АКТУАЛЬНІ ПРОБЛЕМИ МІЖНАРОДНИХ ВІДНОСИН ТА БЕЗПЕКИ

УДК 343
DOI https://doi.org/10.32782/app.v71.2023.21

М. О. Думчиков
orcid.org/0000-0002-4244-2419
кандидат юридичних наук,
старший викладач кафедри кримінально-правових дисциплін
та судочинства
Навчально-наукового інституту права
Сумського державного університету

АНАЛІЗ МІЖНАРОДНИХ НОРМАТИВНИХ АКТІВ В СФЕРІ ВСТАНОВЛЕННЯ КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ЗА СУСПІЛЬНО НЕБЕЗПЕЧНІ ДІЯННЯ ВЧИНЕННІ В КІБЕРПРОСТОРІ

Актуальність теми полягає у встановленні позитивних та негативних наслідків імплементації норм Конвенції «Про кіберзлочинність» в національне законодавство України, шляхом аналізу кримінальних правопорушень, які визначені в Конвенції та тих, що регламентовані Кримінальним кодексом України.

Метою статті є аналіз міжнародних нормативних актів в сфері встановлення кримінальної відповідальності за суспільно небезпечні діяння вчиненні в кіберпросторі.

Виклад основного матеріалу. Неоднорідність легального закріплення складів кримінальних правопорушень, пов'язаних із використанням інформаційно – телекомунікаційних технологій, у законодавстві різних держав актуалізує проблему уніфікації правового регулювання таких відносин на міжнародному рівні. Відправною точкою в цьому питанні має бути теза про відсутність державних кордонів для цього виду кримінальних правопорушень. Робота щодо здійснення правового регулювання в цьому напрямку ведеться на універсальному, міждержавному та регіональному рівнях. Завдяки ратифікації державами учасницями, міжнародних договорів, встановлюються єдині правила міжнародного співробітництва в сфері протидії злочинності з використанням інформаційно – телекомунікаційних технологій.

Міжнародні договори, підписані державами, що їх підписали, встановлюють єдину основу для юрисдикції та правил міжнародного співробітництва між державами у боротьбі зі злочинністю шляхом використання комп'ютерних технологій.

Відомо, що Рада Європи докладає значних зусиль щодо уніфікації законодавства держав – учасниць у сфері правового регулювання кримінальних правопорушень у кіберпросторі.

Історично першим нормативним актом Ради Європи, з питань регулювання кримінальної відповідальності за кримінальні правопорушення, вчинені шляхом використання інформаційно – телекомунікаційних технологій виступала Рекомендація від 13 вересня 1989 № 89 (9) «Про кримінальні правопорушення, які пов'язані з комп'ютером» (Рекомендація Ради Європи, 1989).

Відповідно до зазначеного документа, держави – учасниці Ради Європи, повинні при розробці свого національного законодавства, прийняти о уваги Звіт Європейського комітета по проблемам злочинності, пов'язаної з комп'ютерами. В рамках цього Звіту Комітет дав оцінку, самому явищу комп'ютерної злочинності, та надав рекомендації щодо тих видів криміналь-

них правопорушень у кіберпросторі, які держави – учасниці повинні криміналізувати (Final report of the European Committee on Crime problems, 1989).

Зауважимо, що даний нормативний акт носив лише рекомендаційний, характер, однак саме після його прийняття почався процес фактичного створення кримінального законодавства держав – учасниць в розрізі регулювання відносин за вчинення кримінальних правопорушень у кіберпросторі.

Звіт дає певну класифікацію кримінальним правопорушенням, які держави учасниці повинні криміналізувати, так зокрема, виділяється список мінімально необхідних до введення в національне законодавство та додаткових (необов'язкових).

В свою чергу до мінімальних Рекомендація Ради Європи відносить:

1) Комп'ютерне шахрайство;

2) Комп'ютерну фальсифікацію;

3) Завдання шкоди комп'ютерним даним або комп'ютерними програмам;

4) Комп'ютерний саботаж;

5) Несанкціонований доступ до цифрового пристрою;

6) Несанкціонований перехват цифрової інформації;

7) Несанкціоноване відтворення цифрової інформації;

8) Несанкціоноване використання мікросхем.

Одночасно з цим Рекомендація надавала необов'язковий до криміналізації перелік складів кримінального правопорушення, зокрема:

1) Неправомірна зміна даних та програмного коду в комп'ютері;

2) Комп'ютерне шпигунство;

3) Неправомірне використання комп'ютера;

4) Несанкціоноване використання комп'ютерної програми.

Незважаючи на те, що нормативний акт носив рекомендаційний характер, низька європейський держав, поклала його в основу створення своєї національної системи по боротьбі з кримінальними правопорушеннями у кіберпросторі.

Наступним документом, який по праву можна назвати основоположним у питаннях регулювання кримінальної відповідальності за вчинення кримінальних правопорушень у кіберпросторі є Будапештська Конвенція «Про кіберзлочинність». Конвенція містить норми статей матеріального права, щодо зобов'язання держав ратифікантів імплементувати у національні законодавства зазначених норм (Конвенція «Про кіберзлочинність», 2001).

Норми конвенції містять у собі спробу нормативного регулювання трьох основних блоків питань:

– уніфікація правового закріплення кримінальних правопорушень у сфері комп'ютерної інформації у національних законодавствах країн.

– зближення національних кримінально-процесуальних норм.

– регламентація міжнародного співробітництва щодо запобігання та розслідування комп'ютерних злочинів.

Текст цієї Конвенції відкритий для підписання та ратифікації для усіх держав – учасниць Ради Європи, зокрема Україна ратифікувала конвенцію 7 вересня 2005 року, а вже в 9 червня 2006 набрала чинності (Конвенція «Про кіберзлочинність», 2001).

Конвенція містить перелік основних видів комп'ютерних правопорушень, що розкриває їх дефініції, та встановлює заходи відповідальності за їх вчинення, які слід включити до національного законодавства держав – ратифікантів Конвенції. Закріплені у Конвенції склади кримінальних правопорушень розділені на чотири групи відповідно до об'єкта зазіхання:

1. правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем;

2. правопорушення, пов'язані з комп'ютерами;

3. правопорушення, пов'язані зі змістом;

4. правопорушення, пов'язані з порушенням авторських та суміжних прав.

Крім того, 28 січня 2003 Додатковим протоколом до Конвенції «Про кіберзлочинність» було визначено норму направлену на боротьбу з розповсюдженням через комп'ютерні мере-

жі інформації расистського і ксенофобського характеру (Додатковий протокол до Конвенції «Про кіберзлочинність», 2003).

Кожна із закріплених у Конвенції груп містить типові ознаки кримінальних правопорушень, які необхідно закріпити у національному законодавстві держав – учасниць Конвенції.

Так, перша група правопорушень проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, включає в себе наступні види суспільно небезпечних діянь:

1) незаконний доступ
2) нелегальне перехоплення
3) втручання у дані
4) втручання у систему
5) зловживання пристроями

Зауважимо, що всі зазначені суспільно небезпечні діяння, які вчиняються у кіберпросторі, закріпленні в рамках XVI розділу Особливої частини Кримінального кодексу України в рамках статей 361–362. Питання виникає лише, при тлумаченні такої форми вчинення кримінального правопорушення, як нелегальне перехоплення. Зазначимо, що в Кримінальному кодексі України, діяння у формі перехоплення цифрової інформації регламентоване в частині 2 статті 362 Особливої частини Кримінального кодексу України, однак лише щодо спеціального суб'єкта такого правопорушення. Одночасно, в частині 3 статті 361 Особливої частини Кримінального кодексу України визначаються наслідки у формі порушення процесу маршрутизації цифрової інформації (Кримінальний кодекс України, 2001).

Зауважимо, що в доктринальних джерелах такі суспільно небезпечні дії прирівнюються і розглядаються, як синоніми. Однак, на нашу думку порушення процесу маршрутизації це дії спрямовані на цифровий вплив щодо інформації, яка передається, в кінцевому результаті, така інформація просто змією адресата. В свою чергу, перехоплення, це процес отримання такої інформації без подальшого її копіювання, а результатом буде лише процес ознайомлення з нею.

До правопорушень, пов'язаних з комп'ютерами, Конвенція відносить:

1. шахрайство пов'язане з комп'ютером
2. підробка пов'язана з комп'ютерами

Відповідно до часини 3 статті 190 Особливої частини Кримінального кодексу України, шахрайство вчинене шляхом незаконних операцій з використанням електронно – обчислювальної техніки. З одного боку можемо констатувати факт, імплементації норм Конвенції до Кримінального кодексу України, але з іншого, спостерігаємо проблеми правової кваліфікації такого суспільно небезпечного діяння, вчиненого шляхом використання інформаційно – телекомунікаційних технологій (Кримінальний кодекс України, 2001).

Відповідно до даних офіційного веб – ресурсу Департаменту кіберполіції Національної поліції України, фактично всі діяння, які вчиняються у кіберпросторі, шляхом використання інформаційно – телекомунікаційних технологій, систем або мереж, розглядаються Департаментом Кіберполіції, як шахрайство за частиною 3 статті 190 Особливої частини Кримінального кодексу України (Офіційний веб – сайт Департаменту кіберполіції Національної поліції України, 2023). Однак, при розгляді, справ щодо встановлення вини особи у вчиненні кримінального правопорушення регламентованого частиною 3 статті 190 Особливої частини Кримінального кодексу України, суді перекваліфіковують зазначені суспільно небезпечні дії на 1 частину зазначеної статті, мотивуючи це тим, що обман при вчиненні цього кримінального правопорушення може виразитись у застосуванні програмних засобів, які дають змогу винному будь-яким чином (шляхом відшукання випадкових цифр, паролів тощо) здійснити несанкціонований доступ до інформації, яка зберігається чи обробляється в автоматизованих системах, щоб ввести в оману автоматизовану систему і видати себе за того, хто має право в ній працювати і здійснювати відповідні операції (Вирок Ковальського міськрайонного суду Волинської області, 2017).

Фактично позиція суду збігається з формулюванням комп'ютерного шахрайства передбаченого Конвенцією «Про кіберзлочинність». На нашу думку, об'єктом обману може виступати лише фізична особа, а не інформаційно – телекомунікаційна технологія, тому у випадку

наприклад «фішингу», діяння варто кваліфікувати за сукупністю статей 190 та 361, 361-1 Особливої частини Кримінального кодексу України (Кримінальний кодекс України, 2001).

Щодо питання встановлення кримінальної відповідальності за підробку пов'язану з комп'ютером, то тут варто зазначити, що кримінальний закон України, не містить спеціальної норми, яка встановлювала відповідальність за таке діяння, виходячи зі змісту Конвенції. Однак, норми статті 200 Особливої частини Кримінального кодексу України встановлюють кримінальну відповідальність за відробку платіжних банківських карт, підробка яких у будь якому випадку буде пов'язана з тим чи іншим елементом інформаційно – телекомунікаційної техніки. Одночасно, з цим вважаємо за необхідне закріпити спеціальні норми, в кримінальному законі нашої держави (Кримінальний кодекс України, 2001).

Стаття 9 та 10 Конвенції «Про кіберзлочинність», визначає правопорушення пов'язані з дитячою порнографією та з порушенням авторських та суміжних прав. Криміналізації такі суспільно небезпечні діяння набули в статтях 177, 161, 300, 442 Особливої частини Кримінального кодексу України. Однак, самі елементи інформаційно – телекомунікаційних технологій, систем та мереж не визначаються, які такі що підвищують суспільну небезпечність діяння при їх застосуванні (Конвенція «Про кіберзлочинність», 2001).

Враховуючи, що конвенція зобов'язує не просто криміналізувати суспільно небезпечні діяння, які у ній визначені, а зробити при цьому акцент саме на використання елементів інформаційно – телекомунікаційних технологій, систем та мереж при вчиненні зазначених кримінальних правопорушень.

Крім того, норми Конвенції зобов'язують держави – учасниці. кваліфікувати як кримінально протиправні дії підбурювання до скоєння будь-якого з вищедосліджених кримінальних правопорушень, співучасть у ньому, або замах.

При цьому встановлення відповідальності за підбурювання та співучасть є обов'язком держави-підписанта Конвенції, а криміналізація замаху є правом.

Примітно закріплення у Конвенції необхідності залучення до кримінальної відповідальності юридичних. Відповідно до статті 12 Конвенції, корпоративна відповідальність реалізується за вчинення передбаченого Конвенцією кримінального правопорушення щодо юридичної особи фізичною особою чи членом органу управління юридичної особи.

Аналізуючи норми регламентовані Конвенцією «Про кіберзлочинність», можемо зробити висновок, що Конвенція, незважаючи на різноманітність закріплених в ній норм, встановлює лише загальні положення та аспекти, які регламентують відповідальність за кримінальні правопорушення, які вчиняються шляхом використання інформаційно – телекомунікаційних технологій, систем або мереж. Як результат, в рамках імплементації зазначених норм Конвенції в рамках вітчизняного законодавства, потребується суттєві доповнення та уточнення, зокрема в частині приміток до відповідних статей Особливої частини Кримінального кодексу України. Разом з тим вважаємо, що процес імплементації норм Конвенції «Про кіберзлочинність» у вітчизняне законодавство України пройшов успішно, хоча і потребує виділення в окремих кримінальних правопорушеннях кваліфікаційних ознак, які б визначали підвищену ступінь суспільної небезпеки за вчинення кримінальних правопорушень у кіберпросторі.

Література

Рекомендація Ради Європи «Про комп'ютерні правопорушення» від 13.09.1989 № 89 (9). URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804f78de (дата звернення 03.03.2023)

Final report of the European Committee on Crime problems. Council of Europe. URL: https://www.coe.int/en/web/cdpc (дата звернення 03.03.2023)

Конвенція «Про кіберзлочинність» від 23.11.2001. URL: https://zakononline.com.ua/documents/show/224375___562216 (дата звернення 03.03.2023)

Додатковий протокол до Конвенції «Про кіберзлочинність» від 28.01.2003. URL: https://ips.ligazakon.net/document/MU03364 (дата звернення 03.03.2023)

Кримінальний кодекс України від 05.04.2001 № 2341 – III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення 03.03.2023)

Офіційний веб – сайт Департаменту кіберполіції Національної поліції України. URL: https://cyberpolice.gov.ua/ (дата звернення 03.03.2023)

Вирок Ковальського міськрайонного суду Волинської області від 20.07.2027 № 67836018. URL: https://youcontrol.com.ua/ru/catalog/court-document/67836018/ (дата звернення 03.03.2023)

References

Rekomendaciya Radi Yevropi «Pro komp'yuterni pravoporushennya» vid 13.09.1989 № 89 (9). URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804f78de (data zvernennya 03.03.2023)

Final report of the European Committee on Crime problems. Council of Europe. URL: https://www.coe.int/en/web/cdpc (data zvernennya 03.03.2023)

Konvenciya «Pro kiberzlochinnist» vid 23.11.2001. URL: https://zakononline.com.ua/documents/show/224375___562216 (data zvernennya 03.03.2023)

Dodatkovij protokol do Konvenciyi «Pro kiberzlochinnist» vid 28.01.2003. URL: https://ips.ligazakon.net/document/MU03364 (data zvernennya 03.03.2023)

Kriminalnij kodeks Ukrayini vid 05.04.2001 № 2341 – III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (data zvernennya 03.03.2023)

Oficijnij veb – sajt Departamentu kiberpoliciyi Nacionalnoyi policiyi Ukrayini. URL: https://cyberpolice.gov.ua/ (data zvernennya 03.03.2023)

Virok Kovalskogo miskrajonnogo sudu Volinskoyi oblasti vid 20.07.2027 № 67836018. URL: https://youcontrol.com.ua/ru/catalog/court-document/67836018/ (data zvernennya 03.03.2023)

Анотація

Думчиков М. О. **Аналіз міжнародних нормативних актів в сфері встановлення кримінальної відповідальності за суспільно небезпечні діяння вчиненні в кіберпросторі.** – Стаття.

Аналізуючи проблеми встановлення кримінальної відповідальності за кримінальні правопорушення, які вчиняються у кіберпростір, не можна залишити поза увагою міжнародний досвід протидії цьому суспільно небезпечному явищу.

Перш за все, це пов'язано з транснаціональним характером цього типу кримінальних правопорушень, що фактично зумовлює прийняття єдиних стандартів в рамках встановлення кримінальної відповідальності за такі кримінальні правопорушення, а також співпраця з органами внутрішніх справ інших держав. Зауважимо, що така співпраця можлива лише при повному та чіткому розумінні національних особливостей встановлення та реалізації питань кримінальної відповідальності за кримінальні правопорушення у кіберпросторі. Проведення правового дослідження, завжди дозволяє в більшій мірі по іншому розглянути вітчизняне законодавство з питань регулювання питань пов'язаних з охороною кіберпростору, одночасно з цим побудувати систему пропозицій по його подальшому вдосконаленню.

В нашій роботі ми розглянули два нормативні акти, які встановлюють відповідальність за вчинення кримінальних правопорушень у кіберпросторі, зокрема Рекомендація Ради Європи, яка виступає першим нормативним актом щодо регулювання питання відповідальності в кіберпросторі, незважаючи на рекомендаційний характер.

Основоположним нормативним актом з питань регулювання встановлення кримінальної відповідальності у кіберпросторі виступає Конвенція «Про кіберзлочинність» 2001 року, яка і сьогодні не втратила своєї актуальності, а навпаки, виступає певною «конституцію» в сфері боротьби з кримінальними правопорушеннями у кіберпросторі саме в рамках визначення категорій суспільно небезпечних діянь, які зобов'язані криміналізувати держави – учасниці.

В роботі визначено, які кримінальні правопорушення були імплементовані у кримінальний закон нашої держави. Визначено з якими проблеми формулювання, тлумачення та власне кримінально – правової кваліфікації стикається вітчизняне правове поле.

Наголошено на необхідності закріплення в окремих статтях Особливої частини Кримінального кодексу України кваліфікаційних ознак, які б підвищували кримінальну відповідальність за вчинення кримінальних правопорушень у кіберпросторі.

Ключові слова: комп'ютерне кримінальне правопорушення, кіберзлочин, комп'ютерне шахрайство, кримінальні правопорушення у кіберпросторі, кібершахрайство.

Summary

Dumchykov M. O. **Analysis of international regulatory acts in the field of establishing criminal liability for socially dangerous acts committed in cyberspace.** – Article.

Analyzing the problems of establishing criminal liability for criminal offenses committed in cyberspace, one cannot ignore the international experience of countering this socially dangerous phenomenon.

First of all, this is related to the transnational nature of this type of criminal offense, which in fact requires the adoption of uniform standards in the framework of establishing criminal responsibility for such criminal

offenses, as well as cooperation with internal affairs bodies of other states. Note that such cooperation is possible only with a full and clear understanding of the national peculiarities of establishing and implementing issues of criminal liability for criminal offenses in cyberspace. Conducting a legal study always allows to consider the domestic legislation on the regulation of issues related to the protection of cyberspace to a greater extent, and at the same time to build a system of proposals for its further improvement.

In our work, we considered two normative acts that establish responsibility for committing criminal offenses in cyberspace, in particular the Recommendation of the Council of Europe, which is the first normative act to regulate the issue of responsibility in cyberspace, despite its advisory nature.

The Convention "On Cybercrime" of 2001, which has not lost its relevance even today, is the fundamental normative act on the regulation of the establishment of criminal liability in cyberspace, but on the contrary, acts as a certain "constitution" in the field of combating criminal offenses in cyberspace precisely within the framework of defining categories of social dangerous acts, which the participating states are obliged to criminalize.

The work defines which criminal offenses were implemented in the criminal law of our state. It has been determined what problems of formulation, interpretation and actual criminal-legal qualification the domestic legal field faces.

It was emphasized the need to establish in separate articles of the Special Part of the Criminal Code of Ukraine qualifying features that would increase criminal responsibility for committing criminal offenses in cyberspace.

Key words: computer criminal offense, cyber crime, computer fraud, criminal offenses in cyberspace, cyber fraud.