Ольга ГРИЦУН

здобувач кафедри міжнародного права
Інституту міжнародних відносин
Київського національного університету
імені Тараса Шевченка
olga_markevich@ukr.net

УДК 341: 343.34: 316.774

МІЖНАРОДНО-ПРАВОВЕ РЕГІОНАЛЬНЕ РЕГУЛЮВАННЯ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ ЗЛОЧИННОСТІ

Розробка стратегій боротьби з інформаційною злочинністю та систематичний аналіз останніх досягнень у цій сфері перебуває на порядку денному не тільки таких міжнародних універсальних організацій, як Організація Об'єднаних Націй і Міжнародний союз електрозв'язку, а й багатьох регіональних інституцій. Абсолютно очевидно, що інформаційні злочини мають транскордонний характер, оскільки вчиняються у кіберпросторі, який не має фізичних меж, а тому жодна країна світу не здатна відмежуватись та протистояти загрозі інформаційної злочинності наодинці. Особливої нагальності набуває питання гармонізації правових норм щодо попередження, виявлення, розслідування інформаційних злочинів, а також притягнення до відповідальності осіб, винних у їх вчиненні. Оскільки на сьогодні не існує універсального міжнародного договору, яким було б урегульовано питання боротьби з інформаційною злочинністю, регіональні угоди залишаються ключовими механізмами співробітництва держав у цій сфері.

Окремі питання боротьби з інформаційною злочинністю розглядались у працях М. Гудмана, А. Крутських, Ю. Батурина, М. Форста, М. Герке, Р. Форда, Т. Тропініної, А. Федорова, С. Бренера, В. Сомерса, К. Вілсона й інших учених. Проте комплексного аналізу регіональних підходів до боротьби з інформаційною злочинністю не було здійснено.

Отож мета статті полягає у проведенні комплексного аналізу регіональних підходів до розуміння інформаційної злочинності, класифікації правопорушень, а також основних форм міждержавного співробітництва у сфері боротьби з інформаційними злочинами.

Угода про співробітництво держав – членів Співдружності Незалежних Держав у боротьбі зі злочинами у сфері комп'ютерної інформації від 1 червня 2001 року – перший регіональний документ у цій сфері. У ній надано визначення поняття «злочин у сфері комп'ютерної інформації»: «діяння, за яке передбачено кримінальне покарання та предметом посягання якого є комп'ютерна інформація» [1]. Відповідно до положень цієї Угоди умисними діяннями, що тягнуть за собою кримінальну відповідальність, визнано такі: «1) здійснення неправомірного доступу до комп'ютерної інформації, що охороняється законом, якщо таке діяння призвело до знищення, блокування, модифікації чи копіювання інформації, порушення роботи електронно-обчислювальних машин (ЕОМ), систем ЕОМ чи їх мереж; 2) створення, використання чи поширення шкідливих програм; 3) порушення правил експлуатації ЕОМ, систем ЕОМ чи їх мереж

особою, що має доступ до ЕОМ, до системи ЕОМ чи їх мереж, що спричинило знищення, блокування чи модифікацію інформації ЕОМ, яка охороняється законом, і якщо таке діяння спричинило суттєву шкоду чи тяжкі наслідки; 4) незаконне використання програм для ЕОМ та баз даних, що є об'єктами авторського права, привласнення авторства, якщо таке діяння спричинило суттєві збитки» [1].

Основним механізмом співробітництва згідно з положеннями Угоди є запити компетентних органів сторін-учасниць про надання сприяння. У цьому регіональному документі в указаній сфері детально визначено форму, структуру та механізми виконання або відмови у виконанні такого запиту. При цьому важливо зауважити, що максимальний термін виконання запиту – 30 діб. З урахуванням сучасного рівня розвитку інформаційно-комунікаційних технологій, коли не тільки вчинення злочину, а й знищення доказів займає секунди, 30 діб – це надзвичайно тривалий строк. Тому положення Угоди про співробітництво держав – членів Співдружності Незалежних Держав у боротьбі зі злочинами у сфері комп'ютерної інформації є дещо застарілими та потребують перегляду.

Конвенція Ради Європи про кіберзлочинність від 23 листопада 2001 року не містить визначення поняття «кіберзлочин». У ній використано підхід категоризації злочинних діянь. Злочини у Конвенції класифіковано на чотири групи. До першої групи – правопорушень проти конфіденційності, цілісності та доступності комп'ютерних даних і систем – належать: незаконний доступ; нелегальне перехоплення; втручання у дані; втручання у систему та зловживання пристроями. До другої групи правопорушень, що має назву правопорушення, пов'язані з комп'ютерами, увійшли: підробка, пов'язана з комп'ютерами, та шахрайство, пов'язане з комп'ютерами. Третя група – правопорушення, пов'язані зі змістом інформації, – включає правопорушення, пов'язані з дитячою порнографією, а четверта група передбачає порушення авторських і суміжних прав [2]. Додатковим протоколом від 2003 року до цього переліку було додано п'яту групу правопорушень – правопорушення, пов'язані з діями расистського та ксенофобного характеру, – вчинених через комп'ютерні системи [3]. До того ж у Конвенції визначено відповідальність за навмисну допомогу або співучасть чи навмисну спробу вчинення будь-якого із перерахованих вище злочинів, а також передбачено корпоративну відповідальність за такі правопорушення. Крім матеріальної частини, нормами Конвенції врегульовано широке коло питань процесуального характеру, зокрема визначено, що держави-учасниці вживають законодавчі та інші необхідні заходи для визначення повноважень і процедур з метою конкретних кримінальних розслідувань або переслідувань та їх застосування до кримінальних правопорушень, коло яких визначається відповідними статтями конвенції; інших кримінальних правопорушень, вчинених за допомогою комп'ютерних систем, та збору доказів у електронній формі стосовно кримінального правопорушення [2]. Крім того, Конвенцією врегульовано питання термінового збереження комп'ютерних даних, які зберігаються; термінового збереження та часткового розкриття даних про рух інформації; обшуку й арешту комп'ютерних даних, які зберігаються; порядку представлення; збирання комп'ютерних даних у реальному масштабі часу; перехоплення даних змісту інформації та питання юрисдикції. Окремим розділом Конвенції врегульовано питання міжнародного співробітництва, серед яких: питання екстрадиції; загальні принципи взаємної допомоги; процедури, пов'язані із запитами про взаємну допомогу у разі відсутності відповідних міжнародних угод; взаємна допомога щодо тимчасових заходів; взаємна допомога щодо повноважень на розслідування та визначення уповноваженого органу для здійснення цілодобових контактів між сторонами [2].

Із метою внесення доповнень до положень Конвенції Ради Європи про кіберзлочинність 28 січня 2003 року було прийнято Додатковий протокол до Конвенції, що стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи. Положеннями цього документа врегульовано спірні питання щодо заходів, які мають вживатись

Вісник Національної академії прокуратури України № 4(42)'2015, с. 92–98

на національному рівні для визнання злочинами «розповсюдження або іншим чином надання громадськості доступу через комп'ютерні системи до расистського та ксенофобного матеріалу» [3]. Відповідно до положень Додаткового протоколу злочинами повинні бути визнані також: погрози з расистських і ксенофобних мотивів; образи з расистських та ксенофобних мотивів; заперечення, значна мінімізація, схвалення або виправдання геноциду чи злочинів проти людства; пособництво та підбурювання до вчинення усіх вказаних вище злочинів [3].

На сьогодні Конвенція Ради Європи про кіберзлочинність відкрита для підписання усіма зацікавленими державами. Наразі її ратифікували 47 країн, а підписали – 53. Окрім держав – членів Ради Європи, до Конвенції долучились Австралія, Домініканська Республіка, Японія, Республіка Маврикій, Республіка Панама, Сполучені Штати Америки, а в 2015 році – Канада та Демократична Соціалістична Республіка Шрі-Ланка. Конвенція Ради Європи підтримується різними міжнародними організаціями та є одним із найважливіших документів у боротьбі з кіберзлочинністю. Незважаючи на те, що багато країн використовують її як зразок для створення національного законодавства, учасники XII Конгресу Організації Об'єднаних Націй щодо попередження злочинності та кримінального правосуддя дійшли висновку, що процес підписання та ратифікації Конвенції дуже повільний і, як результат, – застосування її положень територіально досить обмежене. Серед інших аспектів Конвенції, які зазнали критики, були такі: відсутність оцінки ратифікації; обмежене представництво та недостатня участь країн, що розвиваються, в процесі підготовки нормативних документів; процес імплементації стандартів Конвенції, зокрема створення цілодобових контактних центрів, є проблематичним для невеликих країн, а також країн, що розвиваються; відсутність комплексного підходу до врегулювання усіх аспектів кіберзлочинності, наприклад положень про допустимість електронних доказів, положень щодо атак з використанням мереж ботів чи фішингу [4]. Таким чином, Конвенція Ради Європи потребує оновлення відповідно до виникнення нових видів кіберзлочинів та нових загроз у кіберпросторі, розширення сфери її дії й удосконалення положень. Варто зазначити, що з 2012 року обговорюється питання підписання ще одного додаткового протоколу до Конвенції – щодо транскордонного доступу та юрисдикції. Так, у 2013 році робочою групою було опубліковано доповідь, яка висвітлює як питання транскордонного доступу з належною згодою іншої сторони, так і питання доступу без такої згоди.

У 2007 році Радою Європи було прийнято ще один документ – *Конвенцію про захист дітей від сексуальної експлуатації та сексуального насильства*, спрямовану на боротьбу з цими явищами, особливо враховуючи факт широкомасштабного використання інформаційно-комунікаційних технологій як дітьми, так і злочинцями. Відповідно до цієї Конвенції визнано кримінальними злочинами такі діяння, як свідоме одержання доступу до дитячої порнографії за допомогою інформаційно-комунікаційних технологій та умисна пропозиція зустрітися з дитиною для вчинення проти неї одного з правопорушень, передбачених положеннями Конвенції, зроблена за допомогою інформаційно-комунікаційних технологій [5].

У рамках Шанхайської Організації Співробітництва 16 червня 2009 року було прийнято *Угоду між урядами держав – членів ШОС про співробітництво в сфері забезпечення міжнародної інформаційної безпеки*, що також регулює кримінальний аспект міжнародної інформаційної безпеки. У зазначеній Угоді виділено три складові загрози у сфері забезпечення міжнародної інформаційної безпеки. Одна з них – інформаційна злочинність, під якою розуміється «використання інформаційних ресурсів та (чи) вплив на них в інформаційному просторі в протиправних цілях» [6]. Згідно з Додатком 2 до Угоди основним джерелом інформаційної злочинності є особи чи організації, що здійснюють неправомірне використання інформаційних ресурсів або несанкціоноване втручання у такі ресурси зі злочинною метою. Також у Додатку 2 до Угоди визначено ознаки інформаційної злочинності, серед яких: проникнення в інформаційні системи для порушення ці-

лісності, доступності та конфіденційності інформації; навмисне виготовлення та поширення комп'ютерних вірусів й інших шкідливих програм; здійснення DOS-атак та іншого негативного впливу; нанесення шкоди інформаційним ресурсам; порушення законних прав і свобод громадян в інформаційній сфері, прав інтелектуальної власності та недоторканності приватного життя; використання інформаційних ресурсів і методів для здійснення таких злочинів, як шахрайство, крадіжка, вимагання, контрабанда, незаконна торгівля наркотиками, поширення дитячої порнографії тощо. Основними напрямами співробітництва держав – учасниць Угоди є, зокрема: створення системи моніторингу та спільного реагування на загрози, що виникають у цій сфері; протидія інформаційній злочинності; обмін інформацією про законодавчі норми держав щодо питання інформаційної безпеки; взаємодія у рамках міжнародних організацій та форумів; створення умов для взаємодії компетентних органів держав-учасниць, оскільки відповідно до положень Угоди сторони можуть визначати й інші напрями співробітництва [6].

У питаннях боротьби із кіберзлочинністю не становить винятку і регіон арабських держав – у 2010 році було прийнято *Конвенцію про боротьбу із злочинами у сфері інформаційних технологій Ліги Арабських держав*.

У цій Конвенції надається визначення понять «інформаційні технології», «провайдер», «дані», «інформаційна програма», «інформаційна система», «інформаційна мережа», «збір даних», «інформація про користувача». Конвенція передбачає такі види злочинів у сфері інформаційних технологій, як: незаконний доступ; незаконне перехоплення даних; порушення цілісності даних; злочинне використання інформаційних технологій; підробка; шахрайство; порнографія; злочини проти конфіденційності та непорушності приватного життя; злочини, пов'язані з тероризмом, що здійснені за допомогою інформаційних технологій; злочини, пов'язані з організованою злочинністю, що вчинені за допомогою інформаційних технологій; злочини проти авторських та суміжних прав; незаконне використання електронних платіжних інструментів; замах на вчинення та участь у вчиненні зазначених злочинів; а також кримінальну відповідальність фізичних та юридичних осіб і збільшене покарання за традиційні злочини, вчинені за допомогою інформаційних технологій [7].

Також у Конвенції міститься низка процесуальних положень і визначено напрями співробітництва у правовій сфері та сфері судочинства, наприклад визначення компетенції, екстрадиція, взаємна допомога, допоміжна інформація, процедури співпраці та запити про взаємну допомогу, відмова у запиті, конфіденційність, оперативна охорона інформації, що зберігається в інформаційних системах, оперативне відстеження інформації, транскордонний доступ до технічної інформації, співпраця та двостороння допомога щодо доступу до інформації, щодо відстеження інформації та щодо її змісту. Крім того, кожна держава-учасниця зобов'язана забезпечити наявність спеціалізованого органу, що працював би 24 години на добу, з метою виконання усіх положень, передбачених Конвенцією [7].

Конвенцію Африканського Союзу з питань кібербезпеки та захисту персональних даних було прийнято 27 червня 2014 року. У ній відображено широкий підхід до розуміння кібербезпеки, оскільки, крім питань кіберзлочинності, цей документ регулює ще й питання захисту персональних даних та електронної комерції. Структурно Конвенція складається з чотирьох частин: 1) електронна комерція; 2) захист персональних даних; 3) сприяння кібербезпеці та боротьба із кіберзлочинністю; 4) прикінцеві положення.

Розглянемо детальніше третю частину документа, положення якої регулюють питання кримінального аспекту міжнародної інформаційної безпеки.

До злочинів у сфері інформаційно-комунікаційних технологій віднесено: атаки на комп'ютерні системи; незаконне використання комп'ютерних даних; нелегальний контент; злочини, пов'язані із заходами безпеки електронних повідомлень.

До атак на комп'ютерні системи належать такі діяння: отримання чи намагання отримати незаконний доступ до комп'ютер-

Вісник Національної академії прокуратури України № 4(42)'2015, с. 92–98

ної системи або ж перевищення меж авторизованого доступу; отримання чи намагання отримати незаконний доступ до комп'ютерної системи або ж перевищення меж авторизованого доступу з метою вчинення чи сприяння вчиненню іншого злочину; незаконна присутність чи спроба незаконної присутності в комп'ютерній системі; перешкоджання чи спотворення або спроба перешкоджання чи спотворення функціонування комп'ютерної системи; введення чи намагання ввести дані в комп'ютерну систему обманним шляхом; пошкодження, видалення, спотворення, модифікація, зміна комп'ютерних даних обманним шляхом чи спроби таких діянь. Цікавим доповненням до цієї статті є обов'язок комерційних організацій, що займаються продажем продукції у сфері інформаційно-комунікаційних технологій, надавати свою продукцію експертам для оцінки слабких місць та усунення їх у разі виявлення. Також відповідно до положень Конвенції злочином є незаконне виготовлення, продаж, імпорт чи поширення комп'ютерного обладнання, програм або будь-яких інших пристроїв, спеціально адаптованих для вчинення злочинів [8].

Під незаконним використанням комп'ютерних даних розуміють: перехоплення чи спробу перехоплення комп'ютерних даних обманним шляхом із використанням технічних засобів; навмисне введення, зміну, видалення чи спотворення комп'ютерних даних із метою використання їх у правових цілях; навмисне використання даних, отриманих з комп'ютерної системи шахрайським шляхом; навмисне введення, зміну, видалення, спотворення комп'ютерних даних чи інше втручання у функціонування комп'ютерної системи з метою отримання вигоди; порушення процесу обробки персональних даних навіть з необережності; участь в організації, створеній з метою вчинення вказаних вище злочинів.

До злочинів, пов'язаних із використанням нелегального контенту, розробники Конвенції віднесли: виробництво, поширення, передачу дитячої порнографії за допомогою комп'ютерної системи; купівлю, імпорт чи експорт дитячої порнографії через комп'ютерну систему; володіння дитячою порнографією в комп'ютерній системі чи на іншому комп'ютерному носії; сприяння доступу неповнолітніх до інформації порнографічного характеру; поширення інформації расистського чи ксенофобного характеру через комп'ютерну систему; погрозу чи вчинення кримінального злочину за допомогою комп'ютерної системи проти особи, що відрізняється за ознакою раси, кольору шкіри, національного чи етнічного походження або релігії; образу за допомогою комп'ютерної системи особи, яка відрізняється за ознакою раси, кольору шкіри, національного чи етнічного походження або релігії; навмисне заперечення чи виправдання дій, які є геноцидом або злочинами проти людства, за допомогою комп'ютерної системи [8].

У частині Конвенції, присвяченій злочинам, пов'язаним із електронними повідомленнями, йдеться про допустимість письмових електронних повідомлень як доказів у кримінальних справах, якщо вони зберігались та були надані відповідно до усіх необхідних процесуальних норм.

Цікавим є підхід, запропонований у *Конвенції Африканського Союзу стосовно традиційних видів злочинів, учинених з використанням інформаційно-комунікаційних технологій*. У цьому міжнародному документі чітко визначено, що такі види посягання на власність, як крадіжка, шахрайство, володіння викраденою власністю, зловживання довірою, вимагання грошових коштів і шантаж із використанням комп'ютерних даних, є злочинами, а використання інформаційно-комунікаційних технологій для вчинення таких видів злочинів, як: крадіжка, шахрайство, володіння викраденою власністю, зловживання довірою, вимагання грошових коштів, тероризм та відмивання грошей – є обтяжуючою обставиною. Також у Конвенції зазначено про необхідність модернізувати норми, що стосуються засобів поширення інформації, зокрема й цифрових електронних засобів зв'язку, та обмеження доступу до критично важливих структур національної оборони. Усі ці види злочинів однаковою мірою стосуються і юридичних осіб. Що ж до процесуальних норм, то Конвенція містить положення, якими врегульовано збереження комп'ютерних даних, їх перехоплення та вилучення [8].

На підставі аналізу регіональних підходів до проблеми боротьби з інформаційною злочинністю можна дійти висновку, що, безперечно, у розглянутих документах використовується різна термінологія з відмінним змістовним наповненням, різняться також підходи до класифікації інформаційних злочинів, проте механізми та форми міждержавного співробітництва подібні з огляду на прагнення держав до тісної співпраці у протистоянні інформаційним загрозам. Безумовно, сучасний світ і безперервне вдосконалення інформаційно-комунікаційних технологій диктують нові умови, а тому сферу дії угод, прийнятих десять років тому, складно порівняти із сучасними правовими інструментами. Проте до прийняття єдиного уніфікованого документа з питань протидії інформаційній злочинності регіональні угоди залишатимуться дієвим механізмом міждержавного співробітництва.

Список використаних джерел:

1. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 года // Московский журнал международного права. – 2008. – № 4 (72). – С. 244–250.
2. Конвенція про кіберзлочинність від 23 листопада 2001 року [Електронний ресурс]. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/994_575
3. Додатковий протокол до Конвенції про кіберзлочинність від 28 січня 2003 року [Електронний ресурс]. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/994_687
4. *Gercke M.* Understanding cybercrime: phenomena, challenges and legal response/ M. Gercke [Електронний ресурс]. – Режим доступу: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_E.pdf
5. Конвенція Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства від 25 жовтня 2007 року [Електронний ресурс]. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/994_927
6. Соглашение между правительствами государств – членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 года [Электронный ресурс]. – Режим доступа: http://base.spinform.ru/show_doc.fwx?rgn=28340
7. Arab Convention on Combating Information Technology Offences [Електронний ресурс]. – Режим доступу: http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Information_Technology_Offences
8. African Union Convention on Cyber Security and Personal Data Protection [Електронний ресурс]. – Режим доступу: http://pages.au.int/sites/default/files/en_AU%20Convention%20on%20CyberSecurity%20Pers%20Data%20Protec%20AUCyC%20adopted%20Malabo.pdf

Ольга ГРИЦУН

МІЖНАРОДНО-ПРАВОВЕ РЕГІОНАЛЬНЕ РЕГУЛЮВАННЯ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ ЗЛОЧИННОСТІ

Здійснено аналіз регіональних підходів до розуміння інформаційної злочинності, а також класифікацію правопорушень і основних форм міждержавного співробітництва у сфері боротьби з інформаційними злочинами.

Ключові слова: інформаційна злочинність; кіберзлочинність; інформаційно-комунікаційні технології; кримінальний злочин; комп'ютерна система.

Вісник Національної академії прокуратури України № 4(42)'2015, с. 92–98

Ольга ГРИЦУН

МЕЖДУНАРОДНО-ПРАВОВОЕ РЕГИОНАЛЬНОЕ РЕГУЛИРОВАНИЕ ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННОЙ ПРЕСТУПНОСТИ

Осуществлен анализ региональных подходов к пониманию информационной преступности, а также классификация правонарушений и основных форм межгосударственного сотрудничества в сфере борьбы с информационными преступлениями.

Ключевые слова: информационная преступность; киберпреступность; информационно-коммуникационные технологии; уголовное преступление; компьютерная система.

Olga GRYTSUN

INTERNATIONAL LAW OF ANTI-INFORMATION CRIME ACTIVITIES

The article analyzes regional approaches to understanding information crimes, classification of offenses and the main forms of international cooperation in the field of combating information crimes.

Keywords: information crimes; cybercrime; information and communication technologies; criminal offense; computer system.