УДК 343.98

Гринчак Ірина Володимирівна,
магістрант
Львівського національного університету
імені Івана Франка

КІБЕРЗЛОЧИННІСТЬ ЯК ЗЛОЧИН МІЖНАРОДНОГО ХАРАКТЕРУ

Стаття розглядає проблему явища кіберзлочинності як об'єкта міжнародного кримінального права. Основна увага зосереджена на аналізі правової природи та особливостях кіберзлочинності як злочин міжнародного характеру, тобто – відповідного міжнародного стандарту. Акцентується увага на тому, що державам вкрай важливо використовувати однотипні моделі поведінки, які можливі лише у випадку спорідненості чи схожості їх національного карного законодавства або додаткових домовленостей та погоджень щодо переслідування правопорушників. Здійснюється авторський аналіз «Конвенції про кіберзлочинність», та особливостей її імплементації у вітчизняне законодавство.

Ключові слова: *злочин міжнародного характеру, подвійна кримінальність, співробітництво держав у боротьбі зі злочинністю.*

Постановка проблеми. У сучасних умовах стрімкий розвиток інформаційних технологій та необхідність обміну інформацією через використання глобальної інформаційної мережі Інтернет створюють сприятливий клімат для злочинних посягань завдяки можливості необмеженого та неконтрольованого доступу широкого кола користувачів. Привласнення коштів з банківських рахунків інших осіб, у тому числі і на території інших держав, кібератаки на Пентагон та інші держустанови США, блокування діяльності аеропорту у Варшаві яскраве цьому підтвердження. Беззаперечно, кіберзлочини вже набули транснаціонального характеру і міжнародна спільнота, враховуючи можливі негативні наслідки цього явища, намагається мінімізувати їх посягання на міжнародні відносини.

Аналіз останніх досліджень і публікацій. Кримінальному праву загалом відомі декілька моделей протиправної поведінки фізичної особи, яка породжує міжнародно-правові наслідки, оскільки місце скоєння, початок скоєння злочину чи сам правопорушник можуть знаходитися у межах юрисдикції різних держав. Злочином також може бути вчинено посягання на громадян, майна чи інтересів держави закордоном тощо. Видається, необхідність застосовувати єдині підходи до названих ситуацій сумнівів не викликає. Тому, державам вкрай важливо використовувати однотипні моделі поведінки, які можливі лише у випадку спорідненості чи схожості їх національного карного законодавства або додаткових домовленостей та погоджень щодо переслідування правопорушників. Поняття «злочин міжнародного характеру» загалом було запропоновано радянськими вченими для позначення об'єкту міжнародно-правового співробітництва держав у боротьбі зі злочинністю. Його використовували відомі дослідники явища співробітництва держав з питань протиправної поведінки індивіда, яка створювала правові наслідки для

міжнародного права, зокрема Л. Галенская, І. Карпец, А. Решетов та ін. Зазвичай назва явища повністю відповідала категорії правовідносин, зважаючи на те, які наслідки породжували протиправні діяння індивіда.

Методологічною основою нашого дослідження стали праці таких науковців, як В. Бабакіна, І. Карпеця, О. Орлова, Ю. Онищенка, В. Панова, С. Черніченка та ін.

Постановка завдання. Метою нашого дослідження є утвердження явища злочину міжнародного характеру в якості відповідного міжнародного стандарту, визнаного державами та закріпленого нормами міжнародного права; аналіз транснаціонального характеру кіберзлочинності; аналіз конструкції кіберзлочинності як злочину міжнародного характеру.

Виклад основного матеріалу дослідження. Наукова література акцентує увагу на кількох стандартних поняттях злочину міжнародного характеру. Зокрема, І.Карпець розуміє під «злочинами міжнародного характеру» діяння, передбачені міжнародними угодами (конвенціями), що зазіхають на нормальні відносини між державами, наносять шкоду мирному співробітництву в різних сферах відносин (економічних, соціально-культурних, майнових і т.п.), а також організаціям і громадянам, відповідальність за які настає або відповідно до норм, встановлених у міжнародних угодах (конвенціях), ратифікованих у встановленому порядку, або відповідно до норм національного карного законодавства [1, с. 48].

В. Панов, вважає, що терміни «злочин міжнародного характеру» і «міжнародні карні злочини» є синонімами і характеризують ці злочини як такі, «що не мають безпосереднього зв'язку зі злочинною діяльністю конкретної держави, однак зазіхають одночасно на міжнародний і національний правопорядок, на мирне співробітництво держав у галузі економіки, культури, торгівлі, на права і свободи людини, інтереси юридичних осіб і становлять суспільну небезпеку для багатьох держав»[4, с. 13].

С.Черніченко під «злочином проти міжнародного права (злочину відповідно до міжнародного права)» розуміє дії індивідів, що представляють небезпеку в міжнародному масштабі, які визнаються державами злочинними і потребують об'єднання зусиль для боротьби з ними [3, с. 149].

Динаміка формування міждержавних взаємовідносин у питанні співробітництва у боротьбі зі злочинністю завжди вимагала використання або однотипної поведінки переслідування правопорушника за умови співпадіння положень кримінального законодавства договірних сторін, або формування міжнародного стандарту відповідної протиправної поведінки міжнародно-правовими механізмами. У внутрішньому кримінальному праві склад злочину уособлює протиправну поведінку і являє собою сукупність встановлених карним законом ознак, що характеризують конкретне суспільно небезпечне діяння як злочин. Для забезпечення належного співробітництва держав протиправність поведінки індивіда сприймається як факт і зазвичай криміналізується усіма договірними сторонами. Отже, як міжнародно-правове явище, «злочин міжнародного характеру» – це відповідний стандарт протиправної поведінки індивіда, закріплений нормами міжнародного права і визнаний державами, які приймають участь у міжнародному співробітництві з питань боротьби зі злочинністю.

Допустимість такого підходу підтверджує низка конвенцій універсального характеру, прийнятих у тому числі і під егідою ООН. Суть злочину міжнародного характеру як стандарту протиправної поведінки розкривається через галузевий принцип подвійної криміналізації: сторони співробітництва розглядають поведінку фізичної особи у повному її обсязі як протиправну, заборонену і карану. Відповідно, склад злочинів

міжнародного характеру загалом повторює систему ознак протиправної поведінки фізичної особи, що знайшли відбиття в кримінальному праві різних держав і характеризують конкретне суспільно небезпечне діяння як протиправне.

Зміст співробітництва держав у боротьбі зі злочинністю повністю узгоджується із вимогами основних принципів міжнародного права. Повагу до державного суверенітету та правових наслідків, які з нього випливають, гарантує основний принцип міжнародного права «Суверенна рівність держав», який дає змогу встановити одинакові засади співробітництва для всіх держав без будь-яких переваг чи обмежень. У держави, що потерпіла від наслідків протиправної поведінки особи в силу державного суверенітету, завжди виникає так би мовити «право на переслідування», яке має значення і для міжнародного права. Межі цього права є досить широкими, оскільки держава самостійно, на власний розсуд, виходячи з існуючих реальностей і потреб встановлює обсяг і розмір сатисфакції. «Право на переслідування» є достатньою підставою для поведінки іншого суб'єкта міжнародного права у міжнародних відносинах. По суті, поважаючи «право на переслідування», як наслідок, що випливає з державного суверенітету, держава змушена здійснювати певну поведінку на міжнародній арені: співпрацювати з метою забезпечити це право.

Зважаючи на дисбаланс між розвитком технологій і здатністю подолати негативні наслідки їх використання державами самотужки, міжнародно-правове співробітництво є вагомим засобом у боротьбі із кіберзлочинністю. Останніми роками спостерігається активізація зусиль у прийнятті міжнародних та регіональних документів, які регулюють питання протидії цьому явищу. Формування міжнародних стандартів здійснюється на базі інтелектуальних та технічних розробок передових країн, які вже мають певний досвід у боротьбі з ним. Запровадження відповідних передових стандартів суттєво полегшує боротьбу із кіберзлочинністю, оскільки такі категорії злочинів характерні обмеженому колу держав, а мета співробітництва полягає у виявленні та ізоляції, як мінімум, міжнародних хакерів.

Базовим документом у боротьбі з кіберзлочинністю для європейських країн є Конвенція Ради Європи про кіберзлочинність від 23.11.2001 р. [2] (надалі – Конвенція) та Додатковий протокол до неї від 28.01.2003 р. Сьогодні вона є фундаментом для розробки відповідного законодавства європейських держав. Беззаперечно, що ефективність міжнародного співробітництва вимагає одноманітного підходу сторін до кваліфікації міжнародно-правових явищ. У нашому випадку – це факт скоєння злочину, який фіксує не лише наявність протиправної поведінки індивіда, а також кваліфікацію її сторонами співробітництва в якості забороненої.

У міжнародному кримінальному праві це знайшло закріплення у галузевому принципі, який отримав назву «подвійної кримінальності» – особа розцінюється як злочинець договірними сторонами, а її поведінка – протиправною та забороненою. Його суть полягає у наступному: держава що потерпіла від протиправної поведінки і держава до якої звернене клопотання про співробітництво визначену особу за вчинену поведінку можуть притягнути до відповідальності самостійно (або ж іншими словами – паралельно). Як наслідок, можна говорити про ідентичність злочину для обох сторін, якому характерна однакова суспільна небезпека, відповідність санкцій за національним законодавством тощо.

Конвенція формує новий міжнародний стандарт – злочин міжнародного характеру: «кіберзлочин». За своєю правовою конструкцією він є збірним поняттям, яке включає декілька різнопланових протиправних посягань. Так, зокрема криміналізуються: атаки на

комп'ютерні дані і системи, протиправне (злочинне) використання роботи комп'ютерів, а також діяльності, пов'язаної з розповсюдженням забороненої чи використанням захищеної відповідними правами інформації.

Система протиправних дій, визначених Конвенцією, виокремлює наступні категорії правопорушень:

- правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем;
- правопорушення, пов'язані з комп'ютерами;
- правопорушення, пов'язані зі змістом інформації;
- правопорушення у сфері авторських і суміжних прав.

Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (так звані «CIA-злочини») включають незаконний доступ, нелегальне перехоплення комп'ютерних даних, втручання у дані, втручання у систему, зловживання пристроями.

Правопорушення, пов'язані з комп'ютерами, передбачають підробку і шахрайство, здійснені з використанням комп'ютерів.

Правопорушення, пов'язані зі змістом інформації – це дитяча порнографія, расизм та ксенофобія тощо.

Правопорушення, пов'язані з порушенням авторських і суміжних прав, охоплюють незаконне відтворення і використання комп'ютерних програм, аудіо/відео і інших видів цифрової продукції, а також баз даних і книг.

Ознаками, що характеризують кіберзлочинність як злочин міжнародного характеру, є його підвищена суспільна небезпека внаслідок посягання на порядок і режим існування інформації, доступ до якої здійснюється з використанням електронно-технічних засобів. На користь цього свідчить значна вразливість національного і міжнародного правопорядків від цих видів злочинної діяльності, обмежені можливості держав та міжнародного співтовариства щодо попередження, контролю і боротьби з такими злочинами, а також можливий істотний розмір шкоди, завданий кіберзлочинністю.

Сфера високих технологій загалом характеризується значними фінансовими затратами і злочинні посягання на їх результати складає суспільну небезпеку цієї категорії злочинів. Крім того, важливою складовою є співвідношення між власне витратами на підготовку і вчинення злочинів та їх результатами чи наслідками. Відтак, економічна складова кіберзлочинності формує підставу для взаємодії держав у боротьбі з цим негативним явищем у міжнародних відносинах, оскільки сьогодні вже існує створена комп'ютерними мережами та інформаційними технологіями зручна інфраструктура зберігання та використання інформації, постачання товарів, надання послуг, переказу коштів між фізичними і юридичними особами у тому числі – і міжнародних.

Економічна складова – це, по суті, шкода у матеріальному еквіваленті. Вона пронизує усі категорій протиправних дій, які підпадають під термін «кіберзлочинність». Так, посягання на конфіденційність, цілісність та доступності комп'ютерних даних і систем дозволяє правопорушникам перш за все не санкціоновано користуватися інформацією обмеженого доступу. Режим обмеженого доступу вказує на можливі негативні наслідки оприлюднення інформації майнового та немайнового характеру, погіршення іміджу, упущеної вигоди тощо. Зловживання, пов'язані з комп'ютерами безпосередньо спричиняють шкоду, оскільки їх витоки пов'язані з крадіжками коштів, шахрайством тощо. У зміст інформації теж можна від слідкувати економічний інтерес: оплата за отримання відповідної інформації. Як правило, розрахунки проводяться

анонімно, кошти акумулюються та використовуються неконтрольовано, тобто підприємницька діяльність є повністю «тіньовою». У свою чергу порушення авторських та суміжних прав давно виступає, як злочин економічного характеру через існування «піратського» бізнесу на міжнародному рівні.

Кіберзлочини, визначені Конвенцією – це далеко не всі протиправні дії, які наносять шкоду міжнародному економічному співробітництву. На їх основі розвиваються широкі можливості для вчинення так званих «пов'язаних» злочинів, зокрема: фінансування тероризму (приклад України), відмивання грошей, незаконних доходів від використання чужих інтелектуальних прав та заняття нелегальним бізнесом (розповсюдження порнографії, гральний бізнес тощо).

Окрім фінансової вигоди злочинців, шкода може бути нанесена шляхом дискредитації урядів і держав, анонімним вербуванням найманців у зони збройного конфлікту, руйнування ключових систем інформаційно-комунікаційні мереж внесенням до них фальсифікованих даних або постійного виведення цих систем з робочого стану тощо.

Транснаціональний характер протиправних дій доводить, що вони можуть здійснювати свою діяльність з території власної або третьої держави, а також з тих територій, в яких недостатньо розвинений режим протидії. Злочинців зазвичай приваблює відсутність фізичного контакту з потерпілими, складністю виявлення, фіксування та вилучення криміналістично-значущої інформації у віртуальному просторі. З огляду на вищевказані передумови, у міжнародному праві виникають відповідні міжнародно-правові зобов'язання, які вимагають вдосконалення національного законодавства як у галузі карного права, так і кримінального процесу. Вважається, що їх зміст включає попередження злочинності завдяки формуванню відповідних стратегій і заходів, спрямованих на зниження ризику скоєння злочинів і нейтралізацію потенційно шкідливих наслідків для приватних осіб і суспільства. Сьогодні у галузі попередження кіберзлочинності належать прийняття більш досконалих законів протидії, розвиток потенціалу органів кримінального правосуддя і правоохоронних органів, постійного моніторингу та обміну новітньою інформацією про криміногенну ситуацію, пов'язану із кіберзлочинами.

Система злочинів у сфері кіберзлочинності, запропонована національним законодавством України, охоплює кримінальні правопорушення у сфері: використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (у сферах платіжних систем); обігу інформації протиправного характеру із використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; господарських відносин та приватної власності, яка включає в себе незаконні фінансові операції та заборонені види господарської діяльності, що здійснюються за допомогою мереж електрозв'язку чи комп'ютерних мереж.

Висновки. Останнім часом в Україні активізувалися наукові дослідження з питань протидії кіберзлочинності у різних напрямках. Так, А. Широкова-Мурараш акцентує увагу на кіберзлочинності та кібертероризмі у сфері інформаційної безпеки, О. Орлов та Ю. Онищенко аналізують аспекти правової допомоги з питань кіберзлочинності, В. Бабакін – міжнародне співробітництво у розслідуванні кіберзлочинів. Натомість, питання поняття та особливостей кіберзлочинності як злочину міжнародного характеру,

залишаються поза увагою дослідників. Сьогодні вже назріла необхідність напрацювання відповідних концепцій для забезпечення сприйняття міжнародних стандартів у боротьбі з кіберзлочинністю та імплементації їх у національне законодавство України.

Список використаних джерел

1. Карпец И. И. Преступления международного характера / И. И. Карпец. – М. : Юрид. лит., 1979. – 111 с.
2. Конвенція про кіберзлочинність // Відомості Верховної Ради України. – 2006. – № 5- 6. – Ст. 71.
3. Международное уголовное право : учеб. пособие / под общей ред. В Н. Кудрявцева. – 2-е изд., перераб. и доп. – М. : Наука, 1999. – 264 с.
4. Панов В. П. Сотрудничество государств в борьбе с международными уголовными преступлениями: учеб. пособ. / В. П. Панов. – М. : Юрист, 1993. – 160 с.

Грынчак И. В. Киберпреступность как преступления международного характера

Статья рассматривает проблему явления киберпреступности как объекта международного уголовного права. Основное внимание сосредоточено на анализе юридической природы и особенностей киберпреступности как преступления международного характера, тоесть – соответствующего международного стандарта. Акцентируется внимание на том, что государствам крайне важно использовать однотипные модели поведения, которые возможны только в случае родства или сходства их национального уголовного законодательства или дополнительных договоренностей и согласований с преследованием правонарушителей. Осуществляется авторский анализ «Конвенции о киберпреступности», и особенностей ее осуществления в отечественное законодательство.

Ключевые слова: *преступление международного характера, двойственная криминализация, сотрудничество государств в борьбе с преступностью.*

Grynchak I. V. Cybercrime as crimes of an international character

The article reveals the crime of international character as an object of international criminal law. The attention is focused on the analysis of law nature and peculiarities of crimes of international character. The possibility the consider crime of international character as an appropriate standard and object of international law is discussed. The attention is focused on what is essential for States to use the same type of behaviors that are possible only in the case of kinship or similarity of their national criminal legislation or other arrangements and agreements with the prosecution of offenders. Implemented by the author's analysis of the «Convention on Cybercrime» and especially its implementation in domestic legislation.

Key words: *object of international law, minimal standards of the sphere of human rights and fundamental freedoms, crime of international character.*