НАПРЯМ 7. ПРАВОВІ МЕХАНІЗМИ ВЗАЄМОДІЇ УКРАЇНИ ТА ЄС У КОНТЕКСТІ ЄВРОПЕЙСЬКОЇ ІНТЕГРАЦІЇ

DOI https://doi.org/10.36059/978-966-397-601-3-151

ІНСТИТУЦІЙНО-ПРАВОВИЙ МЕХАНІЗМ СПІВРОБІТНИЦТВА УКРАЇНИ З АГЕНТСТВОМ ЄВРОПЕЙСЬКОГО СОЮЗУ З ПИТАНЬ МЕРЕЖЕВОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА CEPOL У СФЕРІ ПРОТИДІЇ КІБЕРЗАГРОЗАМ: ІМПЛЕМЕНТАЦІЯ ACQUIS ЄС ТА ПРАКТИКА РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ

Ольга БАРАБАШ
доктор юридичних наук, професор,
завідувач науково-дослідної лабораторії актуальних проблем правозастосовної та правоохоронної діяльності
навчально-наукового інституту права та правоохоронної діяльності,
голова Ради молодих вчених
Львівський державний університет внутрішніх справ
м. Львів, Україна

За даними Агентства Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA), лише у 2023-2024 роках кількість зареєстрованих кіберінцидентів у державах ЄС зросла більш ніж на 20%, причому більшістю залишаються атаки типу «ransomware» та цілеспрямовані втручання у функціонування критичної інфраструктури[1]. В той же час, як свідчать звіти Міжнародного союзу електрозв'язку, понад 60% держав світу перебувають на стадії часткової нормативної імплементації міжнародних стандартів кібербезпеки, що, без перебільшення, зумовлює істотну нерівномірність глобального кіберзахисту[2]. Україна ж, своєю чергою, витримує надзвичайно високу інтенсивність кібератак, що, за оцінками Держспецзв'язку, обчислюється тисячами інцидентів щомісяця (за 2024 рік опрацьовано 4315 кіберінцидентів, що на 70% більше, ніж у 2023 році – 2541

[1] European Union Agency for Cybersecurity (ENISA). Threat landscape. https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape

[2] International Telecommunication Union. (2024). Global cybersecurity index 2024 (5th ed.). https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

інцидент[3]), а також – здійснює триваючий процес законодавчого та інституційного покращення системи реагування. Власне тому питання співробітництва з європейськими інституціями, зокрема ENISA та CEPOL (Агентство Європейського Союзу з підготовки співробітників правоохоронних органів), не є факультативним напрямом зовнішньої політики, а безпосередньо зумовленою обставинами необхідність, що вимагає як наближення до acquis ЄС, так і перегляду внутрішніх правових та організаційних підходів до протидії кіберзагрозам.

У контексті інституційно-правової взаємодії України з європейськими структурами у сфері кібербезпеки, доречно відразу змістити акцент із декларативного рівня нормативного наближення на площину фактичного функціонування механізмів реагування, де, власне кажучи, і виявляється реальна спроможність декларованих законодавцем приписів. Безперечно, імплементація acquis ЄС в означеному вимірі не може обмежуватися винятково інкорпорацією положень директив чи регламентів; натомість визначальним є питання того, яким чином ці положення «працюють» у конкретному випадку кіберінциденту – від моменту його виявлення до завершення розслідування та відновлення функціонування уражених систем.

З огляду на вищевикладене, звернення до практики функціонування урядової команди CERT-UA дає можливість окреслити низку системних проблем, що мають безпосередній правовий вимір. Так, CERT-UA здійснює збір, аналіз та реагування на кіберінциденти[4], однак порядок інформаційної взаємодії між CERT-UA, Службою безпеки України, Держспецзв'язку та суб'єктами критичної інфраструктури фактично регулюється підзаконними актами та відомчими інструкціями, що не мають достатнього рівня уніфікації. Внаслідок цього, у реальних ситуаціях, скажімо, під час атак типу «wiper» на державні інформаційні ресурси, фіксується затримка у передачі первинної інформації, що прямо впливає на часові параметри реагування.

Відтак, якщо апелювати до положень Директиви (ЄС) 2022/2555 (NIS2)[5], стає очевидним, що європейська модель визначає чітко регламентовані строки повідомлення про інцидент (24 години для первинного сповіщення) та стандартизовані формати обміну інформацією між CSIRT-командами. В Україні ж, попри наявність загального обов'язку інформування, відсутня деталізована процедура

[3] Прасад А. (2025). В Україні за рік кількість кібератак зросла на 70%. Найпоширеніші типи інцидентів і головні цілі хакерів. https://surl.lu/fkaori

[4] Computer Emergency Response Team of Ukraine (CERT-UA). Official website. https://cert.gov.ua/

[5] 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. (2022). https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

щодо змісту повідомлення, каналів передачі та відповідальності за його несвоєчасність. У цьому аспекті вбачається, що запозичення саме процедурної деталізації NIS2, а не лише її концептуальних положень, могло б суттєво підвищити ефективність реагування.

Окремо варто зупинитися на питанні обміну технічною інформацією про кіберзагрози («threat intelligence»), який у співробітництві з ENISA має ключове значення. У межах ЄС функціонує мережа CSIRTs Network, де обмін даними відбувається у режимі, близькому до реального часу, із використанням стандартизованих форматів (STIX/TAXII)[6]. Своєю чергою, у вітчизняній практиці, натомість, обмін часто здійснюється через неформалізовані канали або в рамках окремих міжнародних проєктів. Відтак, у світлі Регламенту (ЄС) 2019/881 (Cybersecurity Act)[7], доцільно говорити про потребу законодавчого закріплення обов'язковості використання уніфікованих протоколів обміну даними, що, без перебільшення, дозволило б уникнути втрати критично важливої інформації на ранніх етапах інциденту.

Звертаючись до співробітництва з CEPOL, варто змістити увагу із загальних освітніх програм на їх практичне використання у діяльності органів досудового розслідування. Як показує практика, участь українських слідчих у тренінгах CEPOL не завжди трансформується у зміну процесуальної поведінки під час розслідування кіберзлочинів. До прикладу, питання фіксації електронних доказів, їх збереження та допустимості у суді нерідко вирішуються із порушенням стандартів, закріплених у Будапештській конвенції про кіберзлочинність[8]. У цьому контексті доцільно внести зміни до Кримінального процесуального кодексу України від 13.04.2012 р. №4651-VI[9], передбачивши, скажімо, окрему процедуру поводження з цифровими доказами, яка б враховувала рекомендації Ради Європи та практику держав-членів ЄС.

Цікаво, що у низці держав ЄС діє інститут так званих «кіберпрокурорів», які спеціалізуються виключно на справах, пов'язаних із кіберзлочинністю[10]. В Україні ж, попри створення

[6] European Union Agency for Cybersecurity (ENISA). CSIRTs network. https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/csirts-network

[7] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). (2019). https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

[8] Council of Europe. (2001). Convention on Cybercrime (ETS No. 185). https://www.coe.int/en/web/cybercrime/the-budapest-convention

[9] Верховна Рада України. (2012). Кримінальний процесуальний кодекс України (Закон №4651-VI від 13 квітня 2012 р.). https://zakon.rada.gov.ua/laws/show/4651-17#Text

[10] Eurojust. Cybercrime. https://www.eurojust.europa.eu/crime-types-and-cases/crime-types/cybercrime

спеціалізованих підрозділів у прокуратурі та поліції, наразі немає подібного рівня спеціалізації, що, безумовно, позначається на якості процесуального керівництва як такого. Відповідно, тут співробітництво з CEPOL могло б бути використане значно ефективніше – не лише як освітня складова, але й як інструмент інституційного моделювання та гармонізації практик.

У площині захисту критичної інфраструктури, яка, в умовах сьогодення, перебуває під постійним тиском кіберзагроз, практична імплементація європейських стандартів видається ще більш сегментованою. Так, Закон України «Про критичну інфраструктуру» від 16.11.2021 р. №1882-IX встановлює загальні засади її захисту[11], однак не містить достатньо деталізованих вимог до кіберзахисту операторів таких об'єктів. На противагу цьому, вищезгаданий NIS2 визначає конкретні обов'язки щодо управління ризиками, проведення аудитів та впровадження заходів кібергігієни. Відтак, у світлі наведеного, доцільно запозичити практику обов'язкової сертифікації систем кіберзахисту операторів критичної інфраструктури, що передбачена Регламентом (ЄС) 2019/881[12].

Достатньо показовим є досвід Федеративної Республіки Німеччина, де Федеральне відомство з безпеки інформаційних технологій (BSI) функціонує як центральний координатор реагування на кіберінциденти. Відповідно до Закону про підвищення безпеки інформаційних технологій («IT-Sicherheitsgesetz 2.0[13]»), оператори критичної інфраструктури зобов'язані негайно повідомляти про інциденти та впроваджувати сертифіковані засоби захисту. Цікаво, що у німецькій моделі передбачено адміністративну відповідальність за неподання або несвоєчасне подання інформації про інцидент, що, безумовно, дисциплінує суб'єктів і формує культуру кіберзвітності.

Аналогічно, у Франції діяльність Національного агентства з безпеки інформаційних систем (ANSSI – Agence nationale de la sécurité des systèmes d'information) свідчить про високий рівень централізації та процесуальної визначеності. Відповідно до декретів 2009-834 та 2011-170, агентство має повноваження щодо операторів життєво

[11] Верховна Рада України. (2021). Про критичну інфраструктуру (Закон №1882-IX від 16 листопада 2021 р.). https://zakon.rada.gov.ua/laws/show/1882-20#Text

[12] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). (2019). https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

[13] Bundesamt für Sicherheit in der Informationstechnik (BSI). (2021). IT-Sicherheitsgesetz 2.0. https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html

важливих послуг (OIV/OES), в тому числі з аудитами та примусовими перевірками[14].

Разом із тим, досвід Естонії, яка після кібератак 2007 року сформувала одну з найбільш ефективних систем кіберзахисту, є особливо релевантним для України. В Естонії існує чітко структурована система взаємодії між державними органами, приватним сектором та міжнародними партнерами, де основну роль має CERT-EE. Обмін інформацією про інциденти відбувається у стандартизованих форматах і є обов'язковим для широкого кола суб'єктів[15].

Звертаючись до досвіду Нідерландів, варто відмітити функціонування Національного центру кібербезпеки (NCSC-NL), який, крім координації реагування, активно залучений до публікації аналітичних звітів та рекомендацій для приватного сектору. Більше того, законодавство Нідерландів дозволяє NCSC передавати чутливу інформацію про кіберзагрози навіть приватним компаніям (законодавчі повноваження – Wbni[16]/NIS2[17]), якщо це необхідно для запобігання інциденту[18].

Окремо варто зупинитися на практиці Італії, де створено Національне агентство кібербезпеки (CAN – Agenzia per la Cybersicurezza Nazionale), яке забезпечує централізоване управління кіберінцидентами. Прикметно, що італійська модель передбачає інтеграцію функцій кіберрозвідки, реагування та стратегічного планування в межах однієї інституції[19]. Вбачається, що подібний підхід міг би бути адаптований в Україні шляхом посилення ролі Національного координаційного центру кібербезпеки при РНБО, надавши йому не тільки координаційні, але й операційні повноваження.

В аспекті аналізу зарубіжних практик доречно зосередитися і на підходах НАТО, які у сфері кібербезпеки формують окремий, фактично автономний рівень стандартів. Принципово важливо, що в межах

[14] Agence nationale de la sécurité des systèmes d'information (ANSSI). (2022). Implementation of the NIS Directive in the French maritime sector. https://www.enisa.europa.eu/sites/default/files/all_files/1.4.%2020221014_ANSSI-NIS%20Directive.pdf

[15] Ottis R. (2008). Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. 6 p. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

[16] Government of the Netherlands. (2024). Wet beveiliging netwerk- en informatiesystemen. https://wetten.overheid.nl/BWBR0041515/2024-10-01

[17] 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. (2022). https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

[18] Government of the Netherlands. Fighting cybercrime in the Netherlands. https://www.government.nl/topics/cybercrime/fighting-cybercrime-in-the-netherlands

[19] European Cybersecurity Competence Centre. Agenzia per la Cybersicurezza Nazionale – Italy. https://cybersecurity-centre.europa.eu/italy-ncc_en

Альянсу **кіберпростір** офіційно визнано *оперативним доменом* поряд із сушею, морем, повітрям та космосом. У цьому контексті варто звернути увагу на діяльність Cooperative Cyber Defence Centre of Excellence (Об'єднаний центр передових технологій з кібероборони НАТО[20]), який, зокрема, розробив відомий «Tallinn Manual»[21], що хоча й не має обов'язкової юридичної сили, однак є важливим орієнтиром щодо застосування норм міжнародного гуманітарного права у кіберпросторі. Для України значення наведеного документа полягає, насамперед, у можливості інтерпретації кібератак як *складових збройного конфлікту*, що, своєю чергою, відкриває перспективи для кваліфікації окремих кібероперацій як воєнних дій.

Окремо слід відзначити надзвичайно важливий крок у напрямі інституційної інтеграції України до євроатлантичного безпекового простору – приєднання до Cooperative Cyber Defence Centre of Excellence у 2023 році і набуття повноправної участі у діяльності названої інституції. Безперечно, офіційний статус відкриває доступ до передових аналітичних розробок, навчальних програм та практик кіберзахисту, що формуються у межах НАТО[22]. Разом із тим, участь у CCDCOE надає можливість безпосереднього залучення українських фахівців, зокрема у сфері застосування міжнародного права в кіберпросторі, а також до участі у масштабних кібернавчаннях, що моделюють реальні сценарії атак на критичну інфраструктуру.

Більш прикладний характер мають механізми колективного реагування НАТО, зокрема через платформу NATO Computer Incident Response Capability, яка забезпечує централізований моніторинг та реагування на інциденти в інформаційних системах Альянсу. Особливістю зазначеної моделі є інтеграція національних CERT-структур із наднаціональними механізмами обміну інформацією, що дає змогу досягати високого рівня ситуаційної обізнаності («situational awareness») у режимі реального часу[23].

Показовим є і те, що в межах НАТО активно розвивається концепція «cyber resilience», яка виходить за межі традиційного захисту і передбачає здатність систем не тільки протидіяти атакам, але й швидко відновлюватися після них[24]. У практичному вимірі – це впровадження

[20] NATO Cooperative Cyber Defence Centre of Excellence. Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/

[21] NATO Cooperative Cyber Defence Centre of Excellence. (2013). The Tallinn Manual. https://ccdcoe.org/research/tallinn-manual/

[22] Suspilne Media. (2023). Україна офіційно приєдналася до Центру НАТО з кіберзахисту. https://suspilne.media/amp/478003-ukraina-oficijno-priednalasa-do-centru-nato-z-kiberzahistu/

[23] NATO. (2024). Cyber defence. https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence

[24] Там само.

обов'язкових сценаріїв безперервності діяльності («business continuity plans») та регулярних кібернавчань («cyber exercises»), таких як Locked Shields[25], що моделюють масштабні кібератаки на критичну інфраструктуру. Для України, з огляду на воєнний контекст, інтеграція до подібних навчальних програм має не лише освітнє, але й безпосередньо прикладне значення.

Крім того, слід відзначити, що підходи НАТО до кібербезпеки тісно пов'язані з питаннями розвідки та обміну інформацією між союзниками. На відміну від цивільних моделей ЄС, де акцент зроблено на регуляторних механізмах, Альянс використовує більш гнучкі інструменти, що дають можливість оперативно передавати чутливу інформацію без надмірних бюрократичних процедур. Відтак, у контексті української правової системи доцільно порушити питання про розширення можливостей міжвідомчого обміну даними, зокрема між сектором безпеки і оборони та цивільними органами.

[25] NATO Cooperative Cyber Defence Centre of Excellence. Locked Shields. CCDCOE. https://ccdcoe.org/locked-shields/