МІЖНАРОДНЕ ПРАВО

УДК 341.456:341.174(4ЄС):(343.3/7+004.056)
DOI https://doi.org/10.32782/pyuv.v1.2025.30

Р. М. Бірюков
orcid.org/0009-0001-9550-6383
кандидат юридичних наук,
докторант кафедри міжнародного та європейського права
Національного університету «Одеська юридична академія»

ФОРМУВАННЯ ТА ПОВНОВАЖЕННЯ ЄВРОПЕЙСЬКОГО ЦЕНТРУ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

Постановка проблеми. Сучасний період характеризується бурхливим розвитком технологій глобальних електронних мереж. Практично всі сфери людської діяльності можуть здійснюватися через або з залученням таких електронних мереж. Не є виключенням і злочинна діяльність, що може погрожувати кібербезпеці цілих держав та суспільств. Відповідно, виникає проблема боротьби з кіберзлочинністю, яка, з урахуванням глобальної природи Інтернету, може бути ефективною лише через взаємодію держав. Ці тенденції вплинули на розвиток міжнародного поліцейського співробітництва в ЄС, яке здійснюється через Європол. Відповіддю на кіберзагрози стало створення нових структур під егідою Європолу.

Метою дослідження є дослідження особливостей формування, повноважень та діяльності Європейського центру боротьби з кіберзлочинністю як органу Європолу, спрямованого на подолання загроз злочинності, що походять із кіберсфери.

Стан опрацювання проблематики формування та розвитку спроможностей Європолу в боротьбі з кіберзлочинністю складно назвати задовільним. В сучасній літературі відсутні дослідження вказаної проблематики. В зарубіжній літературі є ряд окремих несистемних розвідок, наприклад, Л. Буоно, Дж. Сантос Вари, Дж. Колемана,. Водночас, комплексні дослідження вказаної проблематики відсутнє, що робить вказану проблематику актуальною.

Виклад основного матеріалу. В 2000-х роках все більш очевидними ставали загрози для безпеки європейських держав, що походили з кіберпростору. Кібератаки на Естонію в 2007 році та Грузію в 2008 році, поряд з рядом менших інцидентів, продемонстрували вразливість електронних систем для дій зловмисників. В цей період держави-учасниці ЄС вперше включили кібербезпеку та оборону у власні стратегії національної безпеки. Це створило сприятливий політичний момент для реалізації пропозиції зі створення Європейської платформи по боротьбі з кіберзлочинністю (European Cyber Crime Platform) в рамках Європолу. Завданням нового органу стала підтримка національних органів влади в боротьбі з кіберзлочинністю з боку організованих груп [1]. Це дозволило фахівцям Європолу добиватися належного розподілу ресурсів та відігравати проактивну роль в координації інформаційного обміну та операційного співробітництва.

Європейські Рада та Комісія, зі свого боку, створювала необхідний режим правового регулювання. Так, Директивою Ради ЄС № 2008/114 від 8 грудня 2008 року [2] було визначено критичну інфраструктуру ЄС, а держави-учасниці зобов'язувалися здійснити подальші зусилля для захисту таких інфраструктур, в тому числі, в кіберсфері. На підставі цього, Європейська Комісія на початку 2009 року запропонувала стратегію і план дій [3]. Зокрема, Комісія запропонувала створення комп'ютерних груп швидкого реагування (Computer Emergency Response Teams, CERTs) в державах учасницях та виступила з ініціативою дій на рівні ЄС, щодо посилення боротьби з кіберзлочинністю. В світлі кібератак в Естонії та Грузії, ця ініціатива була прихильно зустрінута державами-учасницями, що створило основу для формування мережі швидкого реагування із залученням приватного сектору та громадянського суспільства.

Актори ЄС скористалися цим політичним моментом для формалізації інтеграційних преференцій держав-учасниць. Близько 2010 року наднаціональне політичне підприємництво дозволило налагодити більш тісну співпрацю. Рішення Ради щодо Європолу дозволило останньому просувати свої послуги в сфері кібербезпеки завдяки його положенню як європейського правозастосовного органу, зокрема в просуванні вертикальної інтеграції. Зокрема, Європол постійно підкреслював потребу гармонізації законодавств всередині ЄС стосовно кіберспроможностей.

При цьому, Європол був не єдиним, хто наполягав на посиленні уваги ЄС до кіберзлочинності та кібербезпеки. Важливу роль відігравала також Комісія, яка просувала співробітництво на рівні ЄС як основний спосіб поліцейського співробітництва. Так, після кібератак в Естонії в 2007 році Комісія запропонувала розробку єдиної політики по боротьбі з кіберзлочинністю [4]. Хоча цим документом відзначалися правові обмеження в повноваженнях ЄС в міжурядовій політиці в цій сфері, в ньому наводився ряд можливих заходів на рівні ЄС, що могли реалізовуватися поряд з заходами Комісії. В документі Комісія заявила про свою позицію про необхідність створення центральної контактної точки ЄС з кібербезпеки.

К 2010 року сформувалися сприятливі передумови для створення Європейського центру боротьби з кіберзлочинністю (ЕСЗ), зокрема в діяльності Комісії, що змогла вплинути на преференції держав-учасниць [5, с. 334]. Ці передумови виникли, зокрема, через ряд кібератак, що відбулися напочатку 2011 року, продемонструвавши вразливість кіберінфраструктури ряду країн [6]. Європейська Комісія вказала державам-учасницям, що «загроза більш, ніж реальна. Кількість кібератак в світі зростає, так само, як і наслідки кіберзлочинності» [7]. Комісія тісно співпрацювала з Європолом в поширенні інформації щодо цієї проблематики, зокрема звертаючи урядів держав-учасниць ЄС на те, що в мережі Інтернет стрімко поширюються нові види злочинності. Підкреслюючи економічні та фінансові втрати, пов'язані з кіберзлочинністю, наднаціональні політичні підприємці привертали увагу держав-учасниць до фізичних результатів, що спричиняються кіберзлочинністю та взаємозв'язку між кіберпростором та реальним світом, що зрештою спонукало європейські уряди до здійснення колективних дій.

Слід згадати, що вже напочатку 2004 року Європол повідомляв про диверсифікацію кримінальної злочинності в Інтернеті [8]. За декілька років до масштабних кібератак, Європол підкреслював значення Інтернету та кібертехнологій як засобів, що полегшують організовану злочинність. Події, подібні до нападів на Естонію та Грузію привернули додаткову увагу до вказаної проблематики та створили функціональний тиск до співробітництва.

У висновках Ради, що були випущені в листопаді 2008 року, містилися пропозиції щодо політики в сфері боротьби з кіберзлочинністю. Вони призвели до схвалення єдиної стратегії держав-учасниць та визначили спільні пріоритети [9]. Це, в свою чергу, призвело до ухвалення Європейської стратегії кібербезпеки в лютому 2010 року [10]. Вона визначала кіберзлочинність як основний ризик, пов'язаний зі злочинністю, з яким стикається Європа, відображаючи той дискурс, який вже протягом кількох років відбувався на рівні Європолу та Комісії. Кібер-безпека цілеспрямовано визначалася як спільний виклик для європейського поліцейського співробітництва, впоратись з яким могли тільки спільні зусилля держав-учасниць. Кіберзлочинність визначалася як така, що «створює транскордонну анонімну загрозу нашим інформаційним системам та кидає виклики правоохоронним органам». В цьому контексті, Європейська Комісія підкреслила практичний досвід Європолу та його позитивну репутацію в просуванні проінтеграційного дискурсу та посиленні європейського поліцейського співробітництва.

Таким чином, Європол сам по собі став агенцією, що підвищувала помітність кіберзагроз в Європі та формувала парадигми поліцейського співробітництва в боротьбі з кіберзлочинністю. Це видно, наприклад, з Плану дій з імплементації стратегії по боротьбі з кіберзлочинністю, що був ухвалений в квітні 2010 року [11]. Відповідно до цього плану, Рада ЄС звернулася до Європолу з запитом про проведення стратегічного аналізу кіберзлочинності, та запросила Європол та Комісію підтримувати держави-учасниці в консолідації, та в разі потреби, в перегляди та покращенні функцій, переданих Європейському центру по боротьбі з кіберзлочинністю.

Ухвалення Плану спонукало європейські уряди погодитися з ідеєю Комісії про створення центрального контактного пункту ЄС по боротьбі з кіберзлочинністю. Відповідно, в 2010 році Рада поставила перед Комісією задачу «провести дослідження практичної можливості створення центру та розглянути практичну мету, повноваження та можливе фінансування центру, що мав стати частиною Європолу» [11]. Таким чином, держави-учасниці не тільки визнали ключову роль Комісії та Європолу як ключових структур міжнародного поліцейського співробітництва в Європі за напрямком боротьби з кіберзлочинністю, але й легітимізували їх як самостійних акторів. Відповідно, План дій 2010 року можна розглядати як критичний момент в розробці наднаціонального мандату в боротьбі з кіберзлочинністю. Він став каталізатором створення Європейського центру по боротьбі з кіберзлочинністю, посиливши роль Європейської Комісії, Європолу та інших акторів в цій сфері.

В серпні 2010 року Європейська Комісія представила Цифровий порядок денний для Європи [12]. В цьому документі Комісія закликала держави-учасниці спільно боротися зі зростанням нових форм злочинності та «створити чи адаптувати національні інформаційні платформи до платформи Європолу з кіберзлочинності». Циф-

ровий порядок денний не тільки визнав Платформу в якості центрального інструменту, але й запропонував створення Європейського центру боротьби з кіберзлочинністю. Також Комісія прямо пов'язала ідею центру з імплементацією Стратегії інформаційної безпеки ЄС. В якості ключового пункту Порядку денного зазначалося, що «до 2013 року ЄС створить всередині існуючих структур центр боротьби з кіберзлочинністю, який має стати точкою зосередження зусиль Європи в боротьбі з кіберзлочинністю».

Ця формальна заява відображає зростаючу роль Європейської Комісії з двох причин. По-перше, вона суттєво перевищує очікування, що були викладені державами-учасницями в Плані дій від квітня 2010 року. Хоча останнім Комісія лише запрошувалася до проведення дослідження та оцінки, Порядок дій відображала зовсім інший підхід, який полягав у створенні Європейського центру боротьби з кіберзлочинністю як вирішеної справи, а не як можливої пропозиції. По-друге, Комісія взяла цю ініціативу на себе, замість того, аби виступати простим агентом, що мав розробити пропозиції, що проявилося в рішучому формулюванні «ЄС створить» та пов'язуванні центру з існуючими структурами.

Ще більш очевидним це стає при розгляді меморандуму [13], що супроводжував Порядок денний, відповідно до якого «Комісія створить Центр боротьби з кіберзлочинністю ЄС до 2013 року». Запропоновані Комісією дії вказували на її посилюване бачення себе як актора в сфері кібербезпеки. Зокрема, при просуванні ЄС як основної структури поліцейського співробітництва в боротьбі з загрозами з кіберпростору, Європейська Комісія все більше застосовувала стратегію навмисної політизації з метою посилення громадського тиску для визначення преференцій держав в бік застосування таких європейських інституцій як Європол.

Розгляд становлення Європейського центру боротьби з кіберзлочинністю показує посилення ролі Комісії та акторів ЄС в цілому в сфері кібербезпеки. Вже в 2010 році чиновники Комісії підкреслювали зростаючу взаємозалежність як ключову підставу для розвитку співробітництва. Саме в цей період ця стратегічна політизація змінилася кількісно та якісно. В той час коли попередній дискурс на рівні ЄС залишався порівняно слабко вираженим та підкреслював переважно загальну потребу в співробітництві на національному рівні з огляду на глобалізацію та діджиталізацію, після 2010 року він став більш конкретним. Загрози кібербезпеки розглядалися як такі, що породжують потребу в колективних діях та більш стійких міжурядових рішеннях.

Подібний підхід можна було спостерігати і в заявах Європолу. Наднаціональна політизація поліцейського співробітництва в питаннях кібербезпеки підживлювалася громадським тиском. Раціональні аргументи, що походили від функціональної потреби в інтеграції в цій області доповнювалися аргументами щодо зростаючого запиту з боку громадськості до ЄС проводити діяльність в кіберсфері та боротися з кіберзлочинністю. Комісія навмисно використовувала громадську думку в якості інструменту, аби підштовхнути ЄС до участі в цій боротьбі на рівні політики в галузі правосуддя та внутрішніх справ. Так, Комісія посилалася на опитування громадської думки та покладалася на отримані цифри (понад 60% в підтримку співробітництва на рівні ЄС) для посилення своїх звітів. В листопаді 2010 року Комісія заявила, що «чотири з п'яти європейців бажають більш активних дій на рівні ЄС в боротьбі з організованою злочинністю та тероризмом» [13]. В 2012 році Комісія зазначала, що понад 50% громадян ЄС висловлюють занепокоєння щодо кібербезпеки [14]. Чиновники як від Європейської Комісії, так і від Європолу постійно підкреслювали негативні наслідки для фізичних та юридичних осіб, що походять від кіберзлочинності з одного боку, та ізольованість стратегій боротьби з нею в окремих європейських держав з іншого. Відповідно, обидві організації наполягали на мережевій системі безпеки та інтегрованих підходах до боротьби зі злочинністю, що, в свою чергу, потребувало координації процесів на рівні ЄС. За словами самої Комісії, «ніколи не робилося спроби пов'язати ці політики в послідовну та всеохоплюючу стратегію. Зараз існує унікальна можливість запровадити більш стратегічний підхід та виявити і скористатися синергією між цими багатьма напрямками діяльності» [13]. В цьому контексті, Комісія відводила самій собі центральну роль в координації, гармонізації та інтеграції міжнародного поліцейського співробітництва в ЄС, про що зазначалося в її повідомленнях [13].

Останній повністю відповідав заявленим вимогам, зокрема щодо центрального положення в мережі та можливих видатків. З моменту розширення його мандату на боротьбу з кіберзлочинністю в 2002 році, його компетентність та залучення в даній сфері постійно зростали. До 2012 року Європол накопичив десятилітній досвід та розбудував мережу «клієнтів» та організаційну репутацію серед європейських поліцейських чиновників. Держави-учасниці визнавали його практичні досягнення та функціональну потребу в розбудові існуючих структур на основі досвіду міжнародного поліцейського співробітництва в Європі. Можна говорити, що Європол свідомо скористався функціональним та громадським тиском, а також практичною потребою у власних унікальних послугах для підвищення своєї легітимності.

На цьому тлі Європейська Комісія запропонувала створити Європейський центр боротьби з кіберзлочинністю як частину Європолу та координаційний центр боротьби з кіберзлочинністю в ЄС [15]. Політичний клімат вимагав від держав-учасниць ЄС демонструвати свою готовність до співробітництва на рівні ЄС та посилення спільних інституцій. Хоча найвищі чиновники погоджувалися у тому, що Європол залишався лише інструментом, що мав підтримувати держави-учасниці, він став надійним гравцем у своїй власній якості, і, поряд з Європейською Комісією, все частіше виступав консультантом в ухваленні рішень на внутрішньодержавному рівні [16, с. 454]. Ще до початку роботи Центру та до того, як він став центральним хабом у боротьбі з кіберзлочинністю, Європол виступав в якості політичного радника.

Напочатку червня 2012 року Рада прийняла пропозицію Комісії щодо початку роботи Центру в рамках Європолу. Прийнявши підхід створення координаційного центру та поклавши на Комісію та Європол задачу з розвитку цього напрямку, держави-учасниці фактично передали свої повноваження на наддержавний рівень, таким чином просуваючи вертикальну інтеграцію у міжнародному співробітництві ЄС в сфері кібербезпеки. Завдяки цьому, Центр вдалося зробити з неочікуваною швидкістю. Лише за місяць, 1 липня 2012 року, розпочала роботу підготовча група, що дозволило запустити роботу Центру в січні 2013 року [17].

Таким чином, держави-учасниці здійснили стратегічний вибір на користь міжнародного співробітництва та подальшої інтеграції в боротьбі з кіберзлочинністю. Якщо раніше вони явно віддавали перевагу міжурядовим форматам співробітництва та розглядали Європол лише як технічний орган та координаційну платформу, зростання взаємозалежностей та наднаціональне політичне підприємництво зсунули їхні преференції в бік інтеграції. Відсутність кордонів в кіберпросторі більше, ніж в будь-якій іншій сфері, створювала привабливі можливості для злочинців та терористів. Все більше форм злочинності зловживали можливостями, що існують онлайн чи мають в собі кібер-елементи. Виникали нові форми злочинності, що використовували Інтернет для полегшення взаємодії та співпраці між різними кримінальними та терористичними групами.

Не всі держави мали достатні внутрішні спроможності для ефективного співробітництва та захисту своєї власної кібербезпеки. Деякі з них не відрізнялися високою залежністю від електронних систем, або їм бракувало потрібних ресурсів. В свою чергу, це впливало на всі держави-учасниці. На заваді співробітництву на рівні ЄС ставали різні внутрішньодержавні підходи та розбіжності у спроможностях, внаслідок чого обмін інформацією щодо боротьби з кіберзлочинністю не завжди був доступним чи послідовним. Іншою проблемою була прогалина в знаннях та навичках між різними європейськими країнами. При цьому, асиметричні загрози з кіберпростору накладалися на асиметричні спроможності в сфері кібербезпеки держав-учасниць ЄС, в той час як високі взаємозалежності створювали функціональний тиск на держави-учасниці в бік колективних дій в даній сфері. Передача ЄС повноважень з координації дозволила урядам сфокусуватись на створенні власних національних систем і стратегій, які ґрунтувалися на спільній синергії.

В таких умовах Європол та Європейська Комісія виступили в якості механізмів правозастосування в рамках боротьби поліцій держав-учасниць ЄС з кіберзлочинністю. Формалізація їхнього мандату та утвердження їх як основних медіаторів підвищила надійність колективних дій в інформаційному обміні. Крім того, централізація мінімізувала видатки окремих країн та дозволила економію коштів на міждержавному рівні. Європол та Єврокомісія створили можливості для взаємодії національних органів влади в обміні досвідом та кращими практиками. Також вони були здатні до створення унікальних транскордонних продуктів та надання виключних послуг для держав-учасниць, які вони не могли напрацювати самі.

Слід відзначити, що Європол першим запропонував створити міждержавний аналітичний орган та просував ідею систематичного співробітництва у боротьбі з кіберзлочинами. Комісія, в свою чергу, виступила з ініціативою створення центрального європейського координаційного центру для боротьби з кіберзлочинністю та надала численні конкретні пропозиції щодо сконцентрованих дій в цій галузі. Таким чином, наднаціональне політичне підприємництво фундаментально змінило преференції держав в бік поглиблення міжнародного поліцейського співробітництва в ЄС та сприяло створенню Центру боротьби з кіберзлочинністю.

Висновки. Розвиток спроможностей Європолу в боротьбі з кіберзагрозами, зокрема створення Європейського центру боротьби з кіберзлочинністю було викликане кібернападами, що зазнав ряд європейських країн в другій половині 2000-х років. Під цим впливом, держави були змушені координувати свої позиції та створювати наднаціональні органи боротьби з кіберзлочинністю. Ці ініціативи активно просували органи ЄС, такі як Європейська Комісія. Результатом цієї діяльності стала систематизація боротьби та подальша інтеграція в боротьбі з кіберзлочинні-

стю через наднаціональну діяльність в рамках ЄС. Така діяльність повинна була стати міжнародною, оскільки, через транскордонний характер кіберзлочинності, боротьба з нею могла здійснюватися лише скоординованими міжнародними зусиллями.

Література

1. Quillй, M. Key note address: Current threats and future challenges posed by cybercrime. URL: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f25c6 (дата звернення: 03.10.2024).

2. Директива Ради 2008/114/ЄС від 8 грудня 2008 року про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту. URL: https://zakon.rada.gov.ua/laws/show/984_002-08#Text (дата звернення: 03.10.2024).

3. Communication from the Commission to the European Parliament, the Council and the Committee of the Regions – Towards a general policy on the fight against cyber crime {SEC(2007) 641} {SEC(2007) 642}. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52007DC0267 (дата звернення: 04.10.2024).

4. European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection – "Protecting Europe from large scale cyber-attacks and disruptions: Enhancing preparedness, security and resilience". URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52009DC0149 (дата звернення: 03.10.2024).

5. Buono L. Gearing up the Fight against Cybercrime in the European Union: A New Set of Rules and the Establishment of the European Cybercrime Centre (EC3). *New Journal of European Criminal Law*. 2012, No 3(3-4). P. 332–337.

6. Coleman G. Anonymous in Context: The Politics and Power behind the Mask. URL: https://www.cigionline.org/sites/default/files/no3_8.pdf (дата звернення: 04.10.2024).

7. Cecilia Malmstrцm Commissioner responsible for Home Affairs Stepping up the fight against cyber crime European Cyber Security Conference – Shared threats, shared solutions Brussels, 14 June 2011. URL: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_11_439 (дата звернення: 04.10.2024).

8. European Union Organised Crime Report, 2004. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/en_euorganisedcrimesitrep2004.pdf (дата звернення: 04.10.2024).

9. JHA Council Conclusions from 27-28 November 2008. URL: https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/104584.pdf (дата звернення: 04.10.2024).

10. New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. URL: https://ec.europa.eu/commission/presscorner/detail/ru/ip_20_2391 (дата звернення: 04.10.2024).

11. Council conclusions concerning an Action Plan to implement the concerted strategy to combat cybercrime, 2010. URL: https://www.enisa.europa.eu/media/news-items/council-cyber-crime (дата звернення: 04.10.2024).

12. A Digital Agenda for Europe: Communication from the Commission to the European Parliament and the Council, the European Economic and Social Committee and the Committee of the Regions, 2010. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245R(01)&from=EN (дата звернення: 04.10.2024).

13. The EU Internal Security Strategy in Action: Five steps towards a more secure Europe. MEMO/10/598, 2010. URL: https://ec.europa.eu/commission/presscorner/detail/fr/memo_10_598 (дата звернення: 04.10.2024).

14. Frequently asked questions: The European Cybercrime Center ECi, 2012. URL: https://ec.europa.eu/commission/presscorner/detail/en/memo_13_6 (дата звернення: 04.10.2024).

15. Communication from the Commission to the Council and the European Parliament. Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2012:140:FIN (дата звернення: 25.09.2024).

16. Santos Vara J. The EU's agencies: Ever more important for the governance of the Area of Freedom, Security and Justice. *The Routledge Handbook of Justice and Home Affairs*. A. Ripoll Servent, F. Trauner (eds.). Abingdon: Routledge, 2018. P. 445-457.

17. Europol. First Year Report – European Cybercrime Centre (EC3). URL: https://www.europol.europa.eu/sites/default/files/documents/ec3_first_year_report.pdf (дата звернення: 14.10.2024).

Анотація

Бірюков Р. М. **Формування та повноваження європейського центру боротьби з кіберзлочинністю.** – Стаття.

В статті розглядаються формування та повноваження Європейського центру боротьби з кіберзлочинністю. Досліджуються основоположні причини, що призвели до створення Центру, які полягають в посиленні кіберзагроз в 2000-х роках, які проявилися в систематизованих кібернападах на цифрову інфраструктуру окремих європейських держав. Виявляються події, що призвели до створення Європейської платформи по боротьбі з кіберзлочинністю в рамках Європолу та завдання цього органу. Виявляються напрямки діяльності Європейської Ради та Європейської комісії та характер врегулювання ними міжнародних зусиль по боротьбі з кіберзлочинністю. Окреслюється характер формалізації інтеграційних процесів в Європі, спрямованих на створення системи міжнародного співробітництва у боротьбі з кіберзлочинністю.

Розглядаються преференції держав-учасниць ЄС, сформовані кіберзагрозами, та їхній вплив на формування Європейського центру боротьби з кіберзлочинністю. Досліджуються механізми співпраці європейських держав у відповіді на кіберзагрози, а також вплив діяльності Європолу на таку співпрацю. Простежується формування Європейської стратегії кібербезпеки та Європейського цифрового порядку денного та їхні характеристики. Розглядається вплив кіберзлочинності на посилення ролі наднаціональних органів ЄС в боротьбі з нею, в тому числі шляхом створення Європейського центру боротьби з кіберзлочинністю.

Наголошується, що створення Європейського центру боротьби з кіберзлочинністю відображало зростаючу взаємозалежність між державами в цій сфері та

посилення ролі органів ЄС, а також політизацію міжнародного поліцейського співробітництва в боротьбі з кіберзлочинністю як значущої сфери міжнародної співпраці. Окреслюються прийняті ними інтернаціоналізовані підходи до боротьби з кіберзлочинністю. Виявляються напрямки посилення повноважень та спроможностей Європолу в управлінні міжнародним співробітництвом в боротьбі з кіберзлочинністю. Робиться висновок, що створення Європейського центру боротьби з кіберзлочинністю як частини Європолу та координаційного центру стало ефективною відповіддю на загрозу кіберзлочинності.

Ключові слова: міжнародне поліцейське співробітництво, Європейський центр боротьби з кіберзлочинністю, Європол, кіберзагрози, кіберзлочинність.

Summary

Biriukov R. M. **The formation and powers of the European Cybercrime Center.** – Article.

The article examines the formation and powers of the European Cybercrime Center. The fundamental reasons that led to the creation of the Center are investigated, which are the intensification of cyber threats in the 2000s, which manifested themselves in systematic cyber attacks on the digital infrastructure of individual European states. The events that led to the creation of the European Cybercrime Platform within Europol and the tasks of this body are identified. The areas of activity of the European Council and the European Commission and the nature of their regulation of international efforts to combat cybercrime are identified. The nature of the formalization of integration processes in Europe aimed at creating a system of international cooperation in combating cybercrime is outlined.

The preferences of the EU member states, shaped by cyber threats, and their influence on the formation of the European Cybercrime Center are considered. The mechanisms of cooperation of European states in responding to cyber threats are studied, as well as the impact of Europol's activities on such cooperation. The formation of the European Cybersecurity Strategy and the European Digital Agenda and their characteristics are traced. The impact of cybercrime on the strengthening of the role of supranational EU bodies in combating it is considered, including through the creation of the European Cybercrime Center.

It is emphasized that the creation of the European Cybercrime Center reflected the growing interdependence between states in this area and the strengthening of the role of EU bodies, as well as the politicization of international police cooperation in combating cybercrime as a significant area of international cooperation. The internationalized approaches adopted by them to combating cybercrime are outlined. Directions for strengthening Europol's powers and capabilities in managing international cooperation in combating cybercrime are identified. It is concluded that the creation of the European Cybercrime Centre as part of Europol and a coordination centre has been an effective response to the threat of cybercrime.

Key words: international police cooperation, European cybercrime center, Europol, cybercrime, combatting cybercrime.