КРИМІНАЛЬНИЙ ПРОЦЕС ТА КРИМІНАЛІСТИКА; СУДОВА ЕКСПЕРТИЗА; ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ

УДК 343.98
DOI https://doi.org/10.32844/2618-1258.2021.5.1.21

ЄФІМОВ М.М.

КРИМІНАЛІСТИЧНИЙ АНАЛІЗ ОКРЕМИХ СУЧАСНИХ ВИДІВ ШАХРАЙСТВА: ПРОБЛЕМНІ ПИТАННЯ

CRIMINAL ANALYSIS OF CERTAIN MODERN TYPES OF FRAUD: PROBLEM ISSUES

Наукова стаття присвячена дослідженню деяких аспектів розслідування шахрайства. Автор акцентує увагу на тому, що у сучасному світі шахрайство займає чи не найпершу позицію серед найбільш поширених правопорушень. З огляду на блискавичний розвиток інформаційних технологій упродовж останніх десятиліть можна виділити його окрему групу – інтернет-шахрайство. Щодня громадяни абсолютно всіх країн несуть величезні збитки, стаючи жертвами шахраїв у мережі Інтернет. Так, апаратні засоби та програмне забезпечення з кожним днем удосконалюються, стають більш захищеним, але водночас правопорушники також покращують свої навички і проходять крізь новостворені мережеві бар'єри. На жаль, правоохоронна система не завжди встигає за технологічним розвитком, і попередні протоколи дій втрачають свою актуальність уже сьогодні.

Зазначено, що одним із найпотужніших поштовхів до розвитку шахрайств у мережі Інтернет за останні два роки стала всесвітня пандемія COVID-19. Відсутність роботи у період карантину, перехід на онлайн-торгівлю, намагання людей уникати фізичних контактів спровокували реальний ринок товарів та послуг дуже швидко зануритись у мережеві торгові відносини. Фактично люди були змушені погодитись із сучасними правилами життя і, не маючи достатнього досвіду користування Інтернетом, будучи недостатньо обізнаними у питаннях приватності та інформаційної безпеки у всесвітній мережі, дуже легко перетворились на жертв кібершахраїв.

Наголошено на тому, що правопорушники використовують найновіші технології та обладнання, дуже швидко пристосовуючи їх для своїх злочинних цілей, адаптуються до зростання прогресу, розробляючи нові шахрайські схеми.

Зазначено, що серед усіх видів інтернет-шахрайств можна виділити такі основні та найбільш поширені, як фішинг, сніфферінг, вішинг, кардінг. Користувачам мережі Інтернет, холдерам банківських карт, а також будь-яким пересічним громадянам необхідно бути ознайомленими із сучасними способами інтернет-шахрайства. Зокрема, слід бути дуже обачними, використовуючи онлайн-банкінг, мобільний зв'язок, здійснюючи покупки в інтернет-магазинах, бути уважними під час розголошення власних персональних даних в ході введення інформації у форми на різних сайтах.

Ключові слова: *шахрайство, фішинг, сніфферінг, вішинг, кардінг, спеціальні знання, процесуальні дії.*

© ЄФІМОВ М.М. – доктор юридичних наук, доцент, доцент кафедри криміналістики та домедичної підготовки (Дніпропетровський державний університет внутрішніх справ)

The scientific article is devoted to the study of some aspects of fraud investigation. The author emphasizes that in today's world, fraud is perhaps the first among the most common offenses. And given the rapid development of information technology over the past decades, we can distinguish a separate group – Internet fraud. Every day, citizens of all countries suffer huge losses, becoming victims of fraud on the Internet. Yes, hardware and software are improving every day, more secure, but at the same time, offenders are also improving their skills and breaking through newly created network barriers. Unfortunately, the law enforcement system does not always keep up with technological developments, and previous protocols of action are losing their relevance today.

It is noted that one of the most powerful impetus for the development of fraud on the Internet in the last two years was the global pandemic COVID-19. Lack of work during the quarantine period, transition to online trade, people's attempts to avoid physical contact provoked the real market of goods and services to quickly immerse themselves in network trade relations. In fact, people have been forced to agree with modern rules of life, and having insufficient experience of using the Internet, being insufficiently aware of privacy and information security on the World Wide Web, very easily become victims of cyber fraud.

It is emphasized that offenders use the latest technology and equipment, very quickly adapting them to their criminal purposes, adapting to the growth of progress, developing new fraudulent schemes.

It is indicated that among all types of Internet fraud, the following are the main and most common: phishing, sniffing, vishing, carding. Internet users, bank card holders, and any ordinary citizen need to be familiar with modern methods of Internet fraud. In particular, be very careful when using online banking, mobile communications, shopping in online stores, is careful when disclosing your personal data when entering information into forms on various sites.

Key words: *fraud, phishing, sniffing, vishing, carding, special knowledge, procedural actions.*

Вступ. У сучасному світі шахрайство займає чи не найпершу позицію серед найбільш поширених правопорушень. З огляду на блискавичний розвиток інформаційних технологій упродовж останніх десятиліть можна виділити його окрему групу – інтернет-шахрайство. Щодня громадяни абсолютно усіх країн несуть величезні збитки, стаючи жертвами шахраїв у мережі Інтернет. Так, апаратні засоби та програмне забезпечення з кожним днем удосконалюються, стають більш захищеними, але водночас правопорушники також покращують свої навички і проходять крізь новостворені мережеві бар'єри. На жаль, правоохоронна система не завжди встигає за технологічним розвитком, і попередні протоколи дій втрачають свою актуальність уже сьогодні. В українському законодавстві досліджуване правопорушення кваліфікується за ч. 3 ст. 190 ККУ [1].

Аналіз останніх досліджень і публікацій. Питанням розслідування шахрайств у різний час приділялась увага у працях багатьох відомих дослідників, зокрема С.М. Астапкіної, А.Ф. Волобуєва, В.Ю. Голубовського, В.М. Єгошина, О.В. Журавльова, А.М. Клочка, А.О. Єременка, В.В. Колеснікова, О.І. Лученка, О.С. Овчинського, В.І. Отряхіна, Н.В. Павлової, А.А. Сандрачука, Р.С. Сатуєвої, Г.М. Спіріної, К.В. Суркової, С.С. Чернявського, Є.П. Фірсової, В.О. Фінагеєва. У своїх дослідженнях А.О. Єременко і А.М. Клочко зазначають, що серед усіх видів шахрайського заволодіння чужими коштами у мережі Інтернет найбільш визначними та недостатньо дослідженими є фішинг, вішинг та фармінг, і кваліфікують їх як хакерські дії [2, с. 85]. Слід зазначити, що проблема кібершахрайства розглядалась дослідниками на момент публікації їх робіт, і характеристика цього виду правопорушення щодня втрачає свою актуальність з огляду на стрімкий розвиток ІТ-технологій, і, як наслідок, удосконалюються способи, техніка, обізнаність шахраїв. У статті ми виконаємо криміналістичний аналіз сучасних видів шахрайства у мережі Інтернет із наведенням статистичних даних різних країн стосовно цієї категорії правопорушень.

Постановка завдання. Метою статті є проведення докладного криміналістичного аналізу окремих сучасних видів шахрайства та визначення проблемних питань.

Результати дослідження. Одним із найпотужніших поштовхів до розвитку шахрайств у мережі Інтернет за останні два роки стала всесвітня пандемія COVID-19. Відсутність роботи у період карантину, перехід на онлайн-торгівлю, намагання людей уникати фізичних контактів спровокували реальний ринок товарів та послуг дуже швидко зануритись у мережеві торгові

відносини. Фактично люди були змушені погодитись із сучасними правилами життя і, не маючи достатнього досвіду користування Інтернетом, будучи недостатньо обізнаними у питаннях приватності та інформаційної безпеки у всесвітній мережі, дуже легко перетворились на жертв кібершахраїв.

Згідно з нещодавно опублікованими даними, Федеральна торгова комісія США отримала понад 2,1 мільйонів повідомлень про шахрайство у 2020 році, причому шахрайство із самозванцями залишається найпоширенішим видом шахрайства, про яке повідомляється агентству.

Інтернет-магазини були другою за поширеністю категорією шахрайства, про яку повідомляли споживачі, що було посилено сплеском повідомлень у перші дні пандемії COVID-19. Лотереї, конкурси, інтернет-послуги, призи, телефонні та мобільні послуги виділили п'ять найпоширеніших категорій шахрайства.

Споживачі повідомляли про втрату понад 3,3 мільярдів доларів США від інтернет-шахрайства у 2020 році порівняно з 1,8 мільярдами доларів США у попередньому році. Майже 1,2 мільярда доларів США збитків, про які повідомлялося у 2019 році, були пов'язані з шахрайством із самозванцями, тоді як інтернет-магазини склали близько 246 мільйонів доларів США у звітних збитках. Трохи більше третини споживачів, які подали до FTC звіт про шахрайство, а саме 34%, повідомили про втрату грошей проти 23% у 2019 році.

30 листопада 2020 року громадянина Індії засудили до 20 років ув'язнення та 3 років звільнення під наглядом за свою причетність до шахрайства, що спричинило збитки потерпілим громадянам США на мільйони доларів. Він був відповідальним за функціонування та фінансування кол-центру в Індії між 2013 і 2016 роками. Районний суд південного округу Техасу також зобов'язав Хітеш Хінгладж (громадянина Індії) виплатити компенсацію в розмірі 8 970 396 доларів США [4].

У всесвітній практиці розрізняють такі основні види шахрайства із застосуванням ЕОМ та всесвітньої мережі Інтернет, як сніфферінг, вішинг, фішинг і кардинг.

Першим розглянемо такий вид електронного шахрайства, як сніфферінг. Сніффер – це так званий аналізатор даних, що проходять крізь мережі, походить від англ. "to sniff" («нюхати») – програмне забезпечення для реверсингу пакетних даних з подальшим їх декодуванням і аналізом. Сніфферінг (перехоплення даних) найчастіше зустрічається та застосовується в місцях великого скупчення людей (у ресторанах, на вокзалах, ТЦ, парках, навчальних закладах). Скрізь, де є загальнодоступна мережа Wi-Fi, нічого не підозрюючий користувач Інтернету може стати жертвою зловмисника. На вигляд шахрай може бути звичайним відвідувачем кафе, увага якого прикута до екрану особистого ноутбука [5, с. 86]. Одночасно на апаратних засобах правопорушника працює додаток-сніффер, активована точка доступу Wi-Fi з ім'ям, схожим чи ідентичним до назви точки доступу закладу або місця. Коли звичайний користувач підключається до однієї з наявних загальнодоступних мереж, він може стати потенційною жертвою зловмисника. Весь транзитний трафік перехоплюється сніффером, і піддається аналізу щодо імен і паролів користувача платіжних систем, номерів кредитних карт, паролів підтвердження оплати тощо. Фактично перехоплюється весь трафік, але за умови, що жертва підключилась саме до псевдомережі шахрая.

Довгий час JS-сніффери залишалися поза полем зору антивірусних аналітиків, а банки і платіжні системи не бачили в них серйозної загрози. Експерти "Group-IB" проаналізували 2 440 заражених онлайн-магазинів, відвідувачі яких, сумарно близько 1,5 мільйонів осіб на день, піддавалися ризику компрометації. Серед постраждалих були не тільки користувачі, але й онлайн-магазини, платіжні системи та банки, що випустили скомпрометовані карти.

Звіт "Group-IB" став першим дослідженням даркнет-ринку сніфферів, їх інфраструктури і способів монетизації, що приносить їхнім творцям мільйони доларів. "Group-IB" виявили 38 сімейств сніфферів, з яких лише 12 раніше були відомими слідчим [6].

Наступним розглянемо фішинг – кібератаку, яка використовує замаскований електронний лист як приманку. Мета фішингу полягає в тому, щоб ввести в оману одержувача електронної пошти, щоби жертва повірила, що повідомлення є достовірним, на кшталт запиту від банківської установи або повідомлення від близької людини, і виконала перехід через посилання або завантажила вкладення до електронного листа [7]. Що насправді відрізняє фішинг, так це форма повідомлення: зловмисники маскуються під так звану довірену особу, часто справжню або схожу на реальну людину або компанію, з якою жертва може вести бізнес. Це один із найдавніших типів кібератак, який від 1990-х років і досі залишається одним із найпоширеніших та згубних, завдяки чому фішингові повідомлення та техніки стають все більш досконалими.

За інформацією Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України, серед усіх інцидентів у сфері кібербезпеки було зафіксовано

більш ніж 400 тисяч випадків фішингових атак станом на 29 січня 2021 року [8]. У звіті зазначено, що працівниками Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України було виявлено розсилку фішингових електронних листів, значна частина яких була спрямована державним установам, адресатом яких ніби була Адміністрація Держспецзв'язку України. Так, шахраї використали схожу назву домену електронної поштової скриньки з Адміністрацією Держспецзв'язку України, надіслали спеціальний файл із вірусною комп'ютерною програмою, яка їм відкривала доступ до віддаленого керуванням державними ЕОМ. Після ураження зловмисники могли змінювати інформацію в базах даних, копіювати і використовувати цю інформацію всупереч законам, а також підмінювати дані на державних серверах. Після викриття цього інциденту було оповіщено всі підрозділи і відділи, уражені фішинговою атакою. Після оповіщення НКЦК вдалося попередити більшість негативних наслідків, але також було встановлено факти отримання доступу до державної таємниці.

Між 2013 і 2015 роками "Facebook" та "Google" втратили близько 100 мільйонів доларів через розширену фішингову кампанію. Шахраї скористалися тим, що обидві компанії використовували як постачальника тайванську компанію "Quanta". Зловмисники надіслали серію підроблених рахунків-фактур компанії, яка видавала себе за компанію "Quanta", які оплачували як "Facebook", так і "Google". Зрештою, шахрайство було виявлено, і "Facebook" та "Google" вжили заходів через правову систему США. Зловмисник був заарештований і екстрадований з Литви, в результаті судового розгляду "Facebook" та "Google" змогли повернути 49,7 млн. доларів зі 100 млн. доларів, вкрадених у них.

"Crelan Bank" у Бельгії став жертвою шахрайства з комерційною електронною поштою (BEC), яке обійшлося компанії приблизно у 75,8 мільйонів доларів. Цей тип атаки передбачав, що шахрай компрометував обліковий запис керівника високого рівня в компанії та доручав своїм співробітникам перераховувати гроші на рахунок, який контролювався зловмисником. Фішингова атака "Crelan Bank" була виявлена під час внутрішнього аудиту, і організація змогла покрити збитки, оскільки у неї були достатні внутрішні резерви.

Австрійський виробник аерокосмічних деталей "FACC" також втратив значну суму грошей через аферу BEC. У 2016 році організація оголосила про напад і виявила, що зловмисник, який видає себе за генерального директора компанії, доручив співробітнику бухгалтерії надіслати 61 мільйон доларів на банківський рахунок, що контролюється зловмисниками. Цей випадок був незвичайним, оскільки організація вирішила звільнити і вжити судових заходів проти свого генерального директора та фінансового директора. Компанія вимагала від двох керівників відшкодування збитків у розмірі 11 мільйонів доларів через їх неналежне впровадження контролю безпеки та внутрішнього нагляду, що могло запобігти нападу. Цей позов продемонстрував особистий ризик для керівників організації у разі невиконання належної перевірки щодо кібербезпеки.

У 2015 році "Ubiquiti Networks", компанія з комп'ютерних мереж, що базується в США, стала жертвою фішингової атаки, яка коштувала компанії 46,7 мільйонів доларів. Зловмисник видавав себе за виконавчого директора компанії та адвоката й доручив головному бухгалтеру компанії здійснити серію переказів, щоб закрити таємне придбання. Протягом 17 днів компанія здійснила 14 банківських переказів на рахунки в Росії, Угорщині, Китаї та Польщі. Інцидент привернув увагу "Ubiquiti Networks" лише тоді, коли ФБР повідомило, що банківський рахунок компанії в Гонконзі, можливо, став жертвою шахрайства. Це дало змогу компанії припинити будь-які майбутні перекази та спробувати стягнути якомога більшу частину вкрадених 46,7 мільйонів доларів (що складало приблизно 10% готівкової позиції компанії).

Вішинг – це інша атака, яка підпадає під загальне визначення фішингу та має однакові цілі. Відвідувачі використовують шахрайські номери телефонів, програмне забезпечення для зміни голосу, текстові повідомлення та соціальну інженерію, щоб обманути користувачів і виманити конфіденційну інформацію, тобто вішинг виділяється саме тим, що зазвичай використовується зміна голосу, щоб обдурити користувачів. Вішер може спочатку надіслати текстове повідомлення потенційним жертвам у великій кількості з великого списку номерів телефонів. У повідомленні може бути запропоновано користувачам зателефонувати на номер зловмисника. Інший метод вішингу створює автоматичне повідомлення та озвучує його через автовідповідач [9, с. 38]. Він використовує голосові повідомлення, створені комп'ютером, для усунення акцентів та збільшення довіри жертви. Потім голосове повідомлення змушує користувача підключитися до агента-людини, який продовжує шахрайство, або він може попросити користувачів відкрити вебсайт, що контролюється зловмисником. Незважаючи на незначні відмінності між вішингом та фішингом, кінцева мета завжди одна: облікові дані, дані, що ідентифікують особу, та фінансова інформація.

Користувачі, знайомі з фішингом, можуть бути не знайомими з вішингуванням, тому зловмисники збільшують свої шанси на успіх.

З 2011 по 2014 роки троє румунів скомпрометували комп'ютери, розташовані в США, і встановили на них інтерактивне голосове повідомлення та програмне забезпечення для масової розсилки електронною поштою. Заражені комп'ютери відправляли тисячі телефонних дзвінків та SMS-повідомлень, які змусили одержувачів розкрити особисту інформацію, включаючи номери рахунків, PIN-коди та номери соціального страхування. Чоловіки зберігали вкрадену особову інформацію на скомпрометованих комп'ютерах. Двоє підозрюваних отримали доступ до вкрадених даних, які потім продали або використали інформацію за допомогою третього учасника. На момент їх арештів у першого затриманого було 3 278 номерів фінансових рахунків, у другого – 36 050 номерів, а у третього – 3 465 номерів. Усі дані були отримані шахрайським шляхом за допомогою схем вішингу та смішингу. Виходячи з цих цифр, прокуратура оцінила збиток у понад 21 мільйон доларів США.

Терміном «кардінг» ("carding") називають шахрайські операції з платіжними картами (реквізитами карт), не схвалені власником картки. Кардінг включає такі різні способи обману законних власників матеріальних засобів [10, с. 100].

1) Викрадення або незаконне отримання карти – це або фізичний вплив на власника, або пошук уразливості в процесі видачі, доставки або оформлення банківського продукту і використання карти зловмисником

2) Компрометація даних карти для подальшого виготовлення підробки. Перш за все йдеться про копіювання даних магнітної смуги карти і крадіжки PIN-коду. Найбільш сильно цей вид шахрайства був поширений до масового переведення карт на чіпові технології. Сьогодні така схема зустрічається рідко, оскільки майже по всьому світі діє "Chip Liability Shift", тобто обов'язок банку-еквайєра обслуговувати карту з чіпом виключно за чіпом.

3) Компрометація реквізитів картки для здійснення операцій CNP (без присутності карти). Яскравим прикладом є оплата покупок або послуг в Інтернеті. Кінцева мета злочинців у всіх випадках полягає в отриманні доступу до грошей. Для реалізації своїх задумів шахраї винаходять надто хитрі схеми, нерідко користуючись довірливістю та неуважністю громадян.

Інша група авторів наголошує на тому, що велике значення мають визначення криміналістичних особливостей початкового етапу розслідування шахрайства з фінансовими ресурсами у кіберпросторі, його значення, аналіз та обґрунтування як одного з видів кіберзлочинності, що є небезпечним для кожного, і доведення необхідності вжиття невідкладних заходів щодо попередження та протидії такому кримінальному правопорушенню [11, с. 141].

Висновки. Отже, кількість та варіації способів інтернет-шахрайства зростають буквально щосекунди. Правопорушники використовують найновіші технології та обладнання, дуже швидко пристосовуючи їх до своїх злочинних цілей, адаптуються до зростання прогресу, розробляючи нові шахрайські схеми. Серед усіх видів інтернет-шахрайств можна виділити такі основні та найбільш поширені, як фішинг, сніфферінг, вішинг, кардінг. Користувачам мережі Інтернет, холдерам банківських карт, а також будь-яким пересічним громадянам необхідно бути ознайомленими із сучасними способами інтернет-шахрайства. Зокрема, слід бути дуже обачними, використовуючи онлайн-банкінг, мобільний зв'язок, здійснюючи покупки в інтернет-магазинах, бути уважними під час розголошення власних персональних даних в ході введення інформації у форми на різних сайтах.

Список використаних джерел:

1. Кримінальний процесуальний кодекс України від 13 квітня 2012 року № 4651-VI. Офіційний сайт ВР України. URL: http://zakon4.rada.gov.ua/laws/show/4651-17.

2. Клочко А.М., Єременко А.О. Шахрайство з використанням банківських платіжних карток. *Юридичний науковий електронний журнал.* 2016. № 1. URL: http://www.lsej.org.ua/1_2016/24.pdf.

3. New Data Shows FTC Received 2.2 Million Fraud Reports from Consumers in 2020. *The Federal Trade Commission*. 2021. URL: https://www.ftc.gov/news-events/press-releases/2021/02/new-data-shows-ftc-received-2-2-million-fraud-reports-consumers.

4. Owner and Operator of India-Based Call Centers Sentenced to Prison for Scamming U.S. Victims out of Millions of Dollars. An official website of the United States government. 2020. URL: https://www.justice.gov/opa/pr/owner-and-operator-india-based-call-centers-sentenced-prison-scamming-us-victims-out-millions.

5. Сазонов М.М. Виды мошенничеств с банковскими картами и совершенствование мер виктимологического предупреждения. *Виктимология.* 2018. № 2 (16). С. 55–60.

6. Crime without punishment: Group-IB issues a new report on JS-sniffers that infected 2 440 websites around the world. Group-IB. 2019. URL: https://www.group-ib.com/media/js-sniffers-report.

7. Методичні рекомендації щодо управління операційним ризиком (у тому числі кіберризиком та безперервністю діяльності) та забезпечення зберігання інформації про клієнтів об'єктами платіжної інфраструктури. URL https://bank.gov.ua/ua/news/all/metodichni-rekomendatsiyi-schodo-upravlinnya-operatsiynim-rizikom-u-tomu-chisli-kiberrizikom-ta-bezperervnistyu-diyalnosti-ta-zabezpechennya-zberigannya-informatsiyi-pro-kliyentiv-obyektami-platijnoyi-infrastrukturi.

8. НКЦК: у 2021 році в Україні зафіксовано вже майже 14 мільйонів інцидентів у сфері кібербезпеки / Рада національної безпеки і оборони України. 2021. URL: https://www.rnbo.gov.ua/ua/Diialnist/4797.html.

9. Табак И.С. Мошенничество с банковскими картами. *Современные инновации.* 2018. № 4 (26). № 1 (19). С. 37–40.

10. Октябрева М.С. Кардинг в российской практике. *Экономика и управление: анализ тенденций и перспектив развития.* 2014. № 15. С. 99–103.

11. Reznik O., Fomenko A., Melnychenko A., Pavlova N., Prozorov A. Features of the initial stage of investigating fraud with financial resources in cyberspace. *Amazonia Investiga*. 2021. Vol. 10 (Issue 41). May. P. 141–150.

УДК 343.102
DOI https://doi.org/10.32844/2618-1258.2021.5.1.22

ЛОЗОВА О.С.

ЩОДО ПИТАННЯ СТВОРЕННЯ СПІЛЬНИХ СЛІДЧИХ ГРУП У РАМКАХ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА ПІД ЧАС КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ

ON THE ESTABLISHMENT OF JOINT INVESTIGATION TEAMS WITHIN THE INTERNATIONAL COOPERATION IN CRIMINAL PROCEEDINGS

У статті детально досліджено питання, пов'язані з визначенням сутності однієї з форм проведення спільних розслідувань, а саме такої, як спільні слідчі групи, що використовується державами задля забезпечення ефективного здійснення досудового розслідування та судового розгляду для притягнення винних осіб до кримінальної відповідальності у зв'язку з вчиненням кримінальних правопорушень, які мають транснаціональний характер, що свідчить про актуальність дослідження.

На підставі вивчення міжнародно-правових договорів, національного законодавства і довідкової літератури, прийнятої міжнародними та міжурядовими організаціями ЄС, визначено загальні форми проведення спільних розслідувань; з'ясовано їх правову природу та механізм застосування в порядку здійснення міжнародного співробітництва під час кримінального провадження; окреслено правові основи проведення спільних розслідувань та створення спільних слідчих груп у рамках міжнародного співтовариства; розглянуто моделі спільних слідчих груп, які використовує міжнародна спільнота для боротьби з транснаціональною злочинністю, а також переваги використання такого інструменту, як спільна слідча група, порівняно з традиційною формою міжнародного співробітництва під час кримінального провадження, такою як міжнародна правова допомога під час проведення процесуальних дій.

У науковій роботі сформульовано поняття та ознаки спільних слідчих груп, а також запропоновано положення щодо внесення змін до чинного Кримінального

© ЛОЗОВА О.С. – аспірантка кафедри кримінальної юстиції (Національний юридичний університет імені Ярослава Мудрого)