УДК 343.53:343.346.8

До питання запобігання окремим видам шахрайства, яке вчиняється з використанням можливостей мережі Інтернет

Шапочка Сергій Володимирович –
науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України

У статті проаналізовано соціальні та кримінально-правові аспекти шахрайства, що вчиняється з використанням мережі Інтернет, а також запропоновано заходи протидії такій діяльності як у контексті охорони конституційних прав громадян, так і захисту національної безпеки України.

Ключові слова: шахрайство, Інтернет-шахрайство, криптовалюта, віртуальна валюта.

Постановка проблеми. Сучасна злочинність зростає якісно і кількісно, тому для посилення і результативності боротьби з нею, необхідно глибше та ширше дослідити її нову природу, зміни, що відбуваються [1, с. 5].

З розвитком телекомунікаційних технологій еволюціонують і потенційні загрози національній безпеці, однією з них є високотехнологічні злочини, що вчиняються з використанням мережі Інтернет організованими злочинними угрупованнями.

Відповідно до Закону України "Про основи національної безпеки України" від 19 червня 2003 року № 964-IV [2] система забезпечення інформаційної безпеки є складовою частиною національної безпеки держави, а інформаційна безпека є однією з найважливіших функцій держави, що полягає в захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність та недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій [3].

Варто зазначити, що згідно зі звітом Центру з питань скарг у мережі Інтернет США (Internet Crime Complaint Center), у глобальних масштабах збиток від злочинів, що вчиняються з використанням мережі Інтернет, перевищує 1 трлн дол. США. Здебільшого сума викрадених коштів складає 100–5000 дол. (65 % загальної суми збитків) [4].

При цьому, з усієї сукупності злочинів, що вчиняються з використанням мережі Інтернет, частка шахрайств становить 58 % [5, с. 3].

Шахрайство в мережі Інтернет зберігає сталу тенденцію до еволюціонування, з'являються нові його види (рерайтинг, серфінг, креммінг, шахрайство з криптовалютами) чи удосконалюються вже відомі, такі як: фішинг, скіммінг, використання програм-шпигунів (spyware, keyloggers), обман під час купівлі-продажу товарів у Інтернет-магазинах, шахрайство в Інтернет-аукціонах, SMS-шахрайство тощо.

Згідно зі статистичними даними МВС України за 2013 рік, 46 % (2146 кримінальних проваджень) від загальної кількості злочинів, що знаходились у провадженні підрозділів по боротьбі з кіберзлочинністю, становлять злочини, вчинені з ознаками ст. 190 КК України (Шахрайство). Середньостатистичний показник розкриття даного виду злочинів складає 53 %. А загальна сума збитків від шахрайських операцій, згідно з матеріалами кримінальних проваджень даної категорії, у минулому році перевищила 67,8 млн грн, з яких вдалося заблокувати та повернути потерпілим близько 47,5 млн грн, що становить 70,1 %.

Аналіз останніх публікацій за темою дослідження. Проведенням наукових досліджень окремих аспектів боротьби зі злочинами, що вчиняються з використанням мережі Інтернет взагалі та шахрайства зокрема, займаються такі вчені, як І. Г. Богатирьов, В. М. Бутузов, В. Д. Гавловський, Д. О. Зиков, А. А. Комаров, В. Д. Ларичев, А. К. Лебедєв, О. В. Лисодєд, А. В. Микитчик, О. В. Смаглюк, К. В. Тітуніна, С. С. Чернявський, В. І. Шакун, В. П. Шеломенцев, О. М. Юрченко та інші, а також автор представленої статті.

З огляду на те, що комп'ютери та об'єднані інформаційні системи набувають усе більшого значення, суттєво збільшуються і можливості для злочинної діяльності, що здійснюється з використанням комп'ютерних мереж шляхом обману чи зловживанням довірою, відбувається стрімкий розвиток й удосконалення способів Інтернет-

шахрайства, що спонукає нас до подальших наукових досліджень.

Мета статті. В попередніх наукових публікаціях вивчалися різні аспекти шахрайства, що вчиняється з використанням можливостей мережі Інтернет. Ця стаття є логічним продовженням здійснюваного нами дослідження, а також вироблення заходів протидії такій злочинній діяльності як у контексті охорони конституційних прав громадян, так і захисту національної безпеки України.

Виклад основного матеріалу. Глобальність сучасних можливостей і досягнень людства прямо пропорційна глобальності загроз і злочинних проявів. У той же час, розвиток Інтернет-технологій, дозволили підняти на новий інтернаціонально-континентальний рівень торговельно-економічні відносини та електронну комерцію. Змінилися, зміцнившись і позиції транснаціональної злочинності, набули нових рис, необмежених можливостей [6, с. 63]. Останнім часом широкого розповсюдження і популяризації набуло використання децентралізованих віртуальних криптовалют : Bitcoin (BTC), Litecoin (LTC), Namecoin, Zerocoin, Quark, Megacoin, Namecoin, Peercoin, Worldcoin тощо. Темпи приросту капіталу їх власників складали в окремі дні 100 %, 200 % і навіть 1000 % . Криптовалюта стала одним із видів електронних платіжних засобів для оплати товарів і послуг в мережі Інтернет, її також можна обміняти на реальні гроші.

Точних даних щодо кількості користувачів BTC не встановлено, проте курс цієї валюти з 2011 року виріс більш ніж у 200 разів, зробивши багато її власників мільйонерами. Складність відстеження платіжних операцій, відсутність плати за трансакції, відсутність необхідності надання ідентифікуючих чи дозвільних документів, велика швидкість розрахунків сприяють стрімкому збільшенню попиту, а з ним і котирувального курсу. Сьогодні сотні компаній світу розраховуються криптовалютою купуючи товари, оплачуючи послуги. Так, під час гри в казино у м. Лас-Вегасі, США, приймають ставки в BTC.

До недавнього часу дорожчав лише BTC, який називають "електронним золотом", і LTC – "електронне срібло".

Але, коли наприкінці минулого року курс одного BTC зріс до 1000 дол., на ринку криптовалют виник безпрецедентний ажіотаж. Люди почали вкладати гроші в усі криптовалюти підряд, навіть у неліквідні. Таким чином, найближчі конкуренти BTC, якими можна торгувати на електронній біржі, подорожчали : LTC – з 8,5 дол. до 30 дол., Peercoin – з 1,5 дол. до 6 дол., Namecoin – з 2,5 дол. до 9 дол. Усього за тиждень капіталізація віртуальної платіжної системи Quarkcoin підскочила в 500 разів – з 100 тис. дол. до 50 млн дол., Megacoin виріс у ціні в 30 разів – з 1 млн дол. до 30 млн дол., Worldcoin – у 10 разів до 16 млн дол. [7. По суті, кожна з цих платіжних систем стала новим валютним ринком.

Нерегульована сфера обігу віртуальних валют стала користуватися великою популярністю також серед організованих злочинних угруповань, що приймають оплату за свої послуги у віртуальній валюті, використовуючи альтернативний "темний" Інтернет – DarkNet, який функціонує на основі системи The Onion Router (TOR).

Разом з тим, незважаючи на анонімність, будь-яка трансакція з віртуальними валютами є публічною для пересічного користувача мережі, а учасник настільки анонімний, наскільки анонімний його зв'язок із електронним гаманцем[1].

Продаж і переведення в готівку BTC – складне завдання, оскільки основні BTC-обмінники вимагають документ, що засвідчує особу (зокрема, щоб уникнути звинувачень, що вони беруть участь у відмиванні коштів), тому "паперовий" слід усе одно залишиться. А як тільки з'явиться хоча б один реальний банківських рахунок – виникне можливість викрити зловмисника.

Шахрайство з криптовалютами є серйозною проблемою і для такої розвинутої країни як США, банківські регулятори якої звернули увагу на зростання кількості зазначених злочинів. Управління фінансових послуг м. Нью-Йорк, встановивши, що нерегульована сфера віртуальних валют користується великою популярністю серед Інтернет-шахраїв, дійшло висновку, що цей вид шахрайства загрожує національній безпеці США.

У липні минулого року ФБР було розкрито незаконну фінансову піраміду, створену громадянином США Трендоном Шеверсом, який використав інвестиційну схему BTC Savings and Trust і витратив на власні потреби викрадені 700 тис. BTC, що, виходячи з середнього курсу віртуальної валюти, є еквівалентом близько 700 млн дол. [8].

У травні 2013 року правоохоронні органи США припинили злочинну діяльність однієї з найбільших у світі платіжних систем Liberty Reserve, зареєстрованої в Коста-Ріці. За сім років шахраї встигли украсти 55 млн незаконних угод і відмити з використанням мережі Інтернет 6 млрд дол. У Liberty Reserve було майже 1 млн клієнтів із різних країн світу [9], в тому числі її послугами користувалися злочинні угрупування В'єтнаму, Нігерії, Гонконгу, Китаю і США.

Після реєстрації клієнт міг перевести справжню валюту на рахунки компаній-обмінників, розташованих в інших країнах, у тому числі – в Росії. Там, наприклад, можна було обміняти через третю особу справжні долари або євро на віртуальну валюту і, після цього, кошти у віртуальній валюті надходили на рахунок іншого клієнта, який купував наркотики та викрадені номери кредиток, перевівши потрібну суму на рахунок продавця, відкритий також в Liberty Reserve.

[1] ЕЛЕКТРОННИЙ ГАМАНЕЦЬ (e-purse) – смарт-картка або платіжний додаток до платіжної картки, кошти за операціями з якою(им) обліковуються на консолідованому рахунку емітента. Використання ЕГ дає змогу його держателю в межах установленого ліміту виконувати платіж за товари (послуги) без введення персонального ідентифікаційного номера. ЕГ призначений для здійснення розрахунків і зняття готівки на невеликі суми. ЕГ є одним із типів наперед оплачених платіжних карток.

Користуючись послугами компанії за комісію в 1 %, злочинці без зусиль перекачували за будь-якою адресою свої доходи від незаконної торгівлі наркотиками, шахрайства з кредитними картками або поширення дитячої порнографії.

Ще одним прикладом, що заслуговує на увагу, є шахрайство в мережі Інтернет з використанням криптовалюти BTC й анонімного браузера TOR для забезпечення онлайн-продажу заборонених товарів. Так, у грудні минулого року було викрадено з рахунків клієнтів, постачальників і адміністраторів сайту Sheepmarketplace 96 тис. BTC, а це майже 100 млн дол. [10]. Злочинці підробили залишки BTC на рахунках користувачів у власних гаманцях на сайті, тоді як насправді кошти вже були переведені на рахунки злочинців. Протягом тижня сайт системно спустошувався, а коли адміністрація усвідомила проблему і відреагувала, з рахунків користувачів зникла велика кількість грошей. Все це сталося через декілька днів після того, як інший конкурент Silkroad – Black Market Reloaded оголосив, що припиняє свою діяльність через нездатність забезпечити роботу з великою кількістю нових користувачів, які переходять від Sheepmarketplace. Зазначене шахрайство на сьогодні є одним із найбільших шахрайств у історії з використанням BTC.

Зазначимо, що на початку березня поточного року жертвами Інтернет-шахраїв стали сайти, які працюють із віртуальною валютою BTC, так звані BTC-банки – Flexcoin та Poloniex, сервери яких знаходяться на території США [11]. Відомо, що для вчинення зазначеного злочину зловмисники створили власний обліковий запис у системі Flexcoin і поповнили свій рахунок декількома BTC. Після цього вони вчинили злом системи трансакцій між користувачами, відправили кілька тисяч одночасних запитів, чим сприяли "переходу" монет з одного облікового запису в інший. Набравши необхідну суму, зловмисники перевели викрадені BTC на власні рахунки.

BTC-банк Poloniex від зазначеного злочину втратив 12,3 % BTC, що належали користувачам, а Flexcoin – "перший у світі банк, що працює з BTC", був вимушений закритися. Загальна сума збитків від злочину склала 896 BTC, що становить близько 900 тис. дол.

За твердженням представників Flexcoin, за останні три роки злочинці вчинили понад тисячу замахів на вчинення Інтернет-шахрайства з BTC.

Варто зазначити, що і Німеччина не залишилася поза процесом протидії шахрайству з криптовалютами. Так, під час рейду поліцейського контртерористичного загону (GSG-9) Федеральної служби по боротьбі з криміналом (BKA) Німеччини було затримано підозрюваних у вчиненні шахрайства з BTC, збитки від якого склали 700 тис. євро. Злочинці здійснили генерування віртуальної валюти BTC за допомогою заражених комп'ютерних систем. При цьому Президент BKA Йорг Цирке заявив, що мережа Інтернет забезпечує організовані злочинні групи новими інструментами, що несе великий ризик для фінансової системи країни [12].

Ще одним прикладом боротьби з шахрайством, вчиненим під час продажу віртуальної криптовалюти BTC, стало порушення першої в Естонії кримінальної справи про шахрайство наприкінці лютого поточного року.

Показово, що у Канаді та США вже з'явилися BTC-банкомати, BTC-біржі, що дають можливість створити відчуття попиту і ліквідності віртуальної валюти, а, як наслідок, – призвести до стрімкого росту її курсу, зробити віртуальні гроші платіжним засобом організованих злочинних угруповань і предметом вчинення злочинів у мережі Інтернет.

Також, у деяких країнах, зокрема Китаї, Росії, Таїланді, операції з BTC є незаконними. Так, Національний банк Китаю заборонив кредитно-фінансовим установам держави будь-які операції, пов'язані з BTC, намагаючись уникнути ризиків для вітчизняної економіки. Необхідно зазначити, що заборона стосується лише юридичних осіб, а громадяни можуть вкладати свої заощадження на власний розсуд.

Зазначимо, що реакція Російської Федерації на операції з криптовалютою була ще більш жорсткою. За результатами засідання експертної групи з представників Центробанку, МВС, ФСБ, Генеральна прокуратура РФ заявила, що віртуальні валюти несуть високий ризик порушень майнових прав громадян і не можуть використовуватися фізичними та юридичними особами в РФ.

Так, за матеріалами перевірки прокуратурою Волгоградської області 3 лютого 2014 року було порушено кримінальну справу за ознаками злочинів, передбачених ст. 159 (Шахрайство) та ч. 2 ст. 174 (Легалізація (відмивання) грошових коштів чи іншого майна, набутих іншими особами злочинним шляхом) КК РФ щодо Інтернет-ресурсів з надання послуг з обміну віртуальних валют.

Отже, криптовалютна торгівля перетворилася на глобальну "азартну гру", в яку легко включитися – досить купити віртуальні гроші на біржі. Тобто віртуальні валюти – це величезні світові шахрайські піраміди.

Різке зростання популярності криптовалют змусило багатьох українців також замислитися над тим, щоб здійснювати такі розрахунки, а також заробляти на майнінгу – видобутку BTC. Загальний порядок проведення переказу коштів у межах України, відповідальність суб'єктів переказу коштів, а також правові вимоги до здійснення випуску і використання електронних грошей в Україні встановлені Законом України "Про платіжні системи і переказ коштів в Україні". А відповідно до статей 9 і 15 цього Закону платіжні організації платіжних систем, учасники платіжних систем і оператори послуг платіжної інфраструктури мають право здійснювати діяльність в Україні виключно після їх реєстрації Національним банком України (НБУ), який також має виключне право випуску електронних грошей. На сьогодні в НБУ не зверталися банки або інші юридичні особи з приводу реєстрації платіжної системи BTC або з приводу узгодження правил використання електронних

грошей BTC. НБУ застерігає українців від використання такої системи.

Поряд із вищеозначеним, в Україні BTC можна придбати в Інтернет-банку Приват-24.

Тобто, в Україні жорсткої реакції з боку органів влади та управління щодо операцій з криптовалютами поки що не було. На нашу думку, це пов'язано з недооцінкою рівня можливого негативного впливу криптовалюти на економіку, стан злочинності та функціонування кредитно-банківської системи держави.

Викладені вище факти свідчать про великі потенційні можливості використання віртуальних валют у злочинних цілях. Це створює реальні та потенційні загрози національній безпеці України в частині використання віртуальних валют, а саме: відповідно до ст. 7 Закону України "Про основи національної безпеки України" загрозами в економічній сфері є нестабільність у правовому регулюванні відносин у сфері економіки, в тому числі фінансової (фіскальної) політики держави; зростання кредитних ризиків; ослаблення системи державного регулювання і контролю у сфері економіки; істотне скорочення внутрішнього валового продукту; "тінізація" національної економіки. В першу чергу, це стосується банківської сфери.

Відповідно до Закону України "Про організаційно-правові основи боротьби з організованою злочинністю" [13] систему державних органів, які здійснюють боротьбу з організованою злочинністю, становлять: а) спеціально створені для боротьби з організованою злочинністю державні органи; б) державні органи, які беруть участь у боротьбі з організованою злочинністю в межах виконання покладених на них інших основних функцій. Із числа суб'єктів зазначеної діяльності питаннями запобігання Інтернет-шахрайствам, що вчиняються з використанням криптовалют, в межах своєї компетенції, визначеної на основі відповідних законів, можна виділити таких: Національний банк України, Державна податкова служба України, Служба безпеки України, Міністерство внутрішніх справ України.

Вказані суб'єкти боротьби з організованою злочинністю, згідно з законами, які визначають їх правових статус, повинні:

Національний банк України:

а) на виконання своїх функцій, відповідно до основних засад грошово-кредитної політики, визначати та проводити грошово-кредитну політику в інтересах національної безпеки України під час здійснення у межах своєї компетенції контрольних функцій, з'ясовувати неправомірні дії організацій і громадян, що можуть свідчити про злочинну діяльність або створювати умови для такої діяльності, яка здійснюється з використанням віртуальних валют;

б) передавати СБ України, МВС України одержувані при здійсненні контрольних функцій та аналізі інформації, що надходить, відомості, які можуть свідчити про організовану злочинну діяльність з використанням криптовалюти та використовуватися для виявлення, припинення і попередження такої діяльності;

в) за дорученням СБ України, МВС України проводити у межах своєї компетенції ревізії, перевірки та інші дії щодо контролю за дотриманням законодавства України організаціями і громадянами у сфері обігу криптовалют;

г) розробити пропозиції щодо вдосконалення законодавства, спрямовані на усунення умов, які сприяють злочинній діяльності з використання криптовалют;

д) забезпечити виявлення порушень законодавства у сфері обігу віртуальних валют з боку комерційних банків та інших підконтрольних Національному банку України підприємств, установ, організацій, які створюють умови для організованої злочинної діяльності, й притягнення винних до відповідальності;

е) здійснювати державний фінансовий моніторинг, забезпечуючи формування та реалізацію державної політики у сфері запобігання і протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом або фінансування тероризму, що вчиняється з використанням віртуальних валют;

є) організувати дієву взаємодію з суб'єктами первинного фінансового моніторингу в сфері обігу віртуальних валют.

Державна податкова служба України:

а) за дорученням СБ України, МВС України провести перевірку своєчасності надання і достовірності документів, пов'язаних з обчисленням сум платежів до бюджету, одержаних від операцій з віртуальними валютами;

б) за дорученням СБ України, МВС України проводити перевірку законності операцій із віртуальними валютами організацій і громадян, та здійснювати спільно з Національним банком України комплексний контроль за їх валютними операціями;

Служба безпеки України та Міністерство внутрішніх справ України:

У межах компетенції вжити дієвих заходів щодо попередження, виявлення, припинення та розкриття злочинів, що вчиняються організованими злочинними групами, у сфері економіки, пов'язаних із використанням віртуальних валют, які безпосередньо створюють загрозу життєво важливим інтересам України, фінансуючи вчинення тероризму; здійснюючи легалізацію (відмивання) доходів, одержаних злочинним шляхом, інших злочинів.

На нашу думку, перелічені державні органи з метою всебічного вивчення криптовалют, опрацювання можливих ризиків і загроз, що можуть виникнути чи вже існують, у зв'язку з використанням віртуальних валют, повинні вийти з ініціативою щодо створення міжвідомчої робочої групи з числа представників правоохоронних органів, кредитно-банківської сфери, громадськості, бізнесу під загальною координацією НБУ.

Окрім цього, на підставі викладеного вище, з метою запобігання й нейтралізації реальних і потенційних загроз національній безпеці

України, протидії деструктивному впливу віртуальних валют на розвиток економіки України, запобігання їх використання для вчинення злочинів у мережі Інтернет узагалі та шахрайства зокрема, вважали б за доцільне здійснити наступні заходи:

1) доручити правоохоронним органам у тісній співпраці з представниками кредитно-банківської сфери здійснення моніторингу використання криптовалют, росту і падіння її курсу, забезпечивши широке висвітлення в ЗМІ питань щодо можливих ризиків участі в операціях з використанням криптовалюти;

2) вжити заходів щодо обмеження в Україні трансакцій з використанням криптовалют;

3) за результатами діяльності експертів міжвідомчої робочої групи розглянути питання щодо напрацювання відповідних змін та доповнень до законодавства України стосовно регулювання питань, пов'язаних із операціями з криптовалютами в Україні;

4) налагодити міжнародну співпрацю з державами, які мають відповідний досвід протидії деструктивному впливу криптовалюти.

Висновки. Очевидно, що проблема забезпечення інформаційної безпеки є однією з найбільш актуальних, а небезпека потенційних загроз у вигляді ІТ-злочинності взагалі та шахрайства з криптовалютами зокрема – реальною, що потребує системної, наступальної реакції держави, удосконалення українського законодавства.

Перспективи подальшого використання. На переконання автора, використання у ході правотворчої та правозастосовної практики вказаних вище висновків має сприяти не тільки підвищенню ефективності правової охорони конституційних прав громадян України, а й захисту життєво важливих інтересів нашої держави шляхом запобігання та нейтралізації реальних і потенційних загроз національній безпеці України, протидії деструктивному впливу віртуальних валют, запобігання їх використанню для вчинення шахрайства у мережі Інтернет.

Список використаних джерел

1. Бахин В. П. Материалы к изучению практики борьбы с преступностью / Бахин В. П., Карпов Н. С. – К. : Изд-во Семенко Сергея, 2007. – 489 с.
2. Про основи національної безпеки України : Закон України від 19 черв. 2003 р. № 964-IV / [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=964-15.
3. Про засади інформаційної безпеки України : Проект Закону України від 28 трав. 2014 р. № 4949 / [Електронний ресурс]. – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=51123.
4. Кибермошенничество в эпоху глобализации / [Электронный ресурс]. – Режим доступа : http://univer-nn.ru/it/flood.php.
5. Комаров А. А. Криминологические аспекты мошенничества в глобальной сети Интернет : дис. на соискание ученой степени канд. юрид. наук : спец. 12. 00. 08 "Уголовное право и криминология; уголовно-исполнительное право" / А. А. Комаров. – Саратов, 2011. – 262 с.
6. Shapochka S. Preventing Fraud Using Computer Networks / Serhiy Vladimirovich Shapochka // Internal Security. – 2013. – № 2. – P. 63–75.
7. В мире бум криптовалютных пирамид / [Электронный ресурс]. – Режим доступа : http://ubp.com.ua/finance/2013/12/04/107742/.
8. Регуляторы США начали проверки фактов мошенничества с цифровой валютой / [Электронный ресурс]. – Режим доступа : http://finance.bigmir.net/news/finance/37820-Regylyatori-SShA-nachali-proverki-faktov-moshennichestva-s-cifrovoi-valutoi.
9. Подпольные деньги вывели из обращения / [Электронный ресурс]. – Режим доступа : http://www.kommersant.ru/doc/2200186.
10. У пользователей подпольной онлайн-биржи Sheep Marketplace украли биткоины почти на $100 млн / [Электронный ресурс]. – Режим доступа : http://www.vedomosti.ru/tech/news/19674451/nerealnaya-krazha.
11. Уязвимость в системе транзакций между пользователями позволила похитить Bitcoin на $600 тысяч / [Электронный ресурс]. – Режим доступа : http://www.securitylab.ru/news/450258.php.
12. Немецкая полиция задержала хакеров, пытавшихся завладеть биткойнами / [Электронный ресурс]. – Режим доступа : https://cryptochan.org/news/203.
13. Про організаційно-правові основи боротьби з організованою злочинністю : Закон України від 30 черв. 1993 р. № 3341-XII / [Електронний ресурс]. – Режим доступу : http://zakon1.rada.gov.ua/laws/show/3341-12.

В статье проанализированы социальные и уголовно-правовые аспекты мошенничества, совершаемого с использованием сети Интернет, а также предложены меры противодействия такой деятельности как в контексте охраны конституционных прав граждан, так и защиты национальной безопасности Украины.

The socially and criminal-legal aspects of the fraud committing by the use of the Internet network are analyzed in the article, and also the measures of counteraction of such activity are offered, both in the context of guard of constitutional rights of the citizens and defense of the national security of Ukraine.

Стаття надійшла до редакції журналу 15 квітня 2014 року.