та оцінка ситуації в кіберпросторі та запис відповідної інформації. Для забезпечення високої стійкості критичної інфраструктури проти кібератак створена Державна комп'ютерна команда реагування на надзвичайні ситуації, що управляється Федеральною канцелярією (GovCERT), а також, що є цікавим для України досвідом, CERT.at – національний CERT для приватного сектору Австрії.

Особливістю цієї установи є те, що вона координує реагування на кіберінциденти для недержавних підприємств та організацій, розглядаючи будь-яку інформацію, передану як конфіденційну інформацію, і не передаючи її без згоди, якщо тільки це явно не потрібно для оперативного реагування на інцидент (Національний CERT для приватного сектору Австрії – https://cert.at/de/ueber-uns/zustaendigkeit). Такий приклад вартий уваги для наслідування в Україні, оскільки вирішує питання недовіри приватних суб'єктів до державних установ та знижує їх репутаційні ризики.

Висновки.

Підсумовуючи викладене, зазначимо, що на основі аналізу організаційних та правових підходів ЄС до політики безпеки у сфері кіберпростору відзначено низку актуальних для України прикладів. Зокрема, відзначено активність Програмного офісу з протидії кіберзлочинності Ради Європи – Cybercrime Programme Office (C-PROC), який робить спробу закріпити правові та організаційні передумови для створення спільних слідчих робочих груп з розслідування кіберзлочинів, міждержавної взаємодії із провайдерами Інтернет-послуг тощо. Підтверджено наукову позицію щодо необхідності забезпечення доступу до ресурсів ЕС3 широкого кола вітчизняних правоохоронних органів, зокрема СБ України і Державного бюро розслідувань України.

Аналіз організаційних і правових основ для вирішення проблем протидії кіберпосяганням у окремих державах-членах ЄС дав підстави для формулювання наступних висновків. Подібно до Національного центру кіберзахисту ФРН в Україні на початку 2020 року підвищено роль та повноваження НКЦК, що є важливою передумовою централізації державної політики у сфері кібербезпеки.

Актуальним для України є досвід Польщі у частині створення RCB – надвідомчої структури, спрямованої на оптимізацію та стандартизацію сприйняття загроз урядовими відомствами з метою підвищення їх здатності вирішувати складні ситуації, зокрема і у сфері захисту критичної інфраструктури, куди включено і кібернетичну систему.

Особливої уваги заслуговує приклад функціонування NASK Польщі, на базі якого поєднано наукові дослідження, освітні програми і практичну реалізації заходів протидії кіберпосяганням.

Досвід Австрії заслуговує на врахування в Україні у частині державно-приватного партнерства у сфері кібербезпеки та захисту критичної інфраструктури, а саме існування національного CERTу Австрії для приватного сектору, що дає можливість вирішити питання недовіри приватних суб'єктів до державних установ та знижує їх репутаційні ризики.

Перспективами подальших досліджень визначаємо питання дослідження досвіду країн Азії у протидії кіберпосяганням.

Використана література

1. Лук'янчук Р.В. Міжнародне співробітництво у сфері забезпечення кібернетичної безпеки: державні пріоритети. *Вісн. Нац. акад. держ. упр. при Президентові України*. 2015. № 4. С. 50-56.

2. Міжнародні стандарти з кібербезпеки та їх застосування в Україні: мат-ли "круглого столу", м. Харків, 19 квіт. 2016 р. / ред.: А.П. Гетьман, Б.М. Головкін. – (Нац. юрид. ун-т ім. Ярослава Мудрого). Харків: Право, 2016. 87 с.

3. Кримінальні загрози в секторі безпеки: практики ефективного реагування: мат-ли панельної дискусії III Харків. міжнар. юридичного форуму, м. Харків, 26 вересня 2019 р. – (Нац. юрид. ун-т ім. Ярослава Мудрого). Харків: Право, 2019. 172 с.

4. Міжнародна інформаційна безпека: теорія і практика: підруч. для студентів ВНЗ, які навчаються за напрямом підгот. "Міжнародні відносини" та "Міжнародна інформація" / Є.А.Макаренко, М.М. Рижков, М.А. Ожеван, О.П. Кучмій, О.М. Фролова. – (Нац. ун-т ім. Тараса Шевченка, Ін-т міжнар. відносин). Київ: Центр вільної преси, 2016. 417 с.

5. Марущак А.І. Європейський досвід з питань боротьби з правопорушеннями в інформаційній сфері. *Безпека інформації*. 2019. Т. 25. № 1. С. 13-17.

6. Council conclusions on implementing the EU global strategy in the area of security and defence. URL: https://www.consilium.europa.eu/en/press/press-releases/2016/11/14/conclusions-eu-global-strategy-security-defence

7. EU global strategy on foreign and security policy. URL: http://www.eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

8. Implementation Plan on Security and Defence. URL: https://www.consilium.europa.eu/media/22460/eugs-implementation-plan-st14392en16.pdf

9. Про кіберзлочинність: Конвенція Ради Європи від 21 листопада 2001 р. URL: http://www.zakon4 .rada.gov.ua/laws/show/994_575

10. Global Action on Cybercrime Extended. URL: https://www.coe.int/en/web/cybercrime/glacyplus

11. GLACY+ Third Annual Meeting of the 24/7 Network of Contact Points. URL: https://www.coe.int/en/web/cybercrime/glacyplusactivities

12. Cybercrime Programme Office. URL: https://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc-

13. European Cybercrime Centre. URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

14. Cyber-Sicherheitsstragie für Deutschland 2016. URL: http://www.bmi.bund.de/cybersicherheitsstrategie.

15. Nationales CyberAbwehrzentrum. URL: https://www.bka.de/DE/UnsereAufgaben/Kooperationen/NCAZ/ncaz_node.html

16. Добржанська О.Л. Демцов А.А. Кібербезпека як феномен міжнародних відносин на прикладі Федеративної Республіки Німеччини. *Актуальні проблеми міжнародних відносин*. 2011. Вип. 102(1). С. 111-116.

17. Про внесення змін до Указів Президента України від 27 січня 2015 року № 37 та від 7 червня 2016 року № 242: Указ Президента України № 27/2020. URL: https://www.president.gov.ua/documents/272020-32041

18. Das Bundesamt für Sicherheit in der Informationstechnik. URL: https://www.bsi.bund.de

19. Сайт ENISA – (Агентство ЄС з кібербезпеки). URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies

20. Урядовий центр безпеки Польщі. URL: https://www.rcb.gov.pl/en/about-us

21. Critical infrastructure. URL: https://www. rcb.gov.pl/en/critical-infrastructure

22. Національний науково-дослідний інститут Польщі. URL: https://www.eng.nask.pl

23. Програма захисту критичної інфраструктури Австрії (APCIP). URL: https://www.bundeskanzleramt.gv.at/themen/sicherheitspolitik/schutz-kritischer-infrastrukturen.html

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~