2021/09/24/1040422112/cia-recalls-vienna-station-chief-in-move-related-to-handling-of-havana-syndrome (дата звернення: 14.10.2025).

4. Макух-Федоркова І. І. Сучасні методологічні підходи до визначення понять смислові/когнітивні війни: аналіз інструментів впливу. *Історико-політичні проблеми сучасного світу* : збірник наукових статей. 2024. № 49. С. 120–136. URL: https://mhpi.chnu.edu.ua/mhpi/article/view/19/11 (дата звернення: 14.10.2025).

5. Надурак В. В. Пастка для розуму. Як ворог веде проти України когнітивну війну. URL: https://nv.ua/ukr/amp/filosof-rozkriv-sekreti-kognitivnoji-viyni-yaku-vede-proti-ukrajini-rosiya-50536593.html (дата звернення: 14.10.2025).

6. Мазикін М. А. Когнітивна війна в сучасному світі: психолінгвістичні механізми впливу на свідомість та стратегії захисту. URL: https://ukr-happiness-institute.com/kognityvna-vijna-ta-strategii-zahystu/ (дата звернення: 14.10.2025).

Шеховцова Анна Андріївна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Резнік Ю. С., старший викладач кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО У СФЕРІ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Сучасний світ характеризується високим рівнем цифрової інтеграції, що водночас породжує нові ризики та виклики для безпеки. Кіберзлочинність стала однією з найсерйозніших транснаціональних загроз XXI століття, адже злочинці діють поза межами державних кордонів, використовуючи прогалини у правовому регулюванні та технологічні вразливості [1]. Метою

цього дослідження є аналіз міжнародних механізмів співробітництва у сфері протидії кіберзлочинності, визначення їх ключових елементів, результатів діяльності та основних проблем, що перешкоджають ефективній координації дій держав.

Поняття кіберзлочинності охоплює широкий спектр протиправних дій, які здійснюються із використанням інформаційно-комунікаційних технологій. Відповідно до положень Будапештської конвенції про кіберзлочинність [2], до таких злочинів належать атаки на мережеву інфраструктуру, фінансове шахрайство, використання програм-вимагачів, кібершпигунство, викрадення персональних даних, цифрове насильство, злочини проти дітей і поширення дезінформації [3]. Більшість таких злочинів мають комбінований характер: наприклад, фішинг може бути підготовчим етапом ransomware-атаки, а викрадення даних – способом подальшого шантажу. Це свідчить про необхідність комплексного підходу до протидії, що передбачає міжнародну координацію.

Ефективна боротьба з кіберзлочинністю неможлива без спільних міжнародно-правових засад, які регламентують координацію дій, обмін інформацією та взаємне визнання цифрових доказів. Основу такої системи становить Будапештська конвенція Ради Європи 2001 року – перший міжнародний договір, спрямований на гармонізацію кримінального законодавства у сфері комп'ютерних злочинів, запровадження спільних процедур збирання й збереження електронних доказів та створення каналів оперативного обміну між правоохоронними органами різних країн [2]. Саме цей документ заклав фундамент для формування міжнародного правового простору у сфері кібербезпеки.

Подальший розвиток міжнародного правового регулювання відбувся через укладення угод про взаємну правову допомогу (Mutual Legal Assistance – MLA), які стали ключовим інструментом обміну доказами під час розслідування кіберінцидентів [4]. Ці механізми дозволяють державам отримувати дані, що зберігаються за кордоном, та координувати кримінальні провадження, однак їх ефективність часто обмежується розбіжностями у національних правових системах і тривалістю процедур.

Важливим складником міжнародно-правових рамок є законодавство Європейського Союзу, яке встановлює спільні підходи до запобігання кіберзлочинності. Зокрема, Директива 2013/40/ЄС визначає відповідальність за атаки на інформаційні системи, а Регламент (ЄС) 2016/679 (GDPR) регулює обробку та передачу персональних даних, у тому числі для потреб правоохоронних органів [5]. У такий спосіб формується багаторівнева система – від глобальних норм Будапештської конвенції до регіональних директив і двосторонніх угод, які спільно забезпечують міжнародну кіберстабільність.

Реалізація цих правових механізмів відбувається через діяльність спеціалізованих міжнародних структур. Одним із ключових учасників глобальної системи є Міжнародна організація кримінальної поліції (INTERPOL), що об'єднує понад 190 держав. Її діяльність спрямована на координацію дій правоохоронних органів, організацію спільних операцій та обмін оперативною інформацією. Показовим прикладом ефективності такого підходу стала операція Synergia (2023–2024 рр.), у ході якої було нейтралізовано понад 70 % командно-контрольних серверів (C2), арештовано 31 особу, заблоковано сотні фішингових ресурсів [6].

На європейському рівні центральну роль відіграє Європейський центр із протидії кіберзлочинності (EC3), що функціонує в структурі Europol. Він координує спільні розслідування, здійснює аналітичну підтримку та організовує операції на міждержавному рівні. У травні 2024 року під егідою Europol проведено операцію Endgame, спрямовану на ліквідацію ботнетів, які використовувалися для розповсюдження програм-вимагачів; у результаті було вилучено понад сто серверів і заблоковано близько двох тисяч доменів [7].

Стратегічний вимір міжнародної кібербезпеки забезпечує НАТО через діяльність Центру передового досвіду з кібероборони (CCDCOE) у Таллінні. Центр проводить дослідження, навчання та міжнародні навчальні маневри Locked Shields, які щорічно залучають тисячі експертів із десятків країн і дозволяють перевірити готовність до відбиття масштабних атак на критичну інфраструктуру [8].

Операційне реагування на інциденти забезпечують національні команди реагування CSIRT/CERT. Вони займаються моніторингом кіберзагроз, збором технічних

індикаторів компрометації, взаємодією з приватними компаніями та забезпечують обмін даними між державними структурами. Така співпраця є основою публічно-приватного партнерства, без якого неможливо забезпечити ефективну глобальну кіберстійкість [9].

Практична результативність міжнародної співпраці підтверджується низкою успішних операцій. Серед них – Endgame (Europol, 2024), під час якої нейтралізовано понад сто серверів ботнетів; *Synergia* (INTERPOL, 2023–2024), у межах якої ліквідовано сотні C2-серверів і здійснено десятки арештів; Quicksand (2022–2023), що була спрямована проти груп GandCrab і REvil; а також LockBit Disruption (2024), де за участі Europol, Eurojust і українських правоохоронних органів було знищено інфраструктуру злочинної групи LockBit та арештовано її учасників [6; 7; 9; 10]. Ці операції демонструють ефективність глобальної координації та водночас виявляють проблемні аспекти міжнародної взаємодії.

Попри досягнення, співпраця у сфері протидії кіберзлочинності стикається з низкою труднощів. Насамперед це юридичні розбіжності між країнами у кваліфікації злочинів і процедурах збирання доказів, що ускладнює міжнародне переслідування правопорушників. Процедури взаємної правової допомоги залишаються повільними й бюрократичними, а нерівність технічних можливостей між державами знижує ефективність реагування. Додатковими обмеженнями виступають норми законодавства про захист приватності, зокрема Регламент ЄС (GDPR) [5], а також висока адаптивність злочинців, які активно використовують штучний інтелект, криптовалюти та анонімні мережі [11]. Ускладнює ситуацію й недостатня координація між урядовими структурами, приватним сектором і науковими установами.

Для підвищення ефективності міжнародної взаємодії доцільно вдосконалити існуючі механізми співпраці. Необхідним є розроблення прискорених процедур міжнародної правової допомоги у справах кіберзлочинів, які передбачатимуть швидкий електронний обмін запитами та доказами. Важливо також посилити технічну підтримку і підготовку кадрів у країнах із низьким рівнем кіберготовності, уніфікувати стандарти обміну технічними даними між командами CSIRT/CERT, розширити публічно-приватне

партнерство та запровадити чіткі правові рамки його функціонування. Регулярні багатосторонні навчання, подібні до Locked Shields, сприятимуть підтриманню високого рівня готовності до реагування на загрози. Окремої уваги потребують інвестиції у розвиток технологій штучного інтелекту, квантового шифрування та аналітики загроз, що можуть забезпечити новий рівень глобальної кіберстабільності. Водночас важливо зберігати баланс між захистом персональних даних і потребами правоохоронних органів у доступі до інформації [9].

Отже, кіберзлочинність є глобальною проблемою, подолання якої можливе лише шляхом послідовної міжнародної координації. Досвід INTERPOL, Europol, HATO/CCDCOE та CSIRT/CERT доводить, що об'єднані дії держав і приватного сектору здатні забезпечити реальні результати у боротьбі з транснаціональною злочинністю. Водночас актуальними залишаються питання правової гармонізації, швидкості обміну інформацією та залучення недержавних акторів до спільної роботи.

Міжнародне співробітництво у сфері кібербезпеки має стати ключовим чинником забезпечення стабільності, суверенітету та захисту прав людини у цифровому просторі. Тільки шляхом консолідації зусиль держав, міжнародних організацій і приватних компаній можна гарантувати стійкий розвиток, безпеку критичної інфраструктури та захист громадян у глобальному цифровому середовищі.

Список використаних джерел

1. Василенко О. М. Кібербезпека в системі міжнародних відносин: правові та організаційні аспекти. Київ : НАУ, 2022. 256 с.

2. Council of Europe. Convention on Cybercrime (Budapest Convention). ETS No.185. Budapest, 2001.

3. Яременко Л. П. Кіберзлочинність: правові засади та міжнародне співробітництво. Львів : ЛНУ ім. І. Франка, 2021. 198 с.

4. United Nations Office on Drugs and Crime (UNODC). Practical Guide to Mutual Legal Assistance in Cybercrime Cases. Vienna, 2020.

5. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation, GDPR). — Official Journal of the EU, L 119, 2016.

6. INTERPOL. Operation Synergia Targets Cybercrime Infrastructure. Lyon : INTERPOL News, 2024.

7. Europol. Operation Endgame: Disruption of Ransomware Infrastructure. The Hague, 2024.

8. NATO CCDCOE. Locked Shields 2024 After Action Report. Tallinn, 2024.

9. ENISA. European CSIRT Network Annual Report. Brussels, 2023.

10. Eurojust. Joint Action Against LockBit Ransomware Group. The Hague, 2024.

11. Trend Micro Research. Cybercrime and Artificial Intelligence: Emerging Threats 2025. Tokyo, 2025.