УДК 343.98.06

О. А. Самойленко

ТИПОВІ СЛІДЧІ СИТУАЦІЇ ПОЧАТКОВОГО ЕТАПУ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ, ВЧИНЕНИХ У КІБЕПРОСТОРІ

Постановка проблеми. В умовах загального збільшення рівня кіберзлочинності показник розкриття злочинів, вчинених у кіберпросторі, залишається незмінним протягом п'яти останніх років: в 2014 році слідчими Національної поліції України було складено 797 обвинувальних актів щодо осіб, що вчинили вказаний вид злочинів; у 2015 – 756; у 2016 – 453; у 2017 – 764; у 2018 – 666. Така тенденція свідчить про необхідність підвищення рівня професійної придатності слідчих у питаннях розслідування зазначеної категорії злочинів. Цьому сприятиме розроблення типових слідчих ситуацій для початкового етапу їх розслідування, формулювання відповідних ним тактичних завдань й деталізація комплексу засобів їх виконання.

Аналіз останніх досліджень і публікацій. У криміналістичній науці типові слідчі ситуації початкового етапу розслідування злочинів, вчинених у кіберпросторі, висвітлено не комплексно, у контексті комп'ютерних злочинів, злочинів у сфері новітніх технологій або транснаціональних злочинів у роботах Л.В. Борисової, В.Б. Вєхова, Ю.В. Гаврилова, Д.А. Іллюшина, С.В. Самойлова, К.В. Тітуніної, М.Г. Шурухнова та інших вітчизняних та закордонних криміналістів. Обираючи для типізації слідчих ситуацій початкового етапу розслідування інформаційну визначеність, автори, по суті, описують повноту вихідної інформації про злочин. Проте факт або можливість персоналізації відомостей про користувача-злочинця частіше ігнорується, ніж береться до уваги, що зумовлює потребу продовження наукового пошуку оптимального підходу до типізації слідчих ситуацій початкового етапу розслідування злочинів, вчинених у кіберпросторі.

Метою статті є визначення типових слідчих ситуацій початкового етапу розслідування злочинів, вчинених у кіберпросторі, та характеристика окремих з них у комплексі з відповідними тактичними завданнями та засобами їх вирішення.

Виклад основного матеріалу дослідження. Більшість науковців, посилаючись на інформаційну визначеність як критерій типізації слідчих

ситуацій початкового етапу розслідування, аналізують ситуації з різним набором інформації про злочин, зокрема: зміст джерела інформації про злочин [1, с. 120], очевидні та неочевидні вихідні умови вчинення злочину [2, с. 79], специфіку зв'язків між елементами криміналістичної характеристики окремого виду кіберзлочинів [3, с. 95] тощо.

На нашу думку, в момент відкриття кримінального провадження ступінь повноти вихідної інформації про готування або вчинення злочину визначається насамперед характером інформації про злочинця, зокрема, що визначається:

1) наявністю персоналізованих відомостей (розгорнуті анкетні дані особи злочинця);

2) наявністю неперсоналізованих відомостей (IP-адреси, MAC-адреси, сторінка у соціальній мережі тощо);

3) відсутністю персоналізованих та неперсоналізованих відомостей (через використання злочинцем технологій анонімізації доступу до ресурсів Інтернет, індивідуальної географічної мобільності).

Ступінь повноти (обсяг) та достовірність іншої інформації про злочин (спосіб підготовки та вчинення злочину, настання злочинних наслідків, особа потерпілого) знаходяться у прямій залежності від форми початку кримінального провадження, яка відображає специфіку його відкриття щодо класифікаційних груп/підгруп злочинів, вчинених у кіберпросторі.

Таким чином, типізувати слідчу ситуацію на початковому етапі розслідування злочинів, вчинених у кіберпросторі, дають змогу два взаємопов'язаних чинника: 1) характер інформації про особу злочинця; 2) форма початку кримінального провадження. Останній, відображаючи повноту іншої інформації, специфіка якої зумовлена класифікаційною групою/підгрупою злочинів, вчинених у кіберпросторі, буде використаний з метою визначення особливостей типових слідчих ситуацій груп/підгруп досліджуваних злочинів.

За результатами узагальнення матеріалів слідчо-судової практики розслідування злочинів, вчинених у кіберпросторі, можна виокремити три групи типових слідчих ситуацій початкового етапу розслідування: 1) ситуації, що характеризуються наявністю персоналізованих відомості про користувача як злочинця; 2) ситуації, що характеризуються наявністю неперсоналізованих відомості про користувача як злочинця; 3) ситуації, що характеризуються відсутністю будь-яких відомостей про особу злочинця.

Відобразити особливості типових слідчих ситуацій класифікаційних груп/підгруп злочинів, вчинених у кіберпросторі, дозволить характеристика в межах кожної з вказаних груп типових слідчих ситуацій їх різновидів, зокрема коли: 1) кримінальне провадження розпочато в результаті отримання заяви потерпілого/повідомлення особи про кримінальне правопорушення; 2) кримінальне провадження розпочато в результаті ознайомлення з матеріалами оперативного підрозділу щодо перевірки оперативної інформації; 3) кримінальне провадження розпочато в рамках реалізації матеріалів ОРС.

Показово конкретизуємо у комплексі з тактичними завданнями та засобами їх вирішення ***ситуації, що характеризуються наявністю персоналізованих відомостей про користувача як злочинця.***

Ситуація 1. Кримінальне провадження розпочато в результаті отримання заяви / повідомлення особи про кримінальне правопорушення, матеріали містять персоналізовані відомості про особу злочинця. Ця ситуація типова під час розслідування злочинів, вчинених внутрішнім користувачем мережі, що спрямовані на заволодіння чужим майном, у сфері функціонування електронних розрахунків, і таких, що порушують механізми захисту від монополізму та недобросовісної конкуренції. Потерпіла сторона зазвичай є юридичною особою. Матеріали внутрішньої перевірки (аудит, технічна перевірка, моніторинг мереж тощо) містяться в первинних матеріалах, що значно спрощує планування початкового етапу розслідування. Прикладом є кримінальне провадження щодо гр. А. [4], який, будучи відповідно до посадової інструкції особою, яка володіє інформацією клієнтів, діючи з корисливих мотивів, за попередньою змовою з начальником відділення № 8 ПАТ Б. з метою заволодіння коштами клієнта підробили документи на переказ грошових коштів в електронному вигляді, за допомогою яких здійснили незаконний переказ грошових коштів.

На початковому етапі розслідування основними тактичними завданнями в цій ситуації були: забезпечення збереження документів, у яких фіксують роботу комп'ютерної мережі банку й осіб, що її обслуговують; встановлення обставин проходження фіктивного електронного переведення коштів; встановлення режиму роботи комп'ютерної системи банку для здійснення незаконних дій у мережі; встановлення кола осіб, що мали змогу здійснити зазначений електронний переказ (у конкретний час і дату мали доступ до комп'ютерної системи, паролі для входу у внутрішню мережу банку); встановлення фактів приховування злочину (внесення змін в електронну базу даних банку, особистого впливу на свідків); встановлення зв'язків Б. з представниками інших комерційних структур і даних про його особу (попереднє місце роботи, коло знайомих та інтересів, наявність судимостей тощо); забезпечення відшкодування матеріальних збитків; встановлення злочинних зв'язків між А. та Б.; встановлення зв'язку А. та Б. з представниками компаній-жертв; встановлення того, як і ким були використані викрадені кошти; виявлення ознак вчинення несанкціонованої зміни інформації, яку опрацьовують в автоматизованих системах і зберігають на носіях такої інформації, вчинені особою, яка має право доступу до неї, за попередньою змовою групою осіб.

Окреслені тактичні завдання виконують шляхом проведення комплексу слідчих (розшукових) дій та інших заходів пізнання слідчого: 1) допит службовців і посадових осіб відділення ПАТ(банк), які проводили перевірку та виявили ознаки злочину; 2) тимчасовий доступ до речей і документів (інформація в електронній системі банку); 3) слідчий огляд вилученого; 4) призначення ревізії діяльності ПАТ; 5) допит інших осіб як свідків злочину (керівництва та рядових працівників ПАТ), які можуть поясни-

ти обставини вчинення фіктивного електронного платежу; 6) затримання та обшук за місцем мешкання А. та Б. з метою встановлення наявності злочинних зв'язків з представниками інших комерційних структур, виявлення цінностей, одержаних злочинним шляхом; 7) опитування А. та Б. про обставини вчинення злочину; 8) слідчий огляд вилученого під час обшуку (грошові кошти, документи на переказ, чорнові записи, банківські платіжні картки, ноутбук); 9) призначення комп'ютерно-технічної експертизи; 10) накладення арешту на майно і вклади А. та Б.; 11) доручення оперативному підрозділу в порядку ст. 40 КПК України з метою встановлення майнового становища А. та Б., злочинних зв'язків А. та Б. з іншими посадовими особами банку; 12) оголошення підозри А. та Б., допит їх як підозрюваних.

Ситуація 2. Кримінальне провадження розпочато в результаті перевірки оперативної інформації, матеріали первинної перевірки містять персоналізовані відомості про особу злочинця. Ситуація типова під час розслідування тяжких конвенційних кіберзлочинів злочинцем-звичайним користувачем і злочинцем-упевненим користувачем. Кримінальне провадження розпочинають типово у зв'язку з докладним рапортом співробітника ДКП НП України, при цьому особа або група осіб у визначеному складі вже затримана під час вчинення злочину.

Прикладом є кримінальне провадження щодо гр. Д. та Ч., які, діючи за попередньою змовою з метою вчинення розпусних дій щодо малолітньої особи Н., виготовляли, зберігали з метою розповсюдження та розповсюджували зображення, що містять порнографію. На початковому етапі розслідування основними тактичними завданнями в цій ситуації були: затримання Д. та Ч. й одночасна реєстрація в ЄРДР кримінального правопорушення; персоналізація акаунтів користувачів як злочинців; забезпечення збереження електронних носіїв інформації, у яких зафіксовано роботу Д. та Ч. в мережі; встановлення факту обізнаності Д. та Ч. щодо малолітнього віку потерпілої; встановлення інших фактів розповсюдження продукції порнографічного характеру; встановлення психологічного контакту з малолітньою; встановлення осіб, яким стало відомо про таку діяльність Д. та Ч.; встановлення фактів створення продукції порнографічного змісту; встановлення способів створення та виготовлення продукції порнографічного характеру.

Основні тактичні завдання розслідування виконано шляхом проведення такого комплексу слідчих (розшукових) дій та інших заходів пізнання слідчого: 1) особистий огляд Д. і Ч., під час якого вони видали мобільні телефони, за допомогою яких відбувалося користування соціальною мережею «Вконтакте»; 2) доручення оперативному підрозділу ДКП НП України в порядку ст. 40 КПК України на проведення організаційних заходів з метою персоналізації відомостей про користувачів; 3) слідчий огляд телефонів Д. та Ч.; 4) проведення обшуків за місцем мешкання Д., унаслідок чого вилучено 30 оптичних дисків для лазерних систем зчитування; 5) проведення обшуку за місцем мешкання Ч.; 6) проведення огляду електронної сторін-

ки потерпілої в соціальній мережі, під час якого встановлено багаторазове листування з окремими користувачами (Д. та Ч.), відеозапис; 7) допит потерпілої, свідків (близьких родичів Н.); 8) слідчий огляд вилучених під час обшуку предметів; 9) оголошення підозри Д. і Ч. Момент затримання Д. і Ч. є ключовим моментом виявлення злочинців, адже на той час зміст листування та поширена ними продукція повинні містити ознаки порнографічної продукції та вказувати на навмисні розпусні дії щодо малолітньої особи, тому внаслідок слідчих дій та ОРЗ чітко фіксують момент надіслання користувачем під нік-неймом потерпілої текстового повідомлення про малолітній вік потерпілої – 10 років, у непроцесуальний спосіб до моменту початку кримінального провадження отримують консультацію фахівця з мистецтвознавства та психолога.

Ситуація 3. Кримінальне провадження розпочато в результаті діяльності за оперативно-розшуковою справою; персоналізація особи злочинця для слідчого є закономірною. Ситуація є типовою під час розслідування тяжких та особливо тяжких злочинів, вчинених з корисливих мотивів, тяжких конвенційних злочинів, вчинених злочинцем-досвідченим користувачем.

Таку слідчу ситуацію демонструє кримінальне провадження щодо обвинувачення гр. А., який здійснював за попередньою змовою з гр. Б. неправомірне використання електронних грошей. У процесі судового розгляду незаперечно було доведено вину лише у вчиненні кримінального правопорушення, передбаченого ч. 2 ст. 200 КК України [5]. Унаслідок здійснення контролю за телефонними розмовами та зняття інформації з каналів зв'язку (як ОТЗ протягом року) на момент початку кримінального провадження було відомо, що А. і Б., діючи в порушення чинного законодавства України, а також Закону України «Про платіжні системи та переказ коштів в Україні», постанови Правління Національного банку України від 4 листопада 2010 року № 481, якою затверджене Положення «Про електронні гроші в Україні», застосовували та використовували у фінансово-господарській діяльності фізичної особи – підприємця А. електронні гроші платіжних систем «WebMoney Transfer» і «Liberti Reserve». Ці особи надавали послуги з введення/виведення, обміну, конвертації (переведення в готівку та навпаки) електронних грошей (українська гривня, долар США, євро, російський рубль) за допомогою платіжних систем. Переведення (конвертація) електронних грошей на готівку обвинуваченими відбувалося так: замовники (споживачі, фізичні особи), власники електронних грошей, за допомогою мережі Інтернет через сайт підприємця А. здійснювали замовлення, переважно в телефонному режимі, про виведення (конвертацію) електронних грошей у готівку (здебільшого це долар США, українська гривня) та пересилали необхідну суму електронних грошей зі свого електронного гаманця на електронні гаманці, які знаходилися в користуванні Б. та фізичної особи – підприємця А. Протягом однієї доби споживачі (фізичні особи), власники електронних грошей, приходили за адресою здійснення фінансово-господарської діяльності фізичної

особи – підприємця А. (у м. Чернівцях, різні офіси), на вимогу А. та/або Б. пред'являли паспорт, з якого робили копію й отримували взамін на перераховані електронні гроші електронних платіжних систем «WebMoney Transfer» та «Liberty Reserve» особисто від Б. та/або А. готівку в сумі перерахованих електронних грошей (мінус 3–5% від перерахованої суми як плату за надану послугу). У справі фігурують інші особи, на яких було відкрито банківські рахунки, що за дорученням надані в користування гр. А. та Б., загальний оборот коштів лише на одному з рахунків становив 520 360 доларів США.

На початковому етапі розслідування основними тактичними завданнями в цій ситуації були: забезпечення збереження електронних носіїв інформації, у яких зафіксовано роботу в мережі фізичної особи – підприємця А.; встановлення якомога більшої кількості споживачів (фізичних осіб), власників електронних грошей, що користувалися послугами А. та Б., які можуть бути свідками в провадженні; встановлення фактів фіктивного підприємництва, що супроводжували злочин; встановлення інших осіб, вирішення питання про причетність їх до злочину, зокрема осіб, на яких було відкрито банківські рахунки, що використовували в механізмі злочинної діяльності; встановлення фактів створення продукції порнографічного характеру; встановлення походження грошових коштів на рахунках фірм А. та Б. грошових коштів, що вилучені під час розслідування; встановлення фактів вчинення підроблення документів, які подають для здійснення державної реєстрації юридичної особи та фізичних осіб – підприємців; встановлення фактів легалізації (відмивання) доходів, одержаних злочинним шляхом; встановлення розміру матеріального збитку державі.

Тактичні завдання розслідування виконано шляхом проведення такого комплексу слідчих (розшукових) дій та інших заходів пізнання слідчого: 1) доручення оперативному підрозділу в порядку ст. 40 КПК України проведення заходів з метою отримання орієнтувальних відомостей про чітко визначені рахунки в «WebMoney Transfer», «Liberti Reserve»», а також у Національному банку України щодо реєстрації платіжних систем «WebMoney Transfer», «Liberti Reserve», їх учасників, операторів послуг цих систем, комерційних агентів, правил використання електронних грошей «WebMoney Transfer», «Liberti Reserve»; 2) тимчасовий доступ до речей і документів щодо руху коштів банківськими рахунками, що використовували А. та Б. для переведення в готівку електронних грошей клієнтів; 3) обшук в офісі фірми «Вебмані-Буковіна» та за місцями мешкання А. та Б.; 4) допити осіб-клієнтів фірми «Вебмані-Буковіна»; 5) тимчасовий доступ до речей і документів цих осіб; 6) слідчі огляди вилученого під час обшуків (банківські картки, заяви, копії паспортів, графік і правила роботи офісу, чорнові записи з іменами та сумами коштів, номерами телефонів, квитанції, акти, рахунки, виписані банком «Хрещатик» на ім'я інших осіб, бланк «Вестерн-Юніон» на отримання готівки А., журнал обліку доходів і витрат, грошові кошти в сумі 11 719 доларів США, 1 755 євро, 643 леїв румунських, 3 248 грн, ноутбук та інша оргтехніка); 7) затримання, оголо-

шення підозри й допит А. та Б. Для забезпечення ефективного розслідування в таких кримінальних провадженнях є потреба у своєчасному налагодженні взаємодії слідчого з оперативним підрозділом, створенні спільної слідчо-оперативної групи з кількох слідчих й оперативних працівників.

Висновки. Отже, вважаємо можливим використовувати для типізації слідчих ситуацій початкового етапу розслідування злочинів, вчинених у кіберпросторі, два взаємопов'язаних чинника, зокрема: 1) характер інформації про особу злочинця; 2) форма початку кримінального провадження. Показово розглянуті нами типові слідчі ситуації, що характеризуються наявністю персоналізованих відомостей про користувача як злочинця, є важливими для слідчого в теоретико-методичному аспекті під час планування та організації розслідування конкретного кримінального провадження щодо злочину, вчиненого в кіберпросторі.

Література

1. Пазиніч В.І. Правові та організаційні засади розслідування злочинів у сфері мобільних телекомунікацій України : дис. ... канд. юрид. наук : 12.00.09. Київ, 2009. 217 с.

2. Анапольська А.І. Розслідування шахрайств, пов'язаних із ними злочинів, вчинених у сфері функціонування електронних розрахунків : дис. ... канд. юрид. наук : 12.00.09. Луганськ, 2008. 225 с.

3. Паляничко Д.Г. Методика розслідування злочинів, пов'язаних із дитячою порнографією : дис. ... канд. юрид. наук : 12.00.09. Одеса, 2013. 210 с.

4. Вирок у справі № 569/10370/14-к від 15 липня 2015 року Рівненського міського суду Рівненської області. URL: http://www.reyestr.court.gov.ua/Review/49017035.

5. Вирок у справі № 727/11024/13-к від 05 травня 2014 року Шевченківського районного суду м. Чернівці. URL: http://www.reyestr.court.gov.ua/ Review/46270509.

Анотація

Самойленко О. А. **Типові слідчі ситуації початкового етапу розслідування злочинів, вчинених у кіберпросторі.** – Стаття.

У статті в результаті визначення підстав для типізації слідчих ситуацій початкового етапу розслідування злочинів, вчинених у кіберпросторі, пропонуються типові слідчі ситуації, що характеризуються наявністю персоналізованих відомостей про користувача як злочинця. Вони розглядаються на прикладі конкретних кримінальних проваджень у комплексі з тактичними завданнями та засобами їх вирішення.

Ключові слова: злочинець, кіберпростір, кримінальне провадження, користувач, персоналізація, слідча ситуація, тактичне завдання.

Аннотация

Самойленко Е. А. **Типичные следственные ситуации первоначального этапа расследования преступлений, совершенных в киберпространстве.** – Статья.

В статье в результате определения оснований для типизации следственных ситуаций первоначального этапа расследования преступлений, совершенных в киберпространстве, предлагаются типичные следственные ситуации, характеризующиеся наличием персонализированных сведений о пользователе как преступнике. Они рассматриваются на примере конкретных уголовных производств в комплексе с тактическими задачами и способами их решения.

Ключевые слова: преступник, киберпространство, уголовное производство, пользователь, персонализация, следственная ситуация, тактическая задача.

Summary

Samoilenko O. A. **Typical investigative situations of the initial stage of investigation of crimes committed in cyberspace.** – Article.

The article, as a result of determining the grounds for typifying investigative situations of the initial stage of investigating crimes committed in cyberspace, suggests typical investigative situations characterized by the presence of personalized information about the user as a criminal. They are considered on the example of specific criminal proceedings in combination with tactical tasks and ways to solve them.

Key words: criminal, cyberspace, criminal proceedings, user, personalization, investigative situation, tactical task.