Věda a perspektivy № 4(35) 2024
ISSN 2695-1584 (Print)
ISSN 2695-1592 (Online)

https://doi.org/10.52058/2695-1592-2024-4(35)-135-148

Артур Волобоєв

доктор філософії в галузі права,
завідувач кафедри оперативно-розшукової діяльності та
інформаційної безпеки факультету підготовки фахівців
для підрозділів кримінальної поліції
Донецького державного університету внутрішніх справ,
м. Кропивницький, Україна,
https://orcid.org/0000-0002-7138-5847

ОЦІНКА ПЕРВИННОЇ ІНФОРМАЦІЇ ТА КОЛО ОБСТАВИН, ЩО ПІДЛЯГАЮТЬ ВСТАНОВЛЕННЮ ПІД ЧАС РОЗКРИТТЯ КІБЕРШАХРАЙСТВ

Анотація. У період стрімкого технологічного розвитку та інтегрованого цифрового середовища, безпека у віртуальному просторі стає ключовою складовою національної та міжнародної стабільності. З поширенням кіберзагроз та кібератак формується новий вимір – вимір цифрової вразливості та високотехнологічних загроз. У цьому контексті, розуміння та вирішення питань кібербезпеки стають першочерговим завданням для забезпечення національної безпеки та захисту стратегічних інтересів держави в умовах можливих агресивних дій.

Актуальність теми безпеки у віртуальному просторі в умовах воєнного стану визначається рядом ключових факторів, а кримінально протиправні діяння у цій сфері як складова кіберзлочинності. Очевидно, що на сьогодні кібершахрайство є суттєвою загрозою для цивілізованого суспільства, рівень розкриття якого залишається достатньо низьким.

У зв’язку з цим, нами висвітлені теоретико-прикладні питання оцінки первинної інформації та кола обставин, що підлягають встановленню під час розкриття кібершахрайства.

Акцентовано на ознаках та напрямах роботи слідчих і оперативних підрозділів по «гарячих слідах», джерелах інформації. Конкретизовано, що є приводом та підставою для початку досудового розслідування за фактом вчинення кібершахрайства.

Задля мінімізації ускладнень, з якими стикаються слідчі та оперативні підрозділи під час оцінки первинної інформації запропоновано унормування окремих норм чинного законодавства.

У контексті дослідження проаналізовано думки науковців та узагальнено правозастосовну практику щодо визначення кола обставин, що підлягають

встановленню. Запропоновано виокремити чотири взаємопов'язані групи для формування змісту обставин, що підлягають встановленню під час розкриття кібершахрайства.

Ключові слова: кібершахрайство, віртуальний простір, кібербезпека, первинна інформація, коло обставин, доказування.

Arthur Voloboiev

PhD in Law, Head of the Department of Operational and Investigative Activities and Information Security at the Faculty of Training Specialists for Criminal Police Units of the Donetsk State University of Internal Affairs, Kropyvnytskyi, Ukraine,
https://orcid.org/0000-0002-7138-5847

ASSESSMENT OF PRIMARY INFORMATION AND CIRCUMSTANCES TO BE DETERMINED WHEN DISCOVERING CYBER FRAUDS

Abstract. In a period of rapid technological development and an integrated digital environment, security in virtual space is becoming a key component of national and international stability. With the spread of cyber-threats and cyber-attacks, a new dimension is being formed - the dimension of digital vulnerability and high-tech threats. In this context, understanding and solving cyber security issues become a priority task for ensuring national security and protecting the state's strategic interests in the face of possible aggressive actions.

The relevance of the topic of security in virtual space in the conditions of martial law is determined by a number of key factors, and criminally illegal actions in this area as a component of cybercrime. It is obvious that today cyber fraud is a significant threat to a civilized society, the level of disclosure of which remains quite low.

In this regard, we have highlighted the theoretical and applied issues of primary information assessment and the range of circumstances to be established during the disclosure of cyber fraud.

Emphasis is placed on the signs and directions of work of investigative and operative units on "hot leads", sources of information. It is specified what is the reason and basis for starting a pre-trial investigation into the fact of committing cyber fraud.

In order to minimize the complications faced by investigators and operative units during the evaluation of primary information, it is proposed to standardize certain norms of the current legislation.

In the context of the study, the opinions of scientists were analyzed and law enforcement practice was summarized in determining the range of circumstances to be established. It is proposed to single out four interrelated groups to form the content of the circumstances to be established during the disclosure of cyber fraud.

Keywords: cyber fraud, virtual space, cyber security, primary information, circle of circumstances, evidence.

Постановка проблеми. У крок з сучасним етапом цифрової трансформації суспільства та викликів гібридної війни проти України зросла питома вага злочинної діяльності у віртуальному просторі. Суспільні відносини, що відбуваються в такому середовище, все частіше стають об'єктом для порушення прав громадян на володіння, користування і розпорядження своєю власністю, а також результатами своєї інтелектуальної та творчої діяльності. Як результат, форми правовідносин в Інтернеті залишаються не досить врегульованими, зростає кількість протиправних діянь, порушуючи основоположні приписи статті 41 Конституції України.

За статистичними даними Офісу Генерального прокурора протягом останніх п'яти років у середньому реєструється 204,7 тис. кримінальних правопорушень проти власності, де шахрайство займає друге місце після вчинення крадіжок. З них, близько 12 % становить досліджувана категорія злочину, – шахрайство, учинене шляхом незаконних операцій з використання електронно-обчислювальної техніки [1].

Оцінити реальні масштаби таких шахрайських проявів вкрай важко через високу латентність, особливості обстановки їх вчинення та тонку межу між цивільно-правовими і кримінально-правовими відносинами, що ускладнює прийняття правильного рішення про притягнення особи до відповідальності в міру своєї вини. Тим паче, в період військової агресії спостерігається тенденції до збільшення злочинних схем, що реалізовуються за допомогою електронно-обчислювальної техніки у віртуальному просторі, а рівень їх розкриття залишається достатньо низьким, що свідчить про безсистемну протидію цьому Національної поліції України.

Вказане безсумнівно ставить перед наукою завдання щодо розробки новітніх прийомів, методів і засобів розслідування кримінальних правопорушень, що вчиняються у віртуальному просторі (середовище). І на наш погляд, значної увагу заслуговує оцінка первинної інформації та коло обставин, що підлягають доказуванню.

Аналіз останніх досліджень і публікацій. Окремі питання розслідування та розкриття кримінальних правопорушень, що вчиняються в сфері інформаційних технологій та з використанням електронно-обчислювальної техніки були предметом дослідження вітчизняних та іноземних учених, як: Ю. П. Аленіна, Д. С. Азарова, Б. В. Андрєєва, І. В. Басистої, В. П. Бахіна,

В. Д. Берназа, Р. С. Бєлкіна, М. С. Вертузаєва, О. І. Возгріна, А. Ф. Волобуєва, В. І. Гагаліна, В. Г. Гончаренка, В.О. Голубєва, О. М. Джужі, Л. Я. Драпкіна, В. А. Журавля, А. В. Іщенка, О. В. Кириченка, В. О. Коновалової, В. В. Крилов, Л. М. Лобойка, В. Г. Лукашевича, Є. Д. Лук'янчикова, С. І. Мічнека, О. В. Одерія, М. А. Погорецького, М. В. Салтевського, О. В. Смаглюка, Р. Л. Степанюка, М. П. Стрельбицького, В. Є. Тарасенка, Р. В. Тарасенка, В. М. Тертишника, В. В. Тіщенка, Л. Д Удалової, І. Ф. Хараберюша, М. С. Цуцкіридзе, К. О. Чаплинського, В. В. Шедрика, В. Ю. Шепітька, М. Г. Щербаковського, О. М. Юрченка та ін.

Особливу увагу заслуговують сучасні дослідження шахрайств, учинених через мережу Інтернет, таких учених, як: С. В. Самойлова («Розслідування шахрайств, учинених із використанням мережі «Інтернет», Донецьк 2014 рік), О. В. Герасимова («Протидія злочинності у банківській сфері», Харків 2019 рік), О. А. Самойлека («Основи методики розслідування злочинів, вчинених у кіберпросторі», Одеса 2020 рік), О. В. Ковальчук («Методика розслідування шахрайств, пов'язаного з діяльністю кредитної спілки», Львів 2020 рік), Т. В. Коршикової («Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки», Київ 2021 рік), С. В. Чучкі («Розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет, Дніпро 2021 рік), І. О. Коваленка («Розслідування шахрайств у сфері використання банківських електронних платежів», Дніпро 2022 рік) та ін. Разом з тим, на сьогодні виникла потреба в конкретизації окремої складової слідчо-прокурорської практики.

У зв'язку з цим, **мета статті** полягає у висвітленні теоретико-прикладних питань оцінки первинної інформації та кола обставин, що підлягають встановленню під час розкриття кібершахрайств.

Виклад основного матеріалу. Розкриття будь-якого кримінального правопорушення розпочинається з моменту його виявлення. Процес виявлення є кримінальною процесуальною діяльністю, спрямованою на перевірку первинних фактичних відомостей про ознаки підготовки чи вчинення злочинцем такого суспільно небезпечного діяння. Тобто, полягає в отриманні первинної інформації про кримінальну подію та належній її фіксації у відповідних процесуальних документах, а сама діяльність із розкриття кримінального правопорушення реалізується через пошук та виявлення необхідної інформації, яка свідчить про вчинення такого правопорушення.

Сутність розкриття кримінального правопорушення тісно пов'язано з розшуковою діяльністю і значною мірою залежить від ефективності проведення процесуальних дій і оперативно-розшукових заходів, що здійснюється слідчим у взаємодії з уповноваженими оперативними підрозділами.

Слід зазначити, що у системі розкриття кримінального правопорушення одним із важливих напрямів є робота слідчого та оперативних підрозділів по «гарячих слідах», за результатами чого можна:

– установити просторово-часові зв'язки між окремими слідами кримінального правопорушення та обставинами події;

– ідентифікувати особу злочинця та затримати її в установленому законом порядку;

– з'ясувати причини відсутності або наявності окремих фактів, що суперечать природному перебігу аналогічних подій (негативні обставини).

Підтвердженням такої думки, є позиція О. А. Самойленка, який зазначає, що специфічність механізму вчинення кримінальних правопорушень у кіберпросторі, зокрема особливості їх слідів, які можуть бути легко фальсифіковані або взагалі знищені, обумовлює й особливості початку кримінального провадження щодо цих правопорушень. Тут йдеться про ті особливості, що вимагають їх врахування з огляду забезпечення судової перспективи таких проваджень [2, с. 409].

Як правило, ознаки кримінального правопорушення можуть бути виявлені трьома способами:

– ужиття оперативно-розшукових заходів, які передують початку досудового розслідування;

– звернення громадян, а також представниками державних організацій під час здійснення перевірки та контрольних заходів;

– безпосередньо слідчим, прокурором і судом.

Відповідно до чинного кримінального процесуального законодавства України, будь-яка процесуальна діяльність, – зокрема розслідування кримінального правопорушення, у тому числі й кібершахрайства, можлива лише в межах здійснення досудового розслідування після внесення відповідних відомостей до Єдиного реєстру досудових розслідувань (далі – ЄРДР).

Процесуальний порядок внесення відомостей до ЄРДР регламентований ч. 1 ст. 214 КПК України, відповідно до якого уповноважені суб'єкти (прокурор, слідчий, дізнавач), зобов'язані невідкладно, але не пізніше 24 годин після отримання заяви, повідомлення про вчинене кримінальне правопорушення або після самостійного виявлення ним із будь-якого джерела обставин, що можуть свідчити про вчинення кримінального правопорушення, внести відповідні відомості до ЄРДР, розпочати розслідування та через 24 години з моменту внесення таких відомостей надати заявнику витяг із зазначеного реєстру [3].

Відмова у прийнятті та реєстрації заяви чи повідомлення про кримінальне правопорушення не допускається.

Крім того, відповідно до Порядку ведення єдиного обліку в органах (підрозділах) поліції заяв і повідомлень про кримінальні правопорушення та інші події, затвердженого наказом МВС України від 08.02.2019 № 100 [4], а також Інструкції з організації реагування на заяви і повідомлення про кримінальні, адміністративні правопорушення або події та оперативного

інформування в органах (підрозділах) Національної поліції України, затвердженої наказом МВС від 27.04.2020 № 357 (далі – Інструкція № 357) [5], оперативний черговий органу (підрозділу) поліції або інша уповноважена службова особа, отримавши інформацію про вчинення кримінального правопорушення, відразу реєструє її в журналі єдиного обліку заяв і повідомлень про кримінальні правопорушення та інші події з використанням інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України». Типовий алгоритм попередніх дій та заходів групи реагування передбачений Інструкцією № 357 [5], Інструкцією з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушення, їх виявленні та розслідуванні, затвердженої наказом МВС від 07.07.2017 № 575 [6], Інструкцією про порядок залучення працівників органів досудового розслідування поліції та Експертної служби МВС України як спеціалістів для участі в проведені огляду місця події, затвердженої наказом МВС України від 03.11.2015 № 1339 [7].

Також Порядок введення єдиного обліку в органах (підрозділах) поліції заяв і повідомлень про кримінальні правопорушення та інші події, затвердженого наказом МВС України від 08.02.2019 № 100 [4], конкретизує, що саме відноситься до джерел інформації про кримінальні правопорушення й інші події, а саме ними є:

– заяви (повідомлення) осіб, які надходять до органу (підрозділу) поліції, особи, уповноваженої на здійснення досудового розслідування, або службової особи, уповноваженої на прийняття та реєстрацію заяв (повідомлень);

– самостійно виявлені слідчим (дізнавачем) або іншою посадовою особою органу (підрозділу) поліції з будь-якого джерела обставин кримінального правопорушення;

– повідомлення осіб, які затримали підозрювану особу під час учинення або замаху на вчинення кримінального правопорушення чи безпосередньо після вчинення кримінального правопорушення, чи під час безперервного переслідування особи, яка підозрюється в його вчиненні тощо.

Вивчення матеріалів кримінальних проваджень, пов’язаних із розкриттям кібершахрайств свідчить про те, що приводом для початку досудового розслідування є: 1) отримання заяв від громадян, які стали жертвами шахрайських дій – 60 %; 2) отримання заяв від громадян про роботу сумнівної вебсторінки чи діяльність організацій – 8 %; 3) повідомлення від підприємств, установ, організацій, представників влади, посадових осіб, журналістів тощо – 12 %; 4) повідомлення від невстановленої особи (анонімний дзвінок на лінію «102» або анонімний лист з викладеними обставинами вчинення злочину) – 4 %; 5) самостійне виявлення уповноваженою особою з

різних джерел обставин, що свідчили про вчинення злочину (як правило, при моніторингу інтернет-ресурсів, медіа, форумів тощо) – 16 %.

Слід зазначити, що інформацію про вчинення кібершахрайства не отримується взагалі або отримується вкрай рідко з такого джерела як повідомлення осіб, які затримали підозрювану особу під час учинення або замаху на вчинення злочину чи безпосередньо після вчинення злочину, або під час безперервного переслідування особи, яка підозрюється в його вчиненні.

Причиною цьому, – як пише С. В. Самойлов, є технічна сторона способу вчинення злочину, його географічне розташування злочинця та потерпілого, а також велика розбіжність у часі між вчиненими діями та настанням наслідків [8, с. 68].

Вочевидь це є змістом початкового етапу розслідування та впливає на подальший його хід, безпосередньо залежить саме від повноти відомостей на момент внесення їх до ЄРДР, з одночасним вивченням та оцінкою. Адже підстави для початку досудового розслідування визначає слідчий шляхом правової оцінки джерел отриманої інформації про наявність у них обставин, що можуть свідчити про вчинення злочину (його ознаки) та кола причетних осіб (ч. 1, пп. 3-5 ч. 5, ч. 6 ст. 214 КПК України).

На цьому етапі – оцінки первинної інформації, слідчий обмежений у проведенні процесуальних заходів, бо чинне законодавство забороняє проводити будь-які процесуальні дії, а їх проведення до внесення відомостей до ЄРДР або без такого внесення тягне за собою відповідальність, установлену законом.

У такому контексті доречна позиція окремої плеяди науковців, які стверджують, що «… зазначена діяльність відповідає критеріям самостійного провадження, оскільки є системою процесуальних дій у межах кримінальної процесуальної форми досудового провадження, які зумовлюють виникнення певної сукупності процесуальних відносин та спрямовані на виконання єдиного завдання, і цілком помірним є розуміння й дослідження цієї діяльності саме як самостійного провадження» [9, с. 334]. Тобто, слідчий у взаємодії з оперативним підрозділом на етапі оцінки первинної інформації можуть визначити основні напрями розкриття злочину та вибору спектру процесуальних заходів. Обсяг такого інструментарію залежить від визначення попередньої правової кваліфікації кримінального правопорушення із зазначенням статті (частини статті) Закону України про кримінальну відповідальність, відомості про які обов’язково необхідно зазначити під час внесення відомостей до ЄРДР відповідно до ч. 5 ст. 214 КПК України. Правильна попередня правова кваліфікація кримінального правопорушення впливає і на порядок проведення досудового розслідування.

О. В. Тарасова у своїх дослідженнях акцентує увагу на цій проблематиці, бо як свідчить правозастосовна практика практичні працівники та судді

по-різному кваліфікують кібершахрайство. Наприклад, злочинні дії з розміщення на певних сайтах неправдивої інформації про продаж неіснуючих товарів та отримання винним за них передоплати деякі суди кваліфікують як шахрайство, учинене шляхом незаконних операцій із використанням електронно-обчислювальної техніки (ч. 4 ст. 190 КК України). Інші суди подібні діяння перекваліфіковують на ч. 1 або ч. 2 ст. 190 КК України, обґрунтовуючи це тим, що перерахування грошей потерпілими на рахунок винного не є незаконною операцією з використанням електронно-обчислювальної техніки [10, с. 485–487]. Теж і стосується вчинення такого діяння під час дії воєнного стану. Перекваліфікація на ч. 3 ст. 190 КК України.

Нагальна проблема полягає в конструкції складу злочину, бо поза увагою залишається сам механізм злочинних дій, наприклад, реєстрація на сайтах, розміщення неправдивих оголошень, незаконне отримання грошових коштів у віртуальному просторі (середовищі), там де і відбуваються суспільні відносини. Оскільки кібершахрайство характеризується різними способами за допомогою новітніх технологій, то кваліфікуюча ознака, передбачена ч. 4 ст. 190 КК України у повній мірі не відображає всіх цих можливостей.

Задля мінімізації ускладнень, з якими стикаються слідчі та оперативні підрозділи під час оцінки первинної інформації, доцільно:

– уніфікувати окремі норми КПК України, розширивши спектр процесуальних дій (можливостей) до внесення відомостей в ЄРДР;

– деталізувати момент початку розслідування, розмежувавши та позбавивши залежності в цьому питані від норм Положення про ЄРДР, порядок його формування та ведення, затвердженого наказом Генерального прокурора від 30.06.2020 № 298;

– консолідувати норми КК України з урахуванням нормативної бази про забезпечення безпеки у кіберпросторі, визначити єдину термінологію для використання правозастосовними інституціями.

Як вже зазначалось, після оцінки первинної інформації, визначаються напрями розкриття будь-якого кримінального правопорушення, у тому числі і кібершахрайства, тісно пов’язано з обставинами, що підлягають доказуванню у кримінальному провадженні.

Відповідно до ч. 2 ст. 91 КПК України, доказування – це збирання, перевірка та оцінка доказів із метою встановлення обставин, що мають значення для кримінального провадження. Предметом доказування вважається сукупність типових обставин, передбачених чинним кримінальним процесуальним законодавством, що мають загальний і, в окремих випадках, спеціальний характер. У кожному кримінальному провадженні коло цих обставин не може бути однаковими, оскільки межі доказування орієнтовані на кримінально-правові ознаки кримінального правопорушення, що, у свою чергу, визначають особливості як самого процесу розслідування та розкриття, так і процесу доказування.

Крім того, під час розкриття злочину часто виникає необхідність встановлювати обставини, що не мають правового значення і які не потребують доведення, але мають вагоме методичне та тактичне значення для ефективного розслідування кримінального правопорушення.

Відповідно до ч. 1 ст. 91 КПК України визначено низку обставин, які підлягають доказуванню [3]. Ці обставини є визначальними, базовими для всіх злочинних діянь без винятку, а також означенням для спрямовані діяльності слідчого та оперативних підрозділів. Ураховуючи, що кримінальний процес є частиною галузі кримінально-правового циклу та задля конкретизації обставин досліджуваного злочину доречно використати й інший термін, як «обставини, що підлягають встановленню».

Це видається логічним, оскільки коло обставин, пов'язаних з доказуванням події кримінального правопорушення, винуватості особи в його вчиненні, форми вини, мети і мотивів, деталізується і залежить від того, як сформульовано склад кримінального правопорушення у відповідній нормі кримінального закону. Встановлення цих обставин має послідовно давати відповіді на класичне запитання юриспруденції: «що?», «де?», «коли?», «ким?», «яким чином?» тощо [11, с. 94].

Також вважаємо доречним урахувати думку попередників за останні роки.

Так, С. В. Чучко виокремлює чотири групи обставин, що підлягають встановлення, під час розслідування шахрайств при купівлі-продажу товарів через мережу Інтернет: 1) обставини, що стосуються події шахрайства при купівлі-продажу товарів через мережу Інтернет (відомості про час, місце вчинення шахрайства, відомості про спосіб його вчинення; відомості про знаряддя (засоби) злочину; відомості про сліди злочину; відомості про предмет злочинного посягання; 2) обставини, що стосуються особи потерпілого та злочинця (ознаки суб'єкта злочину: фізична особа, осудність, вік, кваліфікуючі ознаки, які стосуються суб'єкта; кількість злочинців (наявність розподілу ролей серед шахраїв, функції кожного з них); 3) причинкові обставини: наявність причинного зв'язку між діями винних осіб і їх наслідками; виявлення причин та умов, які сприяли вчиненню злочину; заходи, яких необхідно вжити для їх усунення тощо; 4) решта обставин (вид і розмір шкоди, завданої кримінальним правопорушенням; кваліфікуючі ознаки щодо розміру шкоди, завданої злочином; обставини, що обтяжують чи пом'якшують покарання; обставини, що виключають кримінальну відповідальність, чи є підстава для закриття кримінального провадження; обставини, що є підставою для звільнення від кримінальної відповідальності, а також обставини, що виключають факт вчинення підозрюваною особою іншого злочину тощо) [12, с. 108–109].

На думку Т. В. Коршикової, на попередньому етапі досудового розслідування кримінального провадження, пов'язаного з шахрайством, учиненого з

використанням електронно-обчислювальної техніки, доцільно об'єднати в наступні групи: 1) обставини, що стосуються самої події кримі-нального правопорушення; 2) винуватість обвинуваченого у вчиненні кримі-нального правопорушення, форма вини, мотив і мета вчинення кримінального правопорушення; 3) вид і розмір шкоди, завданої кримінальним правопору-шення, - відомості про предмет злочинного посягання (його кількісні та якісні характеристики); 4) відомості, що характеризують особу підозрюваного; 5) обставини, які пом'якшують та обтяжують покарання; 6) звільнення від кримінальної відповідальності; 7) обставини, що є підставою для застосування до юридичних осіб заходів кримінально-правового характеру [11, с. 96].

І. О. Коваленко визначив систему обставин, що підлягають встановлення у кримінальному провадженні за фактом вчинення шахрайств у сфері використання банківських електронних платежів. До її складу входять: 1) обставини, що характеризують вчинення шахрайства у сфері використання банківських електронних платежів (відомості про час, місце вчинення шахрайства, відомості про спосіб його вчинення, наприклад: використання ботів для спаму та потрапляння шкідливих програм до комп'ютерного забезпечення потерпілого; використання реквізитів картки, які викрадені з серверів магазинів електронної торгівлі, платіжних та розрахункових систем, із персональних комп'ютерів користувачів; відомості про сліди протиправного діяння; визначення місця отримання неправомірного доступу та інтеграції до мережі (зсередини чи ззовні) та способи вчинення неправомірного підключення (злам програм захисту даних, маніпуляції з даними, командами та інформа-цією, використання шахрайських програм, технічних прийомів); засоби, що використовуються при скоєнні правопорушення: це можуть бути як технічні, такі як електронно-обчислювальна техніка, смартфони, планшети, модеми, маршрутизатори, так і програмні, такі як VPN, браузери, графічні редактори, програми кодування інформації); 2) обставини, котрі відносяться до характе-ристики особи злочинця та потерпілого (кількість правопорушників – визначе-ння ролі кожного з них); 3) причинно-наслідкові зв'язки: наявність певного зв'язку між діями винних осіб та їх результатами; з'ясування причин та умов, що сприяли вчиненню протиправного діяння); 4) обставини, що обтяжують, пом'якшують покарання чи взагалі виключають кримінальну відповідальність (чи наявні умови та підстави для закриття кримінального провадження); 5) кваліфікуючі ознаки стосовно розміру шкоди завданої протиправним діянням та обставини, що є підставою для звільнення від кримінальної відповідальності; 6) вид та розмір шкоди, завданої вчиненням шахрайства у сфері використання банківських електронних платежів [13, с. 107–108].

З огляду на вказане та враховуючи узагальнення правозастосовної практики, пропонуємо зміст обставин, що підлягають встановленню під час розкриття кібершахрайств, виокремити чотири взаємопов'язані групи:

1) обставини стосовно події злочину:

– відомості про факт вчинення шахрайства в кіберпросторі;
– відомості про час учинення шахрайства – тривалість та періодизація;
– відомості про просторові межі, у яких відбулось шахрайство;
– відомості про особу потерпілого;
– відомості про способи вчинення шахрайства;
– відомості про предмет посягання;
– відомості про характер і розмір завданої шкоди;
– відомості про джерела електронних (цифрових) слідів;

2) інші обставини злочину:

2.1) відомості про причинно-наслідковий зв'язок:

– обставини, що сприяли вчиненню шахрайства – відповідні причини та умови;
– обставини стосовно споріднених видів кримінальних правопорушень, як-то вчинення кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.
– обставини постзлочинної діяльності;

2.2) відомості про особу свідків;

3) обставини стосовно підозрюваного:

– відомості про особу підозрюваного – дані, що характеризують його як особу та особистість;
– відомості про винуватість, мотив та мету підозрюваного;
– відомості про співучасть у вчиненні шахрайства, у тому числі споріднених видів кримінальних правопорушень;

4) обставини, які можуть мати додаткове значення в кримінальному провадженні:

– обставини, що впливають на ступінь тяжкості вчиненого шахрайства, обтяжують чи пом'якшують покарання;
– обставини, що є підставами для закриття кримінального провадження чи звільнення від кримінальної відповідальності або покарання;
– розмір процесуальних витрат.

Висновки. Отже, можемо констатувати, що встановлення всіх цих обставин сприятиме швидкому розкриттю кібершахрайства, повному і неупередженому розслідуванню – з'ясуванню юридично значущих обставин, які будуть доведені або спростовані в цілях обґрунтованого притягнення певної особи до відповідальності в міру своєї вини. А правильна оцінка первинної інформації визначає напрями досудового розслідування, необхідний інструментарій для розкриття кібершахрайства.

Між тим, на сьогодні залишаються недостатньо дослідженим теоретико-прикладні питання стосовно змістовної складової кола обставин, що підлягають

встановленню під час розкриття кібершахрайств, а також потребує більш детальної конкретизації етап оцінки первинної інформації, що і є пріоритетним для подальших наукових досліджень.

Література:

1. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування : статистика. *Офіційна сторінка Офісу Генерального прокурора.* URL: https://gp.gov.ua/ua/posts/statistika.

2. Самойлов О. А. Криміналістичний та правовий аналіз злочинної діяльності в мережі Інтернет. *Порівняльно-аналітичне право.* Вип. № 4. 2015. С. 408–411.

3. Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

4. Порядок ведення єдиного обліку в органах (підрозділах) поліції заяв і повідомлень про кримінальні правопорушення та інші події. Наказ МВС України від 08.02.2019 № 100. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/z0223-19#Text.

5. Інструкція з організації реагування на заяви і повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції України. Наказ МВС України від 27.04.2020 № 357. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/z0443-20#Text.

6. Інструкція з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні. Наказ МВС України від 07.07.2017 № 575. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/z0937-17#Text.

7. Інструкція про порядок залучення працівників органів досудового розслідування поліції та Експертної служби Міністерства внутрішніх справ України як спеціалістів для участі в проведення огляду місця події. Наказ МВС України від 03.11.2015 № 1339. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/z1392-15#Text.

8. Самойлов С. В. Шахрайства на Інтернет-аукціонах як один із способів скоєння шахрайств з використанням мереж Інтернет (криміналістична характеристика способу вчинення). *Форум права.* Вип. № 4. 2011. С. 645–650.

9. Кримінальний процес : підручник / В. Я. Тація, Ю. М. Грошевого, О. В. Капліної, О. Г. Шило. Харків : Право, 2013. 824 с.

10. Тарасова О. В. Удосконалення законодавства щодо кримінальної відповідальності за шахрайство, учинене шляхом незаконних операцій із використанням електронно-обчислювальної техніки. *Актуальні проблеми держави і права.* Вип. № 72. 2014. С. 481–488.

11. Коршикова Т. В. Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки : дис. …. доктор філософії. Київ, 2021. 255 с.

12. Чуйко С. В. Розслідування шахрайств при купівлі-продажу товарів через мережу Інтернет : дис. ... доктор філософії. Дніпро, 2021. 276 с.

13. Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів : дис. ... доктор філософі. Дніпро, 2022. 236 с.

References:

1. Statystyka pro zareiestrovani kryminalni pravoporushennia ta rezultaty yikh dosudovoho rozsliduvannia [Statistics on registered criminal offenses and the results of their pretrial investigation]. *Ofis Heneralnoho prokurora – Prosecutor General's Office*. URL: https://new.gp.gov.ua/ua/posts/statistika [in Ukrainian].

2. Samoilov, O. A. (2015). Kryminalistychnyi ta pravovyi analiz zlochynnoi diialnosti v merezhi Internet [Forensic and legal analysis of criminal activity on the Internet]. *Porivnialno-analitychne pravo – Comparative and analytical law*, 4, 408–411 [in Ukrainian].

3. Kryminalnyi protsesualnyi kodeks Ukrainy vid 13.04.2012 № 4651-VI [Criminal Procedure Code of Ukraine dated April 13 2012, № 4651-VI]. *Ofitsiinyi vebportal Verkhovnoi Rady Ukrainy – Official website of the Verkhovna Rada of Ukraine*. URL: https://zakon. rada.gov.ua/laws/show/4651-17#Text [in Ukrainian].

4. Poriadok vedennia yedynoho obliku v orhanakh (pidrozdilakh) politsii zaiav i povidomlen pro kryminalni pravoporushennia ta inshi podii. Nakaz MVS Ukrainy vid 08.02.2019 № 100 [The procedure for keeping uniform records in police bodies (subdivisions) of statements and reports on criminal offenses and other events. Order of the Ministry of Internal Affairs of Ukraine dated February 8 2019, № 100]. *Ofitsiinyi vebportal Verkhovnoi Rady Ukrainy – Official website of the Verkhovna Rada of Ukraine*. URL: https://zakon.rada.gov.ua/laws/show/z0223-19#Text [in Ukrainian].

5. Instruktsiia z orhanizatsii reahuvannia na zaiavy i povidomlennia pro kryminalni, administratyvni pravoporushennia abo podii ta operatyvnoho informuvannia v orhanakh (pidrozdilakh) Natsionalnoi politsii Ukrainy. Nakaz MVS Ukrainy vid 27.04.2020 № 357 [Instructions on the organization of response to statements and reports on criminal, administrative offenses or events and operational information in bodies (subdivisions) of the National Police of Ukraine. Order of the Ministry of Internal Affairs of Ukraine dated April 27 2020, № 357]. *Ofitsiinyi vebportal Verkhovnoi Rady Ukrainy – Official website of the Verkhovna Rada of Ukraine*. URL: https://zakon.rada.gov.ua/laws/show/z0443-20#Text [in Ukrainian].

6. Instruktsiia z orhanizatsii vzaiemodii orhaniv dosudovoho rozsliduvannia z inshymy orhanamy ta pidrozdilamy Natsionalnoi politsii Ukrainy v zapobihanni kryminalnym pravoporushenniam, yikh vyiavlenni ta rozsliduvanni. Nakaz MVS Ukrainy vid 07.07.2017 № 575 [Instructions on the organization of cooperation of pretrial investigation bodies with other bodies and units of the National Police of Ukraine in the prevention of criminal offenses, their detection and investigation. Order of the Ministry of Internal Affairs of Ukraine dated July 7 2017, № 575]. *Ofitsiinyi vebportal Verkhovnoi Rady Ukrainy – Official website of the Verkhovna Rada of Ukraine*. URL: https://zakon.rada.gov.ua/laws/show/z0937-17#Text [in Ukrainian].

7. Instruktsiia pro poriadok zaluchennia pratsivnykiv orhaniv dosudovoho rozsliduvannia politsii ta Ekspertnoi sluzhby Ministerstva vnutrishnikh sprav Ukrainy yak spetsialistiv dlia uchasti v provedennia ohliadu mistsia podii. Nakaz MVS Ukrainy vid 03.11.2015 № 1339 [Instructions on the procedure for engaging employees of pretrial investigation bodies of the police and the Expert Service of the Ministry of Internal Affairs of Ukraine as specialists to participate in the inspection of the scene of the incident. Order of the Ministry of Internal Affairs of Ukraine dated November 3 2015, № 1339]. *Ofitsiinyi vebportal Verkhovnoi Rady Ukrainy – Official website of the Verkhovna Rada of Ukraine*. URL: https://zakon.rada.gov.ua/laws/show/z1392-15#Text [in Ukrainian].

8. Samoilov, S. V. (2011). Shakhraistva na Internet-auktsionakh yak odyn iz sposobiv skoiennia shakhraistv z vykorystanniam merezh Internet (kryminalistychna kharakterystyka sposobu vchynennia) [Frauds at Internet auctions as one of the methods of committing frauds using Internet networks (forensic characteristics of the method of commission)]. *Forum prava – Law forum*, 4, 645–650 [in Ukrainian].

9. Tatsiia, V. Ya., Hroshevoho, Yu. M., Kaplinoi, O. V., & Shylo O. H. (2013). *Kryminalnyi protses [Criminal process]*. Kharkiv : Pravo [in Ukrainian].

10. Tarasova, O. V. (2014). Udoskonalennia zakonodavstva shchodo kryminalnoi vidpovidalnosti za shakhraistvo, uchynene shliakhom nezakonnykh operatsii iz vykorystanniam elektronno-obchysliuvalnoi tekhniky [Improvement of the legislation on criminal liability for fraud committed through illegal transactions using electronic computing equipment]. *Aktualni problemy derzhavy i prava – Actual problems of the state and law,* 72, 481–488 [in Ukrainian].

11. Korshykova, T. V. (2021). Rozsliduvannia shakhraistv, uchynenykh z vykorystanniam elektronno-obchysliuvalnoi tekhniky [Investigation of fraud committed using electronic computing technology]. *Candidate's thesis.* Kyiv [in Ukrainian].

12. Chuiko, S. V. (2021). Rozsliduvannia shakhraistv pry kupivli-prodazhu tovariv cherez merezhu Internet [Investigation of frauds in the purchase and sale of goods via the Internet]. *Candidate's thesis.* Dnipro [in Ukrainian].

13. Kovalenko, I. O. (2022). Rozsliduvannia shakhraistva u sferi vykorystannia bankivskykh elektronnykh platezhiv [Investigation of fraud in the sphere of use of bank electronic payments]. *Candidate's thesis.* Dnipro [in Ukrainian].