АКТУАЛЬНІ ПИТАННЯ ЗАПОБІГАННЯ І ПРОТИДІЇ ПРАВОПОРУШЕННЯМ: КРИМІНАЛЬНО-ПРАВОВІ, КРИМІНОЛОГІЧНІ ТА КРИМІНАЛЬНО-ВИКОНАВЧІ АСПЕКТИ

УДК 343.8
DOI: 10.31733/2078-3566-2023-1-190-196

Василь БЕРЕЗНЯК©
доктор юридичних наук,
старший науковий співробітник
(Дніпропетровський державний університет внутрішніх справ, м. Дніпро, Україна)

ЗАПОБІГАННЯ ШАХРАЙСТВУ В ІНТЕРНЕТІ

У науковій статті названо та проаналізовано найбільш поширені способи вчинення шахрайства в Інтернеті. Автор досліджує заходи протидії таким кримінальним правопорушенням, зважаючи на існуючі підрозділи у складі Національної поліції та чинне законодавство. У дослідженні наведено офіційні статистичні дані, що надають можливість самостійно дійти висновку про ефективність наявних заходів протидії шахрайству в Інтернеті та необхідність визначення інших стратегічних напрямів його попередження.

Ключові слова: *шахрайство, запобігання, протидія, Інтернет, заходи.*

Постановка проблеми. Інтернет сьогодні є найбільшою інформаційно-телекомунікаційною системою, оскільки вміщує інформацію різних рівнів і з різних галузей знань, створює можливість для виникнення договірних зобов'язань, працевлаштування, надання послуг або виконання робіт тощо. Незважаючи на те, що ця мережа має системи захисту від неправомірних дій з боку правопорушників, вона все ще залишається вразливою і потребує вжиття заходів відповідними суб'єктами для запобігання кримінальним правопорушенням.

Статистичні дані випадків шахрайства в Інтернеті формуються як на міжнародному, так і національному рівнях. Так, нещодавно відповідні звіти оприлюднила Федеральна торгова комісія Сполучених Штатів Америки (далі – США), зазначивши, що у 2021 році шахраї вкрали у користувачів соціальних мереж майже $770 млн. У загальній кількості жертвами правопорушників стало 95 млн людей. Також доречно зауважити, що у 2020 році шахрайськими діями було спричинено шкоду на $258 млн, що значно менше порівняно з 2020 роком [1]. Це свідчить про негативну динаміку шахрайства у світі. У зв'язку з тим, що громадяни України є активними користувачами соціальних мереж і взагалі Інтернету, можна спрогнозувати ймовірність стати жертвою шахрайства. Наразі шахрайство в Інтернеті є глобальною проблемою у криміногенному розрізі, чим зумовлена необхідність вжиття заходів для скорочення випадків такого правопорушення. За національними статистичними даними, у 2021 році з випадками онлайн-шахрайства зіткнулися майже 45 % українців, однак порівняно з 2020 роком цей показник був значно меншим – 22 % [2]. Акцентуємо увагу на наявну певну кількісну взаємозалежність між світовими показниками і національними, що свідчить про нерозривність світової мережі та типовість випадків шахрайства, котрі можуть мати місце будь-де у світі.

Запобігання шахрайству в мережі Інтернет слід розглядати як комплекс

© В. Березняк, 2023
ORCID iD: https://orcid.org/0000-0001-5690-4736
vasiliyberezniak@i.ua

превентивних дій, що здійснюються відповідними суб'єктами з метою захисту і охорони прав користувачів Інтернету, однак, зважаючи на їх доволі широкий спектр, необхідно звертати увагу на ефективність заходів, що вживаються.

Аналіз публікацій, в яких започатковано вирішення цієї проблеми. Вагомий внесок у формування теоретичного підґрунтя розслідування шахрайства в Інтернеті зробили відомі дослідники, серед яких: Т. Авер'янова, Л. Ароцкер, Ю. Аленін, В. Бахін, В. Берназ, Н. Клименко, І. Когутич, О. Колесніченко, В. Колесник, В. Лисенко, В. Лукашевич, Є. Лук'янчиков, Г. Надгорний, Ю. Орлов, М. Погорецький, І. Фрідман, Л. Удалова, П. Цимбал, К. Чаплинський, С. Чернявський, В. Шевчук, В. Шепітько, В. Шиканов, О. Шляхов, Б. Щур та ін.

Метою статті **є** аналіз заходів запобігання шахрайству в мережі Інтернет.

Постановка проблеми. У сучасному інформаційному просторі сьогодні існує чимало способів вчинення шахрайства, а також вживаються заходи щодо його запобігання. Жертвами Інтернет-шахрайства можуть стати не тільки громадяни, але й юридичні особи, органи державної влади, місцевого самоврядування, підприємства, установи та організації різних форм власності. Серед поширених способів вчинення шахрайських дій слід назвати розповсюдження відповідних листів електронною поштою або на сайтах, якими користуються фізичні та юридичні особи, інші суб'єкти управління тощо. Своєчасне вжиття певних заходів безпеки можуть захистити майно та права на майно від протиправних посягань з боку «мережевих» злочинців.

Останнім часом спостерігається тенденція урізноманітнення способів віртуального шахрайства. Спосіб вчинення такого кримінального правопорушення відбивається в інформаційних слідах і є важливим джерелом відомостей про суспільно небезпечну поведінку правопорушника. У межах цього дослідження ми звернулися до теоретичних розробок, що розкривають поняття «спосіб злочину». Так, М. Панов пропонує під останнім розуміти «певний порядок, метод, послідовність рухів і прийомів, застосовуваних особою в процесі вчинення суспільно небезпечного посягання на охоронювані законом суспільні відносини, поєднаний з вибірковим використанням засобів вчинення злочину» [3]. Слід зауважити, що науковець звертає увагу на використання засобів вчинення злочину. У випадку інформаційного шахрайства до засобів вчинення злочину слід відносити комп'ютерну техніку, мобільні пристрої, а також інші мультифункціональні пристрої, за допомогою яких можна збирати, отримувати або зчитувати конкретні дані. В. Кудрявцев підтримує позицію попереднього дослідника, визначаючи спосіб вчинення злочину як «певний порядок, метод, послідовність рухів і прийомів, застосовуваних особою для вчинення злочину» [4]. Фактично ми спостерігаємо одностайність серед дослідників у розумінні терміна «спосіб» як певний метод, інструментарій конкретного кримінального правопорушення. Для здійснення більш повного дослідження обґрунтованим є звернення до тлумачних словників, що розкривають зміст поняття «спосіб». Вони надають декілька визначень поняття «спосіб», однак найбільш дотичним до дослідження є таке: «певна дія, прийом або система прийомів, яка дає можливість зробити, здійснити що-небудь, досягти чогось» [5]. У розкритті поняття «спосіб злочину» науковцями та тлумаченні в загальному значенні словниками можна простежити кореляцію у його концептуальному розумінні. Підводячи підсумки, зауважимо, що спосіб слід ототожнювати з інструментом або прийомом для виконання конкретних алгоритмів, наприклад, здійснення шахрайства в Інтернеті. Як нами уже було зазначено вище, згадане суспільно небезпечне діяння має специфічні спосіб та знаряддя, а тому є більш складним у розкритті та попередженні.

Зважаючи на широкий спектр способів вчинення віртуального шахрайства, існує необхідність у розширенні превентивних заходів для захисту і охорони користувачів мережі від протиправних посягань. Пріоритетним напрямом роботи у попередженні шахрайства в мережі Інтернет залишається захист конфіденційних даних, адже через отримання доступу до конфіденційної інформації реалізується значна кількість шахрайських схем, зокрема, здійснюються протиправні кредитно-грошові операції. Переважна більшість юридичних осіб вживають заходів для захисту таких даних, однак фізичні особи, через відсутність відповідних технічних можливостей, у переважній більшості не можуть це зробити і в подальшому потерпають від протиправних дій шахраїв. На нашу думку, необхідно звернути увагу відповідних суб'єктів, зокрема, спеціально уповноважених підрозділів у сфері протидії вчинення

кіберзлочинів на створення механізмів, що захищали б конфіденційні дані громадян від їх використання шахраями для вчинення суспільно небезпечного діяння, оскільки не завжди просвітницька робота є ефективною через невисокий рівень розуміння громадянами принципів функціонування інформаційного простору.

Для того, щоб ефективно чомусь запобігати, необхідно не тільки розуміти особливості об'єкта запобігання, але й окремо дослідити його різновиди та їхні властивості. Так, види віртуального шахрайства є різноманітними, однак ми спробували виокремити найбільш поширені:

– шахрайство при покупці товарів у мережі Інтернет. Такий вид шахрайства є розповсюдженим через прагнення користувача придбати товар доброї якості за ціною нижче за ринкову, однак схема завершується на отриманні від покупця передоплати;

– шахрайство з банківськими картами у випадку придбання товару в мережі Інтернет. Це стосується повідомлення додаткової інформації про банківську картку, даних з Інтернет-повідомлень, виконання певних операцій з банкоматом тощо;

– шахрайство з пропозицією Інтернет-заробітку та допомоги в погашенні боргу МФО;

– шахрайство через віруси-шифрувальники і сайти-фальшивки [6].

За даними Департаменту кіберполіції Національної поліції України, із населенням проводяться планові консультації та просвітницькі лекції з приводу вчинення віртуального шахрайства, людям роз'яснюється, якими способами вони можуть вберегтися від цього правопорушення, однак наведена нами вище статистика свідчить про недостатню ефективність такої діяльності. Із цього випливає, що вирішення питання стосовно витоку конфіденційних даних потребує професійного підходу [7].

Департамент кіберполіції Національної поліції України забезпечує реалізацію державної політики у сфері боротьби з кібкрзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність в означеній сфері. Стратегічними завданнями підрозділу визнають формування та забезпечення реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, що вчиняються за допомогою електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, а також мереж електрозв'язку шляхом вивчення механізму їх підготовки, вчинення або приховування, а також участь у попередженні, виявленні та припиненні кримінальних правопорушень іншими підрозділами Національної поліції, що не мають навичок у протидії кіберзлочинності, однак у провадженні яких перебувають кримінальні провадження зі згаданим способом вчинення [7].

Що стосується юридичних осіб, то вони повинні також вживати комплекс ефективних заходів у протидії Інтернет-шахрайству. Наприклад, із метою забезпечення безпеки банківських операцій компанії необхідно виокремити комп'ютери, що міститимуть фінансові дані та реквізити юридичної особи, а для вирішення решти питань, зокрема здійснення небанківських операцій, виділити іншу комп'ютерну техніку, з доступом до мережі Інтернет, тобто комп'ютери загального користування. Крім цього, за умови виведення комп'ютера з матеріально-технічної бази юридичної особи, слід пам'ятати про необхідність створення резервної копії наявної інформації та очищення жорсткого диску тощо [8].

На окрему увагу заслуговує той факт, що банківські установи не надсилають електронних листів або текстових повідомлень із проханням надати інформацію конфіденційного характеру, котру не можна повідомляти навіть оператору банку. До того ж раціональною є думка, що за наявності сумнівів у передачі певної інформації банківській установі необхідно звернутися безпосередньо до фахівців відділення або офісу конкретного банку, що в подальшому може запобігти вчиненню кримінального правопорушення шахраями. Стосовно діяльності юридичних осіб зауважимо, що зростає кількість електронних листів, котрі надходять компаніям нібито від постачальників. На кшталт шахрайських банківських електронних листів, ці електронні листи можуть виглядати законними, але містити вимоги щодо конфіденційної фінансової інформації. Якщо отримано такий лист із проханням надати конфіденційну фінансову інформацію (навіть ту, що може виглядати так, ніби вона надійшла від банку чи постачальника), існує необхідність у здійсненні перевірки достовірності даного запиту [8].

Поширеними схемами випадків віртуального шахрайства є отримання правопорушниками паролів та кодів для доступу до банківських даних конкретної

особи. Так, громадяни повинні розуміти, що в переважній більшості попередження випадків шахрайства в Інтернеті залежить саме від них, адже досить часто користувачі самі повідомляють паролі, котрі в принципі не є складними для розпізнавання. Серед поширених порад: регулярна зміна паролів для кращого захисту, з використанням комбінації літер, цифр і спеціальних символів, коли це можливо [8].

Серйозною проблемою в мережі останнім часом став фішинг. Слід зазначити, що 80 % кримінальних проваджень сьогодні зареєстровано в територіальних органах Національної поліції за фактом вчинення кримінального правопорушення, передбаченого ч. 3 ст. 190 Кримінального кодексу України (далі – КК України).

Фішингові електронні листи призначені для того, щоб користувач перейшов за посиланням, наданим в електронному листі, для підтвердження або зміни свого облікового запису. Часто посилання в електронному листі є способом для шахраїв встановити небезпечне програмне забезпечення на комп'ютер або пристрій, що використовується для доступу до електронної пошти [9]. Цю шкідливу програму можна використовувати для отримання особистої інформації і, відповідно, доступу до банківських даних для зняття грошових коштів. За друге півріччя 2022 року Дніпровським районним управлінням поліції було направлено до суду 26 обвинувальних актів за фактом вчинення кримінального правопорушення, передбаченого ч. 3 ст. 190 КК України, скоєного за допомогою фішингових посилань. Це свідчить про розповсюдження серед шахраїв такого способу та необхідність формування у громадян більш відповідального ставлення до переходу за посиланнями, що надходять їм на електронну пошту або з'являються на різних веб-сайтах [10].

Серед превентивних кроків щодо шахрайства фахівці у сфері кібербезпеки вважають встановлення антивірусного програмного забезпечення. Його необхідно систематично оновлювати та запускати для того, щоб запобігти «зараженню» комп'ютера. Як запобігання випадкам шахрайства корисним визнається також встановлення спеціального програмного забезпечення для захисту від спаму: такого, що допомагає запобігти надходженню спаму та непотрібних листів у папку «Вхідні» і додатково захищає від фішингових листів; брандмауера, що сприяє у запобіганні несанкціонованому доступу до комп'ютера через віруси та шкідливе програмне забезпечення; антишпигунського програмного забезпечення, котре блокує встановлення шпигунського програмного забезпечення на комп'ютері, здатного відстежувати або контролювати використання комп'ютера, надсилати спливаючі вікна або перенаправляти на шкідливі веб-сайти тощо [10].

На нашу думку, необхідно також наголосити на необхідності підтримки актуальної операційної системи комп'ютера та Інтернет-браузера, що забезпечить додатковий захист від випадків шахрайства у мережі.

Серед труднощів у попередженні електронного шахрайства слід назвати відсутність особистого контакту між правопорушником і жертвою та подекуди відсутність можливості ідентифікувати особу через недостатність наявних відомостей про час і мету комунікації із потерпілим. Це саме стосується і переказу коштів, адже він також здійснюється дистанційно [11].

Як уже було зазначено вище, серед найбільш поширених схем обману виокремлюють шахрайство у придбанні товарів у мережі Інтернет або замовленні послуг. У межах цього дослідження ми спробували визначити правила запобігання комерційному шахрайству в Інтернеті, зокрема стосовно використання виключно перевірених ресурсів, за умови перевірки правильності назви необхідного сайту. Зміна назви сайту або адреси може вказувати на фішинговий характер конкретного ресурсу тощо. Якщо користувач здійснює онлайн-платіж, то доречним буде перевірити захищеність платіжної операції. На те, що платіж захищений, вказує назва адреси сайту, оскільки вона повинна містити https:// і значок «замочка». Незважаючи на це, найбільш безпечним все одно слід вважати накладений платіж, що виключить можливість незаконного отримання шахраями грошових коштів. Крім того, зважаючи на негативну динаміку випадків шахрайства, спеціалізовані підрозділи вживають додаткових заходів, що можуть бути ефективними у попередженні суспільно небезпечних діянь. Так, на базі сайту кіберполіції функціонує банк даних, в якому можна перевірити номер телефону, банківську картку або посилання на сумнівний сайт, оскільки вони можуть бути вже внесені тули на підставі звернень потерпілих осіб [7; 11].

Г. Бідняк у межах дисертаційного дослідження аргументує позицію стосовно

того, що одним зі способів запобігання вчиненню повторних випадків шахрайства в Інтернеті є вдалі та ретельні експертні дослідження, підкреслюючи, що «однією з форм використання спеціальних знань при розслідуванні шахрайств є призначення судових експертиз», спрямованих на визначення способів і методів вчинення шахрайств, зокрема віртуальних. Розуміння алгоритмів та схем у подальшому полегшує роботу правоохоронних органів у цьому напрямі [12, с. 95–96]. Загалом шахрайство набуває нових форм, модернізується та пристосовується до сучасних умов. Наприклад, останнім часом набули поширення платіжні картки для здійсненні різноманітних грошових операцій. За інформацією Департаменту фінансових розслідувань України, використання платіжних карток дає змогу: зменшити обсяги використання готівки; додатково захистити грошові кошти (при втраті картки грошові кошти блокуються та залишаються на рахунку держателя картки); проводити операції не тільки в національній, але і в іноземній валюті (мультивалютні картки); проводити розрахунки цілодобово та в різних країнах світу [13, с. 12; 14].

Важливим аспектом у запобіганні шахрайству в Інтернеті також є активна взаємодія між службами і підрозділами. На думку І. Гукової, «взаємодія слідчих та оперативних підрозділів Національної поліції, за умов керівної ролі слідчого, складається зі спільних зусиль у питаннях розкриття й розслідування кримінальних правпорушень та встановлення усіх обставин, що підлягають доказуванню у кримінальному провадженні, …встановлення місця перебування підозрюваних осіб…» [15, с. 117].

А. Шраго зазначає, що «існує низка проблем… під час розслідування комп'ютерних кримінальних правопорушень». Дослідниця робить означені висновки, виходячи з аналізу спеціальної літератури та практики розслідування цього виду суспільно небезпечних діянь. Труднощі полягають у пошуку, виявленні, фіксації, вилученні та дослідженні слідів відповідно до механізмів їх утворення, визначенні технічних процесів, котрі були проведені правопорушником для того, щоб реалізувати кримінально протиправну мету [16, с. 263].

Висновки. Зважаючи на статистику випадків шахрайства в Інтернеті, слід констатувати недостатню ефективність заходів запобігання. Під час дослідження нами з'ясовано, що спектр цих заходів доволі широкий. У даному випадку прослідковується парадокс: за значної кількості превентивних заходів комп'ютерні кримінальні правопорушення не зменшуються, а подекуди їхня кількість зростає. Це можна пояснити специфікою знарядь, котрими вони вчиняються, адже виникає проблема у визначенні механізму скоєння кримінального правопорушення, виявленні, фіксації та збиранні доказового матеріалу. З огляду на вищезазначене постає питання про взаємодію між службами і підрозділами для того, щоб притягнути правопорушників до кримінальної відповідальності, адже випадки нерозкритого шахрайства, на жаль, не є винятком у сучасній практиці Національної поліції. Ключовим органом у розкритті комп'ютерних кримінальних правопорушень є Департамент кіберполіції Національної поліції України, до компетенції якого належить формування та забезпечення реалізації державної політики щодо запобігання та протидії кримінальним правопорушенням, котрі вчиняються за допомогою електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, а також мереж електрозв'язку, шляхом вивчення механізму їх підготовки, вчинення або приховування. Також слід зауважити про необхідність розвитку технічних розробок у протидії електронному шахрайству, що мають доповнити стратегічні завдання спеціалізованого підрозділу.

Список використаних джерел

1. Шахраї обікрали користувачів соцмереж на $770 млн у 2021 році: як не стати жертвою. *ФОКУС.* URL : https://focus.ua/uk/digital/504782-moshennniki-obokrali-polzovateley-socsetey-na-770-mln-v-2021-godu-kak-ne-stat-zhertvoy.

2. Українці стали вдвічі частіше натрапляти на шахраїв в інтернеті. *УКРІНФОРМ.* URL : https://www.ukrinform.ua/rubric-yakisne-zhyttia/3304603-ukrainci-stali-vdvici-castise-natraplati-na-sahraiv-v-interneti-opituvanna.html.

3. Панов Н. И. Способ совершения преступления и уголовная ответственность. Харьков : Вища школа, 1982. 161 с.

4. Кудрявцев В. Н. Объективная сторона преступления : монограф. Москва : Госюриздат, 1960. 244 с.

5. Спосіб. *Словник української мови. Академічний тлумачний словник (1970-1980).* URL : http://sum.in.ua/s/sposib#:~:text.

6. Шахрайство в Інтернеті: яким буває, якими наслідками загрожує і як себе убезпечити? URL : https://advokat-zhuk.com.ua/ua/shahrajstvo-v-interneti-jakim-buvaie-jakimi-naslidkami-zagrozhuie-i-jak-sebe-ubezpechiti/.

7. Про підрозділ. *Кіберполіція : Національна поліція України.* URL : https://cyberpolice.gov.ua/contacts/.

8. Avoid online fraud. *Nidirect : government services.* URL : https://www.nidirect.gov.uk/articles/avoid-online-fraud.

9. Безпечний Інтернет або як не стати жертвою шахрайств в онлайн-просторі. *Безоплатна правова допомога.* URL : https://legalaid.gov.ua/publikatsiyi/bezpechnyj-internet-abo-yak-ne-staty-zhertvoyu-shahrajstv-v-onlajn-prostori/.

10. 5 Tips To Prevent Online Fraud. *Banner Bank.* URL : https://www.bannerbank.com/financial-resources/blog/tips-to-prevent-online-fraud#content.

11. Як діяти, якщо став жертвою Інтернет-шахрайства. *Бережанська міська рада.* URL : http://berezhanymrada.gov.ua/index.php/informatsiya-berezhanskoho-byuro-pravovoyi-dopomohy/4645-yak-diiaty-iakshcho-stav-zhertvoiu-internet-shakhraistva.

12. Бідняк Г. С. Використання спеціальних знань при розслідуванні шахрайств : дис. … канд. юрид. наук : 12.00.09 / ДДУВС. Дніпро, 2018. 244 с.

13. Бідняк Г. С. Теорія і практика використання спеціальних знань при розслідуванні шахрайств : монограф. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2019. 152 с.

14. Кіберзлочинність та відмивання коштів. Департамент фінансових розслідувань, Державна служба фінансового моніторингу України, 2013. 53 с. URL : https://fiu.gov.ua/assets/userfiles/411/Типолог%20ДСФМУ/2013%2012%2025_tipolog2013.pdf.

15. Гукова І. А. Криміналістична характеристика та особливості розслідування шахрайства у сфері надання послуг із працевлаштування : дис. … д-ра філософії : 081 / ДДУВС. Дніпро, 2021. 254 с.

16. Шраго А. О. Протидія порнографії як засіб забезпечення інформаційної безпеки в Україні. *Економічна та інформаційна безпека: проблеми та перспективи : матеріали Міжнародної науково-практ. конф.* (м. Дніпро, 27 квіт. 2018 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2018. С. 262–266.

Надійшла до редакції 02.03.2023

References

1. Shakhrai obikraly korystuvachiv sotsmerezh na $770 mln u 2021 rotsi: yak ne staty zhertvoiu [Fraudsters robbed social network users of $770 million in 2021: how not to become a victim]. *FOKUS.* URL: https://focus.ua/uk/digital/504782-moshennniki-obokrali-polzovateley-socsetey-na-770-mln-v-2021-godu-kak-ne-stat-zhertvoy. [in Ukr.].

2. Ukraintsi staly vdvichi chastishe natrapliaty na shakhraiv v interneti [Ukrainians began to come across scammers twice as often on the Internet]. *UKRINFORM.* URL: https://www.ukrinform.ua/rubric-yakisne-zhyttia/3304603-ukrainci-stali-vdvici-castise-natraplati-na-sahraiv-v-interneti-opituvanna.html. [in Ukr.].

3. Panov, N. I. (1982) Sposob soversheniya prestupleniya i ugolovnaya otvetstvennost’ [Method of committing a crime and criminal liability]. Kharkiv : Vyshcha shkola, 161 p. [in russ.].

4. Kudryavtsev, V. N. (1960) Ob»yektivnaya storona prestupleniya [The objective side of the crime] : monograf. Moscow : Gosyurizdat, 244 p. [in russ.].

5. Sposib [Way]. *Slovnyk ukrainskoi movy. Akademichnyi tlumachnyi slovnyk (1970-1980).* URL: http://sum.in.ua/s/sposib#:~:text. [in Ukr.].

6. Shakhraistvo v Interneti: yakym buvaie, yakymy naslidkamy zahrozhuie i yak sebe ubezpechyty? [Fraud on the Internet: what happens, what are the consequences and how to protect yourself?]. URL: https://advokat-zhuk.com.ua/ua/shahrajstvo-v-interneti-jakim-buvaie-jakimi-naslidkami-zagrozhuie-i-jak-sebe-ubezpechiti/. [in Ukr.].

7. Pro pidrozdil [About the unit]. *Kiberpolitsiia : Natsionalna politsiia Ukrainy.* URL : https://cyberpolice.gov.ua/contacts/. [in Ukr.].

8. Avoid online fraud. *Nidirect : government services.* URL : https://www.nidirect.gov.uk/articles/avoid-online-fraud.

9. Bezpechnyi Internet abo yak ne staty zhertvoiu shakhraistv v onlain-prostori [Safe Internet or how not to become a victim of fraud in the online space]. *Bezoplatna pravova dopomoha.* URL: https://legalaid.gov.ua/publikatsiyi/bezpechnyj-internet-abo-yak-ne-staty-zhertvoyu-shahrajstv-v-onlajn-prostori/. [in Ukr.].

10. 5 Tips To Prevent Online Fraud. *Banner Bank.* URL : https://www.bannerbank.com/financial-resources/blog/tips-to-prevent-online-fraud#content.

11. Iak diiaty, yakshcho stav zhertvoiu Internet-shakhraistva [What to do if you are a victim of Internet fraud]. *Berezhanska miska rada.* URL: http://berezhanymrada.gov.ua/index.php/informatsiya-berezhanskoho-byuro-pravovoyi-dopomohy/4645-yak-diiaty-iakshcho-stav-zhertvoiu-internet-shakhraistva. [in Ukr.].

12. Bidniak, H. S. (2018) Vykorystannia spetsialnykh znan pry rozsliduvanni shakhraistv [Use of special knowledge in fraud investigation] : dys. … kand. yuryd. nauk : 12.00.09 / DDUVS.

Dnipro. 244 p. [in Ukr.].

13. Bidniak, H. S. (2019) Teoriia i praktyka vykorystannia spetsialnykh znan pry rozsliduvanni shakhraistv [Theory and practice of using special knowledge in fraud investigation] : monohrafiia. Dnipro : Dniprop. derzh. un-t vnutr. sprav. 152 p. [in Ukr.].

14. Kiberzlochynnist ta vidmyvannia koshtiv [Cybercrime and money laundering]. Departament finansovykh rozsliduvan, Derzhavna sluzhba finansovoho monitorynhu Ukrainy, 2013. 53 p. URL: https://fiu.gov.ua/assets/userfiles/411/Typoloh%20DSFMU/2013%2012%2025_tipolog2013.pdf. [in Ukr.].

15. Hukova, I. A. (2021) Kryminalistychna kharakterystyka ta osoblyvosti rozsliduvannia shakhraistva u sferi nadannia posluh iz pratsevlashtuvannia [Forensic characteristics and peculiarities of the investigation of fraud in the field of providing employment services] : dys. … d-ra filosofii : 081 / DDUVS. Dnipro. 254 p. [in Ukr.].

16. Shraho, A. O. (2018) Protydiia pornohrafii yak zasib zabezpechennia informatsiinoi bezpeky v Ukraini [Countering pornography as a means of ensuring information security in Ukraine]. *Ekonomichna ta informatsiina bezpeka: problemy ta perspektyvy : materialy Mizhnarodnoi naukovo-prakt. konf.* (m. Dnipro, 27 kvit. 2018 r.). Dnipro : Dniprop. derzh. un-t vnutr. sprav. P. 262–266. [in Ukr.].

ABSTRACT

Vasyl Berezniak. Prevention of fraud on the Internet. The Internet today is the largest information and telecommunication system, as it contains information of various levels and fields of knowledge, creates an opportunity for the emergence of contractual obligations, employment, provision of services or performance of works, etc. Despite the fact that this network has systems to protect against wrongdoing by criminals, it is still vulnerable and requires measures to be taken by the relevant actors to prevent criminal offenses in the network.

The scientific article names and analyzes the most common ways of committing fraud on the Internet. The author examines countermeasures against these criminal offenses, taking into account the existing units of the National Police and current legislation. The study represenrs official statistical data that provide an opportunity to independently draw a conclusion about the effectiveness of existing measures to combat fraud on the Internet and the need to determine other strategic directions for its prevention.

Taking into account the statistics of cases of fraud on the Internet, the author found insufficient effectiveness of prevention measures. During the research, he found out that the range of these measures is quite wide. In this case, a paradox is observed: with a significant number of preventive measures, computer criminal offenses do not decrease, and in some places their number increases. This can be explained by the specifics of the tools with which they are committed, because there is a problem in determining the mechanism of committing a criminal offense, identifying, recording and collecting evidence. In view of the above, the question arises about interaction between services and units in order to bring offenders to criminal responsibility, because cases of unsolved fraud, unfortunately, are not an exception in the modern practice of the National Police. The key body in solving computer criminal offenses is the Cyber Police Department of the National Police of Ukraine, whose competence includes the formation and implementation of state policy on the prevention and counteraction of criminal offenses committed with the help of electronic computing machines (computers), systems and computers computer networks, as well as telecommunication networks, by studying the mechanism of their preparation, execution or concealment

***Keywords**: fraud, prevention, counteraction, Internet, measures.*