

DOI: 10.33270/05267202.12
УДК 343.9:341.1/8

КРАСІЙ Марія*

кандидат юридичних наук, доцент, доцент кафедри публічного управління, адміністрування і національної безпеки Івано-Франківського національного технічного університету нафти і газу

76000, вул. Карпатська, 15, м. Івано-Франківськ, Україна

ORCID: <https://orcid.org/0000-0001-8752-7371>

Зовнішня кримінально-правова політика держави в умовах транснаціональної кіберзлочинності

Анотація. У статті здійснено комплексне дослідження сутності й особливостей зовнішньої кримінально-правової політики держави в умовах транснаціональної кіберзлочинності. Обґрунтовано, що стрімкий розвиток інформаційно-комунікаційних технологій і цифровізація суспільних відносин зумовили формування нових форм злочинної діяльності, які характеризуються транснаціональністю, високим рівнем латентності та технологічною складністю. Встановлено, що такі ознаки кіберзлочинності істотно ускладнюють застосування традиційних механізмів кримінально-правового реагування та зумовлюють необхідність активізації міжнародного співробітництва. Проаналізовано міжнародно-правові засади протидії кіберзлочинності, зокрема положення Будапештської конвенції, актів Європейського Союзу й інших міжнародних інструментів, спрямованих на гармонізацію кримінального законодавства та розвиток механізмів взаємодії держав. Визначено, що зовнішня кримінально-правова політика є ключовим інструментом координації міжнародних зусиль у сфері боротьби з кіберзагрозами, забезпечення обміну інформацією, спільного розслідування злочинів і формування уніфікованих підходів до криміналізації кіберзлочинів. Окреслено основні проблеми реалізації зовнішньої кримінально-правової політики України, серед яких: відставання законодавства від динаміки розвитку кіберзлочинності, складність збирання та використання електронних доказів, складнощі визначення юрисдикції в транскордонних справах, а також недостатня ефективність міжнародної взаємодії. Обґрунтовано необхідність подальшого вдосконалення нормативно-правової бази, посилення інституційної спроможності компетентних органів і розширення міжнародного співробітництва.

Ключові слова: кіберзлочинність; транснаціональна злочинність; кримінально-правова політика; міжнародне співробітництво; кібербезпека; гармонізація законодавства.

Історія статті:

Отримано: 25.02.2026

Прийнято: 08.04.2026

Опубліковано: 29.05.2026

Рекомендоване посилання:

Красій М. Зовнішня кримінально-правова політика держави в умовах транснаціональної кіберзлочинності. *Наука і правоохорона*. 2026. Вип. 2 (72). С. 117–122. DOI: 10.33270/05267202.12

*Відповідальний автор



© Красій М., 2026. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (<https://creativecommons.org/licenses/by/4.0/>)

Вступ

Сучасний світ неможливо уявити без цифрових технологій, які радикально трансформували всі сфери людського життя. Електромобілі, мобільні пристрої та комп'ютерні системи стали невід'ємними елементами повсякденності, що свідчить про глибоку залежність суспільства від інформаційно-комунікаційних технологій (Šerpec, & Kočivnik, 2024). Водночас стрімкий розвиток інформаційних технологій та процеси цифровізації суспільних відносин спричинили появу нових форм злочинної діяльності, пов'язаних з використанням інформаційно-комунікаційних систем. Кіберзлочинність набула вираженого транснаціонального характеру, що робить неможливим ефективне протистояння їй виключно в межах національних юрисдикцій.

У цих умовах ключового значення набуває формування ефективної зовнішньої кримінально-правової політики держави, спрямованої на розвиток міжнародного співробітництва, гармонізацію національного кримінального законодавства з міжнародними стандартами та імплементацію глобальних інструментів протидії кіберзлочинності.

Матеріали та методи

Матеріальну основу дослідження становлять міжнародно-правові акти у сфері протидії кіберзлочинності, зокрема положення Конвенції про кіберзлочинність (Будапештської конвенції), Директива Європейського Парламенту та Ради 2013/40/ЄС від 12 серпня 2013 року про атаки на інформаційні системи та заміну Рамкового рішення Ради 2005/222/JHA; Директива Європейського Парламенту і Ради (ЄС) 2022/2555 від 14 грудня 2022 року про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972, скасування Директиви (ЄС) 2016/1148 (Директива NIS 2), а також інші міжнародні документи, що регулюють питання криміналізації кіберзлочинів і міжнародного співробітництва. Важливу групу джерел становлять наукові праці українських і зарубіжних дослідників, присвячені проблемам кіберзлочинності, міжнародного співробітництва та кримінально-правової політики, а саме: В. Аніщука (2024), Л. Бартолі (2025), Н. Вандезанде (2024), В. Гончарука (2025), Г. Дідківської (2023), М. Мордвинцева (2025), І. Татарина (2025), С. Шміц-Берндт (2023) та ін.

Методологічну основу дослідження становить цілісна, внутрішньо узгоджена система загальнонаукових і спеціально-юридичних методів, застосування яких зумовлене складністю, багатовимірністю та міждисциплінарним характером проблематики кіберзлочинності й зовнішньої кримінально-правової політики держави. Базовим є діалектичний метод, який надав можливість проаналізувати кіберзлочинність як динамічне

соціально-правове явище, що трансформується під впливом глобалізаційних процесів, цифровізації та безпекових викликів, зокрема в умовах збройної агресії. Системний підхід у поєднанні із системно-структурним методом дав змогу дослідити кіберзлочинність як складну багаторівневу систему, визначити її елементи, види та взаємозв'язки, а також обґрунтувати місце й роль зовнішньої кримінально-правової політики в загальній системі забезпечення національної та міжнародної безпеки. За допомогою порівняльно-правового методу здійснено зіставлення національного кримінального законодавства України з міжнародно-правовими стандартами та правом Європейського Союзу. Завершальним етапом стало застосування методу узагальнення та наукової абстракції, що дало змогу сформулювати обґрунтовані висновки та пропозиції щодо вдосконалення зовнішньої кримінально-правової політики України у сфері боротьби з кіберзлочинністю.

Мета статті полягає у комплексному дослідженні сутності й особливостей зовнішньої кримінально-правової політики держави в умовах транснаціональної кіберзлочинності.

Результати й обговорення

Кіберзлочинність належить до найсерйозніших загроз сучасності, оскільки становлення інформаційного суспільства зумовило проникнення інформаційних технологій у всі сфери суспільного життя. Кіберзлочини становлять небезпеку як для окремих осіб, так і для державних інституцій та міжнародних організацій. Однією з ключових особливостей, що суттєво ускладнює протидію, є неможливість чіткої територіальної ідентифікації як суб'єкта злочину, так і потерпілого. Інтернет фактично усунув бар'єри між державами, спільнотами та громадянами, забезпечивши глобальну взаємодію та обмін інформацією. Для збереження відкритого, вільного та безпечного кіберпростору в ньому мають застосовуватися ті самі принципи, норми й цінності, що діють в офлайн-середовищі (Anishchuk, & Zitsyk, 2024).

Поряд із позитивними можливостями, які надає розвиток інформаційних технологій для комунікації, бізнесу та науки, відбувається стійке зростання рівня кіберзлочинності. Вона охоплює широкий спектр протиправних діянь – від крадіжки персональних даних і фінансового шахрайства до атак на об'єкти критичної інфраструктури та кібертероризму (Anishchuk, & Zitsyk, 2024).

Для України проблема боротьби з кіберзлочинністю має особливу актуальність через активну цифрову трансформацію держави, а також значне зростання кількості кіберінцидентів, пов'язаних зі збройною агресією проти країни. У таких умовах формування ефективної зовнішньої кримінально-правової політики у сфері кіберзлочинності стає важливим компонентом забезпечення як національної, так і міжнародної безпеки.

Зовнішню кримінально-правову політику глумачать як систему стратегічних дій та рішень держави, спрямованих на забезпечення правопорядку й боротьбу зі злочинністю на міжнародному рівні шляхом співробітництва з іншими державами та міжнародними організаціями. Вона ґрунтується на ратифікованих міжнародних договорах і здійснюється в межах конституційних повноважень органів влади. Основна мета такої політики – гармонізація національного законодавства з міжнародними стандартами, ефективне реагування на транснаціональні злочинні загрози та зміцнення позицій держави в глобальному правовому просторі (Krasii, 2025).

Боротьба з кіберзлочинністю потребує комплексного підходу, що передбачає вдосконалення нормативно-правової бази, розвиток технічних засобів кіберзахисту та активізацію міжнародної співпраці (Honcharuk, 2025). Кіберзлочинність вирізняється низкою специфічних ознак: транснаціональністю, високою латентністю, швидким поширенням злочинних технологій та складністю ідентифікації суб'єктів злочину. Саме тому ефективна протидія можлива лише за умови тісної взаємодії держав на міжнародному рівні.

Серед основних видів кіберзлочинів виокремлюють комп'ютерне шпигунство, поширення шкідливого програмного забезпечення, інтернет-шахрайство, дефейс сайтів, кібертероризм тощо. Особливе занепокоєння викликає потенціал цих діянь набувати масштабного характеру та загрожувати міждержавній безпеці, що зумовлює активізацію міжнародної співпраці. Значну роль у формуванні нормативної бази відіграють міжнародні організації – ООН, Рада Європи, Інтерпол, ОЕСР, G8 (нині G7) (Yakymchuk, 2021).

Важливим етапом розвитку міжнародного регулювання стала діяльність Комітету експертів Ради Європи з питань злочинності в кіберпросторі (PC-CY), створеного 1997 року. Результатом його роботи стала Конвенція про кіберзлочинність (Будапештська конвенція), прийнята 2001 року. Цей документ став першим багатостороннім міжнародним договором, що встановлює спільні стандарти криміналізації певних діянь у кіберпросторі, процесуальних повноважень і міжнародного співробітництва. Конвенція вирізняється гнучкістю та слугує орієнтиром для багатьох держав (Bartoli, 2025).

Глобалізація інформаційних технологій створює необмежені можливості впливу на особу та суспільство, але водночас спричиняє нову форму злочинності – злочинність у сфері високих технологій, де комп'ютери та мережі виступають об'єктом, засобом або способом вчинення злочинів. Жертвами можуть ставати як окремі особи, так і держави, причому безпека тисяч користувачів іноді залежить від дій кількох злочинців. Кількість кіберзлочинів зростає пропорційно кількості користувачів мереж. Про це свідчить, зокрема, статистика Internet Crime

Complaint Center (далі – IC3), який уже 2007 року зареєстрував мільйонну скаргу. Водночас більшість кіберзлочинів залишається латентною (Popko, 2021).

Професіоналізація кіберзлочинців та постійна еволюція технологій створюють нові загрози. Недосконалість визначення поняття кіберзлочину та санкцій за нього дає можливість злочинним групам постійно вдосконалювати методи протиправної діяльності.

Причини кіберзлочинності є комплексними. Економічний фактор полягає у високій прибутковості (кіберзлочини посідають одне з перших місць за дохідністю після торгівлі наркотиками та зброєю). Соціальні причини пов'язані з комп'ютеризацією та формуванням інформаційного простору. Технологічні – з можливістю обходу захисту та вторгнення в мережі. Політичні мотиви включають прагнення дестабілізувати державну політику, дискредитувати опонентів, втручатися у вибори чи здійснювати кібертероризм (Hurzel, 2019).

Гармонізація національних законодавств є необхідною умовою ефективної боротьби з кіберзлочинністю, хоча вона має враховувати регіональні особливості та можливості держав (Didkivska, & Shevchenko, 2023). Багато країн демонструють недостатню готовність реагувати на загрози, що може бути покращено завдяки обміну досвідом та укладанню багатосторонніх угод (Vlajić, & Nikolić, & Gudelj, 2023).

У науковій літературі обґрунтовується необхідність комплексного вдосконалення державної політики у сфері боротьби з кіберзлочинністю. Зокрема, М. В. Мордвинцев, Д. В. Пашнєв, О. В. Хлестков (2025), пропонують: 1) продовжити гармонізацію кримінального та процесуального законодавства України з міжнародними стандартами, зокрема Будапештською конвенцією про кіберзлочинність і директивами ЄС; 2) посилити інституційну спроможність органів кібербезпеки, зокрема через належне фінансування, технічне переоснащення та підвищення кваліфікації кадрів; 3) розвивати міжнародне співробітництво в обміні електронними доказами, спільних розслідуваннях і навчаннях, активно використовуючи інструменти ЄС, НАТО й ООН; 4) забезпечити баланс між національною безпекою та правами людини, уникаючи надмірного розширення повноважень державних органів щодо контролю інформаційного простору; 5) створити систему кіберстійкості, здатну ефективно протидіяти загрозам у воєнний час, поєднуючи правові, організаційні, технічні та дипломатичні інструменти (Mordvyntsev, & Pashniev, Khlietkov, 2025).

Євроінтеграційний курс України передбачає гармонізацію законодавства, зокрема у сфері кібербезпеки та боротьби з кіберзлочинністю. Національне кримінальне законодавство загалом відповідає базовим вимогам Будапештської

конвенції¹ (Україна ратифікувала її 2005 року), проте потребує оновлення для врахування нових форм злочинів (атаки на блокчейн-системи, використання ботнетів тощо) (Kostiuchenko, 2025).

У Європейському Союзі боротьба з кіберзлочинністю інтегрована в ширшу політику безпеки та правосуддя. Директива 2013/40/ЄС² гармонізувала криміналізацію втручання в інформаційні системи. Директива (ЄС) 2022/2555 (NIS 2)³ посилила вимоги до захисту критичної інфраструктури, управління ризиками та функціонування національних органів кібербезпеки (Vandezande, 2024; Schmitz-Berndt, 2023). Розвиваються механізми доступу до електронних доказів (e-evidence), а координацію забезпечують Європол (ЕС3) та ENISA.

Ефективність протидії залежить від співпраці держави та приватного сектору, удосконалення міжнародних і національних інструментів, зокрема збирання цифрових доказів, легалізації вилучення даних з іноземних серверів та створення інституційних механізмів (Tataryn, Yaremchuk, & Litvinova, 2025).

Водночас зберігаються виклики: узгодження правових систем, визначення юрисдикції, оперативність обміну інформацією.

Україна досягла певного прогресу в імplementації стандартів Будапештської конвенції, однак існують проблеми:

- відставання законодавства від нових форм кіберзлочинів;
- складність доказування через технічні особливості фіксації електронних доказів;
- складнощі визначення юрисдикції в транскордонних злочинах;
- недостатня оперативність міжнародної співпраці.

Отже, подальше формування зовнішньої кримінально-правової політики України у сфері кіберзлочинності має базуватися на комплексному поєднанні гармонізації законодавства, поглибленні міжнародного співробітництва та посиленні інституційної спроможності для боротьби з транснаціональними загрозами.

¹ Конвенція про кіберзлочинність : міжнар. док. від 23 листоп. 2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

² Директива Європейського Парламенту та Ради 2013/40/ЄС про атаки на інформаційні системи та заміну Рамкового рішення Ради 2005/222/JHA : міжнар. док. від 12 серп. 2013 р. URL: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32013L0040>

³ Директива Європейського Парламенту і Ради (ЄС) 2022/2555 про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972 та скасування Директиви (ЄС) 2016/1148 (Директива NIS 2) : міжнар. док. від 14 груд. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text

Висновки

У результаті здійсненого дослідження встановлено, що транснаціональний характер кіберзлочинності зумовлює об'єктивну необхідність переосмислення ролі та змісту зовнішньої кримінально-правової політики держави як одного з ключових інструментів забезпечення як національної, так і міжнародної безпеки. Кіберзлочинність як динамічне та високотехнологічне явище характеризується відсутністю чітких територіальних меж, високим рівнем латентності та швидкою еволюцією способів вчинення злочинів, що істотно ускладнює традиційні механізми кримінально-правового реагування.

Ефективна боротьба з кіберзлочинністю неможлива виключно в межах національної юрисдикції, а потребує системної міждержавної взаємодії, гармонізації кримінального та кримінального процесуального законодавства, а також імplementації міжнародно-правових стандартів, насамперед положень Будапештської конвенції та актів Європейського Союзу. У цьому контексті зовнішня кримінально-правова політика є важливим інструментом координації міжнародного співробітництва, обміну інформацією, спільного розслідування злочинів і формування єдиного підходу до криміналізації кіберзагроз.

Попри досягнутий прогрес у наближенні національного законодавства України до міжнародних стандартів, зберігається низка системних проблем, зокрема: відставання правового регулювання від темпів розвитку кіберзлочинності, складність збирання та допустимості електронних доказів, труднощі визначення юрисдикції у транскордонних справах, а також недостатня оперативність міжнародної правової допомоги.

Подальший розвиток зовнішньої кримінально-правової політики України у сфері боротьби з кіберзлочинністю має здійснюватися на засадах комплексності та системності й передбачати: поглиблення міжнародного співробітництва, активне використання механізмів міжнародних організацій, удосконалення нормативно-правової бази з урахуванням новітніх форм кіберзлочинів, зміцнення інституційної спроможності компетентних органів, а також забезпечення балансу між інтересами безпеки та дотриманням прав людини.

Отже, ефективна зовнішня кримінально-правова політика в умовах транснаціональної кіберзлочинності має формуватися як інтегрована багаторівнева система правових, організаційних і міжнародно-коопераційних заходів, спрямованих на адекватне реагування на сучасні кіберзагрози та забезпечення стійкості держави в глобальному цифровому середовищі.

Подяки

Немає.

Фінансування

Немає.

Конфлікт інтересів

Немає.

References

- [1] Anishchuk, V.V., & Zitsyk, S.H. (2024). The problem of combating cybercrime: comparative legal analysis. *Scientific Bulletin of Uzhhorod National University*, 83(3), 19-23. DOI: 10.24144/2307-3322.2024.83.3.2
- [2] Bartoli, L. (2025). Cybersecurity and the fight against cybercrime: Partners or competitors? *European Journal of Risk Regulation*, 16, 498-513. DOI: 10.1017/err.2025.31
- [3] Didkivska, G., & Shevchenko, D. (2023). Basic principles of combating cybercrime: international experience. *Legal Horizons*, 4, 19-23. DOI: 10.54477/LH.25192353.2023.4.pp.19-23
- [4] Honcharuk, V.L. (2025). Legal mechanisms for combating cybercrime: global practice and national context. *Crime control issues*, 49, 178-184. DOI: 10.31359/2079-6242-2025-49-178
- [5] Hurzel, Yu.V. (2019). Cybercrime: main causes and methods of combating. In *Counteracting Cyber Threats and Human Trafficking: Proceedings of the International Scientific and Practical Conference* (pp. 49-51). Kharkiv. Retrieved from https://univd.edu.ua/general/publishing/konf/26_11_2019/pdf/12.pdf
- [6] Kostyuchenko, Ya.M. (2025). Cooperation between Ukraine and the EU in cybersecurity: mechanisms for combating cybercrime. *Problems of modern transformation. Series "Law, public management and administration"*, 15. DOI: 10.54929/2786-5746-2025-15-01-10
- [7] Krasii, M.O. (2024). External criminal law policy of Ukraine as a component of crime prevention policy. *Donbass Legal Journal*, 4, 84-89. DOI: 10.32782/2523-4269-2024-89-84-89
- [8] Mordvyntsev, M.V., Pashniev, D.V., & Khliestkov, O.V. (2025). International models of legal regulation of combating cybercrime: recommendations for Ukraine. *Law and Safety*, 4(99), 59-71. DOI: 10.32631/pb.2025.4.05
- [9] Popko, V.V., & Popko, Ye.V. (2021). International legal regulation of transnational cybercrime in cyberspace. *Scientific Bulletin of Uzhhorod National University*, 66, 276-283. DOI: 10.24144/2307-3322.2021.66.46
- [10] Schmitz-Berndt, S. (2023). Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive. *Journal of Cybersecurity*, 9(1). DOI: 10.1093/cybsec/tyad009
- [11] Šepec, M., & Kočivnik, M. (2024). Combating cyberwarfare crimes in the European Union. *European Integration Studies*, 2(20), 409-432. DOI: 10.46941/2024.2.16
- [12] Tataryn, I.I., Yaremchuk, M.M., & Litvinova, Yu.O. (2025). Methods of prevention and counteraction to cybercrime in modern conditions. *Current problems of state and law*, 106, 165-171. DOI: 10.32782/apdp.v106.2025.21
- [13] Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2 Directive stacks up against its predecessor. *Computer Law & Security Review*, 52. DOI: 10.1016/j.clsr.2023.105890
- [14] Vlajić, I.B., Nikolić, B., & Gudelj, N. (2023). Legal aspects of combating cybercrime in the European Union. *Oditor*, 1(9), 17-45. DOI: 10.5937/Oditor2301017B
- [15] Yakymchuk, M.Yu. (2021). Features of legal regulation of combating cybercrime in Ukraine: comparative legal aspect. *New Ukrainian law*, 4, 182-186. doi: 10.51989/NUL.2021.4.27

Список використаних джерел

- [1] Аніщук В. В., Зицик С. Г. Проблема протидії кіберзлочинності: порівняльно-правовий аналіз. *Науковий вісник Ужгородського національного університету*. 2024. Вип. 83. Ч. 3. С. 19–23. DOI: 10.24144/2307-3322.2024.83.3.2
- [2] Bartoli L. Cybersecurity and the Fight against Cybercrime: Partners or Competitors?. *European Journal of Risk Regulation*. 2025. No. 16. P. 498–513. DOI: 10.1017/err.2025.31
- [3] Didkivska G., Shevchenko D. Basic principles of combating cybercrime: international experience. *Legal Horizons*. 2023. No. 4. P. 19–23. DOI: 10.54477/LH.25192353.2023.4.pp.19-23
- [4] Гончарук В. Л. Правові механізми боротьби з кіберзлочинністю: світова практика та вітчизняний контекст. *Питання боротьби зі злочинністю*. 2025. № 49. С. 178–184. DOI: 10.31359/2079-6242-2025-49-178
- [5] Гурзель Ю. В. Кіберзлочинність: основні причини та методи боротьби. *Протидія кіберзагрозам та торгівлі людьми* : матеріали Міжнар. наук.-практ. конф. (Харків, 26 листоп. 2019 р.). Харків, 2019. С. 49–51. URL: https://univd.edu.ua/general/publishing/konf/26_11_2019/pdf/12.pdf
- [6] Костюченко Я. М. Співпраця України та ЄС у сфері кібербезпеки: механізми боротьби з кіберзлочинністю. *Проблеми сучасних трансформацій. Серія «Право, публічне управління та адміністрування»*. 2025. № 15. DOI: 10.54929/2786-5746-2025-15-01-10
- [7] Красій М. О. Зовнішня кримінально-правова політика України як складовий елемент політики у сфері боротьби із злочинністю. *Правовий часопис Донбасу*. 2024. № 4. С. 84–89. DOI: 10.32782/2523-4269-2024-89-84-89

- [8] Мордвинцев М. В., Пашнєв Д. В., Хлестков О. В. Міжнародні моделі правового регулювання протидії кіберзлочинності: рекомендації для України. *Право і безпека*. 2025. № 4 (99). С. 59–71. DOI: 10.32631/pb.2025.4.05
 - [9] Попко В. В., Попко Є. В. Міжнародно-правова регламентація транснаціональної кіберзлочинності у кіберпросторі. *Науковий вісник Ужгородського національного університету*. 2021. Вип. 66. С. 276–283. DOI: 10.24144/2307-3322.2021.66.46
 - [10] Schmitz-Berndt S. Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive. *Journal of Cybersecurity*. 2023. Vol. 9. Issue 1. DOI: 10.1093/cybsec/tyad009
 - [11] Šepec M., Kočivnik M. Combatting Cyberwarfare Crimes in the European Union. *European Integration Studies*. 2024. No. 2 (20). P. 409–432. DOI: 10.46941/2024.2.16
 - [12] Татарин І. І., Яремчук М. М., Літвінова Ю. О. Методи попередження та протидії кіберзлочинності в умовах сучасності. *Актуальні проблеми держави і права*. 2025. № 106. С. 165–171. DOI: 10.32782/apdp.v106.2025.21
 - [13] Vandezande N. Cybersecurity in the EU: How the NIS2 – directive stacks up against its predecessor. *Computer Law & Security Review*. 2024. Vol. 52. DOI: 10.1016/j.clsr.2023.105890
 - [14] Vlajić I. B., Nikolić B., Gudelj N. Pravni aspekti suprotstavljanja sajber kriminalu u Evropskoj Uniji. *Oditor*. 2023. No. 1 (9). P. 17–45. DOI: 10.5937/Oditor2301017B
 - [15] Якимчук М. Ю. Особливості правового регулювання протидії кіберзлочинності в Україні: порівняльно-правовий аспект. *Нове українське право*. 2021. Вип. 4. С. 182–186. DOI: 10.51989/NUL.2021.4.27
-

KRASII Mariia

PhD in Law, Associate Professor, Associate Professor of the Department of Public Management, Administration and National Security of the Ivano-Frankivsk National Technical University of Oil and Gas

76000, 15 Karpatska Street, Ivano-Frankivsk, Ukraine

ORCID: <https://orcid.org/0000-0001-8752-7371>

Foreign Criminal and Legal Policy of the State in the Context of Transnational Cybercrime

Abstract. The article presents a comprehensive study of the essence and features of the state's foreign criminal and legal policy in the context of transnational cybercrime. It is substantiated that the rapid development of information and communication technologies and the digitalization of social relations have led to the formation of new forms of criminal activity, which are characterized by transnationality, a high level of latency and technological complexity. It is established that such signs of cybercrime significantly complicate the application of traditional mechanisms of criminal and legal response and necessitate the activation of international cooperation. The international legal principles of combating cybercrime are analyzed, in particular the provisions of the Budapest Convention, acts of the European Union and other international instruments aimed at harmonizing criminal legislation and developing mechanisms for interaction between states. It is determined that foreign criminal law policy is a key tool for coordinating international efforts in the field of combating cyber threats, ensuring information exchange, joint investigation of crimes and the formation of unified approaches to the criminalization of cyber crimes. The main problems of implementing foreign criminal law policy of Ukraine are outlined, including: the lag of legislation from the dynamics of cyber crime development, the complexity of collecting and using electronic evidence, the difficulties of determining jurisdiction in cross-border cases, as well as the lack of effectiveness of international cooperation. The need for further improvement of the regulatory framework, strengthening the institutional capacity of competent authorities and expanding international cooperation is substantiated.

Keywords: cyber crime; transnational crime; criminal law policy; international cooperation; cybersecurity; harmonization of legislation.