DOI https://doi.org/10.24144/2307-3322.2021.66.46
УДК 341.4

МІЖНАРОДНО-ПРАВОВА РЕГЛАМЕНТАЦІЯ ТРАНСНАЦІОНАЛЬНОЇ КІБЕРЗЛОЧИННОСТІ У КІБЕРПРОСТОРІ

Попко В.В.,
доктор юридичних наук, доцент,
професор кафедри порівняльного і європейського права
Інституту міжнародних відносин Київського національного
університету імені Тараса Шевченка
vadympopko@gmail.com
ORCID: 0000-0001-8358-7721

Попко Є.В.,
кандидат юридичних наук, асистент кафедри міжнародного
приватного права Інституту міжнародних відносин
Київського національного університету імені Тараса Шевченка
yevgenpopko@gmail.com
ORCID: 0000-0002-7417-7584

Попко В.В., Попко Є.В. Міжнародно-правова регламентація транснаціональної кіберзлочинності у кіберпросторі.

У статті розглядається міжнародно-правова регламентація протидії кіберзлочинності, що розглядається як явище транснаціонального характеру. У групі транснаціональних злочинів, поряд із незаконним обігом наркотичних засобів, терористичними акціями, «відмиванням» брудних коштів, незаконним ввезенням мігрантів, торгівлею людьми, незаконним обігом вогнепальної зброї, фальшуванням грошей тощо, кіберзлочини посідають вагоме місце з огляду суспільної шкоди, безпрецедентного поширення у світі й стрімкого зростання. Вивчаються напрацьовані міжнародним кримінальним правом механізми і напрямки боротьби із кіберзлочинами, серед яких міжнародно-правова регламентація має основоположне значення, й відзначаються складнощі у визначенні понять «кіберзлочинність» та «комп'ютерні злочини». Наводиться класифікація видів кіберзлочинів та виявляються найбільш характерні їх риси.

Автором аналізуються міжнародні нормативні документи, що складають правову основу регулювання відносин у сфері міжнародної кіберзлочинності, серед яких чільне місце посідають конвенції, зокрема Конвенція ООН проти транснаціональної організованої злочинності від 15 листопада 2000 р., Конвенція Ради Європи про кіберзлочинність від 23 листопада 2001 р. та Додатковий протокол до неї від 28 січня 2003 р. Аналізуються зобов'язання держав щодо криміналізації кіберзлочинів у національному законодавстві, розглядаються види протиправних дій, пов'язаних з кіберзлочинністю, зокрема основні чотири групи злочинів, які класифікуються у Конвенції про кіберзлочинність 2001 р. по родовому об'єкту та за видовими ознаками об'єкта посягання: 1) злочини проти конфіденційності, цілісності і доступності комп'ютерних даних і систем; 2) правопорушення, пов'язані з використанням комп'ютерних засобів; 3) правопорушення, пов'язані із змістом даних; 4) правопорушення, пов'язані з порушенням авторського права і сумісних прав, а також додаткові види відповідальності і санкції (замах, співучасть). Протокол до Конвенції про кіберзлочинність 2003 р. розширює це коло злочинів й містить зобов'язання стосовно криміналізації наступних діянь: поширення расистських і ксенофобських матеріалів через комп'ютерні системи. Відзначається обмеженість дії Конвенції про кіберзлочинність 2001 р., ухваленої Радою Європи, й необхідність прийняття універсального документу, що значно б підвищило рівень протидії злочинам у кіберпросторі.

Ключові слова: міжнародне кримінальне право, транснаціональний злочин, кіберзлочин, кіберпростір, конвенція.

Popko V.V., Popko E.V. International legal regulation of transnational cybercrime in cyberspace.

The article considers the international legal regulation of combating cybercrime, which is considered as a transnational phenomenon. In the group of transnational crimes, along with drug trafficking, terrorist acts, money laundering, illegal import of migrants, human trafficking, firearms trafficking, counterfeiting, etc., cybercrimes play an important role in terms of public harm, unprecedented and rapid growth. The mechanisms and directions of the fight against cybercrime developed by international criminal law are studied, among which the international legal regulation is of fundamental importance, and difficulties in defining the concepts of "cybercrime" and "computer crimes" are noted. The classification of types of cybercrimes is given and their most characteristic features are revealed.

The author analyzes the international normative documents that form the legal basis for regulating relations in the field of international cybercrime, among which the most prominent are conventions, including the UN Convention against Transnational Organized Crime of November 15, 2000, the Council of Europe Convention on Cybercrime of November 23, 2001 and Additional Protocol to it of January 28, 2003. The obligations of states to criminalize cybercrime in national legislation are analyzed, the types of illegal actions related to cybercrime are considered, in particular the main four groups of crimes classified in the 2001 Cybercrime Convention by Gender object and on specific grounds of the object of encroachment: 1) crimes against confidentiality, integrity and availability of computer data and systems; 2) offenses related to the use of computer tools; 3) offenses related to the content of data; 4) offenses related to infringement of copyright and compatible rights, as well as additional types of liability and sanctions (attempt, complicity). The Protocol to the 2003 Cybercrime Convention expands this range of crimes and contains obligations to criminalize the following acts: distribution of racist and xenophobic material through computer systems. The limitation of the 2001 Convention on Cybercrime, adopted by the Council of Europe, and the need to adopt a universal instrument that would significantly increase the fight against cybercrime are noted.

Key words: international criminal law, transnational crime, cybercrime, cyberspace, convention.

Постановка проблеми. Процеси глобалізації, у тому числі глобалізації інформаційних технологій, надають необмежені можливості для здійснення впливу на особу і суспільство. Одним з негативних наслідків розвитку інформаційних технологій являється поява і розвиток нової форми злочинності – злочинності у сфері високих технологій, коли комп'ютери чи комп'ютерні мережі виступають в якості об'єкта злочинних посягань, а також засобу чи способу здійснення злочинів. Жертвами злочинців, що діють у віртуальному просторі, можуть стати не тільки люди, але й держави, причому безпека тисяч користувачів може залежати від кількох злочинців. Кількість злочинів, що здійснюються у кіберпросторі, зростає пропорційно числу користувачів комп'ютерних мереж. Сайт Internet Complain Center (IC3), створений у травні 2000 р. для реєстрації заяв користувачів мережі Інтернет про здійснені стосовно них кіберзлочинів, ще 11 червня 2007 р. отримав мільйонну скаргу про інтернет-злочин. Проте більша частина кіберзлочинів залишається за рамками статистики, до офіційних звітів попадає лише невелика їх кількість. Професіоналізм кіберзлочинців зростає і постійне удосконалення інформаційних технологій та, як наслідок, постійна еволюція можливостей для вчинення злочинів, створюють нові загрози для користувачів глобальних інформаційних мереж. Активне зростання різноманітних кіберзагроз у сучасному суспільстві ставить перед кожною державою надзвичайно актуальне завдання – необхідність забезпечення інформаційної безпеки. Не дивлячись на те, що вивчення даної проблеми ведеться вже кілька десятиліть, проте недосконаліть формулювання поняття кіберзлочину та покарання за нього дозволяє злочинним спільнотам винаходити все новіші форми кіберзлочинності. Все зазначене робить дослідження у цій сфері актуальним і своєчасним.

Метою статті є вивчення міжнародно-правової регламентації протидії кіберзлочинам, виявлення їх особливостей та характерних рис.

Аналіз останніх досліджень. Злочинність у кіберпросторі вже давно стала об'єктом пильної уваги дослідників. Вивченню цього феномену посвячені праці Ю. Батуріна, О.Г. Волеводза, В.О. Голубева, М.С. Дашян, В.М. Дрьоміна, Т.Л. Тропіної. У праці «Комп'ютерна злочинність» (2002) авторами (П.Д. Біленчук, В.В. Бут, В.Д. Гавловський, М.В. Гуцалюк, В.В. Кравчук, Б.В. Романюк, В.С. Цимбалюк) дається загальна характеристика комп'ютерної злочинності, її перспектив у світі, наводиться міжнародна класифікація комп'ютерних злочинів, а також форми міжнародного співробітництва у цій сфері. Міжнародно-правовий дискурс злочинності у кіберпросторі аналізує професор Н.А. Зелінська; правове регулювання інформаційної безпеки в Європейському Союзі – предмет вивчення доцента І.М. Забари. Зазвичай вивчаються кримінологічні аспекти злочинності у кіберпросторі, у той же час міжнародно-правове регулювання вимагає глибокого вивчення й удосконалення.

Виклад основного матеріалу. До числа проблем, що викликають стурбованість усієї світової спільноти, належить транснаціональна злочинність, яка являє собою новий рівень організованої злочинності, що

перетинає кордони та ігнорує національні й міжнародні закони і норми. Протидія держав проявам транснаціональної організованої злочинності йде по різним напрямкам, у числі яких боротьба з незаконним обігом наркотичних засобів, терористичними акціями, «відмиванням» брудних коштів, незаконним ввезенням мігрантів, торгівлею людьми, незаконним обігом вогнепальної зброї, фальшуванням грошей, а також із кіберзлочинами. Міжнародним кримінальним правом напрацьовані механізми і напрямки боротьби із транснаціональними злочинами, серед яких міжнародно-правова регламентація протидії кіберзлочинності посідає важливе місце з огляду безпрецедентного поширення зазначеного виду злочинності. Даний вид злочинів здатен стрімко зростати, способи і методи їх здійснення йдуть «в ногу» зі способами захисту комп'ютерної інформації, а іноді й спереду. Згідно Щорічної доповіді про глобальні виклики [19], підготовленої Міжнародною організацією «World Economic Forum», що займається вивченням проблем державного й приватного співробітництва по проблемам глобального, регіонального і галузевого характеру, у 2019 р., проблеми кібербезпеки і кіберзлочинності зайняли четверте і п'яте місця у списку світових загроз. У цьому документі зазначається постійне зростання даних загроз в усіх сферах життя суспільства, а також прогнозується збільшення такого роду злочинних дій у найближчі десять років. Кіберзлочинність мобільна і активно модифікується, виникають нові злочини, нові поняття, технології не стоять на місці, тому і правове співробітництво повинно бути своєчасним.

Організація Об'єднаних Націй, Рада Європи, Європейський Союз, Організація з безпеки і співробітництва в Європі та інші впливові міжнародні організації проводять інтенсивну роботу по розробці концепції протидії кіберзлочинності і виробленню узгодженої політики стримування цієї загрози різними засобами: скликання міжнародних конгресів й форумів, ухвалення конвенцій та резолюцій тощо. Особлива увага злочинності, пов'язаної з використанням комп'ютерів, була приділена на Одинадцятому конгресі ООН з попередження злочинності і кримінальному правосуддю (Бангкок, Таїланд, квітень 2005 р.) [9]. Це питання було включено до порядку денного і розглядалось в рамках проблеми ефективних заходів по протидії транснаціональній організованій злочинності. Експерти ООН в рекомендаціях, підготовлених до Одинадцятого конгресу, звертають увагу на особливий характер кіберзлочинності і необхідності застосування комплексних підходів у протидії їй, а також про невідкладні заходи по оновленню кримінального законодавства держав-учасників ООН, таких як уточнення чи вилучення норм, що не відповідають ситуації, яка склалась, чи прийнятті норм стосовно нових видів кіберзлочинів. На Конгресі відзначалось: «Поширення по всьому світу нових інформаційно-комунікаційних технологій породило численні різноманітні злочини, пов'язані з використанням комп'ютерів, що загрожує не тільки конфіденційності, цілісності чи доступності комп'ютерних систем, але й безпеці важливих елементів інфраструктури. Крім того, технологічні новації породжують й несхожі один на одного тенденції у сфері «кримінальної інновації»; відповідно, несхожість загроз, які несуть у собі злочини, пов'язані з використанням комп'ютерів, відображає розбіжності, що прослідковуються по усьому спектру так званого «розриву у цифрових технологіях» [18]. Глобальна доступність електронних і віртуальних послуг означає, що злочинність в інформаційному просторі природним чином має транснаціональний вимір.

Важливо, на Одинадцятому конгресі було відмічено, що в умовах глобалізації транснаціональної організованої злочинності, практика укладання двосторонніх договорів вважається більш-менш застарілою, так як організована злочинність припускає незаконну діяльність у двох або декількох державах, які не мають один з одним двосторонніх угод про правову допомогу. Нові інструменти міжнародного співробітництва та правової допомоги у кримінальних справах мають відкривати можливості для співробітництва між більшою кількістю держав. При цьому, слід мати на увазі, що наявність багатостороннього договору не перешкоджає укладанню двосторонніх договорів між суб'єктами, що можуть конкретизувати ряд положень багатостороннього договору та врахувати особливості взаємодії між зацікавленими сторонами. Бангкокська декларація, яка стала результатом діяльності Одинадцятого конгресу ООН з попередження злочинності й кримінальному правосуддю, також свідчить про актуальність проблеми кіберзлочинності.

Стримування кіберзлочинності являється складовою частиною національної кібербезпеки і стратегії захисту важливої інформаційної інфраструктури. Як зазначає професор Н.А. Зелінська, «на національному рівні – це спільна відповідальність, яка вимагає скоординованих дій зі сторони урядових організацій, приватного сектора і громадян. На регіональному і міжнародному рівні це тягне за собою кооперацію і координацію зусиль держав» [8, с. 467]. Професор В.М. Дрьомін пише, що існують всі підстави стверджувати, що сучасне інформаційне середовище сприяє відтворенню злочинності, а в зв'язці явищ «інформація – злочинність» виявляється стійкий системний взаємовплив. Суттєвим наслідком розвитку інформаційного мегасередовища являється процес глобалізації злочинності, що стрімко розвивається. Не дивлячись на зовнішню різну природу цих соціальних явищ, виявляється їх вельми жорсткий зв'язок і тенденція до її укріплення

[7, с. 54]. У наш час не існує ані релевантної статистики, яка б відображала реальну картину стану кіберзлочинності, ані надійних методів збору таких даних, а також відсутнє одноманітне національне кримінальне законодавство держав у сфері протидії кіберзлочинності.

Визначення поняття «комп'ютерний злочин» чи «злочин, пов'язаний з використанням комп'ютерів» обговорюються, як мінімум протягом останніх п'ятидесяти років, проте до цього часу не мають однозначного трактування [12, с. 173]. В нормативних правових актах поняття «кіберзлочинність», «комп'ютерні злочини», «злочини, з використанням електронних засобів зв'язку», «злочини у сфері високих технологій», «ІТ-злочини» часто взаємозамінюються. У контексті, що нас цікавить, кіберзлочинністю, у самих загальних рисах, називають злочинність, яка має місце у кіберпросторі [6, с. 165]. Міжурядова група експертів, заснована Комісією з попередження злочинності і кримінальному правосуддю ООН для проведення всебічного дослідження проблеми кіберзлочинності і відповідних заходів по боротьбі з нею, відмітила у своїй Доповіді (2011): «Комп'ютерна злочинність і, більш конкретно, кіберзлочинність – терміни, що використовуються для позначення конкретної категорії злочинних діянь. Пов'язані з цією категорією злочинних діянь виклики включають не тільки широке коло правопорушень, що вже підпадають під цю категорію, але й нові методи вчинення злочинів, що швидко формуються» [16]. У матеріалах ООН ці терміни охоплюють будь-який злочин, який може здійснюватися з допомогою комп'ютерної системи чи мережі, в рамках комп'ютерної системи чи мережі чи проти комп'ютерної системи чи мережі. Таким чином, до кіберзлочинів може бути віднесено будь-який злочин, вчинений в електронному середовищі [17].

Як зазначає М.С. Дашян, комп'ютерні злочини багатоваріантні – протиправний характер мають поширення шкідливих вірусів, злом паролів, викрадення номерів кредитних карток, поширення протиправної інформації (від наклепу до матеріалів порнографічного характеру [6, с. 165]. На початку XXI ст. з'явились нові комп'ютерні злочини – фішинг, атаки з використанням бот-мереж, IP-телефонія тощо. Ґрунтовне дослідження кіберзлочинів провела Т.Л. Тропіна і запропонувала наступну класифікацію:

1) насильницькі чи інші потенційно небезпечні кіберзлочини, що посягають на фізичну безпеку, життя і здоров'я людини;
2) злочини, що посягають на конфіденційність інформації – незаконний доступ до комп'ютерів чи комп'ютерним системам без завдання шкоди інформації;
3) деструктивні кіберзлочини, що полягають у пошкодженні даних і посягають на цілісність даних і безпеку функціонування комп'ютерних систем;
4) злочини, що посягають на майно, майнові права, а також на право власності на інформацію і авторські права;
5) злочини, що посягають на суспільну мораль;
6) інші кіберзлочини – «computer-facilitated» (традиційні злочини, здійснення яких комп'ютер або полегшує або нові можливості для їх здійснення; до цієї групи включені численні злочини такі як реклама послуг проституції в мережі Інтернет (являється злочином не в усіх державах); незаконний обіг наркотиків з використанням мережі Інтернет; азартні ігри в Інтернеті (також не завжди кримінально карні); відмивання коштів з допомогою електронного переміщення; кіберконтрабанда, чи передача нелегальних товарів, наприклад, шифрувальних технологій, заборонених в деяких державах, по мережі Інтернет тощо [13, с. 46-58].

Для більшості злочинів, що вчиняються у глобальних комп'ютерних мережах, характерні наступні особливості: підвищена скритність здійснення злочину, що забезпечується специфікою мережевого інформаційного простору (розвинені механізми анонімності, складність інфраструктури тощо); транснаціональний характер мережевих злочинів, при якому злочинець, об'єкт злочинного посягання, потерпілий можуть знаходитися на територіях різних держав; особлива підготовленість злочинців, інтелектуальний характер злочинної діяльності; нестандартність, складність, багатоманітність і часте оновлення способів вчинення злочинів і спеціальних засобів, що застосовуються; можливість вчинення злочину в автоматизованому режимі в кількох місцях одночасно; багатоепізодний характер злочинних дій при чисельності потерпілих; необізнаність потерпілих про те, що вони піддались злочинному впливу; дистанційний характер злочинних дій в умовах відсутності фізичного контакту злочинця і потерпілого; неможливість попередження і припинення злочину даного виду традиційними засобами.

Кіберзлочинність – це сукупність злочинів, щодо яких передбачена кримінально-правова заборона, які здійснюються у кіберпросторі, де основними безпосередніми об'єктами злочинного посягання виступають конституційні права і свободи людини і громадянина, а також суспільні відносини у сферах комп'ютерної інформації та інформаційних технологій, економічної діяльності, державної влади тощо. Кіберзлочини спрямовані проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних

даних та зловживання ними. Це порушення, що охороняються законом, суспільних відносин у сфері безпечного створення, зберігання, обробки і передачі комп'ютерної інформації, з метою завдання економічної, політичної, моральної, ідеологічної, культурної та інших видів шкоди людині, державі і світу у цілому.

Поняття «кіберзлочинність» вперше з'явилося у середині 70-х р. минулого століття в США, саме у цей час були здійснені перші злочини з використанням інформаційних технологій. У 1973 р. касир місцевого банку в Нью-Йорку використав комп'ютер, щоб викрасти більше двох млн доларів США. Причому здійснив він дане протиправне діяння цілком простим способом - перевів гроші на свій особистий рахунок. Офіційне поняття, а також основні ознаки кіберзлочину були сформульовані лише в 1974 р. на Конференції Американської асоціації адвокатів [14]. Пізніше, тільки в 1986 р. в США був прийнятий перший нормативно-правовий документ протидії кіберзлочинам - «Закон про шахрайство з використанням комп'ютерів» (Computer fraud and abuse act). У Великобританії існує свій нормативно-правовий документ - Акт про комп'ютерні зловживання, прийнятий у 1990 р., який передбачає покарання за вчинення злочину в комп'ютерному просторі – штраф, чи позбавлення волі на строк від 6 місяців до 5 років. У Нідерландах та Німеччині протидія кіберзлочинності ведеться шляхом введення нових статей у чинний Кримінальний кодекс.

На необхідність розвитку міжнародного співробітництва в інформаційному просторі з метою запобігання кіберзлочинам вказують наступні міжнародні документи: Декларація принципів «Побудова інформаційного суспільства - глобальне завдання у новому тисячолітті», прийнята 12 грудня 2003 р. [1] представниками народів світу, що зібралися у Женеві для проведення першого етапу Всесвітньої зустрічі на вищому рівні по питанням інформаційного суспільства; «Окінавська Хартія глобального інформаційного суспільства», ухвалена 22 липня 2000 р. лідерами країн «Великої вісімки», Туніська програма для інформаційного суспільства, прийнята у 2005 р., Програма «Інформація для всіх» (Information for All Programme), прийнята в 2001 р. ЮНЕСКО та інші.

Правову основу протидії кіберзлочинам складають міжнародні нормативно-правові акти універсального та регіонального характеру, зокрема *Конвенція ООН проти транснаціональної організованої злочинності* від 15 листопада 2000 г. [3] в якій відображені основні напрямки міждержавного співробітництва в даній сфері. Як вже зазначалось, кіберзлочини мають транснаціональний характер, до того ж вони можуть завдавати значної шкоди економічному розвитку держав. Як відзначають вчені, «беззаперечно, кіберзлочини вже набули транснаціонального характеру і міжнародна спільнота, враховуючи можливі негативні наслідки цього явища, намагається мінімізувати їх посягання на міжнародні економічні відносини» [10, с. 140]. Радою Європи також було підкреслено транснаціональний характер комп'ютерних злочинів на конференції з економічних злочинів у 1976 р. Характеристика транснаціональності як основної властивості транснаціональних злочинів дається у ст. 3, п. 2 Конвенції 2000 р., в якій зазначається: «злочин носить транснаціональний характер, якщо: a) він вчинений у більш ніж одній державі; b) він вчинений в одній державі, але істотна частина його підготовки, планування, керівництва або контролю має місце в іншій державі; c) він вчинений в одній державі, але за участю організованої злочинної групи, яка здійснює злочинну діяльність у більш ніж одній державі; або d) він вчинений в одній державі, але його істотні наслідки мають місце в іншій державі».

Серед численних регіональних правових інструментів виділимо *Конвенцію про взаємодопомогу в кримінальних справах між державами-членами Європейського Союзу*, ухвалену 29 травня 2000 р. [4], у частині судових доручень про перехоплення телекомунікаційних повідомлень (Розділ III «Перехоплення телекомунікацій»).

Базовим документом у протидії кіберзлочинності для європейських держав, і не тільки, являється *Конвенція Ради Європи про кіберзлочинність* від 23 листопада 2001 р. та Додатковий протокол до неї від 28 січня 2003 р. Вони є «фундаментом для розробки відповідного законодавства європейських держав» [10, с. 140].

Розробка конвенції про кіберзлочинність Радою Європи була започаткована на конференції з економічних злочинів у 1976 р. Було створено спеціальний Комітет експертів з питань злочинності у кіберпросторі, що підготував 25 проектів тексту конвенції, остаточний текст якої був схвалений на засіданні Комітету Міністрів в ранзі постійних представників 19 вересня 2001 р. і прийнятий міністрами іноземних справ на засіданні 8 листопада 2001 р. 23 листопада 2001 р. у Будапешті *Конвенція Ради Європи про кіберзлочинність* **бу**ла відкрита для підписання й набула чинності 1 липня 2004 р. [5]. У 2003 р. був схвалений Додатковий протокол до Конвенції про кіберзлочинність відносно криміналізації діянь расистського і ксенофобського характеру, що здійснюються з допомогою комп'ютерних систем [2].

Конвенція про кіберзлочинність 2001 р. зобов'язує держави, які являються її сторонами, гармонізувати національні закони стосовно визначення основних злочинів. Згідно Конвенції, кожна сторона приймає заходи, необхідні для того, щоб кваліфікувати в якості кримінального злочину згідно її внутрішньодержавного права широке коло діянь.

Конвенція розрізняє два види протиправних дій, пов'язаних з кіберзлочинністю: злочини та правопорушення. Частина І Другого розділу Конвенції («Матеріальне кримінальне право») побудована таким чином, що всі склади злочинів розподілені підрозділами (групами) по родовому об'єкту, а підрозділи, у свою чергу, об'єднують злочини за видовими ознаками об'єкта посягання. У Конвенції виділено чотири види комп'ютерних злочинів: 1) злочини проти конфіденційності, цілісності і доступності комп'ютерних даних і систем; 2) правопорушення, пов'язані з використанням комп'ютерних засобів; 3) правопорушення, пов'язані із змістом даних; 4) правопорушення, пов'язані з порушенням авторського права і сумісних прав, а також додаткові види відповідальності і санкції (замах, співучасть). Протокол до Конвенції про кіберзлочинність 2003 р. розширює це коло злочинів й містить зобов'язання стосовно криміналізації наступних діянь: поширення расистських і ксенофобських матеріалів через комп'ютерні системи (ст. 3), мотивована загроза расизму і ксенофобії через комп'ютерну систему здійснення серйозного кримінального злочину як визначено її внутрішнім правом стосовно осіб по причині того, що вони належать до групи, відмінної по расі, кольору шкіри, національному чи етнічному походження, а також релігії, чи групи осіб з урахуванням цих факторів (ст. 4); публічну расистську і ксенофобську образу через комп'ютерну систему (ст. 5); поширення чи забезпечення доступу для громадськості через комп'ютерну систему матеріалу, який повністю заперечує чи надзвичайно применшує негативні наслідки, схвалює чи виправдовує дії, що являються геноцидом чи злочинами проти людяності, як визначено міжнародним правом та як це визнано остаточними і обов'язковими рішеннями Міжнародного воєнного трибуналу, утвореного відповідно до Лондонської угоди від 8 серпня 1945 р., чи будь-якого іншого міжнародного суду, утвореного згідно відповідного міжнародного документу і юрисдикція яких визнана стороною Протоколу (ст. 6).

Норми Конвенції Ради Європи про кіберзлочинність 2001 р. активно діють і застосовуються, знаходять своє відображення у багатьох національних законодавствах, містять положення, які не знайшли відображення в інших договорах і нормативно-правових актах. Проте положення Конвенції діють на обмеженій території держав-учасниць, що обмежує її вплив на світську спільноту; деякі її положення є спірними, наприклад неузгодженість норми ст. 32 п. b., згідно якої будь-яка Сторона може, не отримуючи дозвіл іншої сторони «здійснювати доступ або отримувати за допомогою комп'ютерної системи, яка знаходиться на її території, комп'ютерні дані, які зберігаються і знаходяться в іншій Стороні, якщо Сторона отримує законну і добровільну згоду особи, яка має законні повноваження розкривати дані такій Стороні за допомогою такої комп'ютерної системи». Даний пункт сповільнює співробітництво держав і ефективне вирішення багатьох проблем по проблемі кібербезпеки, також тягне за собою порушення права на приватне життя, що являється одним з основоположних принципів міжнародного права. Разом з тим існують утруднення при підписанні та імплементації норм у національне законодавство, про що свідчить той факт, що за 20 років, що минули з часу підписання Конвенції, її ратифікували лише 47 держав, з яких 37 – це держави-члени Ради Європи. Крім того, міжнародний характер Конвенції, який передбачає відкритість приєднання до неї всіх бажаючих держав, проте містить ряд застережень, зокрема процедура приєднання країн, що не входять до Ради Європи, вимагає консультації і одноголосного рішення про приєднання до Конвенції держав-членів Ради Європи (ст. 37).

Держави, що підписали дану Конвенцію, беруть зобов'язання реалізовувати політику, спрямовану на здійснення протидії кіберзлочинності, на міжнародному рівні сприяти цій протидії, а також розслідувати злочини, здійснювані в рамках глобальної інформаційно-цифрової мережі, й брати участь у створенні нових заходів протидії кіберзлочинності.

Основні проблеми, що виникають при міжнародно-правовому регулюванні протидії кіберзлочинності, полягають у відмінностях національних законів у сфері кібербезпеки; відсутності чіткого уніфікованого категоріального апарату; недостатньому рівні координації діяльності правоохоронних органів при розслідуванні кіберзлочинів, низькому рівні обміну інформацією про кіберінциденти між державами; недостатньому рівні державного й приватного співробітництва у цій сфері. Як наголошує професор Н.А. Зелінська, «потреба в міжнародно-правових стандартах зумовлена необхідністю стимулювати встановлення кримінально-правової заборони і гармонізувати національне законодавство. Внутрішньодержавне право багатьох країн загалом має значний ступінь подібності щодо більшості традиційних видів транснаціональних злочинів, проте нові види злочинності вимагають серйозних зусиль у виробленні узгоджених визначень. У питаннях боротьби з кіберзлочинністю проблема гармонізації кримінально-правової заборони набуває особливої значущості» [11, с. 568-569].

Важливою рисою кіберзлочинності є її глобальний, інтернаціональний характер, що обумовлює низьку ефективність традиційних методів припинення злочинів. Слід зазначити, що для організації ефективної боротьби з кіберзлочинністю держави мають співпрацювати між собою – проте такого роду співпраця

в певній ступені зачіпає державний суверенітет та його повноваження у сфері захисту інформації. Міжнародна взаємодія між державами, спрямована на боротьбу з кіберзлочинністю, кібертероризмом, є найбільш ефективною в районах, де між державами існує високий рівень політичної довіри – наприклад, в рамках Європейського Союзу. На протидію кіберзлочинності спрямована діяльність Міжнародного центру протидії кіберзлочинності [15], створеного у 2013 р. у Гаазі, однією з головних завдань якого є створення нових методів розслідування кіберзлочинів. Центральне місце у цьому процесі займає Організація Об'єднаних Націй, а також її спеціалізовані установи. Особливі функції щодо боротьби з високотехнологічними злочинами покладені на Управління ООН з наркотиків та злочинності (United Nations Office on Drugsand Crime – UNODC), у рамках якого здійснюється Глобальна програма з кіберзлочинності (Global Program on Cybercrime – GPC), а також функціонує Міжурядова експертна група відкритого складу з кіберзлочинності (Open-ended Intergovernmental Expert Group on Cybercrime). UNODC сприяє довгостроковому і стійкому нарощуванню потенціалу в боротьбі з кіберзлочинністю шляхом підтримки національних структур і дій.

Висновки: У наш час існує механізм протидії злочинам транснаціонального характеру, у тому числі кіберзлочинам, що вчиняються у кіберпросторі. Він базується на міжнародно-правових документах, які забезпечують правове регулювання відносин у сфері міжнародної злочинності у кіберпросторі. Правову основу такого регулювання відносин становлять конвенції, серед яких чільне місце посідають Конвенція ООН проти транснаціональної організованої злочинності 2000 р. та Конвенція Ради Європи про кіберзлочинність 2001 р. та Додатковий протокол до неї 2003 р. Проте нагальною є потреба у розробці й прийнятті універсальної міжнародної конвенції щодо протидії кіберзлочинності, а також загального кодексу принципів поведінки держав у світовому інформаційному просторі. Протидія кіберзлочинності повинні здійснюватися на міжнародному рівні. Для ефективного розкриття даного виду злочинів необхідно активне міжнародне співробітництво, взаємодопомога й підтримка, а також постійне оновлення міждержавних та національних законів.

Встановлення кримінально-правової заборони і необхідність гармонізувати національне законодавство у протидії кіберзлочинності обумовлює потребу у міжнародно-правових стандартах криміналізації кіберзлочинів. Національне право багатьох держав у цілому має значну ступінь подібності відносно більшості традиційних видів транснаціональних злочинів, проте нові види злочинності вимагають напрацювання особливого механізму протидії їм, у тому числі формулювання чітких узгоджених визначень.

Кіберпростір по своїй природі глобальний й вимагає глобального підходу у вирішенні питань боротьби з міжнародною кіберзлочинністю. Злочинність у кіберпросторі являється однією з самих складних проблем, з якими міжнародна спільнота стикається останніми роками у зв'язку з розвитком інформаційних і комунікаційних технологій. Забезпечення кібербезпеки, дотримання прав людини і захист важливої інформаційної інфраструктури вимагають від держав значних зусиль як на національному так й на міжнародному рівнях. Одним з аспектів цієї проблеми являється пріоритетне завдання світової спільноти по розробці й прийняттю універсальної конвенції щодо протидії кіберзлочинності.

Список використаних джерел:

1. Декларація принципів «Побудова інформаційного суспільства - глобальне завдання у новому тисячолітті», прийнята 12 грудня 2003 р. / URL: / https://zakon.rada.gov.ua/laws/show/995_c57#Text

2. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи від 28 січня 2003 р. / URL: https://zakon.rada.gov.ua/laws/show/994_687

3. Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності, ухвалена Резолюцією 55/25 Генеральної Асамблеї від 15 листопада 2000 р. / URL: / http://zakon.rada.gov.ua/laws/show/995_789

4. Конвенція про взаємодопомогу в кримінальних справах між державами-членами Європейського Союзу, ухвалену 29 травня 2000 р. / URL: / https://zakon.rada.gov.ua/laws/show/994_238#Text

5. Конвенція про кіберзлочинність, ухвалена Радою Європи 23 листопада 2001 р. / URL: https://zakon.rada.gov.ua/laws/show/994_575

6. Дашян М.С. Право информационных магистралей (Law of information highways): вопросы правового регулирования в сфере Интернет. М.: Волтерс Клувер, 2007. 248 с. С. 165.

7. Дремин В.Н. Глобализация информационных систем как фактор глобализации преступности / Інформаційні технології та безпека: зб. наук. праць. К., 2002. Вип. 1. С. 54-61.

8. *Зелинская Н.А*. Преступность в киберпространстве: международно-правовой дискурс / *Актуальні проблеми держави і права*. Випуск 67, 2013. С. 465-477. С. 467.

9. Конгрессы ООН по предупреждению преступности и уголовному правосудию: сборник материалов: в 3-х книгах / Под общ. ред. В.В. Голины. Киев-Харьков: Право, 2013. Кн. 3. 2013. 168 с.

10. Міжнародне кримінальне право (співробітництво держав у протидії злочинності): підручник / В.А. Грінчак, І.В. Земан, І.І. Когутич, О.К. Марін. Харків: Право, 2019. 440 с.

11. Теорія та практика міжнародного кримінального права: підручник / Зелінська Н.А., Андрейченко С.С., Дрьоміна-Волок Н.В., Коваль Д.О.; за ред. проф. Зелінської Н. А. Одеса: Фенікс, 2017. 582 с.

12. Тропина Т.Л. Киберпреступность и кибертерроризм: поговорим о понятийном аппарате / Сборник научных трудов международной конференции «Информационные технологии и безопасность. – К.: Нац. Акад. наук Украины, 2003. Вып. 2. С. 173-181.

13. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: Дис. канд. юрид. наук по специальности 12.00.08. Владивосток: Дальневосточный государственный университет, 2005. 234 с.

14. Юридический интернет-журнал «Первый юрист». URL: https://urist.one/dolzh-rnstnyprestupleniya/kiberprestupnost/kiberprestuplenie.html

15. Веб-сайт: https://iccc.pro/

16. Док. ООН. E/CN.15/2011/19. П. 10.

17. Док. ООН. A/CONF. 187/10.

18. Док. ООН. A/CONF. 203/14.

19. The Global Risks Report 2019 (14th Edition) / World Economic Forum / URL://http://www3.weforum.org/docs/WEF_Glo-bal_Risks_Report_2019.pdf