УДК 340.1
DOI https://doi.org/10.24144/2788-6018.2023.02.4

ПОШИРЕННЯ ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ ЗА ПРАВОПОРУШЕННЯ В МЕРЕЖІ ІНТЕРНЕТ В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ

Загребельна Н.А.,
кандидат юридичних наук, доцент кафедри теорії та історії держави і права ВНЗ «Університет економіки та права «КРОК»
https://orcid.org/0000-0002-3390-7149

Загребельна Н.А. Поширення юридичної відповідальності за правопорушення в мережі Інтернет в умовах воєнного стану в Україні.

У статті досліджується сучасний стан та тенденції розвитку в питанні поширення юридичної відповідальності за правопорушення в мережі Інтернет. Воно є актуальним, оскільки наша країна живе в умовах повномасштабного вторгнення загарбників і постійно перебуває в умовах не лише воєнного захисту, а й на терені захисту в інформаційному просторі. Постійний розвиток та діджиталізація всіх ланок життя потребують наявності чіткої системи захисту суспільства й індивідуума зокрема, попередження та встановлення відповідальності за вчинення відповідних протиправних діянь.

У статті виявлено основні недоліки та запропоновано шляхи вирішення проблем у питанні відповідальності й порушення законів у мережі Інтернет. Проведено аналіз статистики таких правопорушень та зроблено висновки, що допоможуть їх попередити. Сучасний стан розвитку суспільства нерозривно пов'язаний з тенденціями в різних сферах людської діяльності. Соціум стає повністю залежним від інформаційної складової. Сьогодні без комп'ютерних та мережевих технологій важко уявити найпростіші завдання, які постають перед нами. Діджиталізація не оминула й правову науку. За останні 20 років з'явилися нові правові норми, що регулюють юридичні відносини у сфері інформаційних технологій. У карних та адміністративних законах розширено кількість протиправних діянь у мережі Internet.

Водночас, такі тенденції розкривають прогалини, через які кіберзлочинці стають безкарними навіть при відкритій протиправності свого діяння. Для боротьби з кібершахраями в багатьох країнах створюються спеціальні підрозділи і структури. Поштовхом до створення та вдосконалення системи протидії кіберзлочинам стало підписання у 2001 році "Конвенції про кіберзлочинність", що розкрила й пояснила основні правові засади таких злочинів, встановила рамки юридичної відповідальності за їх порушення. В Україні положення Конвенції було ратифіковано у 2005 році.

Ключові слова: правопорушення, мережа Інтернет, кіберзлочин, інфопростір, діджиталізація, інформаційний злочин.

Zahrebelna N.A. The spread of legal responsibility for offenses on the Internet in the conditions of martial law in Ukraine.

The article examines the current state and development trends in the issue of the spread of legal responsibility for offenses on the Internet. It is relevant because our country lives in the conditions of a full-scale invasion of invaders and is constantly in conditions not only of military protection, but also in the field of protection in the information space. Continuous development and digitization of all areas of life require a clear system of protection of society and the individual, in particular, prevention and establishment of responsibility for the commission of relevant illegal acts.

The article identifies the main shortcomings and suggests ways to solve problems in the issue of responsibility and violation of laws on the Internet. An analysis of the statistics of such crimes was carried out and conclusions were drawn that will help prevent them. The current state of social development is inextricably linked with trends in various spheres of human activity. Society becomes completely dependent on the information component. Today, without computer and network technologies, it is difficult to imagine the simplest tasks we face. Digitalization has not bypassed legal science either. Over the past 20 years, new legal norms regulating legal relations in the field of information technologies have appeared. Criminal and administrative laws have expanded the number of illegal acts on the Internet.

At the same time, such trends reveal loopholes through which cybercriminals become unpunished even when their actions are openly illegal. Special units and structures are being created in many countries to combat cyber fraudsters. The impetus for the creation and improvement of the cybercrime

countermeasure system was the signing of the «Cybercrime Convention» in 2001, which disclosed and explained the basic legal principles of such crimes and established the framework of legal responsibility for their violation. In Ukraine, the provisions of the Convention were ratified in 2005.

Keywords: crime, Internet, cybercrime, infospace, digitalization, information crime.

Постановка проблеми. Основною проблемою недосконалості сучасної правової системи в питанні кібербезпеки є те, що ця галузь розвивається блискавично. А консервативна бюрократична машина інституту правової відповідальності не встигає за цими змінами. Правові інститути не можуть розробити чітких дієвих правил поведінки для охоплення всього розмаїття кіберзлочинів, оскільки розроблені раніше правила вже не є дієвими, так як наразі інший бік таких правопорушень вийшов на новий рівень, що випереджає всі попередні напрацювання правових інституцій.

Аналіз останніх досліджень і публікацій. Розмаїття варіацій і характер інфоправопорушень зумовили написання та висвітлення значної кількості публікацій на дану тему. Цим питанням приділено увагу науковцями різних правових підгалузей. Українська теоретична наука почала досліджувати це питання з 90-х років XX століття. Виокремлюються праці Д. Азарова, Н. Ахтирської, В. Бутузова, В. Гавловського, В. Голубєва, Р. Калюжного, В. Цимбалюка та ін.

Мета статті – виділити аспекти й види мережевих правопорушень та зазначити, як держава реагує на зміни в цьому питанні, викликані воєнним станом.

Виклад основного матеріалу. Сучасна наукова дефініція протиправного діяння в інформаційному просторі визначена терміном "інформаційний злочин". Ним вважається будь-яка протизаконна дія, що має на меті розкраданняабоування інформації в інформаційних системах і мережах, які виходять з корисливих або хуліганських спонукань" [2].

Обов'язковим елементом такого діяння має бути використання при їх вчиненні комп'ютерів чи інших обчислювальних засобів і машин. Вони є анонімними, високотехнологічними (потребують наявність спеціалізованої техніки, доступу до мережі Інтернет) та не мають вікових або гендерних обмежень. Ще однією відмінною рисою вважається латентність як зі сторони злочинців, так і зі сторони, яка є потерпілою. Це пов'язано з тим, що далеко не завжди гарантується притягнення до відповідальності, а також з тим, що потерпіла сторона інколи не бажає розкривати свої безпекові моменти та, таким чином, сприяти падінню рівня власної репутації перед своїми клієнтами.

Аналізуючи судову практику в сфері інформаційних злочинів за останні два десятиліття, можна виділити декілька найбільш типових інфоправопорушень:

- здійснення операцій з електронними грошима без відповідної ліцензії;

- викрадення персональних даних. Це може бути брутфорс (шляхом програмного підбору комбінації пароля), втручання в роботу корпоративних серверів, операції з інтернет-магазинами з виведенням коштів через банківську систему, кардинг, фішинг та інші;

– підробка платіжних карток – створення дублікатів та їх використання для здійснення незаконних платежів. Схема відмивання така: платіжна картка – подарунковий сертифікат – криптовалюта – гроші. Це дозволяє швидко і майже безслідно проводити операції;

– торгівля через мережу Інтернет наркотичними речовинами. У таких схемах "мимовільними помічниками" є соцмережі як платформи для рекламування та збуту товару, поштові оператори, через які відбувається пересилання, і банківські установи, що переводять безготівкові кошти в готівку;

– передача даних, пов'язаних зі службовою діяльністю. Їх суб'єктами виступають посадовці різних органів та установ, які за грошову винагороду передають інформацію, бази даних третім особам через мережу Інтернет;

– інформаційне шахрайство – через розсилання так званих "нігерійських листів", створення фейкових інтернет-магазинів чи фінансових пірамід, діяльність фіктивних брокерських фірм та інше [2];

– здійснення кібератак на сервери установ, підприємств та організацій;

– організація інтернет-казино.

Міжнародне співтовариство ще в 1991 році класифікувало кіберзлочини за певними групами, давши їм певні класифікаційні абревіатури: QA – несанкціонований доступ, QDT – троянський кінь, QAT – крадіжка часу, QDV – комп'ютерний вірус, QD – зміна комп'ютерних даних, QFC – шахрайство з банкоматами, QF – комп'ютерне шахрайство, QZ – інші комп'ютерні злочини, QR – незаконне копіювання, QFT – телефонне шахрайство, QS – комп'ютерний саботаж, QFF – комп'ютерна підробка [1].

Усе більшого поширення набувають також такі правопорушення, як розповсюдження дитячої порнографії, роздмухування проявів ксенофобії й расизму, комп'ютерне піратство з програмним забезпеченням, мальваре, рефайлінг та інші. Вони активно прогресують і їх важко відслідковувати, попередити й зупинити. Для кіберзлочинців немає ніяких перешкод, ні стін, ні замків чи сховищ, якщо те, за чим вони "полюють", знаходиться в інфовимірі.

Задля збільшення протидії та визначення відповідальності за наслідки інфозлочинів законо-

давча гілка влади в Україні розробила декілька нормативно-правових і підзаконних актів (далі – НПА). Основою є Конвенція про кіберзлочинність (з усіма її протоколами та роз'ясненнями), Кримінальний кодекс України (далі – ККУ), а також деякі інші НПА.

Для узагальнення всіх злочинів у мережі Інтернет у ККУ виокремлено Розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», а саме:

- стаття 361 – Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;

стаття 361-1 – Передбачає покарання за створення та розповсюдження вірусів, незалежно від мети таких дій [5];

стаття 362 – Несанкціоновані дії з інформацією, що оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї [5];

стаття 361-2 – Передбачає санкції за зловживання правом доступу до інформації [5].

Окремо слід також звернути увагу на такі статті з ККУ, що також стосуються теми:

– стаття 176 – Порушення авторських та суміжних прав [5].

До них слід віднести такий приклад, як інсталяція ліцензійних програмних продуктів в обхід інтегрованих систем захисту за допомогою "кряків" чи патчів;

– статті 190 та 209 – шахрайство та легалізація [5].

Здійснюються через фіктивні інтернет-магазини чи псевдопрацівників банків.

Головною проблемою притягнення до відповідальності за вчинення правопорушень у мережі Інтернет є те, що майже відсутній дієвий процесуальний механізм їх розгляду. Тому вони розглядаються довго та інколи не доходять до фінальної крапки – винесення обвинувального висновку. Періодично кримінальні справи перекваліфіковуються в цивільні й розглядаються як неналежне виконання умов цивільно-правових угод.

Не менш складним є питання винесення вироків за порушення основ безпеки чи тероризму, адже досить важко виокремити суб'єкта злочину, тобто саме ту особу, саме ту техніку, з якої проводилися протиправні дії. Треба проводити низку дороговартісних та довготривалих судових експертиз.

Проблемним є й питання притягнення до відповідальності за доведення до самогубства через Інтернет. Саме зараз проводяться дискусії щодо внесення відповідних змін до статті 120 ККУ для розширення складу злочину, оскільки зараз практично неможливо покарати за це небезпечне явище.

Аналіз судової практики показує, що майже 80% справ щодо інформаційних правопорушень закінчуються або укладенням угоди обвинувачених зі слідством, або призначенням у вигляді покарання випробувального терміну чи штрафу. Лише близько 15% справ було доведено до тюремних ув'язнень. Це доводить, що держава не сприймає належно ту небезпеку, яку несуть у собі такі злочини.

Проблемою під час розгляду кіберспрaв є також те, що судді при винесенні висновку щодо обмеження доступу до інформації спираються лише на інформацію, надану судовими експертами, а не на власний аналіз стану справи. Вони не розуміються на тонкощах того чи того матеріалу, як прийнято за міжнародними правовими стандартами, не аналізують вплив інформації на суспільство. Не завжди враховують обсяг поширення та кількість аудиторії, залученої до інформації. Рішення все одно буде однаковим. Лише в окремих випадках перевіряється факт припинення протиправної діяльності та видаляється незаконний контент після вироку суду.

На сьогодні в Україні спостерігається динаміка до швидкого зростання кіберзлочинів. Найбільше зростання шахрайств. Щороку кількість виявлених фактів збільшується вдвічі, не краща динаміка і щодо злочинів з обігом документів та платіжних карток [4].

Так, наприклад, шахрайства в банківській сфері за 2021 рік перетнули позначку 2000 справ, а ще в 2010 році їх фіксувалося не більше 1000. Зростає й "вилов" шахраїв. Якщо в 2015 році такими діями було привласнено 25 млн грн, то в 2021 році ця сума складає більше 100 млн грн. Однак, завдяки високим показникам розкриття біля 80% вкраденого вдається зберегти та повернути власникам. Гірша ситуація з розкриттям у таких сферах, як кардинг, поширення порнографії й порушення авторських прав [5].

Такий стан речей з розкриттям правопорушень у мережі Інтернет пов'язаний з тим, що в Україні ми маємо досить розвинену та непогано кваліфіковану мережу спеціалістів. Проте вони, з одного боку, є розробниками систем захисту, ПЗ й антивірусних програм, які дозволяють захистити ресурси та інформацію чи виявити порушників, а з іншого - саме знання таких "спеціалістів" і є допоміжним фактором для розробки шкідливого ПЗ з метою обходу систем захисту або розповсюдження незаконного контенту в мережі.

За останні роки українське судочинство засуджувало до відповідальності за інфоправопорушення за такими статтями ККУ:

– дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади;

– посягання на територіальну цілісність і недоторканність;

– державна зрада;

– перешкоджання законній діяльності Збройних Сил та інших військових формувань;

– публічні заклики до вчинення терористичного акту;

– пропаганда війни [5].

Причому посягання на територіальну цілісність і недоторканність України та дії, спрямовані на насильницьку зміну чи повалення конституційного ладу, склали 85% (123 вироки) від загальної кількості.

Значна роль у загальному обсязі злочинів у інфопросторі приділяється соціальним мережам, особливо Telegram та платформі META. На їх "просторах" вчиняється більше 70% злочинів. На "третьому" місці за розповсюдженням незаконної інформації та вчиненням протиправних дій є мережа Youtube. Через неї поширювалося близько 7% незаконного контенту.

Аналіз також показує особистісний характер злочинів, оскільки з 95% випадків на лаві підсудних знаходився один обвинувачений. Також факт доводить, що близько 7% судових рішень підтверджували зв'язок підсудного з державою-агресором при вчиненні суспільно-небезпечних діянь [4].

Особливого значення набувають питання захисту в умовах воєнного стану, в якому зараз перебуває Україна. Такий статус зумовлює необхідність розробки більш дієвих методів боротьби, а також надання достовірної інформації суспільству про стан речей у військовому, гуманітарному та міжнародному напрямках.

За час з 24 лютого 2022 року відбулася реструктуризація та закриття деяких державних сервісів щодо надання інформації, аби убезпечити суспільство від дезінформації. Указ Президента України «Про введення воєнного стану в Україні» №64/2022 (затверджено Законом України «Про затвердження Указу Президента України «Про введення воєнного стану в Україні» реєстр. № 2102-IX від 24.02.2022) тимчасово обмежив деякі конституційні права та свободи громадян і юридичних осіб щодо доступу до інформації.

Упроваджено додатковий контроль за контентом, обмежено доступ до пропагандистських російських та білоруських ресурсів на території України, заборонено використання персональних радіостанцій у військових цілях. Цей перелік оновлюється і розширюється.

Для адаптації до нових умов воєнного часу було внесено корективи до чинного Кримінального та Кримінального процесуального кодексів: Закон України "Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану" від 24.03.22 року (далі - Закон № 2160-IX).

Він заборонив через Інтернет поширювати інформацію про дислокацію та переміщення військових ЗСУ й інших військових формувань із зазначенням конкретної міри покарання - позбавлення волі на строк від 5 до 8 років. При наявності додаткових обтяжуючих обставин (групова змова, корисливий мотив, тяжкі наслідки) - строк до 12 років. Під заборону потрапило поширення відео чи фотофіксацію ракет, роботи ППО та місць влучання снарядів чи обстрілів.

Новостворeним державним органом Кіберполіцією за останній рік розроблено Telegram чат-бот для блокування сервісів дезінформації, який блокує підсанкційні Telegram-канали, YouTube-канали, Facebook-групи, Instagram-профілі, що розповсюджують вищеназвану інформацію.

Держава розробила також нові процесуальні положення, які стосувалися дій усіх гілок влади в умовах воєнного стану. Зміни викладено в таких Законах: «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» № 2137-IX від 15.03.2022, а також «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» № 2149-IX від 24.03.2022.

За період війни значно зросла кількість кібератак на об'єкти державної та критичної інфраструктури. Здебільшого у вигляді розповсюдження комп'ютерних вірусів і намаганнями зламу систем захисту для отримання повного доступу до керування цими об'єктами. Саме Закон 2149-IX направлено на посилення безпеки від кіберзагроз.

Відбулося посилення відповідальності за розповсюдження або збут шкідливих програм (ч. 1 ст. 361-1 ККУ). Змінився і склад злочину за ч. 1 ст. 361 ККУ. Тепер не треба наявності шкідливих наслідків, що суттєво спрощує настання кримінальної відповідальності. Додано нові склади злочинів:

– дії, передбачені частиною 1 або 2 цієї статті, якщо вони призвели до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення порядку її маршрутизації (ч. 3 ст. 361 ККУ);

– дії, передбачені частиною 1 або 2 цієї статті, якщо вони створили небезпеку тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших наслідків (ч. 4 ст. 361 ККУ);

– дії, передбачені частиною 3 або 4 цієї статті, вчинені під час дії воєнного стану (ч. 5 ст. 361 ККУ).

Закон 2149-IX також передбачає відсутність складу злочину та визначення і визнання стороннього втручання в систему та мережу непротиправним, якщо воно здійснювалося згідно з затвердженим порядком пошуку й виявлення потенційних вразливостей таких систем чи мереж Держспецзв'язку.

Зміни в ККУ були похідними від тих змін, які були внесені до КПКУ (Закон № 2137-IX від 15.03.2022). Завдяки ньому впроваджено зміни, що значно підвищили ефективність кримінального провадження кіберзлочинів. Закон тепер дозволяє накладення арешту на техніку та системи, які використовувалися для несанкціонованого доступу чи були отримані в результаті протиправної діяльності незалежно від будь-яких обмежень ззовні (ст. 170 КПК). За абз. 2 ч. 6 ст. 236 КПК органам слідства дозволено отримувати вільний доступ до техніки та систем, якщо на них є значуща для слідства інформація. Слідчі органи або прокуратура з відображенням своїх дій у відповідному протоколі можуть проводити фото- та/або відеоогляд комп'ютерних даних (ч. 2 ст. 237 КПК) та знімати показання технічних приладів і технічних засобів (ст. 245-1 КПК).

Це лише вибірковий аналіз змін, що вплинули на нововведення в питанні правопорушень у мережі Інтернет, але й ці факти підтверджують системний підхід до реалій сьогодення. Усі законодавчі зміни дозволяють підвищити кримінально-правове забезпечення питань кібербезпеки та мережі Інтернет. Нові закони значно розширили повноваження слідчих органів у питанні злочинів у мережі Інтернет, а посилення санкцій чинить психологічний вплив на попередження майбутніх злочинів.

Резюмуючи зміни, слід виокремити певні рекомендації для органів влади, їх посадовців та громадян щодо майбутніх дій в умовах воєнного стану в питанні правопорушень у мережі Інтернет і для забезпечення кібербезпеки:

– необхідно мати у штаті кваліфікованих спеціалістів у цій галузі, що значно підвищить ступінь захисту від протиправних діянь;

– проводити постійні інструктажі працівників щодо дій у мережі Інтернет;

– проводити моніторинг офіційних повідомлень системи CERT-UA та Держспецзв'язку;

– повідомляти відповідні органи про факт виникнення протиправного діяння та осіб, постраждалих від цього.

Це дозволить притягнути винних до відповідальності й блокування поширення наслідків протиправного діяння в подальшому.

Висновки. Підсумовуючи сказане, зазначимо, що протиправними діяннями в мережі Інтернет є ті, що особа вчиняє з використанням комп'ютерних систем та ЕОМ у мережі Інтернет і мережі електрозв'язку.

Специфіка правопорушень у мережі Інтернет та їх динамічне зростання, як у кількості, так і в складності, дозволяє стверджувати, що такі правопорушення є нагальними та становлять достатньо велику загрозу не лише для особистості, а й для загальної суспільної безпеки. Обов'язковим "атрибутом" таких злочинів є корисливий мотив. А основна задача державних органів - розробити дієві механізми для попередження, виявлення, дослідження та притягнення до відповідальності за вчинення таких злочинів. Без подальшого вдосконалення цієї ніші неможливий стабільний і безпечний розвиток та функціювання держави загалом й її окремих механізмів та інституцій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Конвенція про кіберзлочинність: міжнародний документ від 23.11.2001. URL: http://zakon.rada.gov.ua.
2. Правдюк С.А. Класифікація інформаційних правопорушень. *Порівняльно-аналітичне право.* URL: http://www.pap.in.ua.
3. Основи інформаційної безпеки України: навч. посіб. / за заг. ред. А.І. Марущака. К.: Наук.-вид. центр НА СБ України, 2013. 388 с.
4. Статистика МВС України: стан та структура злочинності. URL: http://mvs.gov.ua.
5. Кримінальний кодекс України від 5 квітня 2001 року. *Відомості Верховної Ради України.* 2001. № 25-26. URL: http://zakon3.rada.gov.ua/laws/show/2341-14.
6. Незаконні дії з банківськими документами та платіжними картками. Велика українська юридична енциклопедія: у 20 т. / відп. ред. В.Я. Тацій. Харків : Право, 2017. Т. 17. С. 589.
7. Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до Законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану: Закон України від 24.03.2022 № 21600-IX. URL: https://ips.ligazakon.net/document/view/t222160?an=1&ed=2022_03_24.