УДК 342.5 (477)
DOI https://doi.org/10.32782/TNU-2707-0581/2026.2/08

Мазійчук В. А.
https://orcid.org/0009-0002-2471-1811
Національна академія Служби Безпеки України

ЗАРУБІЖНИЙ ДОСВІД ПРОТИДІЇ ПРАВОПОРУШЕННЯМ В ІНФОРМАЦІЙНІЙ СФЕРІ ТА МОЖЛИВОСТІ ЙОГО ВИКОРИСТАННЯ В УКРАЇНІ

У статті здійснено комплексний аналіз зарубіжного досвіду протидії правопорушенням в інформаційній сфері та визначено можливості його використання в Україні з урахуванням сучасних безпекових викликів. Наголошено, що правопорушення в інформаційній сфері є однією з найбільш динамічних і небезпечних загроз сучасному суспільству, оскільки вони безпосередньо впливають на національну безпеку держав, стабільність функціонування публічних інституцій, економічну безпеку, а також на реалізацію і захист прав та свобод людини. Обґрунтовано, що в умовах цифровізації суспільства та зростання кількості кіберзагроз правопорушення в інформаційній сфері набувають транснаціонального характеру, що потребує системного правового, організаційного та технологічного реагування

Встановлено, що ефективність зарубіжних моделей забезпечується поєднанням кримінально-правових механізмів, адміністративного регулювання, стандартизації інформаційної безпеки, міжвідомчої координації та активної співпраці держави з приватним сектором. Особливу увагу приділено аналізу нормативно-правових актів та діяльності спеціалізованих органів кібербезпеки, які здійснюють моніторинг, запобігання та реагування на інформаційні загрози. Здійснено порівняльно-правову характеристику зазначених моделей і визначено їх ключові переваги та недоліки. Окреслено основні проблеми функціонування системи протидії правопорушенням в інформаційній сфері в Україні, зокрема недостатню координацію між суб'єктами забезпечення кібербезпеки, потребу в удосконаленні законодавства та низький рівень цифрової грамотності населення.

На підставі проведеного дослідження сформульовано пропозиції щодо адаптації зарубіжного досвіду в Україні, які полягають у впровадженні європейських стандартів захисту інформаційної інфраструктури, посиленні міжвідомчої взаємодії, удосконаленні механізмів превенції правопорушень та розвитку системи кіберосвіти. Зроблено висновок, що імплементація кращих міжнародних практик сприятиме підвищенню рівня інформаційної безпеки держави та зміцненню національної стійкості до сучасних інформаційних загроз.

Ключові слова: *інформаційна сфера, правопорушення в інформаційній сфері, кіберзлочинність, кібербезпека, інформаційна безпека, дезінформація, міжнародні стандарти.*

Постановка проблеми. Стрімкий розвиток інформаційно-комунікаційних технологій, глобалізація цифрового простору та активна інтеграція України до світового інформаційного середовища зумовили суттєве зростання кількості та складності правопорушень в інформаційній сфері. Кіберзлочинність, несанкціоноване втручання в роботу інформаційно-телекомунікаційних систем, поширення дезінформації, посягання на персональні дані та об'єкти критичної інформаційної інфраструктури становлять реальну загрозу національній безпеці, правам і свободам людини та стабільності функціонування державних інституцій.

Особливої актуальності зазначена проблема набуває в умовах збройної агресії проти України, коли інформаційна сфера використовується як інструмент гібридного впливу. Інформаційні атаки, кібершпигунство, втручання в діяльність державних органів та об'єктів критичної інфраструктури мають системний характер і часто здійснюються з-за меж національної юрисдикції, що ускладнює їх розслідування та притягнення винних осіб до відповідальності.

Незважаючи на наявність в Україні нормативно-правової бази у сфері кібербезпеки та протидії інформаційним правопорушенням, існують

проблеми фрагментарності правового регулювання, недостатньої координації між суб'єктами забезпечення інформаційної безпеки, а також невідповідності окремих положень національного законодавства сучасним міжнародним стандартам. Крім того, потребує вдосконалення система превенції правопорушень в інформаційній сфері та підвищення рівня цифрової грамотності населення. У зв'язку з цим виникає об'єктивна необхідність комплексного дослідження зарубіжного досвіду протидії правопорушенням в інформаційній сфері з метою визначення ефективних механізмів, які можуть бути імплементовані в національну правову систему. Вивчення кращих міжнародних практик дозволить сформувати науково обґрунтовані пропозиції щодо вдосконалення законодавства та організаційних механізмів протидії інформаційним загрозам в Україні.

Постановка завдання. Метою статті є комплексне дослідження зарубіжного досвіду протидії правопорушенням в інформаційній сфері шляхом аналізу правових, організаційних та інституційних моделей, що застосовуються у провідних державах і наднаціональних утвореннях, а також визначення можливостей і напрямів їх адаптації та використання в Україні.

Аналіз останніх досліджень і публікацій. Проблематику визначення зарубіжного досвіду протидії правопорушенням в інформаційній сфері у своїх наукових працях досліджували такі вчені, як: І. В. Арістова, К. І. Бєляков, В. В. Бєлєвцева, О. І. Воронкова, О. А. Заярний, С. С. Єсімов, К. Є. Ковальов, Л. П. Коваленко, М. В. Ковалів, Б. Д. Леонов, С. В. Міловідова, В. І. Олійник, В. Я. Настюк, С. М. Правдюк, О. М. Рєзнік, О. М. Солодка, В. В. Сидоренко, О. В. Чуприна, О.Ю. Шостко, О. Г. Ярема та інші.

Виклад основного матеріалу. Європейський вектор розвитку України та її послідовні євроінтеграційні прагнення об'єктивно зумовлюють необхідність гармонізації національної правової системи зі стандартами, зокрема у сфері забезпечення національної та інформаційної безпеки. Як стверджує С. В. Міловідова, організація діяльності із протидії правопорушенням повинна базуватися на безумовній повазі до фундаментальних прав і свобод людини та громадянина як визначальному критерії ефективності правозастосування. Такий підхід має універсальний характер і підлягає реалізації незалежно від процесуального статусу особи в адміністративно-деліктних правовідносинах [1, с. 129–130]. У контексті протидії правопорушенням в інформаційній сфері таке положення набуває особливого значення, оскільки баланс між потребами безпеки та гарантіями прав людини є ключовою ознакою демократичної правової держави.

Потреба у зверненні до зарубіжного досвіду зумовлена тим, що в умовах стрімкої цифровізації суспільних відносин інформаційний простір перетворюється на один із ключових вимірів національної безпеки. Відтак ефективність протидії правопорушенням у цій сфері значною мірою залежить від здатності держави застосовувати сучасні організаційно-правові механізми, апробовані у провідних демократичних країнах [2, с. 41]. Одним із базових принципів функціонування сектору безпеки у демократичних державах є забезпечення ефективного цивільного демократичного контролю за діяльністю відповідних органів, включаючи спеціальні служби. Зарубіжна практика демонструє наявність розвинених механізмів такого контролю, які дозволяють досягти оптимального балансу між необхідністю збереження державної та службової таємниці та вимогами прозорості й підзвітності безпекових інституцій [3, с. 159–160]. Запровадження подібних механізмів в Україні сприятиме підвищенню рівня суспільної довіри до правоохоронних органів і водночас посиленню гарантій законності у процесі реалізації ними владних повноважень.

Визначаючи коло держав, досвід яких є найбільш релевантним для України, доцільно враховувати різноманіття моделей організаційно-функціональної побудови служб безпеки, сформованих під впливом історичних, політичних, соціально-економічних та культурних чинників. У цьому контексті особливий науковий інтерес становить досвід держав Центральної та Східної Європи, що пройшли складний шлях трансформації сектору безпеки після завершення існування соціалістичних режимів. Їхній досвід є цінним насамперед через подібність стартових умов реформування та спільність стратегічних орієнтирів, пов'язаних із європейською інтеграцією [4, с. 575].

У контексті протидії правопорушення в інформаційній сфері інтерес викликає досвід Великої Британії щодо системи захисту інформації з обмеженим доступом. Важливим нормативним актом у цій сфері є Закон «Про державну таємницю» (Official Secrets Act 1989), який встановлює юридичну відповідальність за неправомірне розголошення відомостей, що стосуються діяльності служб безпеки та розвідки. Відповідно до його положень, працівник спеціальних служб, який без належних підстав розкриває інформацію

або документи, отримані у зв'язку з виконанням службових обов'язків, вчиняє правопорушення незалежно від форми такого розголошення – фактичної передачі даних чи створення умов для їх оприлюднення [5]. Характерною рисою британської системи тривалий час була багаторівнева класифікація урядової інформації, яка до 2014 року передбачала п'ять ступенів секретності. Надалі вона була трансформована у спрощену модель урядової політики безпекових класифікацій (Government Security Classifications Policy), що включає рівні Top Secret, Secret та Official із можливістю застосування додаткових дескрипторів залежно від сфери інформації (фінансової, політичної, медичної тощо). Слід констатувати, що британська модель протидії правопорушенням у сфері обігу інформації характеризується чіткою правовою регламентацією режиму секретності, ефективною системою класифікації даних, інституційною багаторівневістю захисту та розвинутими механізмами парламентського контролю.

Водночас інший підхід реалізовано у Швейцарії, де до повноважень муніципальної поліції (City Police) віднесено розгляд адміністративних правопорушень і проступків незначної тяжкості поряд з іншими суб'єктами адміністративного нагляду. Така модель дозволяє забезпечити оперативність реагування на правопорушення та розвантажити судову систему [6, с. 145].

Незважаючи на певну подібність процедур кримінального провадження та провадження у справах про адміністративні правопорушення в розвинених європейських державах, їх правове регулювання характеризується істотною варіативністю моделей і підходів. Передусім це проявляється у нормативних джерелах, які визначають порядок здійснення адміністративно-юрисдикційної діяльності правоохоронних органів. Так, у ряді держав відповідні процедури регламентуються нормами кримінального права (зокрема, у Данії та Франції), в інших – спеціалізованими кодифікованими актами про адміністративні проступки (Чехія, Польща), тоді як окремі країни застосовують змішану модель, що передбачає одночасне використання норм кримінального та адміністративно-деліктного законодавства (Естонія, Болгарія, Хорватія). Така багатоманітність свідчить про відсутність єдиного універсального підходу до правового реагування на деліктну поведінку та водночас демонструє прагнення держав забезпечити оптимальний баланс між ефективністю юрисдикційної діяльності й процесуальними гарантіями прав особи [7, с. 159–160].

Показовим є досвід Федеративної Республіки Німеччина, де адміністративно-деліктне законодавство має децентралізований характер і складається з кількох взаємопов'язаних елементів: Федерального закону «Про адміністративні правопорушення» (Gesetz über Ordnungswidrigkeiten – OWiG), офіційних тлумачень Федерального конституційного суду та нормативно-правових актів федеральних земель. Закон визначає критерії відмежування адміністративних правопорушень від злочинів – ступінь суспільної небезпеки, цінність об'єкта посягання, підвідомчість органів розгляду справ, вид юридичної відповідальності та характер санкцій – і передбачає такі заходи впливу, як адміністративний штраф, попередження або попередження із грошовим стягненням [8, с. 177–178].

Німецьке адміністративно-деліктне право охоплює як матеріальні, так і процесуальні норми, що регулюють досудове провадження в органах адміністративної юрисдикції та судовий розгляд відповідних справ. Попри високий рівень законодавчої техніки, його характерною рисою залишається некодифікованість у широкому розумінні, що пояснюється відносною новизною цієї підгалузі права та незавершеністю процесів її систематизації. Водночас особливістю німецької моделі є те, що адміністративні правопорушення фактично розглядаються як складова кримінального права, що підтверджено практикою Європейського суду з прав людини, зокрема у справі «Öztürk v. Germany», де наголошено на необхідності поширення на такі провадження основних кримінально-процесуальних гарантій – презумпції невинуватості, права на захист та інших стандартів справедливого судочинства.

Своєрідний підхід реалізовано в Естонській Республіці, де провадження у справах про адміністративні правопорушення інтегроване у ширшу систему так званого карального права, що зумовлює застосування загальних положень кримінального процесу до розгляду проступків. Законодавство цієї держави передбачає декілька видів провадження – попереджувальне, прискорене та загальне, – що відображає принцип процесуальної економії та дозволяє оптимізувати витрати ресурсів залежно від складності справи [9, с. 117–118].

Ефективність протидії правопорушенням в інформаційній сфері у провідних державах світу зумовлена поєднанням кримінально-правових, адміністративно-правових, організаційних та технологічних механізмів. Зарубіжні моделі протидії правопорушенням в інформаційній сфері, характеризуються високим рівнем інституційної коор-

динації, стандартизації вимог до інформаційної безпеки та активною співпрацею держави з приватним сектором. Можна виокремити такі моделі:

– ***Модель Сполучених Штатів Америки.*** Американська модель є однією з найбільш розвинених і орієнтована насамперед на оперативне реагування та кримінальне переслідування правопорушників. Особливостями цієї моделі є: жорсткі кримінальні санкції; активна участь спецслужб; тісна взаємодія з технологічними корпораціями; розвинена система публічно-приватного партнерства.

– ***Європейська модель.*** Європейський підхід ґрунтується на принципах гармонізації законодавства, стандартизації безпеки та превенції. Ця модель характеризується: обов'язковою оцінкою ризиків; системою повідомлення про кіберінциденти; значними штрафами за порушення (особливо у сфері захисту персональних даних); орієнтацією на превенцію.

– ***Модель Японії.*** Японія формує централізовану модель кіберзахисту з акцентом на державний контроль та підвищення кіберграмотності населення. Особливості японської моделі: державна стратегія кібербезпеки переглядається регулярно; активна взаємодія з приватним сектором; обов'язкові стандарти безпеки для операторів критичної інфраструктури; масштабні освітні програми.

– **Модель Ізраїлю.** Ізраїль вважається одним із світових лідерів у сфері кіберзахисту. Центральним органом є Israel National Cyber Directorate, який координує кібероборону держави. Особливості ізраїльської моделі: поєднання військових та цивільних інструментів; активна підтримка стартап-екосистеми кібербезпеки; раннє виявлення та нейтралізація загроз; потужна система підготовки фахівців.

– ***Модель Німеччини.*** У Німеччині ключову роль відіграє Federal Office for Information Security **(BSI)**, що здійснює технічний нагляд та координацію безпеки інформаційних систем. Особливості: суворі вимоги до операторів критичної інфраструктури; регулярні аудити безпеки; обов'язкове повідомлення про інциденти; чітке нормативне регулювання цифрових сервісів [10, с. 123–124].

Зарубіжні моделі демонструють, що ефективна протидія правопорушенням в інформаційній сфері можлива лише за умов системного підходу, що поєднує правові, організаційні та технологічні механізми. Найбільш результативними є ті держави, які розвивають не лише каральні інструменти, а й превентивні механізми, стандартизацію та партнерство з приватним сектором. Саме такий комплексний підхід може бути орієнтиром для подальшого вдосконалення національної системи інформаційної безпеки України.

Варто також зазначити, що в окремих країнах адміністративно-юрисдикційні провадження правоохоронних органів обмежуються стадією фіксації правопорушення та підготовки матеріалів із подальшою передачею їх до суду. В інших, автономні адміністративні провадження взагалі не виділяються, оскільки основна функція правоохоронних органів полягає не у притягненні особи до адміністративної відповідальності, а у забезпеченні публічного порядку та превенції правопорушень [11, с. 15].

Таким чином, європейська практика демонструє наявність різних моделей правового реагування на делікти – від їх криміналізації до адміністративного врегулювання. Використання цих підходів із урахуванням національних правових традицій та сучасних безпекових викликів сприятиме підвищенню ефективності оперативно-службової діяльності СБ України та формуванню більш адаптивної системи протидії правопорушенням в інформаційному просторі. У контексті вдосконалення діяльності СБ України щодо протидії адміністративним правопорушенням в інформаційній сфері наведений зарубіжний досвід має суттєве методологічне значення [12, с. 115–116]. Передусім він свідчить про доцільність: посилення інституційної взаємодії між суб'єктами безпеки та правоохоронними органами; розвитку спрощених процедур реагування на правопорушення невеликої тяжкості в інформаційному середовищі; нормативного уточнення співвідношення кримінальної та адміністративної відповідальності у сфері інформаційної безпеки; розширення повноважень уповноважених органів щодо припинення правопорушень без надмірної судової формалізації.

Висновки. Проведене дослідження засвідчує, що правопорушення в інформаційній сфері є однією з найбільш динамічних і небезпечних загроз сучасному суспільству, оскільки вони безпосередньо впливають на національну безпеку держав, стабільність функціонування публічних інституцій, економічну безпеку, а також на реалізацію і захист прав та свобод людини. Зарубіжний досвід протидії таким правопорушенням переконливо доводить, що ефективність державної політики у цій сфері залежить не від окремих правових чи організаційних заходів, а від цілісної, багаторівневої та скоординованої системи реагування на інформаційні загрози.

Аналіз моделей Сполучених Штатів Америки, Європейського Союзу, Японії, Ізраїлю та окремих європейських держав показав, що спільними рисами успішних систем протидії є наявність чіткої нормативно-правової бази, функціонування спеціалізованих органів кібербезпеки, запровадження обов'язкових стандартів захисту інформаційних ресурсів і критичної інфраструктури, а також ефективна міжвідомча координація. Важливе значення у зарубіжних моделях надається превентивним заходам, ранньому виявленню кіберзагроз, системі обов'язкового інформування про кіберінциденти та активній співпраці держави з приватним сектором, який володіє значною частиною інформаційних ресурсів.

Водночас встановлено, що українська система протидії правопорушенням в інформаційній сфері, незважаючи на наявність базових правових і інституційних елементів, потребує подальшого вдосконалення. Серед ключових проблем виокремлено фрагментарність правового регулювання, недостатній рівень координації між суб'єктами забезпечення інформаційної та кібербезпеки, відсутність єдиних обов'язкових стандартів захисту інформаційних систем, а також обмежену увагу до питань превенції та підвищення цифрової грамотності населення.

Список літератури:

1. Міловідова С. В. Попередження та протидія адміністративним правопорушенням в Україні. дис. … канд. юрид. наук: 12.00.07. Київ, 2016. 231 с.

2. Солодка О. М. Інформаційний простір держави як сфера реалізації інформаційного суверенітету. *Інформація і право*. 2020. № 4 (35). С. 39–46. DOI: https://doi.org/10.37750/2616-6798.2020.4(35).221216

3. Рєзнік О. М. Адміністративно-правові засади діяльності правоохоронних органів із забезпечення фінансово-економічної безпеки України: монограф. Суми, 2018. 475 с.

4. Воронкова О. І. Інформаційна сфера України в умовах сталого розвитку. *Юридичний науковий електронний журнал*. 2024. № 11. С. 574–579. DOI: https://doi.org/10.32782/2524-0374/2024-11/135

5. Official Secrets Act 1989. URL: https://www.legislation.gov.uk/ukpga/1989/6

6. Колодяжний М. Г. Стратегія зменшення можливостей учинення злочинів: зарубіжні реалії, перспективи запровадження в Україні : монографія. Харків : Право, 2018. 228 с.

7. Ковалів М. В., Єсімов С. С., Ярема О. Г. Інформаційне право України : навч. посіб. Львів : Львів. держ. ун-т внутр. справ, 2022. 416 с. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/4844?utm_source=chatgpt.com

8. Шостко О. Ю. Аналіз ефективної діяльності системи кримінальної юстиції у сфері протидії організованій злочинності в окремих європейських країнах. *Проблеми законності.* 2009. № 1. С. 176–185.

9. Ковальов К. Є., Леонов Б. Д. Забезпечення охорони державної та службової таємниці у сфері оперативно-розшукової діяльності за законодавством окремих держав: порівняльний аналіз. *Інформація і право.* 2017. № 1 (20). С. 115–125.

10. Олійник В. І. Досвід кримінально-правового забезпечення охорони державної таємниці країн близького зарубіжжя. *Юридична наука.* 2020. № 12. С. 122–125.

11. Арістова І. В. Національний механізм реалізації цілей сталого розвитку в умовах інформаційного суспільства в Україні: роль юридичного механізму та його складових. Монографія: Сучасна парадигма публічного та приватного права в умовах сталого розвитку. *Scientific monograph*. Vol. 1. Riga, Latvia: Baltija Publishing, 2023. P. 1–31 DOI: 10.30525/978-9934-26-331-6-1.

12. Коваленко Л. П. Інформаційне право: підручник. Київ: Видавничий дім «Гельветика», 2022. 284 с. URL: https://jurkniga.ua/informatsiyne-pravo-pidruchnik?utm_source=chatgpt.com

Maziychuk V. A. FOREIGN EXPERIENCE OF COMBATING INFORMATION OFFENSES AND POSSIBILITIES OF ITS USE IN UKRAINE

The article provides a comprehensive analysis of foreign experience of combating information offenses and identifies possibilities of its use in Ukraine, taking into account modern security challenges. It is emphasized that information offenses are one of the most dynamic and dangerous threats to modern society, since they directly affect the national security of states, the stability of the functioning of public institutions, economic security, as well as the implementation and protection of human rights and freedoms. It is substantiated that in the conditions of digitalization of society and the growth of the number of cyber threats, offenses in the information sphere are becoming transnational in nature, which requires a systematic legal, organizational and technological response.

It is established that the effectiveness of foreign models is ensured by a combination of criminal law mechanisms, administrative regulation, standardization of information security, interagency coordination and

active cooperation of the state with the private sector. Particular attention is paid to the analysis of regulatory legal acts and the activities of specialized cybersecurity bodies that monitor, prevent and respond to information threats. A comparative legal characteristic of the above models is carried out and their key advantages and disadvantages are identified. The main problems of the functioning of the system for combating offenses in the information sphere in Ukraine are outlined, in particular, insufficient coordination between entities providing cybersecurity, the need to improve legislation and the low level of digital literacy of the population.

Based on the research, proposals have been formulated for adapting foreign experience in Ukraine, which consist in implementing European standards for protecting information infrastructure, strengthening interdepartmental cooperation, improving mechanisms for preventing offenses and developing a cyber education system. It was concluded that the implementation of best international practices will contribute to increasing the level of information security of the state and strengthening national resilience to modern information threats.

Keywords: *information sphere, offenses in the information sphere, cybercrime, cybersecurity, information security, disinformation, international standards.*

Дата першого надходження статті до видання: 18.02.2026
Дата прийняття статті до друку після рецензування: 20.03.2026
Дата публікації (оприлюднення) статті: 11.05.2026