УДК 343.132;343.98
DOI https://doi.org/10.32841/2307-1745.2021.52.19

Майстренко М. М.,
кандидат юридичних наук,
старший викладач кафедри кримінального процесу та криміналістики
Львівського державного університету внутрішніх справ

Татарин І. І.,
кандидат юридичних наук,
старший викладач кафедри кримінального процесу та криміналістики
Львівського державного університету внутрішніх справ

ПРОБЛЕМНІ АСПЕКТИ ДОКАЗУВАННЯ ШАХРАЙСТВ, ВЧИНЕНИХ У КІБЕРПРОСТОРІ

Анотація. Стаття присвячена проблемам розкриття шахрайств, що вчиняються у віртуальному просторі (кіберпросторі). Охарактеризовані окремі аспекти процесу доказування, що пов'язаний із застосуванням спеціальних знань (незабезпеченість програмними та апаратними комплексами експертів цього напряму дослідження), малорозвиненими навичками аналізу даних під час виявлення слідів, які утворюються внаслідок зовнішнього або внутрішнього неправомірного впливу на телекомунікаційну систему чи певний електронний пристрій, програму чи на комп'ютерну інформацію, що виражається в будь-якій зміни комп'ютерної інформації. Констатовано типові помилки під час вилучення та упакування смартфону.

Розглядаються проблеми проведення судової телекомунікаційної експертизи, а саме: відсутність упорядкованої сукупності зведень виключно для такого роду експертиз, використання несертифікованих технічних засобів і програмного забезпечення, а також чітко розробленої та нормативно закріпленої методологічної основи проведення таких експертиз.

Вкотре наголошується та доводиться неефективність у чинній редакції такого заходу забезпечення кримінального провадження, як тимчасовий доступ до речей та документів, зокрема положення щодо присутності представника того чи іншого органу, у володінні котрого знаходяться речі чи документи, до яких необхідно отримати доступ, відсутність у КПК України норми, що встановлювала б термін, протягом якого слідчий суддя зобов'язаний розглянути таке клопотання, що має особливе значення у розкритті злочинів вчинених із використанням інформаційних технологій. Підтримується пропозиція щодо внесення змін у ст. 166 КПК України: «У разі невиконання ухвали про тимчасовий доступ до речей і документів прокурор, слідчий, дізнавач із метою відшукання та вилучення зазначених в ухвалі речей і документів вправі невідкладно провести обшук. У такому разі прокурор, слідчий, дізнавач за погодженням із прокурором зобов'язаний невідкладно після здійснення таких дій звернутися до слідчого судді з клопотанням про проведення обшуку».

Відповідно, виникають складнощі зі встановленням тих користувачів, які безпосередньо вчиняють шахрайські дії. Проте цю ситуацію можна полегшити, якщо ввести на державному рівні обмеження щодо реалізації SIM-карт лише за наявності паспорта громадянина України або іншого документа, що посвідчує особу, для іноземців чи осіб без громадянства. Як свідчить практика, на підготовчій стадії кримінального правопорушення зловмисники часто купляють нові SIM-карти, а після його вчинення позбавляються таких карт. Вбачається, що таке обмеження значно ускладнить вчинення кримінальних правопорушень та слугуватиме стримувальним фактором.

З огляду на встановлену недосконаліть кримінальної процесуальної процедури, а також брак спеціальних знань, науково-обґрунтованих методик та економічного забезпечення експертних установ визнається ефективною позиція активної протидії цьому виду кримінальних правопорушень у напрямі превенції.

Ключові слова: шахрайство, кіберпростір, докази, судова експертиза, телекомунікаційна експертиза, тимчасовий доступ до речей та документів, превенція.

Постановка питання. XXI ст. характеризується тотальною цифровізацією, особливо гостро тенденція проявилася після оголошення світового локдауну, пов'язаного з поширенням вірусу COVID-19, під час якого актуалізувалася не тільки сфера Інтернет-комерції, а й інших сфер людської життєдіяльності. Сучасне суспільство переживає інформаційний бум через значне збільшення кількості джерел інформації, зокрема в онлайн-режимі. Глобальна діджиталізація світової економіки зумовлює появу нових видів кримінальних правопорушень, зокрема, таких, що вчиняються в кіберпросторі.

За даними Департаменту кіберполіції України, повідомлення про шахрайські дії в Інтернеті становлять 80% від усіх звернень громадян, що дорівнює 32 000 звернень громадян. Найчастіше злодії ошукують громадян, продаючи неіснуючі товари на майданчиках оголошень або в соцмережах. Зростання числа користувачів мережею Інтернет корелює з одночасним зростанням кількості постраждалих від шахрайських дій правопорушників.

Свої наукові доробки як загалом, так і окремо проблемі розслідування шахрайств, які вчиняються в кіберпросторі, присвятили Н.М. Ахтирська, А.Ф. Волобуєва, І.В. Діордіца, Н.Ю. Кириленко, А.А. Комаров, Л.І. Криушенко, А.В. Кушик, А.В. Микитчик, М.П. Лоцько, Т.В. Рудий, В.В. Сеник, Т.Л. Сироїд, В.Є. Ткаліч, К.В. Тутуніна, Д.М. Цехан, В.І. Шакун, С.В. Шандра, С.В. Шапочка, А.М. Юрчук, Н.П. Яблоков та інші.

Слід наголосити, що однією з головних проблем досліджуваного виду шахрайств є низький рівень їх розкриття через брак спеціальних знань у зв'язку з тим, що бурхливий розвиток інформаційних технологій методики судово-експерт-

ного дослідження цих об'єктів вимагає постійного оновлення та доопрацювання. Кожного року змінюються операційні системи, формати даних, протоколи і середовище перенесення даних, технічні засоби, що забезпечують процеси передання та обробки інформації.

Метою статті є дослідження актуальних проблем доказування шахрайств, що вчиняються у віртуальному просторі.

Виклад основного матеріалу дослідження. На початковому етапі розслідування шахрайств дії сторони обвинувачення визначаються залежно від характеру наявних даних. Багатоетапний процес доказування передбачає обов'язковість доведення таких обставин, як подія шахрайства (час, місце, спосіб вчинення злочину та ін.), винуватість конкретної особи у шахрайстві і мотиви вчинення діяння, обставини, що впливають на ступінь і характер відповідальності обвинуваченого, характер і розміри шкоди, заподіяної шахрайством, обставини, що сприяли вчиненню шахрайства.

Відповідно до ст.ст. 214, 237 Кримінального процесуального кодексу України (далі – КПК України) [1] слідчий, дізнавач проводить огляд місця події з метою виявлення слідів кримінального правопорушення та речових доказів, з'ясування обстановки кримінального правопорушення, а також інших обставин, які мають значення в конкретному кримінальному провадженні. Огляд місця події є первинною і невідкладною слідчою дією.

Огляд місця події в процесі розслідування шахрайств, вчинених у віртуальному просторі, має свою специфіку. «Кіберпростір» ми визначаємо як віртуальний штучно створений простір, в якому моделюється, зберігається, переміщається інформація закодована, як правило, з використанням двійкового коду, яка може становити найрізноманітніші відомості про об'єктивний світ. Така інформація зберігається в пам'яті будь-якого фізичного або віртуального пристрою, а також іншого носія, спеціально призначеного для їх зберігання, обробки й передачі, таких як жорсткі диски, кластери логічних дисків, сервери – data center, онлайн-сховища – cloud storage, внутрішні енергозалежні флеш-пам'яті, зовнішні карти пам'яті тощо.

Утворена індивідуальна слідова картина зумовлює труднощі у виявленні та дослідженні, а також використанні в доказуванні. У таких випадках фактично завжди доводиться застосовувати спеціальні заходи для фіксування «недовговічної інформації», наприклад щодо поточних мережевих IP-з'єднань. Це своєю чергою вимагає застосування спеціальних знань з урахуванням вірогідності швидкого знищення злочинцем електронних слідів, тому своєчасність виявлення слідів злочину має виключне значення.

Зазвичай сліди злочинів, що вчинені в кіберпросторі, утворюються в результаті зовнішнього або внутрішнього неправомірного впливу на телекомунікаційну систему, окремий електронний пристрій, програму чи на комп'ютерну інформацію і являють собою будь-які зміни комп'ютерної інформації [2, с. 62].

Відповідно, основоположним моментом під час розслідування шахрайств, вчинених із використанням інформаційних технологій, є фіксація виявлених слідів. Для побудови належної і цілісної системи доказів, тобто перетворення невидимої інформації та слідів кіберзлочинів на докази є проведення судової експертизи, наприклад, комп'ютерно-технічної, предметом якої є закономірності формування і дослідження комп'ютерних систем і рух цифрової інформації, дослідження фактів і обставин, пов'язаних із проявом цих закономірностей.

Своєю чергою вдосконалення комп'ютерної техніки (системні блоки комп'ютера, ноутбуки, сервери тощо), цифрових електронних носіїв інформації (жорсткі диски, твердотілі накопичувачі даних, карти пам'яті, планшетні комп'ютери, мобільні телефони, розумні годинники), а саме збільшення об'єму дослідження даних, використання захисту, вимагають від експертів використання аналітичного підходу, поглиблених знань, а також новітніх експертних програмних продуктів, апаратних пристроїв задля досягнення максимального результату дослідження [3].

В. Коршенко зазначає, що для вирішення усіх питань, що пов'язані з комп'ютерно-технічними засобами, телекомунікаційними системами, електронними пристроями, програмами тощо, до 2006 року в Україні призначали судову комп'ютерно-технічну експертизу. Однак через те, що перелік питань, які стояли перед експертом, постійно розширювався, настав час для виділення в окремий рід інженерно-технічних експертиз судову телекомунікаційну експертизу [4, с. 198].

Проте нині в Україні непроста ситуація саме із застосуванням спеціальних знань як під час виявлення вищезазначених слідів, так і під час проведення експертних досліджень.

Малорозвинені навички аналізу даних, незабезпеченість програмними та апаратними комплексами експертів цього напряму дослідження, а також неналежне упакування об'єктів дослідження оперативними та слідчими підрозділами під час огляду місця події можуть суттєво вплинути на результат не тільки дослідження, а розслідування протиправного діяння загалом [3].

Мобільні телефони (смартфони, фаблети) стали невід'ємним аксесуаром сучасного життя, як вже було зазначено, кібершахрайства часто вчиняють з їх використанням, а отже, виникає необхідність дослідити інформацію, яку вони містять. Докази, пов'язані з кіберзлочинами, тобто цифрові докази, вилучені із віртуального простору, вразливі, їх пошкодження чи втрата може статися через помилки під час їх вилучення, дослідження. До найбільш типових помилок у процесі вилучення та упакування телефону належать:

1) невмикання «режиму польоту» або незабезпечення його захисту від зовнішнього впливу через мережу мобільного оператора та мережі бездротового зв'язку;

2) вимикання телефону без його попереднього огляду;

3) витягнення SIM-карти безпосередньо на ввімкненому телефоні, що призводить до його автоматичного перезавантаження та втрати можливості розблокування відбитком пальця або системою розпізнавання обличчя;

4) втрата можливості дослідження телефону після його розблокування відбитком пальця або системою розпізнавання обличчя [5, с. 103].

Очевидно, що перспектива розслідування шахрайств, вчинених із використанням мобільних телефонів, в основному залежить від вміння уповноваженої особи правильно вилучити термінал.

Правильність вилучення телефону, на думку експертів, є такою: в разі можливості розблокування особою телефону відбитком пальця або системою розпізнавання обличчя розблокований телефон переводиться у «РЕЖИМ ПОЛЬОТУ»,

після чого у його налаштуваннях дисплею та меню налаштувань безпеки встановлюють параметри: «ВИМИКАННЯ ЕКРАНУ» – «НІКОЛИ», «БЛОКУВАННЯ ЕКРАНУ / РЕЖИМ ОЧІКУВАННЯ» – «НІКОЛИ», яскравість екрану виставляється на мінімум із метою збільшення строку збереження заряду батареї, телефон під'єднують до зовнішнього носія живлення (power bank) та упаковують у пакет, що блокує радіохвилі [5, с. 103].

Однак такий порядок вилучення телефону викликає низку запитань процесуального характеру, наприклад, щодо зовнішнього носія живлення, якщо такий носій надається уповноваженою особою, яка здійснює вилучення. Як описати вміст пакета, в якому вкладено носій живлення, що не стосується події кримінального правопорушення?

Крім того, під час дослідження об'єктів телекомунікаційних експертиз необхідно оперувати великим обсягом різноманітної довідкової інформації з різних галузей комп'ютерних знань. Проте нині не існує упорядкованої сукупності зведень виключно для такого роду експертиз, а самі експерти черпають знання з інструкцій, довідкової літератури та інформації, що розміщена на численних сайтах мережі Інтернет, що ставить під питання її надійність та достовірність. Також наголошується на такій істотній проблемі, як використання несертифікованих технічних засобів і програмного забезпечення, механізм дії яких найчастіше до кінця не вивчений і походження яких невідоме [4, с. 198].

У методології проведення телекомунікаційної експертизи пропонують використовувати методи, що характерні для інших видів експертиз та апробовані часом. Серед таких – метод візуального дослідження, спостереження, органолептичні методи, вимірювання, порівняння, тестування тощо [6].

Поширенню кібершахрайств сприяє той факт, що часто неможливо встановити осіб, які вчиняють такого роду злочини. Також поширена практика не вносити відомості про шахрайство, що вчинене у віртуальному просторі, зокрема, яке виразилося в обмані покупців під час здійснення купівлі товару чи послуги, до Єдиного реєстру досудових розслідувань або закривати таке кримінальне провадження за відсутністю складу злочину, мотивуючи свою відмову переведенням вирішення конфлікту з кримінальної у цивільно-правову площину.

Крім того, часто виникає ситуація, за якої стає неможливим встановлення причинно-наслідкового зв'язку між використанням спецобладнання для отримання інформації про платіжні інструменти та подальшим підробленням самих платіжних інструментів із метою незаконного отримання матеріальних благ. Аналіз помилок, що допускаються під час розслідування, свідчить про певну однобічність і неповноту досудового розслідування, що призводило до невстановлення осіб, причетних до кримінального правопорушення, або неможливості участі у вчиненому [7, с. 43].

Досить неефективним (93% опитаних практичних працівників вважають норму ст. 166 КПК України неефективною) у чинній редакції, однак доволі поширеним заходом забезпечення кримінального провадження є тимчасовий доступ до речей і документів. Поширений цей захід, зокрема, тому, що фактично усі відомості, які можуть становити інтерес слідчого, дізнавача чи прокурора, законодавець уналежнює до охоронюваної законом таємниці і встановив правила розгляду такого клопотання, найбільш недієве з яких – присутність представника того чи іншого органу, у володінні якого знаходяться речі чи документи, до чого необхідно отримати доступ. Наприклад, представника банківської установи, оператора чи провайдера телекомунікаційних послуг. Крім того, у КПК України прямо не вказаний термін, протягом якого слідчий суддя зобов'язаний розглянути таке клопотання, а з огляду на специфіку досліджуваного виду шахрайств фактор часу є пріоритетною позицією.

Здобуття інформації, яка становить банківську таємницю, штучно ускладнюється самими банківськими установами. У ст. 62 Закону України «Про банки та банківську діяльність» [8] зазначено порядок розкриття банківської таємниці із вказівкою на те, що інформація щодо юридичних та фізичних осіб, яка містить банківську таємницю, розкривається банками не тільки за рішенням суду, а й на письмову вимогу органів, що уповноважені на здійснення досудового розслідування стосовно операцій за рахунками конкретної юридичної особи або фізичної особи – суб'єкта підприємницької діяльності за конкретний проміжок часу. Утім, як свідчать опитування слідчих Національної поліції, поширена практика, за якої банківські установи переважно відмовляють у наданні такої інформації за запитом, вимагаючи рішення суду. Тим самим, знову ж таки нівелюється часовий фактор, що негативно впливає на процес розслідування.

Крім того встановлено, що в разі невиконання ухвали про тимчасовий доступ до речей і документів слідчий суддя, суд за клопотанням сторони кримінального провадження, якій надано право на доступ до речей і документів на підставі ухвали, має право постановити ухвалу про дозвіл на проведення обшуку згідно з положеннями КПК України з метою відшукання та вилучення зазначених речей і документів [1].

Завищено формалізований стандарт доказування, закладений у вказану норму, видається абсурдним з позицій не тільки швидкості досудового розслідування, а і його ефективності, адже за таких обставин не тільки затягується час, а й створюються передумови, за яких фізичні чи юридичні особи, що володіють речами чи документами (інформацією), можуть їх позбутися, спотворити, тим самим перешкодити встановленню істини в кримінальному провадженні.

Від початку реформаційного процесу в Україні і теоретики, і практики відмічають надмірну гуманізацію законодавства. За нинішніх обставин акцентується на захисті прав і свобод правопорушника замість того, щоб поновлювати в правах жертву кримінального правопорушення, основним запитом якої є відшкодування та компенсація шкоди, завданої кримінальним правопорушенням.

Згідно з теорією відновного правосуддя основним питанням має бути не «як слід вчинити з правопорушником?» чи «на що правопорушник заслуговує?», а «що треба зробити для відновлення справедливості?». Відповідно, правосуддя не має бути відплатою, не має приносити додаткову шкоду, а навпаки, діяти на відновлення, створення умов, в який цей процес міг би початися, а отже, першочерговою метою правосуддя має бути відшкодування шкоди та зцілення потерпілих [9].

З цією метою необхідно змінювати законодавство таким чином, щоб створити умови для проведення ефективного досудового розслідування, забезпечити принцип наступальності та дієвості. А тому підтримується думка та пропонується спростити порядок реалізації тимчасового доступу як до інформа-

ції, що містить банківську таємницю, а також до інформації операторів та провайдерів телекомунікацій на підставі ухвали слідчого судді в частині невідкладного надання відомостей у режимі реального часу.

Тим самим треба внести зміни у ст. 166 КПК України, виклавши її в такій редакції: «У разі невиконання ухвали про тимчасовий доступ до речей і документів прокурор, слідчий, дізнавач із метою відшукання та вилучення зазначених в ухвалі речей і документів вправі невідкладно провести обшук. У такому разі прокурор, слідчий, дізнавач за погодженням із прокурором зобов'язаний невідкладно після здійснення таких дій звернутися до слідчого судді із клопотанням про проведення обшуку».

У процесі розслідування шахрайств, вчинених у кіберпросторі, часто виникають проблеми із визначенням конкретного користувача, який здійснив під'єднання до мережі Інтернет через динамічну IP-адресу.

Загалом IP-адреса складається з адреси мережі, підмережі та локальної гост-адреси (Host), яка є унікальна для кожного вузла. Кожен гост може мати не тільки IP-адресу, але й ім'я, які діляться на частини, що розділяються крапками. Список таких імен зберігається в спеціальній базі даних доменів служби імен DNS (Domain Name System) [10].

Отже, за IP-адресою неможливо встановити конкретний унікальний комп'ютер, з якого зайшли у віртуальний простір, проте вона показує адресу вузла, з якого своєю чергою можуть заходити різні фізичні користувачі.

Відповідно, виникають складнощі зі встановленням тих користувачів, які безпосередньо вчиняють шахрайські дії. Проте цю ситуацію можна полегшити, якщо зобов'язати провайдерів вести облік користувачів із прив'язкою до номера мобільного телефону. Часто реєстрація на певному ресурсі чи створення облікового запису передбачає зазначення номеру мобільного телефону.

Крім того, пропонується ввести на державному рівні обмеження щодо реалізації SIM-карт лише за наявності паспорта громадянина України або іншого документа, що посвідчує особу, для іноземців чи осіб без громадянства. Як свідчить практика, на підготовчій стадії кримінального правопорушення зловмисники часто купляють нові SIM-карти, а після його вчинення позбавляються таких карт. Вбачається, що таке обмеження значно ускладнить вчинення кримінальних правопорушень та слугуватиме стримувальним фактором.

Висновки. Особливістю першочергових та подальших слідчих (розшукових) дій у процесі розслідування шахрайств, вчинених у кіберпросторі, є спрямування на виявлення і фіксацію цифрових слідів, які характеризуються нестійкістю та вимагають спеціальних знань.

Особи, що уповноважені на здійснення розслідування шахрайств у кіберпросторі, перебувають у досить складному становищі через недосконаліть кримінальної процесуальної процедури, ресурсовитратність зазначених кримінальних проваджень, брак спеціальних знань, науково-обґрунтованих методик та економічного забезпечення експертних установ.

За таких умов на цьому етапі ефективною є позиція активної протидії цьому виду кримінальних правопорушень у напрямі превенції. З цією метою необхідно активно підвищувати рівень обізнаності громадян щодо того, як не стати жертвою шахраїв у мережі Інтернет.

Література:

1. Кримінальний процесуальний кодекс України в редакції від 11.09.2020 р. URL: https://zakon.rada.gov.ua/laws/show/4651-17
2. Пашнєв Д.В. Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій : дис. … канд. юрид. наук : 12.00.09. Харків, 2007. 228 с.
3. Золотарьов С.О. Судова комп'ютерно-технічна експертиза та її роль у боротьбі з кіберзлочинами. *Протидія кіберзлочинності та торгівлі людьми*. Збірник матеріалів Міжнар. наук.-практ. конференції. Харків, 27 травня 2020 р. С. 95–96.
4. Коршенко В. Судова телекомунікаційна експертиза як джерело доказів під час розслідування кіберзлочинів. *National law journal: theory and practice*. 2017. Вип. 2. С. 197–199.
5. Колесник В.Г. Проблемні питання збереження, фіксації та дослідження інформації в сучасних мобільних телефонах. *Протидія кіберзлочинності та торгівлі людьми*. Збірник матер. Міжнар. наук.-практ. конференції. Харків, 27 травня 2020 р. С. 102–105.
6. Коршенко В.А. Методи судової телекомунікаційної експертизи. *Вісник ЛДУВС ім. Е.О. Дідоренка*. 2017. Вип. 3 (79). С. 224–230.
7. Щербакова Г. Досудове розслідування злочинів, учинених із використанням платіжних інструментів. *Наукові записки Інституту законодавства Верховної Ради України*. Кримінальне права і кримінальний процес. 2017. Вип. 3. С. 41–46.
8. Про банки та банківську діяльність : Закон України № 2121-III від 7 грудня 2000 р. в редакції від 05.08.2021 р. URL: https://zakon.rada.gov.ua/laws/show/2121-14#Text
9. Зер Х. Восстановительное правосудие: новый взгляд на преступление и наказание : Пер. с англ. / Общ. ред. Л.М. Карнозовой. Коммент. Л.М. Карнозовой и С.А. Пашина. Москва : МОО Центр «Судебно-правовая реформа», 2002. 328 с.
10. Горлач В.М., Макар В.М. Побудова та адміністрування INTRANET-мереж. Ч. 1. Основи мережних технологій : Тексти лекцій. Львів, 1999. 45 с.

Maistrenko M., Tataryn I. Problem aspects of proving fraud committed in cyberspace

Summary. The article is devoted to the problems of detecting fraud committed in cyberspace. Some aspects of the proof process related to the application of special knowledge (lack of software and hardware of experts in this area of research), underdeveloped skills of data analysis in detecting traces formed as a result of external or internal improper influence on the telecommunications system, or certain electronic device, program or computer information, which is expressed in any changes in computer information. Typical errors when removing and packing a smartphone are indicated.

The problems of forensic telecommunication examination are considered, namely: the lack of an orderly set of reports exclusively for such examinations, the use of non-certified hardware and software, as well as a clearly developed and normatively established methodological basis for such examinations.

Emphasizes and proves the ineffectiveness, in the current version, of such a measure to ensure criminal proceedings as temporary access to things and documents. In particular, the provision on the presence of a representative of a body in possession of things or documents to which access must be obtained, the absence in the CPC of Ukraine of a rule that would establish the period during which the investigating judge is obliged to consider such a petition of particular importance. in the disclosure of crimes committed with the use of information technology.

The proposal to amend Art. 166 of the CPC of Ukraine: "In case of non-compliance with the decision on temporary access to things and documents, the prosecutor, investigator, coroner in order to find and seize the things and documents specified in the decision may immediately search. In this case, the prosecutor, investigator, coroner, in agreement with the prosecutor, is obliged to immediately after such actions to apply to the investigating judge with a request to conduct a search".

Given the established imperfection of the criminal procedure, as well as the lack of special knowledge, scientifically sound methods and economic support of expert institutions, is recognized as an effective position to actively combat this type of criminal offense in the direction of prevention.

Key words: fraud, cyberspace, evidence, forensic examination, telecommunication examination, temporary access to things and documents, prevention.