УДК 343.98
DOI https://doi.org/10.32782/pyuv.v2.2023.19

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

І. В. Каріх
orcid.org/0000-0003-3665-4826
кандидат політичних наук,
старший викладач кафедри адміністративно-господарського права,
фінансово-економічної безпеки
Навчально-наукового інституту права Сумського державного університету

ЗАРУБІЖНИЙ ДОСВІД ПРОТИДІЇ КРИМІНАЛЬНИМ ПРАВОПОРУШЕННЯМ ПРОТИ ВЛАСНОСТІ ВЧИНЕНОМУ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Сьогодні злочинність у кібернетичному просторі оголошена глобальною міжнародною проблемою, перш за все, це випливає з прийнятих міжнародних домовленостей та виробленню нових форм співпраці в рамках охорони кіберпростору, а також передбачають взаємодію щодо боротьби з цим високотехнологічним, суспільно небезпечним явищем. В умовах збройної агресії Російської Федерації кількість кібератак на державний інформаційний сектор збільшилася у 35 разів [1]. Одночасно, відповідно до даних Національного банку України кількість кримінальних правопорушень у кіберпросторі в фінансовому секторі за 2022 рік збільшилася на 46% [2].

Масштаби злочинності у кіберпросторі зростають пропорційно кількості нових користувачів. Згідно, статистики Генеральної прокуратури України в період з 2015 по 2020 рік, було обліковано понад 12000 кримінальних правопорушень, які передбачені XVI розділом Особливої частини Кримінального кодексу України, при цьому, зазначається, що у 3 кварталі 2022 року за допомогою засобів Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки було опрацьовано 24 млрд подій інформаційної безпеки, що свідчить про їх архівелику латентність.

Варто відмітити, що власне процес розкриття кримінальних правопорушень у кіберпросторі залишається досить складним завданням для працівників правоохоронних органів. На нашу думку це обумовлене, перш за все самою специфікою цього типу кримінальних правопорушень, а також відсутності методичних рекомендацій, як щодо організації розслідування цього типу суспільно небезпечних діянь, так і щодо тактики провадження слідчих дій. Недостатня кваліфікація працівників правоохоронних органів, щодо роботи з джерелами доказової інформації, зокрема оцифрування електронних повідомлень, сторінок, сайтів, виступає каталізатором вироблення сучасних засобів та методів розслідування кримінальних правопорушень у кіберпросторі.

Це підтверджує той факт, що вдосконалення інформаційно-телекомунікаційних технологій породжує якісну зміну кримінальних правопорушень у кіберпросторі, і сьогодні вже має місце спеціалізація в цій частині злочинного середовища, залежно від якого стали з'являтися такі види кримінальних правопорушень, як кардери, фішери (особи, які займаються шахрайством у кіберпросторі шляхом отримання незаконного доступу до банківських реквізитів, номерів пластикових платіжних карток тощо).

Проблеми протидії зазначеним видам незаконного заволодіння чужим майном гостро стоять перед світовою спільнотою, яка адекватно оцінює ситуацію, що склалася, визнаючи обов'язковість вжиття невідкладних міжнародних заходів.

Перші кроки, які були зроблені з цією метою, було прийняття Рекомендацій № 89 (9) 13 вересня 1989 року на засіданні Комітету міністрів Ради Європи, що містили список кримінальних правопорушень у кіберпросторі. Наступним кроком було прийняття Окінавської хартії Глобального Інформаційного суспільства 22 липня 2000 року. У зв'язку із цим доцільно звернути увагу на те, як на сучасному етапі міжнародні організації розвивають свою діяльність у цьому напрямі [3], [4].

Значний внесок у вирішення проблеми протидії кримінальним правопорушень у кіберпросторі робить ООН. Управлінням ООН з наркотиків та злочинності з метою вивчення проблеми протидії, розробки пропозицій щодо вдосконалення

міжнародних правових заходів та національних законодавств проведено всебічне дослідження проблеми злочинності у кіберпросторі. Для проведення дослідження на прохання Генеральної Асамблеї ООН Комісією з попередження злочинності та кримінального правосуддя було створено міжурядову групу експертів відкритого складу, яка визначила теми та методологію дослідження, прийняла до уваги саме дослідження, а також заходи на нього з боку держав-учасниць, міжнародної спільноти та приватного сектору і вже в 2017 році запропонувала виконувати функції платформи для подальшого обговорення питань, що стосуються злочинності у кіберпросторі, уважно стежити за новими тенденціями [5].

Однак насамперед необхідно проаналізувати Конвенцію Ради Європи «Про кіберзлочинність», прийняту 23 листопада 2001 року, відому також як Будапештська конвенція. В даний час це єдиний глобальний документ міжнародного рівня, який є обов'язковим для держав-учасниць, який регулює дії боротьби з кіберзлочинністю. Україна є державою-учасницею Конвенції з 2005 року.

По-перше, Конвенція визначила види кримінальних правопорушень у кіберпросторі і зобов'язала держави-учасниці вжити законодавчих та інших заходів, необхідних для того, щоб кваліфікувати діяння як кримінальні злочини відповідно до внутрішньодержавного права. Кримінальні правопорушення у кіберпросторі в Конвенції поділено на 5 груп: 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; 5) правопорушення, пов'язані з виявом расизму та ксенофобії, скоєні за допомогою комп'ютерних систем (Додатковий Протокол до Конвенції «Про кіберзлочинність» (Страсбург, 28 січня 2003 р.) [6].

По-друге, Конвенція торкнулася процесуальних питань, питань взаємодії правоохоронних органів держав і, найважливіше, – питання юрисдикції, пропонуючи визначати її територіальною ознакою держави, включаючи борт судна або борт літака держави, а також громадянством особи, що вчинила кримінальне правопорушення. Але в цьому випадку не можна не враховувати те, що віртуальний простір не має фізичних кордонів. Запобігаючи виникненню можливих правових спорів, Конвенція не виключає юрисдикцію, що здійснюється відповідно до норм внутрішньодержавного права, а також пропонує в міру необхідності проводити консультації з метою визначення найбільш підходящої юрисдикції для здійснення судового переслідування.

Можна стверджувати, що Конвенція виступає фундаментальним документом, який визначає основні положення, зміст та напрями міжнародної протидії злочинність у кіберпросторі. Водночас вона визнана й одним із найжорсткіших міжнародних документів. Так, наприклад, Конвенція наділяє провайдерів обов'язком надавати будь-які комп'ютерні дані, відомості про абонентів, за допомогою яких можна встановити вид використовуваної комунікаційної послуги, вжиті з цією метою заходи технічного забезпечення та період надання послуги, особистість користувача, його поштовий чи географічний адрес, відомості про виставлені йому рахунки та здійснені ним платежі, що є в угоді або договорі на обслуговування, будь-які інші відомості про місце встановлення комунікаційного обладнання, що є в угоді або договорі на обслуговування такого користувача [7]. Ще одним міжнародним документом, обов'язковим для його учасників, є Угода Шанхайської організації співробітництва «Про співробітництво у галузі забезпечення міжнародної інформаційної безпеки». Однак у цьому документі акцент зроблено на протидії та виявленні терористичним загрозам у кіберпросторі, загрозам міжнародної безпеки, а питанням криміналізації діянь уваги не приділено [8]. Розглянувши основні міжнародно-правові нормативні акти, з питань регулювання охорони кіберпростору, вбачаємо за необхідне звернути увагу на кримінально-правове регулювання кримінальних правопорушень у кіберпросторі проти власності в окремих зарубіжних країнах.

Англосаксонська правова система не передбачає кодифікацію законодавства, у зв'язку з чим у Великій Британії відповідальність за вчинення кримінальних правопорушень у кіберпросторі встановлюють різні статути: Закон про неправомірне використання комп'ютера, Закон про телекомунікації (обман), Закон про електронному повідомленні, а також Закон про захист персональних даних, Закон про телевізійні ліцензії (розкриття інформації), Закон про боротьбу з обманом у галузі соціального забезпечення [9, с. 211].

Проте жоден із перелічених статутів безпосередньо не встановлює відповідальності за скоєння розкрадань у сфері цифрової інформації. Законом про неправомірне використання комп'ютера передбачено відповідальність за несанкціонований доступ до комп'ютерних матеріалів; несанкціонований доступ із наміром вчинити або полегшити вчинення подальших правопорушень; несанкціоновані дії з наміром завдати шкоди щодо порушення роботи комп'ютера тощо; несанкціоновані дії, що спричиняють або створюють небезпеку значних збитків; виготовлення, постачання або одержання виробів для

використання у вищезгаданих правопорушеннях. Інакше кажучи, комп'ютерна інформація в одних випадках є об'єктом злочину, в інших – предметом і, нарешті, є засобом, способом скоєння суспільно небезпечного діяння.

У Кримінальному кодексі Франції норми, які передбачають відповідальність за кримінальні правопорушення у кіберпросторі, містяться у двох книгах. Так, до книги другої «Про кримінальні правопорушення та провини проти особи», що містить розділ «Про посягання на особистість», включено склади таких суспільно небезпечних діянь, як незаконні дії з особистими даними у телекомунікаційних системах. У книзі третьої «Про майнові кримінальні правопорушення та провини» розміщено главу «Про посягання на системи автоматизованої обробки даних», норми якої передбачають кримінальну відповідальність за її неправомірне використання. З цього випливає, що кримінально-правовій охороні підлягають особисті дані та телекомунікаційні системи. Спеціальних норм про розкрадання, які здійснюються з використанням інформаційно-телекомунікаційних технологій, Кримінальний кодекс Франції не містить [10].

Кримінальним кодексом Швейцарії передбачено відповідальність за кібершпигунство, яке вчинене з корисною метою. Так, відповідно до статті 143 кримінальному покаранню зазнає той, хто з метою власного незаконного збагачення чи збагачення іншої набуває для себе чи іншої особи дані, зібрані чи передані електронним чи іншим подібним способом. Крім цього, статтею 147 встановлено кримінальну відповідальність за шахрайське зловживання із установкою для обробки даних. Глава 9 кримінального закону Швеції присвячена шахрайству. Згідно зі статтею 1 особа, яка шляхом надання неправильної або неповної інформації, або внесення змін до програми чи звітності, або будь-якими іншими способами незаконно впливає на результат автоматичної обробки інформації або будь-якої іншої подібної автоматичної обробки, яка тягне вигоду для особи, яка вчинила злочин, і збитки для будь-якої іншої особи, має бути засуджена за скоєння шахрайства і така ж покарання [11].

Кримінальне законодавство Німеччини комп'ютерне шахрайство виділяє в окреме кримінальне правопорушення, параграфом 263а встановлено відповідальність за дії з метою отримання для себе або третьої особи протиправної майнової вигоди, якими завдається шкода майну іншої особи за допомогою впливу на результат обробки даних комп'ютера шляхом – користування неправильними або неповними даними, несанкціонованим застосуванням даних або іншим неправомірним впливом на процес обробки даних. Комп'ютерна інформація у разі виступає способом скоєння розкрадання [12].

Статтею 246-II Кримінального кодексу Японії передбачено відповідальність за протиправне отримання вигоди за допомогою виготовлення електромагнітного запису, що суперечить істині, а саме встановлено, що особа, яка шляхом подання до інформаційно-телекомунікаційної технології, яка використовується у професійній діяльності іншої особи, сфальсифікованої цифрової інформації або неправомірної команди надало для використання у веденні справ іншої особи електромагнітний запис, що суперечить істині, щодо придбання, втрати або зміни майнового права і таким чином набуло протиправної майнової вигоди або дозволило це іншій особі, яка карається позбавленням волі з примусовим. фізичною працею терміном не понад 10 років [13]. Крім того, в Японії кримінальна відповідальність за незаконне проникнення в комп'ютерні системи та інформаційні мережі з метою крадіжки, псування інформації, а також використання з метою отримання доходу та заподіяння шкоди законним власникам передбачено в законі «Про несанкціоноване проникнення у комп'ютерні мережі» 2000 року [14].

У Кримінальному кодексі Республіки Корея міститься стаття 347-2 «Шахрайство з використанням комп'ютера», згідно з якою особа, яка отримує будь-яку вигоду від власності або сприяє отриманню такої вигоди третьою особою шляхом використання інформації, введення неправдивих чи підроблених даних у технічні засоби, включаючи комп'ютер, підлягає кримінальному покаранню [15].

Кримінальним кодексом Туреччини склад комп'ютерного шахрайства не передбачено, однак пунктом 3 статті 504 встановлено відповідальність за вчинення шахрайства з використанням як знаряддя злочину засобів зв'язку поштових, телеграфних, телефонних установ [16].

Відповідно до параграфу 279а Кримінального кодексу Данії під комп'ютерним шахрайством розуміється незаконна зміна, доповнення, знищення інформації або програми, що використовуються для електронної обробки даних, вчинена для отримання незаконної вигоди [17].

Проаналізувавши міжнародні норми та норми законодавств зарубіжних країн, щодо встановлення кримінальної відповідальності за кримінальні правопорушення у кіберпросторі проти власності у формі шахрайства, можемо визначити наступне: 1) діяльність міжнародних організацій дає змогу з упевненістю наголосити, що світова спільнота активно вживає заходів щодо боротьби з кримінальними правопорушеннями у кіберпросторі, докладає зусиль з реформування законодавства. Але при цьому, визнаючи, що ефективне

протистояння можливе лише за спільних комплексних, узгоджених дій. Прийняті документи міжнародного характеру у зазначеній сфері характеризуються певним ступенем фрагментації з погляду криміналізації діянь. Одночасно, спостерігаємо, що у більшості країн світової спільноти визнається, що для боротьби з феноменом злочинності у кіберпросторі потрібне зміцнення правових заходів, удосконалення законодавства, у тому числі в галузі кримінального права; 2) сьогодні в зарубіжних країнах у частині криміналізації суспільно небезпечних діянь, у формі викрадення та заволодіння чужим майном, що здійснюються з використанням інформаційно-телекомунікаційних технологій, застосовують різні підходи. Ряд країн, таких як, Великобританія та Франція, щодо зазначених кримінальних правопорушень використовують загальні норми про майнові злочини із застосуванням положень, що відображають складові елементи діянь, таких як неправомірний доступ, втручання в персональні дані та інші кримінальні правопорушення у сфері інформаційної та цифрової безпеки. Крім цього, реалізується підхід, при якому застосування інформаційно-телекомунікаційних технологій передбачається як кваліфікуюча ознака складів майнових суспільно небезпечних діянь (Туреччина). В інших країнах, таких Німеччина, Японія, Швейцарія, Данія, Корея, такі кримінальні правопорушення, виділені в окремі склади у системі кримінальних правопорушень проти власності.

Література

1. Кількість кібератак на Україну продовжує зростати – Держспецзв'язку. Офіційний сайт журналу Економічна правд. URL: https://www.epravda.com.ua/news/2022/11/10/693694/

2. Збитки від карткового шахрайства минулого року зросли на 46% – НБУ. Офіційний сайт журналу Економічна правд. URL: https://www.epravda.com.ua/rus/news/2023/05/3/699747/

3. Окінавська хартія глобального інформаційного суспільства. URL: https://studies.in.ua/inform-pravo-shporu/2201-oknavska-hartya-globalnogo-nformacynogo-susplstva.html

4. Рекомендації Комітету міністрів Ради Європи № 89(9) від 13 вересня 1989 року. URL: https://rm.coe.int/168047ebb5

5. Global Programme on Cybercrime. URL: http://www.unodc.org

6. Конвенція Ради Європи «Про кіберзлочинність»: від 21.11.2001 URL: http://zakon.rada.gov.ua/laws/show/994_575

7. Comprehensive Study on Cybercrime. URL: http:///www.unodc.org

8. О. В. Фролова. Міжнародне співробітництво в галузі забезпечення інформаційної безпеки.URL: http://publications.lnu.edu.ua/bulletins/index.php/intrel/article/view/10365

9. Jahankhani H., Al-Nemrat A., Hosseinian-Far A. Cybercrime classification and characteristics. Cyber Crime and Cyber Terrorism Investigator's Handbook. Waltham, 2015. 393 p.

10. Кримінальний кодекс Франції. URL: https://www.equalrightstrust.org/ertdocumentbank/french_penal_code_33.pdf

11. Кримінальний кодекс Швейцарії. URL: https://www.fedlex.admin.ch/eli/cc/54/757_781_799/en

12. Кримінальний кодекс Німеччини. URL: https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html

13. Кримінальний кодекс Швейцарії. URL: https://www.japaneselawtranslation.go.jp/en/laws/view/3581/en

14. Карчевський М.В. Злочини в сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. URL: http://it-crime.at.ua/index/tezi_lekcij/0-31

15. Кримінальний кодекс Республіки Корея. URL: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=28627&lang=ENG

16. Кримінальний кодекс Туреччини. URL: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-REF(2016)011-e

17. Кримінальний кодекс Республіки Корея. URL: https://www.globalwps.org/data/DNK/files/Danish%20Criminal%20Code.pdf

Анотація

Думчиков М. О., І. В. Каріх. **Зарубіжний досвід протидії кримінальним правопорушенням проти власності вчиненому з використанням інформаційно-телекомунікаційних технологій.** – Стаття.

У статті досліджуються питання протидії кримінальним правопорушенням проти власності, які вчиняються з використанням інформаційно-телекомунікаційних технологій, систем та мереж. Визначаються міжнародно-правові стандарти, щодо регулювання цього суспільно небезпечного явища. Наголошується, що що останнім часом поряд із загальнообов'язковими міжнародними та регіональними документами з питань кібербезпеки приймаються й акти рекомендаційного характеру, які можуть використовуватись у правотворчій діяльності будь-якої держави. В дослідженні особливу увагу приділено вивченню проблеми криміналізації суспільно небезпечних діянь, які вчиняються у кіберпросторі.

Наведено приклади того, як по-різному законодавчі органи різних держав підійшли до вирішення проблеми протидії з кримінальними правопорушеннями проти власності, які вчиняються у кіберпросторі, застосовуючи й спеціальні норми про «комп'ютерні» розкрадання, та загальні норми про майнові кримінальні правопорушення в сукупності з нормами про злочини у сфері інформаційної безпеки, а також враховуючи факт використання комп'ютерної техніки як кваліфікуючу ознаку.

У Кримінальному кодексі України, відсутні окремі склади кримінальних правопорушень, які б визначали відповідальність за вчинення цього типу суспільно небезпечних діянь, однак в частині 3 статті 190 Особливої частини Кримінального кодексу України виділяється кваліфікуюча ознака, при вчиненні шахрайства у кіберпросторі.

Акцентовано увагу на регулюванні питання встановлення кримінальної відповідальності у різних правових системах світу, зокрема здійснено аналіз Кримінального кодексу Німеччини, Франції,

Великобританії, Данії, Швейцарії, Туреччини та Республіки Корея.

Проаналізувавши міжнародні норми та норми законодавств зарубіжних країн встановлено, що діяльність міжнародних організацій дає змогу з упевненістю наголосити, що світова спільнота активно вживає заходів щодо боротьби з кримінальними правопорушеннями у кіберпросторі, докладає зусиль з реформування законодавства. Тим не менш, сьогодні в зарубіжних країнах у частині криміналізації суспільно небезпечних діянь, у формі викрадення та заволодіння чужим майном, що здійснюються з використанням інформаційно-телекомунікаційних технологій, застосовують різні підходи.

Ключові слова: кримінальні правопорушення у кіберпросторі, кіберзлочини, кібершахрайство, шахрайство у кіберпросторі, цифрові кримінальні правопорушення, злочинність у кіберпросторі.

Abstract

Dumchykov M. O., Karikh I. V. **Foreign experience of combating criminal offenses against property committed with the use of information and telecommunication technologies.** – Article.

The article examines the issues of combating criminal offenses against property, which are committed with the use of information and telecommunication technologies, systems and networks. International legal standards for the regulation of this socially dangerous phenomenon are determined. It is emphasized that recently, along with the universally binding international and regional documents on cyber security, acts of a recommendatory nature have also been adopted, which can be used in the law-making activities of any state. In the study, special attention is paid to the study of the problem of criminalization of socially dangerous acts committed in cyberspace.

Examples are given of how the legislative bodies of different states approached the problem of dealing with criminal offenses against property committed in cyberspace in different ways, applying both special norms on «computer» theft and general norms on property criminal offenses in combination with norms on crimes in the field of information security, as well as taking into account the fact of using computer equipment as a qualifying feature.

In the Criminal Code of Ukraine, there are no separate categories of criminal offenses that would determine responsibility for committing this type of socially dangerous acts, however, in part 3 of Article 190 of the Special Part of the Criminal Code of Ukraine, a qualifying feature is distinguished when committing fraud in cyberspace.

Attention is focused on the regulation of the issue of establishing criminal liability in various legal systems of the world, in particular, an analysis of the Criminal Code of Germany, France, Great Britain, Denmark, Switzerland, Turkey, and the Republic of Korea was carried out.

Having analyzed the international norms and legislation of foreign countries, it was established that the activities of international organizations make it possible to emphasize with confidence that the world community is actively taking measures to combat criminal offenses in cyberspace, and is making efforts to reform legislation. Nevertheless, today in foreign countries, in terms of criminalizing socially dangerous acts, in the form of theft and taking possession of other people's property, which are carried out using information and telecommunication technologies, different approaches are used.

Key words: criminal offenses in cyberspace, cybercrime, cyber fraudster, fraud in cyberspace, digital criminal offenses, crime in cyberspace.