DOI:10.35774/app2022.03.183
УДК 343.3

Ігор Метельський,
кандидат юридичних наук, ст. викладач кафедри кримінального права та процесу Західноукраїнського національного університету
ORCID: https://orcid.org/0000-0001-8518-9321

ОСОБЛИВОСТІ ІНТЕРНЕТ-ШАХРАЙСТВА В ПЕРІОД ПАНДЕМІЇ COVID-19

Досліджено актуальність питання поширення правопорушень у мережі Інтернет. Це зумовлює необхідність вивчення та дослідження сутності кібершахрайства як одного із кримінальних правопрушень, що вчиняються у глобальній мережі, та особливостей його вчинення. Зокрема, важливо відмітити складові елементи шахрайства в мережі Інтернет. Крім того, у роботі розкрито питання, що стосуються кіберзлочинця та його ознак. Потребує уваги також поширеність шахрайства в інтернеті залежно від віку та статі порушників. Окремо варто вказати на дослідженість проблеми жертви від кібершахрайства. Висловлено рекомендації щодо запобігання та протидії такого виду злочинів.

Ключові слова: *кібербезпека, Інтрнет-шахрайство, забезпечення кібербезпеки, пандемія, COVID-19.*

Metelskiy I. Features of Internet fraud during the pandemic COVID-19

The scientific article is devoted to the study of the relevance of the issue of the spread of offenses on the Internet, which is an extremely relevant issue in the conditions of the development of modern society, especially during the global pandemic of COVID-19. This problem necessitates the study and research of the essence of cyber fraud as one of the most common criminal offenses committed in the global network and the features of its commission. Moreover, the problem of protecting Internet users both during work and during leisure time is more acute than ever. In particular, it is important to note the constituent elements of fraud on the Internet, as they express the peculiarities of the essence of this type of offense. In addition, the work highlights issues related to the cybercriminal and his criminological features, which, in particular, is important for the detection and prevention of cyberfraud. The prevalence of fraud on the Internet, depending on the age and gender of the offenders, also needs attention. Separately, it is worth noting the study of the problem of victims of cyber fraud, which again allows us to understand the prevalence of cyber fraud among Internet users. Recommendations for preventing and combating this type of crime were also made.

Keywords: *cyber security, internet fraud, cyber security, pandemic, COVID-19.*

Постановка проблеми. В умовах всесвітньої пандемії через поширення коронавірусу (*COVID-19*), коли громадяни всіх країн, у т. ч. українці, намагаються мінімалізувати реальні контакти з іншими людьми, шляхом проведення життєво-важливих операцій через мережу Інтернет зростає ризик стати жертвою шахраїв у мережі Інтернет. У 2020 р. запропоновано людству новий рівень розвитку сфер суспільного життя: робота, спілкування, дружба, стосунки, обслуговування та багато іншого тепер можна зробити вдома. Саме завдяки цьому активно розвивається платформа онлайн діяльності, що у наш час є великим досягненням та позитивом, проте водночас така ситуація ще більше дала поштовх розвитку та поширення кіберзлочинності. Так, дійсно, проаналізувавши офіційні статистичні дані Офісу Генерального прокурора, можна побачити, що кількість зареєстрованих злочинів у сфері використання електронно-обчислювальних машин (комп›ютерів), систем та комп'ютерних мереж і мереж електрозв›язку за період із 2016 р. по 2020 р. зростала та знаходилася на високому рівні. З огляду на ситуацію, що склалася у світі у зв'язку із пандемією коронавірусу, можна передбачити, що така злочинність буде далі зростати. Щодо 2020 р., то протягом цього року було обліковано 2498 кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Загалом статистика вчинення таких злочинів має такий вигляд.

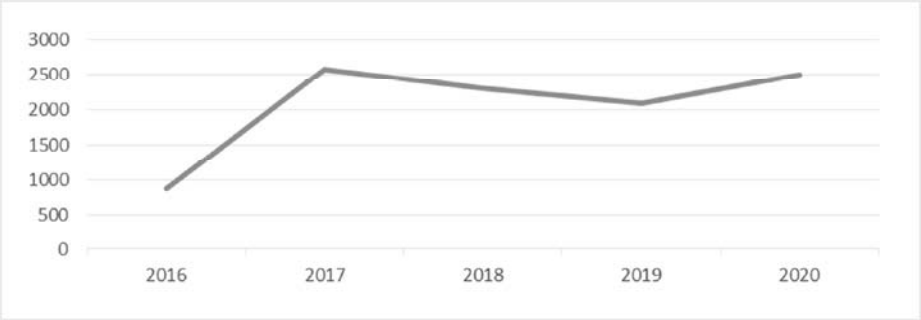

Рис. 1 Кількість облікованих кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку [7]

Аналіз останніх досліджень та публікацій. Деякі питання та аспекти проблеми Інтернет-злочинності, кібербезпеки розглядали у своїх роботах І. В. Басиста, А. В. Тарасюк, О. М. Юрченко, О. М. Комар, В. П. Сабадаш, Ю. М. Батурін, Д. О. Зиков, С. С. Чернявський, О. В. Лисодєд та ін. Однак у зв'язку із постійним розвитком цієї сфери окремі праці уже не відповідають реаліям часу та потребують наступного дослідження.

Мета статті. Відомо чимало випадків, коли особа довірилась рекламі сайтів з продажу різних товарів, перерахувала кошти, а після того вже не змогла зв'язатись із адресатом. Як наслідок втрачені кошти, не реалізовані покупки та негативний досвід! Тож, раціональним видається потреба в визначенні такого шахрайства в науці та практиці сьогодення.

Виклад основного матеріалу дослідженняя. Проблема кібершахрайства сягає своєю глибиною у визначення його поняття. Можна лише констатувати той факт, що законодавство України не містить визначення кібершахрайства чи шахрайських дій у мережі, що, на нашу думку, є глобальною проблемою. Адже як можна боротися з чимось, не знаючи з чим. Вирішення цієї проблеми дасть змогу належним чином компетентним органам боротися із комп'ютерним шахрайством. Та все ж, потрібно згадати про ч. 3 ст. 190 КК України, яка визнає кримінальним правопорушенням шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки [10], під яким розуміється кібершахрайство. Крім того, спробу відновити законодавчу справедливість робили науковці у своїх працях. Так, В. П. Сабадаш вважає, що «…шахрайство в Інтернеті – слід зазначати як певний рід шахрайських дій чи махінацій, де застосовується один чи декілька елементів Інтернету: чати, дошки оголошень, електронна пошта, сайти із товарами різного роду та інші елементи, що дають змогу потенційному злочинцю заманити потенційну жертву, зацікавивши її певною інформацією» [4]. З наведеного поняття видно, чим може бути насправді, з першого погляду, безпечна інтернет-сторінка будь-якого користувача, що пропонує різні товари та послуги.

На думку Ю. М. Батуріна та Д. О. Зикова, інтернет-шахрайство – це різновид традиційного шахрайства, що становить розкрадання чужого майна або набуття права на майно шляхом обману та зловживання довірою, вчинене з використанням мережі Інтернет [6]. Найбільш повно на нашу думку визначає кібершахрайство С. В. Шапочка, який говорить, що комп'ютерне шахрайство – це «… кіберзлочин, що полягає в заволодінні чужим майном або надбанні права на майно шляхом обману чи зловживання довірою та вчиняється у кіберпросторі за допомогою або з використанням комп'ютерно-телекомунікаційних пристроїв, систем чи мереж, а також інших засобів доступу до кіберпростору в рамках комп'ютерних систем або мереж і проти комп'ютерних систем, комп'ютерних мереж й комп'ютерних даних. останнє визначення» [11, с. 231]. Проте ми не погоджуємося із застосуванням словосполучення «надбанні права на майно» і вважаємо, що більш доцільно використовувати законодавчі терміни, якщо вони відомі. Тому варто вживати «…придбання права на майно…» і цим поняттям доповнити законодавство України. Здебільшого для визначення інтернет-шахрайства застосовують поняття, що розуміють як тотожні: «комп'ютерне шахрайство», «кібер-шахрайство», «мережеве шахрайство» та ін. Більшість авторів не наводять критерії розмежування цих понять, що, на нашу думку, доволі прийнятно.

Однією із специфік інтернет-шахрайства, на нашу думку, є те, що інтернет-шахраї від себе роблять лише необхідний мінімум – створюють інтернет-ресурс зі злочинними намірами, зокрема збагатитися за рахунок інших осіб злочинним шляхом, а решта залежить від конкретної особи та безпосередньо її подальших дій. Тут мова йде про віктимогенну поведінку потенційної жертви.

Спробуємо розібрати, що насправді породжує таке тотальне поширення інтернет-злочинності. На думку деяких вчених, це зумовлено багатокомпонентністю таких злочинів. Зокрема, виокремлюють психологічну та технологічну складову [5]. Дійсно, дуже важливе значення має аналіз таких правопорушень різносторонньо, адже вивчаючи їх однобічно ми не отримаємо достатньої кількості знань, що необхідна для досягнення цілей.

На думку С. С. Чернявського, психологічна складова – це бажання потенційної жертви швидко збагатитися без особливих затрат та зусиль [5, с. 100–103]. Погоджуємось із таким твердженням. Зокрема, в умовах пандемії COVID-19 чимало людей залишилося без стабільного заробітку, а отже, і без засобів для нормального життя. Тож, майже кожен, хто побачить в інтернеті оголошення про легкий заробіток, перейде за посиланням та виконає необхідний він нього мінімум, щоб отримати бажаний заробіток, не замислюючись про те, що в той самий час він стає вже не потенційною, а реальною жертвою інтернет-шахраїв.

На офіційному сайті «Єдиний портал органів системи МВС України» наведено актуальний приклад, як шахраї, маніпулюючи довірою громадян до влади, вчиняють шахрайські дії. Конкретно мова йде про оголошення, в яких, зловмисники в мережі Інтернет виманюють гроші у громадян під виглядом надання державних компенсаційних виплат. Лише за грудень місяць вже минулого 2020 р. до кіберполіції надійшло близько 100 звернень потерпілих від таких схем [2].

Варто проаналізувати, як це відбувається: зазвичай, правопорушники розміщують відео чи допис, в якому Президент України розповідає про нібито реальні виплати матеріальної допомоги підприємцям у розмірі 8 тис. грн. У цьому дописі шахраї розміщують посилання на ресурс, перейшовши за яким, нібито можна подати заявку на отримання виплати. І звісно, автори відео стверджують, що таку матеріальну допомогу може отримати кожен. А далі все вже за пропрацьовано схемою: громадянам пропонується ввести персональні дані та номер банківської картки для зарахування обіцяних грошей. Однак надалі шахраї просять сплатити послуги юриста за оформлення заяви, отримання електронного підпису, проходження ідентифікації тощо. Здебільшого для цього використовують вбудований чат-бот. Як стверджують фахівці, після виконання таких дій громадяни не лише переказують гроші за неіснуючі послуги, а й передають персональні дані аферистам [2].

Аналізуючи наведений приклад, можна зробити висновок про доцільність визначення психологічної складової інтернет-злочинів. Адже, як бачимо, мета легкого заробітку, який тим більше обіцяє нібито довірена особа – представник держави, провокує громадян переходити за злочинними посиланнями та власноручно переводити гроші злочинцям.

Щодо другого елемента злочинів у мережі Інтернет, а саме: технологічної складової – Інтернету, то останній використовують як інструмент для вчинення злочинних дій, що дає можливість шахраям донести необхідну інформацію до потенційної жертви, отримати від неї кошти, зберігаючи свою анонімність [5, с. 102].

На думку О. В. Лисодєд, жертва не лише самостійно виконує всі необхідні вказівки, аби інтернет-злочин було вчинено, вона своєю поведінкою також може викликати у злочинця рішучість здійснити цей злочин та зумовити його перехід до активних неправомірних дій [3].

Щодо особливостей кіберзлочинця, то, за даними Департаменту кіберполіції України, такі злочини вчиняють переважно чоловіки. Їхня частка становить 67%. Кіберзлочини за участі жінок становлять 33%. Схематично це співвідношення можна відобразити на рисунку.

Щодо віку, то серед чоловіків та жінок, основна частка належить особам віком 25-40 років (39% та 20% відповідно) [8].

За даними Департаменту кіберполіції України, шахрайство в Інтернеті переважно вчиняють чоловіки (77%), жінки займаються інформаційним шахрайством у 33% випадків [8].

Щодо особливостей жертв, то поширення кіберзлочинів серед юридичних осіб становить 13%, а серед фізичних осіб – 85%. У віковій категорії найбільше страждають від злочинності у мережі особи віком від 15 до 49 років. Щодо статевого критерію, то чоловіки страждають від кіберзлочинності в три рази більше, ніж жінки [9, с. 3].

Висновки. З огляду на вищевказане вважаємо, що законодавство України потребує вдосконалення, а саме: законодавець має виправити прогалини та ввести у законодавчий обіг поняття кібершахрайства. Крім того, необхідно визначити зміст понять «мережеве шахрайство», «кібершахрайство», «комп'ютерне шахрайство» та співвідношень між ними, що на нашу думку, сприятиме одноманітному застосуванню цих термінів на практиці та більш ефективній протидії таким явищам.

Щодо безпеки у мережі, то пропонуємо деякі заходи безпеки для активних користувачів мережі Інтернет, які вплинуть на зменшення випадків кібершахрайства, зокрема:

– необхідно отримувати інформацію щодо фінансових виплат лише через офіційні та перевірені джерела;

– за жодних умов не переходити за сумнівними посиланнями;

– в жодному разі не повідомляти конфіденційну інформацію стороннім особам;

– якщо ви все-таки розгубилися та надали особисту (персональну) інформацію сторонній особі – негайно зверніться до банку та заблокуйте картку;

– у разі підозри щодо шахрайських дій – негайно повідомляти правоохоронні органи.

Список використаних джерел

1. Брисковська О. М. Аспекти віктимологічної профілактики інтернет-шахрайства. URL: http://elar.naiau.kiev.ua/jspui/bitstream/123456789/17743/1/_%D0%97%D0%91I%D0%A0%D0%9D%D0%98%D0%9A_%D0%BA%D1%80%D0%B8%D0%BC%D0%B8%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F_2020_%D0%A7.1__%D1%84%D0%BE%D1%82%D0%BE_p135-137.pdf (дата звернення: 20.08.2022).
2. Єдиний портал органів системи МВС України. URL: https://mvs.gov.ua/ua/news/37181_Kiberpoliciya_zasteriga_vid_shahraystva_pid_viglyadom_derzhavnih_viplat.htm (дата звернення: 20.08.2022).
3. Лисодєд О. В. Проблеми профілактики віктимної поведінки жертв шахрайства. URL: http://dspace.nlu.edu.ua/bitstream/ 123456789/12233/1/Lysodyed_164-167.pdf (дата звернення: 20.08.2022).
4. Сабадаш В. П. Фішинг як найбільш розвинений вид шахрайства в інтернеті. Університетські наукові записки. 2006. № 1 (17). С. 228–233.
5. Чернявський С. С. Інтернет-шахрайство як об'єкт досліджень правових наук. Матеріали Всеукр. наук-практ. конф. Протидія злочинності у сфері інтелектуальної власності та комп'ютерних технологій органами внутрішніх справ: стан, проблеми та шляхи їх вирішення (Донецьк, 12 листоп. 2010 р.). Донецьк : ДЮІ ЛДУВС, 2010. С. 100–103.
6. Чернявський С. С. Фінансове шахрайство: методологічні засади розслідування: монографія. Київ, 2010. 624 с.
7. Єдиний звіт про кримінальні правопорушення по державі за період з 2016 по 2020 рік. URL: https://old.gp.gov.ua/ua/stst2011.html?dir_id=114140&libid=100820 (дата звернення: 23.08.2022).
8. Офіційний сайт кіберполіції України. URL: https://www.cyberpolice.gov.ua/results/2018/ (дата звернення: 19.08.2022).
9. Cyber Crime – Victimology Analysis: February 2016/ National Fraud Intelligence Burea// City of London Police – National Policing Lead For Fraud. – 2010. URL: https://www/cityoflondon.police.uk/news-and-appeals/Documents/Victimology%20Analysis-latest.pdf (дата звернення: 20.08.2022).
10. Кримінальний кодекс України : Закон України від 05.04.2001 р. № 2341-III. Відомості Верховної Ради України. 2001. № 25–26. Ст. 131.
11. Шапочка С. В. Щодо поняття шахрайства, що вчиняється з використанням комп'ютерних мереж (кібершахрайства). Вісник асоціації кримінального права України, 2015. № 1 (4). С. 221–232.

References

1. Bryskovska, O.M. *Aspekty viktymolohichnoi profilaktyky internet-shakhraistva. [Aspects of victimological prevention of Internet fraud]*. URL: http://elar.naiau.kiev.ua/jspui/bitstream/123456789/17743/1/_%D0%97%D0%91I%D0%A0%D0%9D%D0%98%D0%9A_%D0%BA%D1%80%D0%B8%D0%BC%D0%B8%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F_2020_%D0%A7.1__%D1%84%D0%BE%D1%82%D0%BE_p135-137.pdf [in Ukrainian].
2. *Yedynyi portal orhaniv systemy MVS Ukrainy [The only portal of the bodies of the Ministry of Internal Affairs of Ukraine]*. URL: https://mvs.gov.ua/ua/news/37181_Kiberpoliciya_zasteriga_vid_shahraystva_pid_viglyadom_derzhavnih_viplat.htm [in Ukrainian].
3. Lysodied, O. V. *Problemy profilaktyky viktymnoi povedinky zhertv shakhraistva. [Problems of prevention of victim behavior of victims of fraud]*. URL: http://dspace.nlu.edu.ua/bitstream/ 123456789/12233/1/ Lysodyed_164-167.pdf [in Ukrainian].

4. Sabadash, V. P. (2006). Fishynh yak naibilsh rozvynenyi vyd shakhraistva v interneti [Phishing is the most developed type of fraud on the Internet] *Universytetski naukovi zapysky – University Scientific Bulletin, 1 (17),* 228-233 [in Ukrainian].
5. Cherniavskyi, S. S. (2010). Internet-shakhraistvo yak obiekt doslidzhen pravovykh nauk [Internet fraud as an object of research in legal sciences]. *Materialy Vseukr. nauk-prakt. konf. Protydiia zlochynnosti u sferi intelektualnoi vlasnosti ta kompiuternykh tekhnolohii orhanamy vnutrishnikh sprav: stan, problemy ta shliakhy yikh vyrishennia (Donetsk, 12 lystop. 2010 r.).* Donetsk: DIuI LDUVS, 100-103 [in Ukrainian].
6. Cherniavskyi, S. S. (2010). *Finansove shakhraistvo: metodolohichni zasady rozsliduvannia [Financial fraud: methodological principles of investigation]:* monohrafiia. Kyiv[in Ukrainian].
7. *Yedynyi zvit pro kryminalni pravoporushennia po derzhavi za period z 2016 po 2020 rik [Unified report on criminal offenses by state for the period from 2016 to 2020].* URL: https://old.gp.gov.ua/ua/stst2011.html?dir_id=114140&libid=100820 [in Ukrainian].
8. *Ofitsiinyi sait kiberpolitsii Ukrainy [Official website of the cyber police of Ukraine].* URL: https://www.cyberpolice.gov.ua/results/2018/ [in Ukrainian].
9. *Cyber Crime – Victimology Analysis: February 2016 / National Fraud Intelligence Burea. City of London Police – National Policing Lead For Fraud. – 2010.* URL: https://www/cityoflondon.police.uk/news-and-appeals/Documents/Victimology%20Analysis-latest.pdf [in English].
10. Kryminalnyi kodeks Ukrainy [Criminal code of Ukraine]: Zakon Ukrainy vid 05.04.2001 r. № 2341-III. *Vidomosti Verkhovnoi Rady Ukrainy – Bulletin of Verkhovna Rada of Ukraine,* 25-26, 131 [in Ukrainian].
11. Shapochka, S. V. (2015). Shchodo poniattia shakhraistva, shcho vchyniaietsia z vykorystanniam kompiuternykh merezh (kibershakhraistva) [Regarding the concept of fraud committed using computer networks (cyber fraud)]. Visnyk *Asotsiatsii kryminalnoho prava Ukrainy – Bulletin of Association of Criminal Law of Ukraine, 1 (4),* 221-232 [in Ukrainian].

Стаття надійшла до редакції 14.09.2022.