УДК 343.9.024:343.72 DOI https://doi.org/10.26661/2616-9444-2020-4.1-32

Організовані форми інтернет-шахрайства на сучасному етапі

Брисковська О. М.
кандидат юридичних наук, старший науковий співробітник,
провідний науковий співробітник наукової лабораторії
із проблем протидії злочинності
Навчально-науковий інститут № 1
Національної академії внутрішніх справ
Солом'янська площа, 1, Київ, Україна
orcid.org/0000-0001-6902-9969
oksanuhka@ukr.net

Пустовіт В. А.
старший науковий співробітник
Міжвідомчий науково-дослідний центр
з проблем боротьби з організованою злочинністю
при Раді національної безпеки і оборони України
Солом'янська площа, 1, Київ, Україна
orcid.org/0000-0002-5566-669X
valark37t@gmail.com

Ключові слова:
інтернет-шахрайство, інтернет-шахраї, мережа Інтернет, група осіб, організована злочинність, організована злочинна група, злочинне об'єднання, злочинна організація.

Кількість злочинів, що вчиняють із використанням мережі Інтернет в Україні, з кожним роком збільшується на декілька тисяч. Сьогодні найпоширеніший вид злочину – шахрайство в мережі Інтернет. У статті піднімається питання щодо форм організації інтернет-шахрайства. А саме виокремлено види груп інтернет-шахраїв різного рівня організованості, встановлені особливості вчинення злочинів щодо організованих форм інтернет-шахрайств на сучасному етапі, розкриті найпопулярніші методи інтернет-шахрайства, що вчиняють такі групи, висвітлений предмет злочину інтернет-шахрайства, вчиненого групами інтернет-шахраїв різного рівня організованості, а також роль потерпілого у процесі незаконного вилучення коштів або майна чи передачі права на нього зловмисникам, зроблено висновок, що для вчинення кожного із розглянутих методів інтернет-шахрайства організовані злочинні групи та злочинні об'єднання заздалегідь готовляться до їх вчинення, а саме: оснащуються комп'ютерною технікою, мобільними телефонами, сім-картами, канцелярським приладдям, а з випадками call-центрів орендують приміщення під офіс та наймають працівників зі знанням декількох мов, прописують інструкції та проводять тренінги своїм співробітникам щодо спілкування з різними типами людей, від інтересів, професійної направленості, вікових особливостей, ментальних до особливостей характеру та темпераменту. Отже, інтернет-шахрайство вчиняють групи від двох осіб за попередньою змовою, а також групи осіб, які зорганізувалися у стійке злочинне об'єднання та злочинну організацію, кількість яких може не обмежитися і сотнею осіб.

На нашу думку, форма організованого шахрайства в мережі Інтернет – це група осіб, які об'єдналися для вчинення злочинної діяльності економічної спрямованості з використанням Інтернету як інструменту для досягнення своїх злочинних цілей, шляхом введення в оману потерпілого для передачі ним уявно добровільно, начебто, у своїх інтересах грошових коштів або права на майно на користь зловмисникам. Успішність запобігання

інтернет-шахрайствам, їх викриття і притягнення винних осіб до відповідальності в даний час є досить рідкісним явищем, якщо порівнювати з їх кількістю. А тому питання вивчення видів груп інтернет-шахраїв різного рівня організованості потребує подальших наукових досліджень.

Organized forms of Internet fraud at the present stage

Bryskovska O. M.
Candidate of Law, Senior Researcher,
Leading Researcher at the Scientific Laboratory
on the Problems of Combating Crime
Educational and Scientific Institute № 1
of the National Academy of Internal Affairs
Solom'ianska sq., 1, Kyiv, Ukraine
orcid.org/0000-0001-6902-9969
oksanuhka@ukr.net

Pustovit V. A.
Senior Researcher
Interdepartmental Research Center for Combating Organized Crime
at the National Security and Defense Council of Ukraine
Solom'ianska sq., 1, Kyiv, Ukraine
valark37t@gmail.com

Key words:
internet fraud; Internet fraudsters, the Internet, a group of people, organized crime; organized criminal group; criminal association, criminal organization.

The number of crimes committed using the Internet in Ukraine is increasing by several thousand every year. Today, the most common type of crime is fraud on the Internet. The article raises the question of the forms of organization of Internet fraud. Namely, the types of groups of Internet fraudsters of different levels of organization are singled out, the peculiarities of committing crimes against organized forms of Internet fraud at the present stage are revealed, the most popular methods of Internet fraud committed by such groups are revealed. level of organization, as well as the role of the victim in the process of illegal seizure of funds or property or transfer of the right to it to criminals, it is concluded that to commit each of these methods of Internet fraud, organized criminal groups and criminal associations prepare in advance to commit them, namely: equipped with computers, mobile phones, SIM cards, stationery, and with cases of call centers, rent office space and hire employees with knowledge of several languages, prescribe instructions and conduct training for their employees to communicate with different types of people, from interests, professional orientation, age, mental to character and temperament. Thus, online fraud is committed by groups of two people by prior conspiracy and groups of people who have organized into a stable criminal association and criminal organization, the number of which may not be limited to a hundred people. In our opinion, a form of organized fraud on the Internet is a group of persons who have joined together to commit economic economic activity using the Internet as a tool to achieve their criminal goals, by misleading the victim to transfer it seemingly voluntarily, as if in their interests in cash or property rights in favor of the perpetrators. The success of preventing online fraud, exposing it and bringing perpetrators to justice is now quite rare compared to their number. Therefore, the question of studying the types of groups of Internet fraudsters of different levels of organization requires further research.

Шахраї використовують мережу Інтернет, тому що вона надає широкі можливості для реалізації різноманітних способів вчинення злочину, а також значного збільшення кількості учинення таких злочинів, не обмежених ані простором, ані часом. Якщо раніше зловмисники вчиняли Інтернет-шахрайства одноосібно, то сьогодні вони стали згуртовуватися, починаючи від групи осіб за попередньою змовою до більш складного рівня організованості, формуючи організовані групи та об'єднання, щоб діяти більш масштабно та зухвало, за короткий термін часу значно збільшуючи суму збитків та кількість постраждалих від такого шахрайства, забезпечуючи прикриття від виявлення, контролю та відповідальності. Такі організовані злочинні групи, як правило, є організованими злочинними групами економічної спрямованості. Як зазначав американський вчений кримінолог Д. Албанезе (Albanese, Jay S.), організована злочинність є постійно діючим кримінальним підприємством, яке працює раціонально для одержання прибутку від незаконної діяльності, що користується суспільним попитом [1, с. 3].

На думку Чернявського С.С., до головних ознак інтернет-шахрайства можна віднести:

1) високий ступінь латентності;

2) багатоманітність способів учинення шахрайства (пов'язано із широким спектром послуг у мережі Інтернет);

3) глобальний характер (інформаційний простір, на відміну від фізичного, не має чітких кордонів й обмежень);

4) складнощі виявлення та запобігання [2, с. 226].

Відповідно до ст. 55 КПК України потерпілим у кримінальному провадженні може бути фізична особа, якій кримінальним правопорушенням завдано моральної, фізичної або майнової шкоди, а також юридична особа, якій кримінальним правопорушенням завдано майнової шкоди [3].

Аналіз публікацій за даною темою. Розглядали окремі питання щодо злочинів, що вчиняються з використанням мережі Інтернет взагалі та шахрайства зокрема, у своїх роботах такі вчені, як І.Г. Богатирьов, О.В. Бишовець, В.М. Бутузов, С.А. Буяджи, В.Д. Гавловський, І.В. Діордіца, Д.О. Зиков, Д.В. Кунець, М.О. Кравцова, Н.С. Козак, О.О. Косиченко, В.Д. Ларичев, О.В. Лисодєд, А.В. Микитчик, О.А. Самойленко, О.В. Смаглюк, С.С. Чернявський, В.І. Шакун, С.В. Шапочка, В.П. Шеломенцев, В.Г. Хахановський, О.М. Юрченко та інші.

В опублікованих працях приділялась увага загальним аспектам злочинів у мережі Інтернет, а також інтернет-шахрайствам. А питання щодо вчинення шахрайства організованими злочинними угрупуваннями з використанням мережі Інтернет згадувалося лише у криміналістичній характеристиці інтернет-шахрая, або в площині вивчення окремих видів шахрайства, які вчиняються з використанням мережі Інтернет, або в питаннях розслідування інтернет-шахрайства, але питанню щодо форм, видів організації інтернет-шахрайства, окремої уваги науковцями приділено не було.

Кримінальна практика свідчить, що деякі злочинці інтернет-шахрайства діють без співучасників, тоді як більшість із них скоюють злочини у складі організованих злочинних угрупувань [4, с. 83].

Традиційно у кримінології виокремлюють три види рівнів організованої злочинності:

Перший рівень – найнижчий. Злочин хоча і вчинено організованою групою, але в ній при всій згуртованості й стійкості немає складної структури, ієрархії, функції організаторів і виконавців чітко не розподілено. Другий рівень організованої злочинності являє собою ієрархічну побудову груп або їх об'єднання. На третьому рівні здійснюється об'єднання лідерів організованих груп у злочинні співтовариства [5, с. 34]. Зміни у функціонуванні суспільства зумовлюють зміни й в організованій злочинності [6, с. 23].

Виокремимо **рівні організованості шахрайства в мережі Інтернет**:

– група осіб за попередньою змовою, які заздалегідь домовилися про спільне вчинення злочинів, яка не має складної структури й ієрархії, ролі чітко не розподілені, до її складу входить від двох осіб;

– група осіб, які зорганізувалися у стійке злочинне об'єднання, складається з більше, ніж три особи, має чітку ієрархічну побудову та розприділення ролей. Такі злочинні об'єднання створюють із метою багаторазового вчинення шахрайства в мережі Інтернет;

– найвищий ступінь організованості злочинної групи – це злочинна організація, в якій наявна не тільки складна структура, розподілення ролей та ієрархічність, але й спільна мета злочинної діяльності для заволодіння грошовими коштами та права на майно у великих та особливо великих розмірах. Має спрямованість на отримання постійних та систематично високих прибутків, забезпечуючи їх легалізацію.

Відповідно до ст. 190 КК України шахрайство – це заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою [7]. У більшості випадків під час вчинення інтернет-шахрайства безпосереднім предметом злочину є грошові кошти, але, як правило, придбання права на майно пізніше перепродається.

Безпосередня участь потерпілого в передачі коштів, майнових благ і добровільність його дій є обов'язковими ознаками шахрайства, які відрізняють його від викрадення коштів або майна та інших злочинів проти власності. За ознакою

безпосередньої участі потерпілого у процесі незаконного вилучення майна шахрайство схоже з вимаганням, яке також передбачає передачу майна чи права на нього винній особі самим потерпілим. Однак якщо при вимаганні потерпілий робить це вимушено, то при шахрайстві потерпілий переконаний у тому, що він розпоряджається майном за власною волею, у своїх інтересах або принаймні не на шкоду цим інтересам [8]. Така переконаність потерпілого є результатом безпосереднього впливу на нього самого шахрая, а в нашому випадку – групи шахраїв, а саме введенням в оману потерпілого відносно правомірності передачі ним зловмиснику грошових коштів чи надання зловмиснику чи зловмисникам права на майно. При шахрайстві добровільність має уявний характер, оскільки зумовлена обманом.

В Україні, як і у світі, **найпопулярнішим методом інтернет-шахрайства, що вчиняється**, є шахрайство із платіжними картками, тобто соціальна інженерія – це коли:

1) постраждалі самі розкривають зловмисникам дані своїх банківських карток;

2) жертви самі переказують гроші аферистам;

3) «Online-banking», тобто привласнення банківських карт потерпілих для збільшення ліміту та перерахування всіх коштів на підконтрольні рахунки або платіжні системи мережі Інтернет.

Потерпіли самі розкривають їм дані своїх карток

Створюють шахрайські call-центри для виманювання коштів у населення з використанням платіжних карток. Тобто **вчиняють фішинг** – це коли злочинці під час телефонної розмови намагаються випитати у власника дані карти і банківські sms-паролі. Відповідно до статистики 76% власників платіжних карт, які стали об'єктом фішингу, розголошують шахраям реквізити своїх банківських карт, забезпечуючи доступ злочинцям до своїх рахунків.

Найпоширенішим в Україні способом, за допомогою якого шахраї намагаються випитати у громадян реквізити карти по телефону, є звернення під виглядом працівника банку (в 94% випадках), поліції, СБУ, НБУ, Пенсійного фонду, благодійної організації або покупця під різними приводами (перевірка служби безпеки, блокування карти, нарахування надбавки до пенсії, придбання товару).

Шахраї, використовуючи статус анонімності, несучи за свої дії мінімальну відповідальність, мають можливість, використовуючи комп'ютерно-телекомунікаційні пристрої, вчиняти злочини у будь-якій країні, без обмеження в часі й просторі, а також мають змогу обрати об'єкт посягання у країні, де відсутня відповідальність за таку діяльність, чи покарання є достатньо м'яким, у порівнянні з іншими державами [9 с. 180].

Наприклад, співробітники відділу протидії кіберзлочинам Сумщини спільно зі слідчими Головного слідчого управління Нацполіції під процесуальним керівництвом Офісу Генерального прокурора викрила шахрайський call-центр в центрі міста в орендованому офісі, оператори якого видавали себе за працівників банку. Зловмисники телефонували громадянам сусідньої країни та випитували в них конфіденційну інформацію, зокрема CVV-коди, номери та пін-коди банківських карт. Далі, використовуючи ці дані, фігуранти виводили гроші з карток потерпілих на підконтрольні рахунки. Потерпілим завдано збитків на майже 3 мільйони гривень.

Відкрито кримінальне провадження за ч. 4 ст. 190 (Шахрайство) Кримінального кодексу України. Санкція статті передбачає позбавлення волі на строк до 12 років з конфіскацією майна [10].

Також кіберполіцейськими Слобожанщини виявлено та задокументовано злочинну групу з ознаками організованості, учасники якої,починаючи з вересня 2016 року до червня 2017 р. шахрайським шляхом заволоділи 46 банківськими картками громадян, а в подальшому несанкціоновано втрутились у роботу електронно-обчислювальних машин (комп'ютерів) АТ «Ощадбанк» і за допомогою системи WEB-банкінг «Ощад 24/7» переприв'язували їх до мобільного телефону учасника злочинної групи та вчиняли заволодіння грошовими коштами громадян у значних розмірах [11].

Потерпілі самі переказують гроші аферистам

Злочинні групи, які створюють та підтримують функціонування онлайн-казино. Приміром, працівники кіберполіції в місті Києві припинили протиправну діяльність компанії, яка створювала онлайн-казино. Для технічної підтримки вебресурсів у штаті налічувалось більше 80-ти IT-спеціалістів. Встановлено більше 20-ти онлайн-казино, розробниками та адміністраторами яких є вказана компанія. База користувачів їх вебресурсів налічувала близько пів мільйона осіб. За попередніми даними, щомісячний прибуток від протиправної діяльності становив понад 500 тисяч доларів.

Сьогодні **продаж неіснуючих товарів** готується та вчиняється в більшості випадків групою осіб. **Створення та функціонування декількох фейкових інтернет магазинів** із залучення посередників.

Приміром, група молодиків з м. Южноукраїнськ, Миколаївської області, які створили не менше 10 інтернет-магазинів на Інтернет-платформах, таких як «zakupka.com», «etov.ua», та розмістили на них оголошення про продаж мобільних телефонів, материнських плат та іншої техніки, яких насправді не мали в наявності та не

мали наміру продавати. Умовою поставки товару була 100% передплата. Із метою конспірування своєї діяльності зловмисники задіяли посередників, які використовували банківські картки різних банків, відкриті на різних осіб, отримували на них грошові кошти від потерпілих та в подальшому пересилали їх шахраям [12].

Створення злочинної групи для виманювання коштів через **шахрайські телефонні дзвінки.**

Шахраї повідомляють, що сталась якась протизаконна трагедія з членами їхніх сімей чи родичами та, що їх забрали до поліції, а для вирішення питання необхідна відповідна сума грошей. Або телефонують представляючись лікарями і терміново просять перерахувати кошти на лікування онуків, дітей, або батьків. Такі дзвінки здійснюють, по декілька раз передаючи слухавку, начебто інфіціоністу та головному лікарю, які стверджують про нагальну потребу в невідкладному лікуванні, та називають необхідну для цього суму грошей.

Приміром, члени злочинної групи здійснювали телефонні дзвінки з території виправної колонії (розташованої на тимчасово окупованій території Луганської області) із прихованого номеру телефону та, представляючись працівниками поліції, під приводом непритягнення близької особи до відповідальності, вимагали переказати грошові кошти в розмірі від 2 тис. доларів США на карти АТ «Ощадбанк». У подальшому отримані злочинним шляхом грошові кошти знімались через банкомати АТ «Ощадбанк» в Полтавській та Харківській областях, а також ыз використанням терміналів ПАТ КБ «ПриватБанк» розподілялися серед учасниками злочинної групи. Крім того, значна сума грошових коштів, отриманих шахраями, з використанням сервісу переказу коштів «Western Union» конвертувалася в російські рублі та обготівковування на території так званої «ЛНР». На сьогодні задокументовано більше 300 епізодів злочинної діяльності групи, які заподіяли шкоду громадянам на суму понад 4 млн. грн.

У ході проведення обшуків вилучено комп'ютерну техніку, мобільні термінали, понад 70 сімкарт різних мобільних операторів, котрі використовувалися як фінансові номери, грошові кошти, понад 400 чеків із банкоматів з підтвердженням успішного зняття грошових коштів, чорнові записи з номерами карт та пін-кодами до них, а також чорнові записи з підрахунками отриманих злочинним шляхом коштів та 50 банківських карток АТ «Ощадбанк» та КБ «Приватбанк», на які постраждалі переказували грошові кошти [11].

Інші злочинні групи, яким притаманна інша злочинна діяльність, долучаються до вчинення шахрайства в мережі Інтернет. Приміром, на Черкащині діяла злочинна організація, члени якої спочатку під час крадіжок, розбоїв та грабежів привласнювали мобільні телефони та банківські картки потерпілих, а потім збільшували ліміт по кредитним банківським карткам та перераховували кошти на різноманітні банківські рахунки та платіжні системи мережі Інтернет. Кіберполіцейськими проведено обшуки за місцями проживання всіх учасників зазначеного злочинного угрупування, у ході яких вилучено комп'ютерну техніку, мобільні пристрої, банківські картки, що використовувалися злочинцями в їх протиправних цілях, а також «чорнові» записи. Виявлено близько двадцяти постраждалих, що стали жертвами вказаної злочинної групи, яким було нанесено збитків на загальну суму близько 500 тис. грн. [13].

Для вчинення кожного із розглянутих методів інтернет-шахрайства організовані злочинні групи та злочинні об'єднання заздалегідь готовилися до їх вчинення, а саме оснащувалися комп'ютерною технікою, мобільними телефонами, сім-картами, канцелярським приладдям, а з випадками call-центрів орендували приміщення під офіс та наймали працівників зі знанням декількох мов, прописували інструкції та проводили тренінги для співробітників щодо спілкування з різними типами людей, від інтересів, професійної направленості, вікових особливостей, ментальних до особливостей характеру та темпераменту.

Отже, інтернет-шахрайства вчиняють як групи від двох осіб за попередньою змовою, так і групи осіб, які зорганізувалися в стійке злочинне об'єднання та злочинну організацію, кількість яких не обмежується і сотнею.

На нашу думку, **форма організованого шахрайства в мережі Інтернет** – це група осіб, які об'єдналися для вчинення злочинної діяльності економічної спрямованості з використанням Інтернету як інструменту для досягнення своїх злочинних цілей, шляхом введення в оману потерпілого для передачі ним уявно добровільно начебто у своїх інтересах грошових коштів або права на майно на користь зловмисникам.

Успішне запобігання інтернет-шахрайствам, їх викриття і притягнення винних осіб до відповідальності сьогодні є досить рідкісним явищем, якщо порівнювати з їх кількістю. А тому питання вивчення видів груп інтернет-шахраїв різного рівня організованості потребує подальших наукових досліджень.

Література

1. Jay S. Albanese Organized Crime In Our Times (2015) vol. 6, p. 390. URL : http://www.organizedcrime.de/organizedcrimedefinitions.htm#albanese (дата звернення: 04.10.2020).
2. Чернявський С.С. Інтернет шахрайство як об'єкт дослідження правових наук. *Протидія злочинності у сфері інтелектуальної власності та комп'ютерних технологій органами внутрішніх справ: стан, проблеми та шляхи вирішення* : тези доп. Всеукр. наук.-практ. конф., (Донецьк, 12 листоп. 2010 р.). Донецьк : ДЮІ ЛДУВС, 2010. С. 100–103.
3. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 р. № 4651-VI. Дата оновлення: 11.09.2020. URL : https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 15.10.2020).
4. Бишовець О.В., Романенко Т.В. Особа злочинця як елемент криміналістичної характеристики шахрайств, що вчиняються в мережі Інтернет *Вісник кримінального судочинства* 2016. № 1. С. 81–87.
5. Микитчик А.В. Організовані форми шахрайства в системі сучасної злочинності в Україні *Науковий вісник Національної академії внутрішніх справ.* 2015. № 3. С. 33–39.
6. Афанасенко С.І. Стойков І.М. Види та класифікація організованої злочинності. *Південноукраїнський правничий часопис.* 2014. № 4. С. 22–26.
7. Кримінальний кодекс України : Закон України від 2001 р. № 25-26. Дата оновлення: 25.09.2020. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 15.10.2020).
8. Науково-практичний коментар (чинний). Науково-практичний коментар до ст. 190 Кримінального кодексу України *Інформаційно-правова система Ліга-Закон.* URL : https://ips.ligazakon.net/document/KK004696 (дата звернення: 13.10.2020).
9. Шапочка С.В. Стосовно деяких аспектів запобігання шахрайству, що вчиняється організованими злочинними групами з використанням комп'ютерних мереж. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2014. № 2(33). С. 179–182.
10. Кіберполіція викрила шахрайський call-центр, працівники якого спустошували рахунки іноземних громадян 02 жовтня 2020 р. *Офіційний сайт кіберполіції України* URL : https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-shaxrajskyj-call-czentr-praczivnyky-yakogo-spustoshuvaly-raxunky-inozemnyx-gromadyan-26/ (дата звернення: 03.10.2020).
11. Кіберполіцією Слобожанщини ліквідовано злочинну групу шахраїв 21 червня 2017 р *Офіційний сайт кіберполіції України* URL : https://cyberpolice.gov.ua/news/Sohodni-pracivnykamy-Slobozanskoho-upravlinnja-kiberpolicii/ (дата звернення 03.10.2020).
12. Ліквідація ряд шахрайських схем в Миколаївський області. 21 червня 2017. *Офіційний сайт кіберполіції України* URL : https://cyberpolice.gov.ua/news/likvidovano-ryad-shaxrajskyx-932/ (дата звернення 02.10.2020).
13. Кіберполіцією затримано шахраїв, що вчиняли злочини у сфері «Online-banking» 21 червня 2017. *Офіційний сайт кіберполіції України.* URL : https://cyberpolice.gov.ua/news/kiberpolicziyeyu-zatrymano-shaxrayiv-603/ (дата звернення: 02.10.2020).

References

1. Jay S. Albanese (2015) Orhanizovana zlochynnist' u nash chas [Organized Crime In Our Times]. vol. 6, p. 390. URL: http://www.organizedcrime.de/organizedcrimedefinitions.htm#albanese (data zvernennia 04.10.2020).
2. Chernyavsky S.S. (2010). Internet shakhraystvo yak ob"yekt doslidzhennya pravovykh nauk. [Internet fraud as an object of study of legal sciences]. *Countering crime in the field of intellectual property and computer technology by law enforcement agencies: the state, problems and solutions*: theses add. All-Ukrainian scientific-practical conf., (Donetsk, November 12, 2010). Donetsk: DUI LDUVS, pp. 100–103.
3. Kryminalnyi protsesualnyi kodeks Ukrainy: Zakon Ukrainy vid 13.04.2012 № 4651-VI. [Criminal Procedure Code of Ukraine: Law of Ukraine dd. 13.04.2012 № 4651-VI] Data onovlennia: 01.07.2020. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (data zvernennia 15.10.2020) [In Ukrainian]
4. Byshovets O.V., Romanenko T.V. (2016). Osoba zlochyntsya yak element kryminalistychnoyi kharakterystyky shakhraystv, shcho vchynyayut'sya v merezhi Internet [The identity of the offender as an element of the forensic characteristics of fraud committed on the Internet] *Bulletin of criminal proceedings,* no. 1, pp. 81–87.
5. Mikitchik A.V. (2015) Orhanizovani formy shakhraystva v systemi suchasnoyi zlochynnosti v Ukrayini [Organized forms of fraud in the system of modern crime in Ukraine] *Scientific Bulletin of the National Academy of Internal Affairs*, no. 3, pp. 33–39.

6. Afanasenko S.I. Stoykov I.M. (2014) Vydy ta klasyfikatsiya orhanizovanoyi zlochynnosti [Types and classification of organized crime]. *South Ukrainian Law Journal,* no. 4, pp. 22–26.
7. Kryminal'nyy kodeks Ukrayiny: Zakon Ukrainy vid 05.04.2001 № 2341-III Criminal Code of Ukraine [Criminal Code of Ukraine: Law of Ukraine dd. 05.04.2001 № 2341-III] Data onovlennia: 25.09.2020. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text. (data zvernennia 15.10.2020). [In Ukrainian].
8. Naukovo-praktychnyy komentar (chynnyy). Naukovo-praktychnyy komentar do st. 190 Kryminal'noho kodeksu Ukrayiny [Scientific and practical commentary (current). Scientific and practical commentary to Art. 190 of the Criminal code of Ukraine] Information and legal system League-Law [Electronic resource] URL : https://ips.ligazakon.net/document/KK004696 (data zvernennia 13.10.2020).
9. Shapochka S.V. (2014) Stosovno deyakykh aspektiv zapobihannya shakhraystvu, shcho vchynyayet'sya orhanizovanymy zlochynnymy hrupamy z vykorystannyam komp'yuternykh merezh [On some aspects of prevention of fraud committed by organized criminal groups using computer networks]. *Fight against organized crime and corruption (theory and practice)*. vol. 33, no. 2, pp. 179–182.
10. Kiberpolitsiyeyu Slobozhanshchyny likvidovano zlochynnu hrupu shakhrayiv [Cyberpolice exposed a fraudulent call-center, whose employees ravaged the accounts of foreign nationals] on October 2, 2020. *Official site of the Cyberpolice of Ukraine* URL : https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-shaxrajskyj-call-czentr-praczivnyky-yakogo-spustoshuvaly-raxunky-inozemnyx-gromadyan-26/ (data zvernennia 03.10.2020)
11. Kiberpolitsiyeyu Slobozhanshchyny likvidovano zlochynnu hrupu shakhrayiv [Cyberpolice of Slobozhanshchyna liquidates criminal group of swindlers] June 21, 2017 *Official site of cyberpolice of Ukraine* URL : https://cyberpolice.gov.ua/news/Sohodni-pracivnykamy-Slobozanskoho-upravlinnja-kiberpolicii/ (data zvernennia 03.10.2020).
12. Likvidatsiya ryad shakhrays'kykh skhem v Mykolayivs'kyy oblasti. [Elimination of a number of fraudulent schemes in the Nikolaev area.] June 21, 2017. *Official site of the cyberpolice of Ukraine* URL : https://cyberpolice.gov.ua/news/likvidovano-ryad-shaxrajskyx-932/ (data zvernennia 02.10.2020).
13. Kiberpolitsiyeyu zatrymano shakhrayiv, shcho vchynyaly zlochyny u sferi onlayn-bankinh [Cyberpolice have detained fraudsters who committed crimes in the area "Online-banking»] June 21, 2017. *Official site of the cyberpolice of Ukraine* URL : https://cyberpolice.gov.ua/news/kiberpolicziyeyu-zatrymano-shaxrayiv-603/ (data zvernennia 02.10.2020).