ФП 2017-5
ISSN 1995-6134

УДК *343.71*
DOI: http://doi.org/10.5281/zenodo.1202450

О.І. КРИВЕНКО,
здобувач Харківського національного університету внутрішніх справ,
м. Харків, Україна

МІЖНАРОДНИЙ ДОСВІД ПРОТИДІЇ ШАХРАЙСТВАМ, ЩО ВЧИНЯЮТЬСЯ ЧЕРЕЗ МЕРЕЖУ ІНТЕРНЕТ (НА ПРИКЛАДІ ЄВРОПЕЙСЬКОГО СОЮЗУ ТА СПОЛУЧЕНИХ ШТАТІВ АМЕРИКИ)

O.I. KRIVENKO,
Applicant of a Ph.D., Kharkiv National University of Internal Affairs,
Kharkiv, Ukraine

INTERNATIONAL EXPERIENCE OF COUNTERING FRAUD COMMITTED THROUGH THE INTERNET (BY THE EXAMPLE OF THE EUROPEAN UNION AND THE UNITED STATES OF AMERICA)

В останнє десятиріччя все більше фізичних та юридичних осіб використовують Інтернет та інші форми електронної зв'язку для проведення транзакцій, що призводить до того, що незаконна діяльність з використанням тих же ресурсів також збільшується. Як відмічають експерти Європейського Союзу з питань протидії Інтернет-шахрайствам, розпочинаючи з середини першого десятиріччя XXI сторіччя, Інтернет-злочинність з кожним роком стає все більш серйозною проблемою. Багато шахраїв, які мігрували в Інтернет-сферу, існували в тій або іншій формі протягом багатьох років, але за допомогою Інтернету останні можуть досягати величезної кількості споживачів одночасно і через кордон. Вказаний технологічний засіб також дозволяє використовувати все більш досконалу технологію шахрайства. Один вірус, що спалахнув у 1999 році, був звинувачений у збитках понад 80 мільйонів доларів, а хакерство на веб-сайтах на початку 2000 року коштувало сотні мільйонів. [1]. Зазначене призводить до того, що правоохоронні органи більшості країн світу витрачають великі суми грошей на оновлення комп'ютерної техніки, підвищення кваліфікації працівників та запровадження інноваційних технологій, однак сучасні шахрайські схеми, що використовуються в мережі Інтернет, як правило, важко відстежувати і доказувати в подальшому судовому порядку. Вказане призводить до того, що в іноземних країнах створюються спеціальні підрозділи як правоохоронної так й суспільно-превентивної направленості, основним обов'язком яких є протидія шахрайствам через мережу Інтернет. Враховуючи викладене, актуальним є розгляд окремих аспектів міжнародного досвіду протидії вказаному виду злочинності на прикладі Європейського Союзу та Сполучених Штатів Америки.

Аналізуючи фахову юридичну літературу, слід відзначити, що фахівцями у сфері кримінології, криміналістики, кримінального процесу, спеціальної техніки та оперативно-розшукової діяльності під різними кутами зору розглядались питання протидії шахрайствам взагалі, та, зокрема шахрайствам, що вчинюються через мережу Інтернет (наприклад, такими вченими, як: С.В. Албул, Л.І. Аркуша, К.В. Антонов, О.М. Бандурка, О.В. Кириченко, А.М. Кислий, І.П. Козаченко, Д.Й. Никифорчук, В.Л. Ортинський, Ю.Ю. Орлов, В.Д. Пчолкін, С.В. Слінько, М.В. Стащак, Р.Л. Степанюк, В.В. Шендрик, О.О. Юхно та ін.). Однак, аналізуючи їх наукові праці та безумовно визнаючи наявні досягнення, слід відзначити, що питання міжнародного досвіду протидії шахрайствам, що вчиняються через мережу Інтерет залишились не розглянутими. Тому метою статті є визначення міжнародного досвіду протидії шахрайствам, що вчиняються через мережу Інтернет на прикладі Європейського Союзу та Сполучених Штатів Америки.

Шахрайство, що вчинюється через мережу Інтернет, підриває не тільки міжурядовий імідж нашої країни, а й економічно-соціальну ситуацію в середині країни. Враховуючи позитивний

ISSN 1995-6134

досвід у цій сфері США та країн ЄС, вважаємо доцільним визначити основні напрямки протидії досліджуваному виду злочинності у названих країнах та окреслити перспективні шляхи впровадження у вітчизняну практику.

Взагалі законодавство ЄС захищає споживачів при купівлі товарів або послуг в Інтернеті, однак постійно зростає число споживачів, які відчувають інтернет-шахрайство. Шахрайство в ЄС за визначенням спільної групи країн ЄС по проблемам Інтернет-шахрайства (на чолі з ECC Lithuania разом із ECC Ireland, ECC Belgium і ECC Slovenia) – це навмисний обман, зробленим для особистої вигоди або з метою заподіяння шкоди іншій особі. Інтернет-шахрайство означає шахрайство, яке здійснюється за допомогою Інтернету. Це стосується шахрайства, скоєного за допомогою електронних покупок, але також за допомогою використання інтернет-послуг, таких як чати, електронні листи, дошки оголошень або навіть програмне забезпечення, щоб нібито обманювати жертв або іншим чином використовувати їх. Шахрайство може бути пов'язано з підробленими аукціонами, продуктами, які навмисно не будуть доставлені, шахрайство з кредитними і дебетовими картами, крадіжки особистих даних і фішингу [2]. Враховуючи вказане, не є дивним, що протидія вказаному виду злочинів покладена на підрозділи Європейського відділу по боротьбі з шахрайством та Європолу.

Що стосується Європейського відділу по боротьбі з шахрайством (OLAF), то до його компетенції входить:

– розслідування випадків шахрайства, корупції та інших видів незаконної діяльності;

– виявлення і розслідування серйозних порушень з боку співробітників ЄС пов'язаними із шахрайськими діями;

– надання допомоги Європейській комісії у формулюванні і впровадженні політики запобігання та виявлення шахрайства [3].

Розслідування можуть включати співбесіди та огляд приміщень, у тому числі, за межами ЄС. Європейський відділ по боротьбі з шахрайством також координує інспекції національних агентств по боротьбі з шахрайством.

Після проведення розслідування Європейський відділ по боротьбі з шахрайством рекомендує вжити заходів щодо інститутів ЄС і відповідних національних урядів: кримінальні розслідування, судове переслідування, фінансове оздоровлення або інші дисциплінарні заходи. Європейський відділ по боротьбі з шахрайством також контролює виконання цих рекомендацій.

В свою чергу, Europol створив в 2013 році Європейський центр кіберзлочинності (EC3), щоб посилити реакцію правоохоронних органів на кіберзлочинність в ЄС і, таким чином, допомогти захистити громадян Європи, бізнесу та уряду від онлайн-злочинності [2].

Мета Європейського центру кіберзлочинності – надати поліції ЄС центральну платформу для координації розслідувань і збору інформації про діяльність в області кіберзлочинності. Він повинен підвищити здатність ЄС виявляти і ліквідовувати винних у злочинній діяльності, здійснюваної в Інтернеті.

Відповідно до мандату Європолу, Європейський центр кіберзлочинності створений для розширення співпраці в правоохоронних операціях, але не має права отримувати прямі звіти від потерпілих та не проводити розслідування на їх основі [2].

Означений центр уповноважений вирішувати проблеми у сфері кіберзлочинності, зокрема ті, що:

– здійснюються організованими групами для отримання великих доходів, одержаних злочинним шляхом, таких як онлайн-шахрайство;

– завдають серйозну шкоду жертві (наприклад, сексуальна експлуатація дітей в Інтернеті та ін.);

– впливають на критичну інфраструктуру і інформаційні системи в Європейському Союзі [2].

Так, Робоча група Європейського Союзу з протидії Інтернет-шахрайствам констатувала, що, по-перше, найбільш часто повідомляються випадки шахрайства у транскордонній електронній торгівлі; по-друге, відповідно до практики Європейського центру кіберзлочинності, фальшиві пропозиції, старі автомобілі і контрафактна продукція були найбільш поширеними видами шахрайства в Інтернеті, а фішинг-шахрайство, які були менш частими, але все ж значними за матеріальними збитками, що завдали; по-третє, компетентність Робочої групи Європейського Союзу з протидії Інтернет-шахрайствам в разі шахрайства обмежена, оскільки їх роль в основному полягає в консультуванні з питань прав споживачів та допомоги у вирішенні торгових суперечок з чесними торговцями. У випадку шахрайства, що походять від недобросовісних торговців, зазвичай важко знайти винного, споживачам завжди рекомендується звернутися до поліції або правоохоронних органів [2].

На рівні Європейського Союзу Європейський центр кіберзлочинності (EC3) надає платформу для координація розслідувань національної поліції з питань кіберзлочинності. Він також збирає

ISSN 1995-6134

інформацію про кіберзлочинність з широкого кола державних, приватних і відкритих джерел, щоб збагатити наявні поліцейські дані, забезпечує судову підтримку, а також інші послуги, які в кінцевому підсумку спрямовані на захист громадян ЄС від онлайн-шахрайства. Тому важливо, щоб споживачі повідомляли про шахрайство.

Водночас, у 2015 році для оптимізації та покращення роботи Європейського центру кіберзлочинності була створена Робоча група Європейського Союзу з протидії Інтернет-шахрайствам, яка готує звіт про «повернення грошей», тобто можливість для споживачів отримати відшкодування від компанії кредитної карти в разі, якщо замовлений продукт не буде доставлений. Незалежно від того, чи наданий варіант платежу за договором з емітентом кредитної картки або національним законодавством, споживачі завжди повинні спочатку звернутися до постачальника кредитних карт, щоб отримати відшкодування [3].

Багато шахраїв, які мігрують в Інтернет, існують у тій чи іншій формі протягом багатьох років, але розвиваються за допомогою технологій. Споживачі повинні бути обережні і розуміти, що шахрайство буде продовжувати розвиватися в нові форми і платформи. Оскільки майже половина споживачів в ЄС купують онлайн, з 11 % шопінгом у трейдерів, які базуються в іншій європейській країні, неминучим є те, що онлайн-шопи можуть зіткнутися з шахрайством з електронною комерцією на певному етапі.

У зв'язку з цим, важливо підкреслити, що, хоча Робоча група Європейського Союзу з протидії Інтернет-шахрайствам має обмежені повноваження у частині забезпечення відшкодування шкоди, якщо вони стають жертвами шахрайства, однак вона є дуже активна в просуванні обізнаності про шахрайство. Сайти більшості членів Робочої групи Європейського Союзу з протидії Інтернет-шахрайствам містять безліч інформації національною мовою для громадян про шахрайські дії і про те, як уникнути їх. Крім того, вона регулярно висвітлює проблеми, пов'язані із шахрайством у місцевих ЗМІ. Тобто, по суті Робоча група Європейського Союзу з протидії Інтернет-шахрайствам відіграє превентивну роль в діяльності Європейського центру кіберзлочинності [2].

Окремо відмітимо, що однією із найбільших проблем протидії Інтернет-шахрайствам в ЄС є те, що дії по боротьбі з шахрайством в ЄС як і раніше мають певні відмінності в залежності від країни-члену. Щоб вирішити ці проблеми, ЄС у даний час обговорює нову Директиву щодо захисту фінансових інтересів ЄС за допомогою кримінального права. Ця директива забезпечить правову основу для функціонування пропонованої Європейської прокуратури, яка буде здатна розглядати питання, пов'язані з Інтернет-шахрайством. Так, Робоча група Європейського Союзу з протидії Інтернет-шахрайствам зазначає, що поява Європейської прокуратури повинна поліпшити розслідування і судове переслідування за злочини, що зачіпають фінансові сторони життєдіяльності країн-членів ЄС. Це обґрунтовано необхідністю забезпечення ефективного розслідування, в масштабах всієї ЄС, з огляду на складність багатьох видів великомасштабного шахрайства, в яких часто бере участь більше однієї країни, і тому виходить за рамки національної юрисдикції [4].

Що стосується Сполучених Штатів Америки (далі – США), то там протидія досліджуваному виду злочинності покладена на Федеральне бюро розслідування, в складі якого створено Центр скарг на Інтернет-злочинність. Вказаний Центр приймає Інтернет-скарги про злочини від фактичної жертви або від третьої сторони в онлайн режимі.

Для подання скарги необхідно надати наступну інформацію:

– ім'я жертви, адреса, телефон та електронна пошта;

– інформація про фінансові операції (наприклад, інформація про обліковий запис, дата здійснення операції та сума, що надійшли гроші);

– ім'я суб'єкта, адреса, телефон, електронна адреса, веб-сайт та IP-адреса;

– конкретні подробиці про те, як громадянин став жертвою злочину;

– заголовки електронної пошти;

– будь-яка інша важлива інформація, яку громадяни вважають необхідною для розгляду скарги [5].

У той же час, на сайті ФБР постійно оновлюються списки найбільш розповсюджених видів Інтернет-шахрайств, фізичних та юридичних осіб, які підозрюються або підозрювались у вказаних злочинах, способи убезпечення від Інтернет-шахраїв, списки шкідливого програмного забезпечення на комп'ютерну та мобільну техніку.

Отже, головною відмінністю процесу протидії шахрайствам, що вчиняються через мережу Інтернет між вітчизняною практикою та практикою Європейського Союзу й США є те, що у вказаних зарубіжних країнах діяльність досліджуваного виду, головним чином, спрямована

ISSN 1995-6134

на превенцію зазначених злочинів та роботу із населенням, а не на розслідування вже вчинених злочинів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Internet Fraud. URL: https://legal-dictionary.thefreedictionary.com/Internet+Fraud.
2. Fraud in cross-border e-commerce. URL: http://ecc-croatia.hr/resources/files/Fraud%20in%20cross-border%20e-commerce.pdf.
3. Phenomenon of Economic Criminality and the Legal Tools for its Elimination. URL: https://lawconference.sk/bpf/sprava/files/zborniky/9.sekcia.pdf.
4. Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2017.198.01.0029.01.ENG.
5. Scams and Safety. Internet Fraud. URL: https://www.fbi.gov/scams-and-safety/common-fraud-schemes/internet-fraud.

REFERENCES

1. Internet Fraud. Retrieved from: https://legal-dictionary.thefreedictionary.com/Internet+Fraud (in En.).
2. Fraud in cross-border e-commerce. Retrieved from: http://ecc-croatia.hr/resources/files/Fraud%20in%20cross-border%20e-commerce.pdf (in En.).
3. Phenomenon of Economic Criminality and the Legal Tools for its Elimination. Retrieved from: https://lawconference.sk/bpf/sprava/files/zborniky/9.sekcia.pdf (in En.).
4. Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law. Retrieved from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2017.198.01.0029.01.ENG (in En.).
5. Scams and Safety. Internet Fraud. Retrieved from: https://www.fbi.gov/scams-and-safety/common-fraud-schemes/internet-fraud (in En.).

Надійшла 24.11.2017

Кривенко О. І. Міжнародний досвід протидії шахрайствам, що вчиняються через мережу Інтернет (на прикладі Європейського Союзу та Сполучених Штатів Америки). Форум права: електрон. наук. фахове вид. 2017. № 5. С. 208–212. URL: http://nbuv.gov.ua/j-pdf/FP_index.htm_2017_5_32.pdf

DOI: http://doi.org/10.5281/zenodo.1202450

Відмічається, що в Європейському Союзі протидія вказаному виду злочинів покладена на підрозділи Європейського відділу по боротьбі з шахрайством, а в Сполучених Штатів Америки – на Федеральне бюро розслідування, в складі якого створено Центр скарг на Інтернет-злочинність. Аналізується юридичні підстави діяльності вказаних суб'єктів, їх права та обов'язки.

Ключові слова: *шахрайство, що вчиняється через мережу Інтернет, міжнародний досвід, Європейський Союз, Сполучені Штати Америки, оперативно-розшукова протидія*

***

Кривенко А.И. Международный опыт противодействия мошенничеству, совершаемых через Интернет (на примере Европейского Союза и Соединенных Штатов Америки)

Отмечается, что в Европейском Союзе противодействие указанном вида преступлений возложена на подразделения Европейского отдела по борьбе с мошенничеством, а в США – на Федеральное бюро расследования, в составе которого создан Центр жалоб на Интернет-преступность. Анализируется юридические основания деятельности указанных субъектов, их права и обязанности.

Ключевые слова: *мошенничество, которое совершается через Интернет, международный опыт, Европейский Союз, Соединенные Штаты Америки, оперативно-розыскная противодействие*

***

Krivenko O.I. International Experience of Countering Fraud Committed Through the Internet (By the Example of the European Union and the United States of America)

It is shown that fraud committed through the Internet undermines not only the intergovernmental image of our country, but also the economic and social situation in the middle of the country. Taking into account the positive experience in this area of the USA and the EU, it is important to determine the main directions of counteraction to the investigated type of crime in the named countries and to outline the prospective ways of introduction into the domestic practice.

It is noted that in the European Union, the counteraction to this type of crime lies with the units of the European Anti-Fraud Office, and in the United States – to the Federal Bureau of Investigation, which created the Center for Internet Crime complaints. The legal grounds for the activities of the abovementioned subjects, their rights and obligations are analyzed.
It has been shown that although the European Union Anti-Fraud Working Group has limited powers to provide redress if they become victims of fraud, it is very active in promoting fraud awareness. Sites of the majority of the members of the European Union Anti-Internet Fraud Working Group contain a wealth of information in the national language for citizens about fraudulent actions and how to avoid them.

Key words: *Internet fraud, international experience, European Union, United States of America, operative-search counteraction*