Юркевич І. І.
доктор філософії у галузі права,
доцент кафедри кримінального права та процесу
Західноукраїнського національного університету

ПРАВОВЕ РЕГУЛЮВАННЯ БОРОТЬБИ З КІБЕЗЛОЧИННІСТЮ : ПОРІВНЯЛЬНИЙ АНАЛІЗ ЗАКОНОДАВСТВА РІЗНИХ КРАЇН

Поступова трансформація життя багатьох людей у віртуальний простір й розширення можливостей та способів застосування технологій дають змогу спрощувати роботу й допомагати у повсякденні. Проте, мережа Інтернет стає також й новим майданчиком діяльності злочинців, що використовують технологічні можливості для вчинення крадіжок, шахрайства, переслідувань, вимагання та інших кримінальних правопорушень уже в новому форматі. Зважаючи на розповсюдження кіберзлочинності та небезпечні наслідки, які вона несе, кожна держава повинна криміналізувати такий тип правопорушень та врегулювати порядок протидії й запобігання ним.

Кіберзлочинність як явище є закономірним, зважаючи на розвиток інформаційно-телекомунікаційних технологій. Задля захисту прав, свобод та інтересів людини в кіберпросторі, а також забезпечення відповідної безпеки в суспільстві та державі, в Україні прийнято Закон України «Про основні засади забезпечення кібербезпеки України». Пунктом 8 частини 1 статті 1 згаданого Закону встановлено поняття кіберзлочин (комп'ютерний злочин) як «суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України» [1].

Оскільки з своєю сутністю кіберзлочин охоплює доволі різносторонні кримінальні правопорушення, їх класифікація є необхідною для ефективної протидії. Положеннями Конвенції про кіберзлочинність від 23.11.2001 та Додатковим протоколом до даної Конвенції від 28.01.2003 виділено наступні види кіберзлочинів [2; 3]:

1. Скоєні проти конфіденційності, цілісності комп'ютерних даних і систем. До такої групи відносяться як незаконний доступ й незаконне перехоплення, так і втручання в систему чи дані.

2. У яких комп'ютер використовується правопорушником як засіб скоєння злочину чи вчинення маніпуляцій з інформацією). До таких злочинів слід відносити комп'ютерне підроблення та комп'ютерне шахрайство.

3. Стосуються контенту, який собою являє певний вміст даних, розміщених у комп'ютерних мережах. Таку групу в основному складають злочини пов'язані з дитячою порнографією.

4. Такі, що порушують авторське і суміжні права, проте безпосереднє віднесення певних діянь до такої групи злочинів здійснюється державами самостійно.

5. Злочини, які собою являють акти расизму та ксенофобії скоєні за допомогою комп'ютерних мереж.

Протидія ж кіберзлочинності має місце у більшості країн світу, задля чого створюються відповідні установи. Так, у державах ЄС активно діють дві групи спеціальних органів з боротьби з кіберзлочинністю. Частина з них розробляють та реалізовують відповідні національні стратегії. Інші ж суб'єкти в свою чергу здійснюють безпосередні роботу з запобігання та розслідування скоєних у кіберпросторі правопорушень [4, с. 183].

В Україні ж, за приписами Закону України «Про основні засади забезпечення кібербезпеки України», існують органи, які: координують та здійснюють організацію боротьби з кіберзлочинністю (Президент України через очолювану ним Раду національної безпеки і оборони України), розробляють відповідні стратегії та сприяють їх реалізації (Кабінет Міністрів України), безпосередньо здійснюють заходи із забезпечення кібербезпеки (окремі міністерства, правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності, Збройні Сили України, місцеві державні адміністрації, органи місцевого самоврядування та інші суб'єкти, визначені законом) [1].

Якісна та ефективна протидія кіберзлочинності є завданням усього міжнародного співтовариства, з огляду на те, що кіберзлочини можуть вчинятися на території не лише однієї країни, до злочинних угруповань можуть входити громадяни різних держав, а кібератаки можуть спрямовуватись на доволі широке суспільне коло.

Міжнародне співробітництво є критичною необхідністю для усунення правових невідповідностей, що виникли у зв'язку з динамічним розвитком інформаційних технологій. Реакція держав на сучасні кіберзагрози в законодавчому полі є не співмірною з наявними небезпеками. Так, для покращення ситуації міжнародне співробітництво спрямовується на зміцнення довіри у сфері кібербезпеки, розробка спільного підходу до протидії кіберзагрозам, здійснення ефективнішого попередження кіберзлочинності. Окремо також варто виділити ще одну спільну ціль – оптимізація надання міжнародної технічної допомоги, що виявляється у безпосередній співпраці національних та міжнародних органів та [5, с. 52].

Необхідно звернути увагу, що деякі акти, які мають на меті боротьбу з кіберзлочинністю, утворення нових міжнародних організацій, є таким що самі несуть загрозу. Так, 28 грудня 2019 року Генеральна Асамблея ООН схвалила резолюцію про боротьбу з кіберзлочинністю, яка б мала набути чинності в серпні 2020 року, однак США, Канада, країни Європи, а особливо Україна, виступили проти, вважаючи, що запропонована ініціатива може призвести до встановлення інтернет-цензури та обмеження свободи слова в глобальних мережах. Також, США заявили, що прийнята резолюція може підірвати усю міжнародну співпрацю проти кіберзлочинності [5, с. 54].

Тому варто не забувати, що міжнародна співпраця з метою забезпечити безпеку у кіберпросторі повинна захищати основоположні права людини й не

суперечити базовим принципам гармонійного співіснування.

Кіберзлочини як закономірне соціальне явище, що виникло у відповідь на розвиток інформаційно-телекомунікаційних технологій, являє собою кримінально карну діяльність осіб, що вчинена за допомогою комп'ютерів, мережі Інтернет чи інших відповідних технологій. Такі правопорушення можуть завдавати шкоди різним аспектам життя людини, суспільства чи держави, проте кожний злочин є небезпечним. З метою запобігання держави розробляють стратегії протидії кіберзлочинності та забезпечення кібербезпеки, а міжнародне співтовариство приймає необхідні правові акти. При цьому, варто не забувати, що для ефективного попередження та виявлення кіберзлочинності необхідно постійно вдосконалювати методи боротьби з нею та розвивати державну політику у даній галузі.

Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 19.03.2023 р.).
2. Конвенція про кіберзлочинність: Конвенція від 23.11.2001. *Рада Європи*. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення 19.03.2023 р.).
3. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : Протокол від 28.01.2003. *Рада Європи.* URL: https://zakon.rada.gov.ua/laws/show/994_687#Text (дата звернення 19.03.2023 р.).
4. Лугіна Н.А., Лучук А.М. Порівняльний аналіз вітчизняного та європейського законодавства з питань запобігання кіберзлочинності. Ірпінський юридичний часопис. 2023. № 1 (10). С. 180-186.
5. Шуліченко М.В. Міжнародно-правове регулювання співробітництва держав щодо протидії злочинам у сфері інформаційних технологій : дипломна робота на здобуття ступеня бакалавр спеціальності «Міжнародне право». *Національний авіаційний університет*. Київ, 2022. 76 с.