УДК 341.456:341.174(4ЄС):004.056
DOI https://doi.org/10.32782/apdp.v105.2025.1

М. Р. Аракелян, Р. М. Бірюков

СТАНОВЛЕННЯ ТА РОЗВИТОК СПРОМОЖНОСТЕЙ ЄВРОПОЛА В БОРОТЬБІ З КІБЕРЗАГРОЗАМИ

Постановка проблеми. Створення Європейського поліцейського управління (Європолу) збіглося у часі з вибухоподібним розвитком мережевих технологій обміну інформацією, з яких не могли не скористатися злочинні структури. Виникає цілий новий вид злочинності – кіберзлочинність. Особливістю цього виду злочинності є те, що вона, за визначенням, є транскордонною і такою, що зачіпає громадян в багатьох державах. Відповідно, реагування на таку злочинність повинне бути також транскордонним. Це призвело європейські держави до переконання, що деякі функції боротьби з кіберзлочинністю повинні бути передані Європолу, і з тих пір ці повноваження тільки розширювалися, намагаючись встигнути за розвитком мережевих технологій.

Метою дослідження є виявлення спроможностей Європолу в сфері боротьби з кіберзлочинністю, встановлення правових основ боротьби з таким видом злочинності, окреслення взаємовідносин Європолу з окремими державам та органами ЄС в питаннях боротьби з кіберзлочинністю.

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, Р. Оттіса, Г. Шпонгенберга, П. Шакінян. Водночас, комплексні дослідження вказаної проблематики відсутнє, що робить вказану проблематику актуальною.

Виклад основного матеріалу. В 2016 році був укладений Регламент про Європол [1]. Ухвалення регламенту означало подальшу передачу повноважень на рівень ЄС в декількох аспектах. Так, було змінено порядок голосування в правлінні Європолу з голосування двома третинам до голосування простою більшістю. Регламент також посилив позиції Європолу щодо держав, розширивши аналітичні повноваження та дозволивши йому надсилати запити державам-учасницям щодо початку кримінальних проваджень та операційного співробітництва. Крім того, Регламентом було запроваджено формальні мандати Спільної групи парламентського контролю та Європейської наглядової групи з захисту даних. Таким чином, ухвалення Регламенту знаменувало собою пік інтеграційної динаміки в поліцейському співробітництві ЄС.

Період після ухвалення рішення про Європол показує континуїтет окремих трендів та рушіїв поліцейської інтеграції, що тягнуться з початку 2000-х років. Зокрема, це стосується наростання взаємозалежностей, що продовжувалося проявлятися в 2010-х роках. Внутрішні та зовнішні взаємозалежності між європейськими поліцейськими органами поглиблювалися, зокрема в боротьбі зі спільними

загрозами, окремими видами злочинності та тероризмом. Завдяки новому статусу Європолу як агенції ЄС, організація отримала сильні позиції як актор в міжнародному поліцейському співробітництві в рамках ЄС. Вона продовжувала отримувати вигоду від процесів, що були запущені в 2000-х роках, зокрема при підписанні Лісабонського договору. Зросла і роль наднаціонального політичного підприємництва.

Рішення Ради про Європол формально підтвердило його статус як центрального хабу поліцейського співробітництва та обміну інформацією. Після трансформації організації в агенцію ЄС в 2010 році, Європол швидко перетворився на центр правозастосування, що концентрувався на аналізі злочинності та підтримці держав-учасниць. В його рамках було створено три центри, а саме Європейський центр боротьби з кіберзлочинністю (ЄЦК), Європейський контр-терористичний центр (ЄКЦ) та Європейський центр з боротьби з нелегальною міграцією (ЄЦБНМ). Всі вони представляли собою реакцію на зростання взаємозалежності в цих сферах, а також демонстрували вплив наднаціонального політичного підприємництва.

В цьому контексті основними рушіями рішень урядів стали глобалізація та діджиталізація. Однак, ступінь в якому вони впливали на інтеграцію в рамках Європолу відрізнявся в різних сферах. Так, функціональний тиск від зростаючої взаємозалежності був достатньо високим лише в сфері кібербезпеки, натомість рішення про створення ЄКЦ та ЄЦБНМ були викликані громадським тиском та політизацією. Створення цих операційних центрів та ухвалення Регламенту про Європол демонструють, що висока взаємозалежність може виступати достатньою передумовою для проінтеграційних преференцій, в той час як політизація посилює такі тиски, створюючи належні умови для утворення відповідних структурних підрозділів.

ЄКЦ розпочав свою роботу в січні 2013 року на виконання пріоритетів цілі 3 Стратегії внутрішньої безпеки ЄС, відповідно до якої «безпека ІТ-мереж є важливим фактором добре функціонуючого інформаційного суспільства...швидкий розвиток і застосування нових інформаційних технологій створив нові форми злочинної діяльності. Кіберзлочинність є глобальним феноменом, що наносить суттєву шкоду внутрішньому ринку ЄС. В той час як сама структура Інтернету не знає кордонів, юрисдикція для засудження кіберзлочинів зупиняється на національних кордонах. Держави-учасниці мають об'єднати свої зусилля на рівні ЄС. Центр по боротьбі з високотехнологічною злочинністю ЄС вже грає важливу координуючу роль в правозастосуванні, однак існує потреба в подальших діях» [2]. ЄЦК офіційно перетворив Європол на центральний хаб ЄС з боротьби з кіберзлочинністю та суттєво розширив його мандат, що покривав кіберзлочинність з боку організованих злочинних груп, торгівлю дитячою порнографією та інші посягання на дітей в комп'ютерних мережах та кібератаки [3]. Слід відзначити, що розвиток спроможностей Європолу в боротьбі з кіберзлочинністю розпочався задовго до початку роботи ЄЦК. Так, в 2002 році розпочав свою роботу Центр боротьби з високотехнологічною злочинністю (ЦБВЗ), хоча його штати залишалися досить скромними (4 службовця станом на 2010 рік) [4].

Зростаючі внутрішні та зовнішні взаємозалежності в кіберпросторі стали основними драйверами, що призвели до створення ЄЦК. Відповідне міжнародне

поліцейське співробітництво ставало все більш важливим в світлі глобалізації та діджиталізації. Ці феномени все більше пов'язували між собою реальний та віртуальний світ, трансформуючи характер соціальних взаємодій. Спостерігалося зростання взаємозв'язку між фізичними особами, фізичними комп'ютерними системами, технологіями та кіберпростором, що призводило до інтенсифікації та професіоналізації нових мере. Внаслідок цього, територіальні обмеження ставали все більш ілюзорними. Виникали нові форми злочинності в мережі, що користувалися з відсутності належного управління Інтернетом. Бізнес-модель злочинної діяльності повністю змінилася, перевівши в онлайн тероризм, торгівлю наркотиками, відмивання грошей та інші види злочинності.

Таким чином, зростаючі взаємозалежності мали суттєвий вплив на роботу поліції. Старі моделі, що покладалися на односторонню чи неформальну багатосторонню взаємодію не могли ефективно боротися з новими формами злочинності, яких не існувало двадцять років тому. Злочинці становили таку саму загрозу в кіберсфері, як і в фізичній реальності, причому складність їхніх злочинних операцій зростала. Транснаціональна організована злочинність отримувала шалені переваги від появи Інтернету та мобільних комунікаційних технологій. Якщо наприкінці 1990-х років злочинну діяльність проводили ієрархічні злочинні групи, що були прив'язані до території та покладалися на традиційні засоби зв'язку, то напочатку нового тисячоліття вони ставали все більш інтернаціоналізованими.

Інтернет постійно розширював обсяги злочинної діяльності онлайн. Для його злочинного використання потребувалися відносно дешеві та низькотехнологічні засоби, що дозволяло практично будь-якій особі бути залученою до такої злочинної діяльності в будь-який час. Недивно, що така злочинність ставала все більш помітною в повсякденній поліцейській діяльності. Управління новими загрозами безпеці ставало неможливим на національному рівні, що створювало функціональний тиск на держави-учасниці ЄС щодо розширення міжнародного поліцейського співробітництва, особливо в боротьбі зі злочинністю, ціллю якої стали самі по собі структури співробітництва в сфері безпеки та структури Союзу в цілому.

Посиленню поліцейського співробітництва в кіберсфері сприяли наростаючий функціональний тиск та політизація. Ряд подій, таких як кібератаки в Естонії [5] в 2007 році та Грузії [6] в 2008 році показали всю вразливість комп'ютерних мереж для злочинної діяльності. Вони підвищили рівень усвідомлення кіберзагроз поліцейськими чиновниками та створили можливості для взаємодії між ними. Це стосувалося не тільки боротьби з кібератаками, але й іншими проявами злочинності, наприклад, поширенням екстремістських матеріалів.

Терористична загроза в Європі демонструвала взаємозв'язок в сфері боротьби з тероризмом та організованою злочинністю в кіберпросторі [7, с. 148], зокрема те, що боротьба з тероризмом та організованою злочинністю була б неможливою без боротьби з кіберзлочинністю. Усвідомлення цього дозволило визначити цю сферу як пріоритетну для ЄС, що видно з декількох міжурядових інтеграційних ініціатив початку 2000-х років. Так, після терористичних нападів в Мадриді в 2004 році європейські голови держав та урядів погодилися на розробку стратегії та плану дій по боротьбі з радикалізацією та залученням до терористичних груп

[8]. Відповідна стратегія була розроблена роком пізніше та включала в себе заходи з боротьби з терористичною активністю в Інтернеті [9]. В ній особливо підкреслювалася важливість колективних дій на рівні ЄС та висвітлювалася роль Європейської Комісії в цьому контексті.

Так, через рік після нападів в Лондоні, Комісія за запитом Ради оголосила про свій намір дослідити можливості боротьби з контентом, що використовувався для радикалізації осіб та тероризму в Інтернеті [10]. На національному рівні держави-учасниці запустили проект з перевірки глобальних мереж в 2007 році. Передбачалося створення центрального інформаційного порталу та технічної платформи для збору та зберігання даних, пов'язаних з терористичною пропагандою та екстремістськими матеріалами онлайн [11].

Пропозицію щодо створення такого порталу подала Німеччина, і проект спочатку обговорювався поза межами ЄС [12]. Німеччина навмисно обрала варіант запуску платформи як невеликого пілотного проекту за участі лише кількох держав, оскільки можливості по боротьбі з кіберзлочинністю суттєво відрізнялися від держави до держави. Отже для авторів проекту простішим було застосувати гнучкий підхід за участі групи держав, ніж формальні канали ЄС. Запуск проекту, таким чином, виходив з тих самих передумов, що й EUCARIS, тобто його запуск визначався практичними потребами на внутрішньодержавному рівні, які вимагали швидкого просування проекту для досягнення операційних результатів.

Таким чином, асиметрія існуючих спроможностей та внурішньодержавне політичне підприємництво відіграли важливу роль у визначенні преференцій держав на користь диференціації проекту перевірки мережі. Успіх проекту дозволив його формальну передачу під егіду Європола, внаслідок чого він поширився на всі держави-учасниці ЄС, що відбулося в 2007 році. Ця передача не тільки розширила формальні повноваження Європолу на кіберпростір та сприяла горизонтальній інтеграції, розширивши проект на нові держави, вона також посилила вертикальну інтеграцію, надавши Європолу ключову роль в координації цієї діяльності.

Інтеграційні преференції держав-учасниць ЄС визначалися високим та постійно зростаючим рівнем взаємозалежності в кіберсфері. Так, на зборах Ради 22-23 травня 2007 року обговорювався запуск проекту та заходи для боротьби з використанням Інтернету в терористичних цілях. Держави-учасниці підкреслили, що «навряд чи можливо, аби одна держава-учасниця змогла покрити всі підозрілі активності, пов'язані з тероризмом в Інтернеті...В цій діяльності слід цілеспрямовано координувати діяльність різних акторів (держав-учасниць, Комісії, Європолу) [13].

Подальші події продемонстрували зростання функціонального тиску до співробітництва та вплинули на інтеграційні преференції держав. Йдеться про кібератаки в Естонії та Грузії в 2007 та 2008 роках відповідно. Так, 27 квітня 2007 року Естонія зазнала серії DDoS атак, що були спрямовані на критичну інфраструктуру. Нові напади відбулися 18 травня того ж року, причому їхніми цілями стали сайти державних установ, два великих банки та декілька політичних партій, а також сервер парламенту країни [14, с. 49]. Як і в більшості держав-учасниць ЄС, критична інфраструктура Естонії все більше покладалася на Інтернет та електронні форми

комунікації та обробки інформації. Відповідно, кібератаки вивели з ладу значну частину онлайн сервісів, в такий спосіб суттєво підірвавши повсякденні операції державних чиновників та простих громадян.

Ці безпрецедентні за масштабами атаки продемонстрували недоліки діджиталізації, адже хакери змогли скористатися кіберпростором для того, аби проникнути в систему управління внутрішньодержавною інфраструктурою цілої держави. Вони стали одним з перших помітних випадків кібертероризму, тобто використання комп'ютерних мереж для нападу на критичну інфраструктуру, зокрема енергетичну, транспорту та урядову, для того, аби примусити уряд та цивільне населення до певних дій. Щодо кібератак в Естонії С. Герцог зауважує, що вони розглядалися як знаряддя помсти з боку певних груп (в даному випадку – російської меншини в Естонії) шляхом загрози суверенному кіберпростору держав [14, с. 49]. Ці атаки на практиці продемонстрували потенціал злочинного та терористичного використання кіберпростору.

Ще одним прикладом стали кібератаки проти Грузії в серпня 2008 року. Так, починаючи з 20 липня 2008 року грузинські сервери були переповнені злочинним трафіком [15, с. 60]. Наступний, значно більш сильний раунд DDoS атак відбувся напочатку серпня 2008 року. Вони були спрямовані, переважно, проти вебсайтів грузинського уряду та засобів масової інформації, а також банків та громадських інституцій [16, с. 23]. Ці напади вивели з ладу значну частину серверів та підірвали діяльність та комунікації уряду, паралізували банківську систему на декілька днів, внаслідок чого країна була відрізана від інформації з зовнішнього світу. Однак, слід відзначити, що грузинський уряд протидіяв цим атакам, що дозволило коментаторам говорити про те, що російський напад на Грузію в серпні 2008 році створив перший прецедент кібервійни [16], оскільки ці кібернапади збіглися у часі з російською агресією проти Грузії і більшість злочинного трафіку надходила з росії [17, с. 24].

Ці кібератаки розглядалися як частина цілеспрямованої кібероперації як частини російської інформаційної війни проти Грузії в ширшому контексті російсько-грузинської війни. Як такі, вони стали першим прикладом гібридної війни, на якій були використані як звичайні методи ведення кібероперацій, так і методи кібернападу. Кібератаки 2008 року, без сумніву, мали сильний психологічний вплив на уряди по всьому світу, і особливо в Європі та США. Вони продемонстрували як взаємозалежність в кіберсфері може загрожувати безпеці цілих держав, і наскільки вразливим для нападів різних акторів, від окремих злочинних груп до держав, є Інтернет. Як пише С.П. Уайт, «кібератаки під час російсько-грузинської війни надають емпіричне підтвердження того, силу якого масштабу отримали недержавні актори в сучасному конфлікті» [16, с. 5].

Хоча ці напади не вдалося поставити в провину російському уряду, наявна інформація явно вказувала на залученість недержавних акторів, що були розташовані в російській федерації [18]. Йдеться про злочинні групи, професійних хакерів та звичайних громадян. Зокрема, інформація про кібератаки широко розповсюджувалася в соціальних мережах, а злочинне програмне забезпечення було доступне онлайн, що дозволяло приватним особам взяти участь у нападі [15, с. 62].

Крім того, слід враховувати, що хоча зловмисне програмне забезпечення було спрямоване проти Грузії, потенційною його жертвою могла стати будь-яка держава, чий кіберпростір був пов'язаний з грузинським.

Зокрема, недоліки в системах кібербепеки приватних компаній, що були пов'язані з Грузією, могли вплинути на кіберпростір держав, в яких розташовані ці компанії. Так, термінове перенесення урядових вебсайтів Грузії на хостінги, розташовані в США, що мало на меті уникнути DDoS атак, могло вплинути на самі Сполучені Штати [15, с. 64]. Таким чином, кібернапади на Грузію в 2008 році продемонстрували взаємозв'язок раніше не пов'язаних акторів по всій Земній кулі та загрозу, що може надходити до них з кіберпростору.

Кібератаки на Естонію та Грузію різко підвищили усвідомлення кіберпростору як питання, що потребує регулювання, та підкреслили необхідність міжнародного співробітництва в часи глобалізації та цифрової взаємопов'язаності. Ці події підвищили політичний тиск в середині ЄС та на міжнародному рівні щодо здійснення зусиль з попередження подібних нападів у майбутньому. Особливий вплив ці події мали на посадових осіб сфери безпеки, які могли оцінити потенційний згубний вплив кібератак, що створювали загрозу, порівняну з загрозою бомбового тероризму. Ці напади суттєво вплинули на преференції держав в бік глибшої інтеграції в боротьбі з кіберзлочинністю.

Висновки. Надання Європолу спроможностей з боротьби з кіберзлочинністю було необхідним кроком через бурхливий розвиток кіберзагроз європейській безпеці наприкінці 1990-х та в 2000-х роках. Особливу роль в цьому зіграли яскраві політизуючи події, такі як напади на кіберсистеми окремих держав, таких як Грузія та Естонія, які, очевидно, носили системний та організований характер і були спрямовані третьою державою. Перші успіхи Європолу в боротьбі з кіберзлочинністю, поряд із зростанням кіберзагроз, змусили держави передавати Європолу все більше повноважень в даній сфері.

Література

1. Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA. URL: https://eur-lex.europa.eu/eli/reg/2016/794/oj (дата звернення: 24.09.2024).

2. Communication from the Commission to the European Parliament and the Council. The EU Internal Security Strategy in Action: Five steps towards a more secure Europe. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52010DC0673 (дата звернення: 25.09.2024).

3. 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).

4. Protecting Europe against large-scale cyber-attacks report with evidence : 5th report of Session 2009-10. URL: https://catalogue.sipri.org/cgi-bin/koha/opac-detail.pl?biblionumber=74902 (дата звернення: 25.09.2024).

5. Ottis R. Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. URL: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformation WarfarePerspective.pdf (дата звернення: 25.09.2024).

6. Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace. URL: https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace (дата звернення: 25.09.2024.

7. Carrapiço, H., & Farrand, B. Cyber crime as a fragmented policy field in the context of area of freedom, security and justice. *Routledge Handbook of Justice and Home Affairs*. Servent A.R., Trauner F. (eds.). Abingdon: Routledge, 2018. P. 146–156.

8. Press Release: 'The European Union Strategy for Combating Radicalisation and Recruitment to Terrorism'—Justice and Home Affairs Council meeting, Brussels 1 December 2005. URL: https://ec.europa.eu/commission/presscorner/detail/en/PRES_05_296 (дата звернення: 27.09.2024).

9. The European Union Strategy for Combating Radicalisation and Recruitment to Terrorism, 2005. URL: https://data.consilium.europa.eu/doc/document/ST% 2014469% 202005% 20REV% 204/EN/pdf (дата звернення: 27.09.2024).

10. Council meeting of 22-23 May: Council Conclusions (8457/3/07) on cooperation to combat terrorist use of the Internet, 2007. URL: https://data.consilium.europa.eu/doc/document/ST% 208457% 20 2007% 20REV% 203/EN/pdf (дата звернення: 27.09.2024).

11. The EU Internet Referral Unit (IRU): Addressing terrorist content online. URL: https://voxpol.eu/the-eu-internet-referral-unit-iru-addressing-terrorist-content-online (дата звернення: 27.09.2024).

12. H. Spongenberg. EU to strengthen surveillance of terrorist websites. URL: https://euobserver.com/justice/24162 (дата звернення: 27.09.2024).

13. Council meeting of 22–23 May: Council Conclusions (8457/3/07) on cooperation to combat terrorist use of the Internet, 2007. URL: https://data.consilium.europa.eu/doc/document/ST% 208457% 202007% 20REV% 203/EN/pdf (дата звернення: 27.09.2024).

14. Herzog S. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security*. 2011. No. 4(2). P. 49–60.

15. Korns S.W., Kastenberg J.E. Georgia's cyber left hook. *Parameters*. 2009, No 38(4). P. 60–76.

16. White S.P. Understanding Cyberwarfare: Lessons from the Russia-Georgia War. Modern War Institute at West Point, 2018. URL: https://mwi.westpoint.edu/understanding-cyberwarfare-lessons-russia-georgia-war/ (дата звернення: 27.09.2024).

17. Shakarian P., Sharakian J. Ruef A. How Cyber Attacks Augmented Russian Military Operations. *Introduction to Cyber-Warfare: A Multidisciplinary Approach*. Waltham: Elsevier Inc., 2013. P. 23–32

18. Nazario J. Politically Motivated Denial of Service Attacks. URL: https://ccdcoe.org/uploads/2018/10/12_NAZARIO-Politically-Motivated-DDoS.pdf (дата звернення: 03.10.2024).

Анотація

Аракелян М. Р., Бірюков Р. М. **Становлення та розвиток спроможностей Європола в боротьбі з кіберзагрозами.** – Стаття.

В статті розглядається поява, становлення та розвиток спроможностей Європейського поліцейського управління в боротьбі з кіберзагрозами. Досліджуються події, що спонукали до включення повноважень боротьби з кіберзагрозами до Регламенту Європолу. Наголошується на тому, що кіберзагрози створювали взаємозалежності між європейськими державами, спонукаючи їх до активнішої передачі певних повноважень на користь Європолу. Наголошується на нових позиціях Європолу, що він отримав завдяки визнанню себе в якості актора ЄС, а також центрального хабу поліцейського співробітництва та обміну інформації з питань безпеки в Європі.

Рішучі кроки в боротьбі з кіберзлочинністю були зроблені із створенням Європейського центру боротьби з кіберзлочинністю, Європейського центру боротьби з тероризмом та Європейського центру боротьби з нелегальною міграцією. Ці органи повинні були реагувати на нові виклики, спричинені глобалізацією та діджиталізацією. Підкреслюються пріоритети ЄС в кіберсфері, що полягали в гарантуванні безпеки для інформаційного суспільства. В статті звертається увага на неможливість подолання нових загроз із застосуванням старих методів, що полягали в боротьбі з відповідними загрозами виключно всередині держав та неформальній двосторонній взаємодії. Нова епоха викликала до життя формалізоване співробітництво поліцейських структур, покликаних боротися з кіберзлочинністю.

В статті окремо розглядається порядок та особливості боротьби з небезпечним онлайн-контентом, наприклад, таким, що спонукав вчинення терористичних актів. Перевірки мереж всередині держав показала потребу також в наддержавному реагуванні, в результаті чого проект було передано на рівень Європолу. Підкреслюється, що ця діяльність дозволила виявляти авторів кібератак та їхній взаємозв'язок із злочинними структурами, а в деяких випадках – державами. Завдяки цьому з'являється можливість в боротьбі з кіберзагрозами, наприклад, шляхом перенесення серверів. Робиться висновок, що кібернапади змінили сприйняття кіберпростору державами, та змусили їх розглядати ймо-

вірні загрози, що походять з цього простору так само як ті – що походять з реального простору, а отже здійснювати заходи міжнародного поліцейського співробітництва для боротьби з цими загрозами.

Ключові слова: міжнародне поліцейське співробітництво, поліцейська інтеграція в Європі, Європол, кіберзагрози, кіберзлочинність.

Summary

Arakelian M. R., Biriukov R. M. **The development of the Europol capacities in combatting cyber threats.** – Article.

The article examines the emergence, formation and development of the capabilities of the European Police Office in combating cyber threats. The events that prompted the inclusion of the powers to combat cyber threats in the Europol Regulation are investigated. It is emphasized that cyber threats created interdependencies between European states, prompting them to more actively transfer certain powers in favor of Europol. It emphasizes the new positions of Europol, which it received due to the recognition of itself as an EU actor, as well as the central hub of police cooperation and information exchange on security issues in Europe.

Decisive steps in the fight against cybercrime were taken with the creation of the European Cybercrime Center, the European Counter-Terrorism Center and the European Center for Combating Illegal Migration. These bodies had to respond to new challenges caused by globalization and digitalization. The EU's priorities in cyberspace are emphasized, which were to ensure security for the information society. The article draws attention to the impossibility of overcoming new threats using old methods, which consisted in combating the corresponding threats exclusively within states and informal bilateral interaction. The new era gave rise to formalized cooperation between police structures designed to combat cybercrime.

The article separately examines the procedure and features of combating dangerous online content, for example, such as that which incited terrorist acts. Checks of networks within states also showed the need for a supranational response, as a result of which the project was transferred to the Europol level. It is emphasized that this activity made it possible to identify the authors of cyberattacks and their relationship with criminal structures, and in some cases, states. Thanks to this, an opportunity arises in combating cyber threats, for example, by transferring servers. It is concluded that cyberattacks have changed the perception of cyberspace by states, forcing them to consider potential threats emanating from this space in the same way as those emanating from real space, and therefore to implement international police cooperation measures to combat these threats.

Key words: international police cooperation, police integration in Europe, Europol, cybercrime, combatting cybercrime.