УДК 336.747:004:343.359

В.Д. Никифорчук,
головний спеціаліст Державного бюро розслідувань, м. Київ,
ORCID ID 0000-0003-4406-7349

ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ, ЩО ВЧИНЯЮТЬСЯ У СФЕРІ БАНКІВСЬКИХ ЕЛЕКТРОННИХ ПЛАТЕЖІВ

Стаття присвячена дослідженню особливостей розслідування злочинів, що вчиняються у сфері банківських електронних платежів. Проаналізовано правову колізію щодо надання права слідчим на здійснення розшукових дій. Досліджено ознаки злочину у сфері банківських електронних платежів. До ознак такого злочину віднесено: корисливість дій; протиправність дій та поведінку (дію), заборонені законом; безоплатність привласнення; вилучення і (або) звернення на користь винного або інших осіб викрадених грошових коштів; заподіяння шкоди власнику; правову охорону інформації, до якої отриманий доступ сторонніх осіб; факт неправомірного доступу до інформації з можливістю отримання інформації та її використання; модифікацію або копіювання інформації. Визначено об'єктивні та суб'єктивних фактори, що впливають на слідчі ситуації цієї категорії злочину.

Ключові слова: *електронні гроші, досудове розслідування, ознаки злочину, платежі, розкриття злочину, слідчі (розшукові) дії, слідчі ситуації.*

Статья посвящена исследованию особенностей расследования преступлений, совершаемых в сфере банковских электронных платежей. Проанализировано правовую коллизию предоставления права следователю на проведение розыскных действий. Исследованы признаки преступлений, совершаемых в сфере банковских электронных платежей. К таким признакам отнесены: корыстность действий; противоправность действий и поведения (действие), которые запрещены законом; бесплатное присвоение; изъятие и (или) обращение в пользу виновного или других лиц похищенных денежных средств; причинение ущерба собственнику; правовая охрана информации, к которой был получен доступ посторонними лицами; факт неправомерного доступа к информации, с возможностью получения информации и ее использования; модификация либо копирование информации. Определены объективные и субъективные факторы, влияющие на следственные ситуации этой категории преступлений.

Ключевые слова: *электронные деньги, досудебное расследование, признаки преступления, платежи, раскрытие преступления, следственные (розыскные) действия, следственные ситуации.*

Швидкий розвиток науково-технічного прогресу впливає не тільки на сферу науки і техніки, а й на економіку. З'являються нові напрями економіки, серед яких і цифрова економіка, з новими елементами – електронними платежами, електронними грошима, технологією "блокчейн" (англ. blockchain). Усі ці нововведення збіглися в часі із прийняттям та становленням нового кримінального процесуального законодавства, що призвело до відповідних проблем, пов'язаних із тактикою діяльності оперативних підрозділів та слідчих під час фіксації ознак злочинів у сфері банківських електронних платежів. Адже виявлення ознак злочинів – це тільки початок процесу розкриття злочину, первинна інформація підлягає перевірці з метою фіксації дій осіб, що вчиняють злочин.

Мета статті полягає в дослідженні особливостей розслідування злочинів, що вчиняються у сфері банківських електронних платежів, виявленні ознак злочину у

сфері банківських електронних платежів та встановленні факторів, що впливають на слідчі ситуації цієї категорії злочину.

Перш за все слід зазначити, що розслідування складних латентних злочинів без застосування сучасних методів і засобів оперативно-розшукової діяльності неможливе. Але нині така форма оперативно-розшукової діяльності, як оперативна розробка, вдосконалюється в межах дії принципово нової процесуальної моделі, тому науковці і практики намагаються збалансувати можливості застосування слідчих (розшукових) дій та негласних слідчих (розшукових) дій з оперативно-розшуковими заходами, а також визначити межі, підстави та обставини їх застосування, запропонувати принципово нове розуміння оперативно-розшукової діяльності [1, с. 120–121]. З урахуванням зазначеного, нами визначається наступне.

Новим Кримінальним процесуальним кодексом України в чинне кримінальне процесуальне законодавство введено поняття негласні слідчі (розшукові) дії (далі – НС(Р)Д), система та методика проведення яких ще задовго до затвердження закону стали предметом активних наукових дискусій. Негласні слідчі (розшукові) дії, закріплені главою 21 Кримінального процесуального кодексу України [5], за сутністю та змістом впроваджувальних дій корелюються із оперативно-розшуковими заходами, закріпленими частиною 1 статті 8 Закону України "Про оперативно-розшукову діяльність" [6]. Відповідно до пункту 1 статті 246 Кримінального процесуального кодексу України, НС(Р)Д – це різновид слідчих (розшукових) дій, відомості про факт і методи проведення яких не підлягають розголошенню, за винятком випадків, передбачених Кримінальним процесуальним кодексом України [5]. Негласні слідчі (розшукові) дії проводяться у випадках, якщо відомості про злочин та особу, яка його вчинила, неможливо отримати в інший спосіб та виключно у кримінальному провадженні щодо тяжких або особливо тяжких злочинів [5].

Під час розслідування будь-яких злочинів, слідчий змушений діяти в різних умовах і за різних обставин, що виникають унаслідок впливу особливостей цього злочину, зокрема, місця його вчинення, способів його вчинення та приховування взаємозв'язку вчинення злочину з іншими процесами об'єктивної реальності, а також поведінкою і взаємодією учасників кримінального процесу тощо. Усвідомлений і неусвідомлений, а також випадковий вплив зазначених чинників на розслідування злочину формує конкретну обстановку, яка в науці криміналістики називається слідчою ситуацією, тому її врахування слідчим у кожному конкретному випадку дозволяє обрати найефективніші напрями розслідування [7, с. 79–80].

При цьому, не залежно від етапу розкриття, необхідно визначити наявність та зафіксувати певні протиправні факти. Це означає, що треба встановити та зафіксувати певні дані, характерні для цього виду злочину, що й визначить ознаки конкретного виду злочину.

Тому, на нашу думку, визначаючи ознаки злочину у сфері банківських електронних платежів, у першочерговому порядку мають бути враховані дані, що підтверджують: корисливість дій; протиправність дій та поведінку (дію), заборонені законом; безоплатність привласнення; вилучення і (або) звернення на користь винного або інших осіб викрадених грошових коштів; заподіяння шкоди власнику; правову охорону інформації, до якої отриманий доступ сторонніх осіб; факт неправомірного доступу до інформації з можливістю отримання інформації та її використання; модифікацію або копіювання інформації. Розглянемо ці ознаки більш детально на прикладах.

Корисливість дій передбачає доведеність зацікавленості крадія в протиправному привласненні предмета злочину, наприклад, при переказі електронних грошей (грошових коштів) з рахунку на рахунок з використанням титульних знаків має бути доведена зацікавленість особи у привласненні коштів.

Протиправність дій та поведінка (дія), заборонені законом, підтверджуються відсутністю в особи права на предмет злочину (електронні гроші), яким вона

заволоділа; протиправне привласнення особою предмета злочину (електронні гроші) всупереч волі власника. Такі дані можуть міститися: в заяві про злочин; в наданих заявником договорах з власниками електронної платіжної системи; в правилах користування електронною платіжною системою; в інших документах організації і платіжної системи; в положеннях законодавства, що регламентує правову охорону відомостей, що становлять певний вид таємниці.

Безоплатність привласнення. Така безоплатність свідомо передбачається, оскільки електронні грошові кошти з рахунку потерпілого переводяться на рахунки, оформлені, як правило, на викрадені паспорти; перерахування коштів здійснюється по "ланцюжку" аналогічних рахунків; окремі рахунки в електронній платіжній системі, використані при викраденні грошових коштів, досить швидко закриваються злочинцями. Встановлення фактичного власника рахунку, використаного для викрадення грошових коштів, неможливе, тому і звернутися до нього з проханням про повернення коштів неможливо.

Вилучення і (або) звернення на користь винного або інших осіб викрадених грошових коштів. На цьому етапі особа, яка підозрюється у вчиненні злочину, невідома. Водночас факт перерахування з рахунку потерпілого електронних грошових коштів завжди передбачає наявність їх одержувача, яким є фактичний власник електронного рахунку, на котрий першим переведені викрадені електронні грошові кошти. На користь цього власника рахунку і здійснений переказ електронних грошових коштів за допомогою титульних знаків. Шляхом відстеження ланцюжка електронних рахунків, що беруть участь у перерахуванні викрадених грошових коштів, цей фактичний власник рахунку може бути встановлений.

Заподіяння шкоди власнику. Зазначені дані можуть міститися в заяві про злочин; в наданих заявником документах організації; в документах, отриманих від працівників банківської платіжної системи.

Правова охорона інформації, до якої був отриманий доступ сторонніми.

Аналіз кримінальних проваджень засвідчив, що на практиці щодо правової охорони інформації виникають деякі проблеми. Наприклад, інформація про реквізити доступу до рахунку в платіжній системі (логін і пароль) іноді визначається як охоронювана законом комп'ютерна інформація, що може бути правильним тільки в тому випадку, якщо така інформація становить комерційну таємницю, тобто стосовно неї встановлено режим комерційної таємниці (в іншому випадку така комп'ютерна інформація не охороняється законом). Викликає ускладнення й вирішення питання про охорону законом інформації, якою оперує власне платіжна система, а саме титульних знаків. Так, у досліджених нами кримінальних провадженнях переказ титульних знаків з рахунку клієнта без його відома кваліфікувався як готування до вчинення злочину, а сам злочин був вчинений у момент виведення з платіжної системи грошових коштів. Такий підхід ми вважаємо правильним, але він не повною мірою враховує специфіку роботи електронної платіжної системи і статус титульних знаків, які використовуються в ній. За своєю суттю титульні знаки електронної платіжної системи є сурогатом цінних паперів, оскільки спеціально введені як еквівалент вартості і уособлюють її. У цьому випадку предмет злочину (електронні гроші) явний, а вартість усіх переведених на чужий рахунок титульних знаків становить ту суму, яку за них може отримати власник рахунку під час виведення грошових коштів з електронної платіжної системи.

Факт неправомірного доступу до інформації, тобто можливість отримання інформації та її використання. При переказі титульних знаків з рахунку клієнта електронної платіжної системи без його відома невстановлена на цьому етапі особа має можливість отримати інформацію та використати її. Ці дані, як і дані про неправомірність доступу, тобто здійснення доступу з порушенням встановленого в організації або електронній платіжній системі порядку і правил, можуть міститися в

заяві про злочин; у наданих заявником документах організації; в документах, отриманих від працівників платіжної системи.

Модифікація або копіювання інформації. При привласненні грошових коштів з рахунку клієнта електронної платіжної системи не відбувається знищення або блокування інформації, оскільки клієнт платіжної системи після події злочину зберігає повний набір можливостей з керування своїм рахунком. Враховуючи це, відсутній факт порушення роботи ЕОМ, системи ЕОМ або їх мережі.

Важливе значення має джерело та спосіб отримання первинної інформації, яка є підставою початку розслідування цієї категорії злочинів.

На формування слідчих ситуацій при розслідуванні цього виду злочину впливають як об'єктивні, так і суб'єктивні фактори, які залежать від низки чинників, а саме:

– необхідності залучення осіб, що володіють спеціальними знаннями в сфері комп'ютерних технологій, та знаннями порядку і правил обліку фінансово-господарських операцій, що здійснюється автоматизованим способом, в тому числі порядку і правил використання електронних платіжних засобів і систем, під час проведення слідчих (розшукових) дій та оперативно-розшукових заходів;

– потреби вивчення в процесі розкриття цього виду злочину значного обсягу даних, які знаходяться переважно в електронному вигляді; особливе значення при цьому мають дані і регістри про передачу і прийом електронних засобів, інші джерела інформації про переведення або обміні таких засобів [4, с. 92];

– дефіциту часу й динамічності обстановки в мережевому оточенні, пов'язаної з обмеженістю дискової пам'яті серверів, що не дозволяє тривало зберігати технічну інформацію про мережеві взаємодії комп'ютерів, іншу інформацію доказового і орієнтуючого характеру; висока мінливість окремих видів доказів у електронній формі (наприклад, багато масивів службової інформації організовані таким чином, що нова інформація перезаписує стару в безперервному циклі);

– усунення протидії розслідуванню, у процесі якого злочинці здійснюють дії щодо приховування слідів злочину, які знаходяться в електронному вигляді.

Відзначається важлива роль у формуванні слідчих ситуацій об'єктивних факторів, оскільки вони не можуть бути усунуті діями слідчих або оперативних підрозділів. Діяльність правоохоронних органів в умовах нового кримінального процесуального законодавства викрила низку проблемних моментів, що суттєво впливають на результативність роботи слідчих та оперативних підрозділів. Один із них стосується підстав для проведення оперативно-розшукових заходів. Відповідно до статті 6 Закону України "Про оперативно-розшукову діяльність", підставами для проведення оперативно-розшукових заходів оперативними підрозділами Національної поліції України є наявність достатньої інформації, отриманої в установленому законом порядку, що потребує перевірки за допомогою оперативно-розшукових заходів і засобів про кримінальні правопорушення, що готуються; осіб, які готують вчинення кримінального правопорушення [6]. У разі, якщо ознаки кримінального правопорушення виявлено під час проведення оперативно-розшукових заходів, які тривають і припинення яких може негативно вплинути на результати кримінального провадження, підрозділ, що здійснює оперативно-розшукову діяльність, повідомляє відповідний орган досудового розслідування про виявлення ознак кримінального правопорушення, закінчує проведення оперативно-розшукового заходу, після чого направляє зібрані матеріали, в яких зафіксовано фактичні дані про протиправні діяння окремих осіб та груп, відповідальність за які передбачена Кримінальним кодексом України, до відповідного органу досудового розслідування [6]. У процесі виявлення кримінального правопорушення виникає необхідність проведення низки оперативно-розшукових заходів за відсутності всіх елементів кримінального правопорушення (тобто неможливо стверджувати, що в діях особи вбачаються ознаки злочину), що пов'язано зі специфікою вчинення злочинів у сфері банківських електронних платежів, адже до моменту

вчинення злочину особа вчинює легальні дії: отримує навички роботи на комп'ютері, купує певне комп'ютерне обладнання, створює програми для роботи з ним, і тому неможливо стверджувати, що особа готується до вчинення злочину.

Окрім цього, Закон України "Про оперативно-розшукову діяльність" у статті 8 передбачає певні права оперативних підрозділів, які реалізуються шляхом проведення оперативно-розшукових заходів та негласних слідчих (розшукових) дій [6]. Аналізуючи сучасну редакцію зазначеного Закону, можна дійти логічного висновку, що права, зазначені в пунктах, у яких присутнє посилання на конкретну статтю Кримінального процесуального кодексу України [5], можуть бути реалізовані виключно шляхом проведення НС(Р)Д. Тобто в процесі оперативного пошуку, перевірки первинної інформації, а також оперативної розробки осіб, які готують кримінальне правопорушення, можуть реалізуватися виключно права оперативних підрозділів, що зазначені в пунктах статті 8 Закону України "Про оперативно-розшукову діяльність" [6].

Підсумовуючи викладене, зазначаємо, що розслідування злочинів, що вчиняються у сфері банківських електронних платежів, має свої особливості. Визначені ознаки злочинів, що вчиняються у сфері банківських електронних платежів, є практично значимими в діяльності з розслідування злочинів, вчинюваних у сфері банківських електронних розрахунків та платежів. Проаналізовані об'єктивні та суб'єктивні фактори допоможуть працівникам правоохоронних органів ефективно вирішувати організаційні питання щодо розслідування злочинів цієї категорії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Айдемський Є.В.* Боротьба зі злочинами у сфері грального бізнесу: оперативно-розшуковий аспект: дис. ... канд. юрид. наук: 12.00.09. Львів, 2014. 236 с.

2. *Айдемський Є.В. Некрасов В.А.* Взаємодія оперативних підрозділів з іншими правоохоронними та контролюючими органами, установами та організаціями при пошуку та отриманні первинної оперативної інформації про факти та ознаки злочинної діяльності у сфері грального бізнесу. Актуальні проблеми взаємодії оперативних та слідчих підрозділів у протидії організованій злочинності: матеріали Всеукр. наук.-практ. конф. (Одеса, 18 квіт. 2008 р.). Одеса: ОДУВС, 2008. С. 76–85.

3. *Баганець О.* Переваги та недоліки нового КПК. Пропозиції щодо внесення змін та доповнень до нового Кримінального процесуального кодексу України URL: http://www. yurincom. com/ua/ consultation/faq/?id=10636 (дата звернення: 07.03.2018).

4. *Дикова Н.В.* Особенности расследования преступлений, совершенных с использованием электронных платежных средств и систем: дис. ... канд. юрид. наук: 12.00.09. Саратовский юридический институт МВД России, 2011. 227 с.

5. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 р. № 4651-VI. Голос України. 2012. 19 травня (№ 90–91).

6. Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992 року № 2135–XII. Відомості Верховної Ради України. 1992. № 22. Ст. 303.

7. *Топорецька З.М.* Особливості розслідування зайняття гральним бізнесом: дис. ... канд. юрид. наук: 12.00.09. Київ, 2012. 225 с.

REFERENCES

1. *Aidemsky, Y.V.,* 2014, "Fighting Crimes in the Field of Gambling Business: Operational-Search Aspect": thesis ... cand. of jurid. sciences: 12.00.09, Lviv, 236 p.

2. *Aidemsky Y.,V., Nekrasov, V.A.,* 2008, "An Interaction of Operational Units with Other Law Enforcement and Controlling Bodies, Institutions and Organizations in the Search and Reception of Primary Operational Information about the Facts and Signs of Criminal Activity in the Field of Gambling", Actual Issues of an Interaction of Operational and Iinvestigative Units in Counteraction to Organized Crime: materials of All-Ukainian scient.-pract. conf. (Odesa, April 18, 2008), Odesa: ODUVS, 76–85.

3. *Baganets, O.* "The Benefits and Lacks of the New CPC. Proposals for the Amendments and Additions to the New Criminal Procedure Code of Ukraine", URL: http: // www. yurincom com /en/sonsultation/faq/?id=10636 (application date: 07.03.2018).

4. *Dykova, N.V.,* 2011, "Features of Investigation of Crimes Committed by Use of Electronic Payment Means and Systems: thesis ... cand. jurid. sciences: 12.00.09, Saratov Law Institute of the Ministry of Internal Affairs of Russia, 227 p.

5. Criminal Procedural Code of Ukraine: Bill of Ukraine dated April 13, 2012, Voice of Ukraine 90–91.
6. "About Operational Search Activities": Bill of Ukraine dated February 18, 1992 No 2135-XII, Bulletin of the Supreme Soviet of Ukraine 22, 1992. Art. 303.
7. *Toporetsky, Z.M.,* 2012, "Features of the Investigation of Gambling Engagement": thesis ... cand. of legal sciences: 12.00.09, 225 p.

UDC 336.747:004:343.359

V.D. Nykyforchuk,
Chief Specialist of the State Bureau of Investigations, Kyiv,
ORCID ID 0000-0003-4406-7349

FEATURES OF INVESTIGATORS OF CRIMES COMMITTED IN THE SPHERE OF BANK ELECTRONIC PAYMENTS

Paper considers the investigation of peculiarities of the study of crimes committed in the field of bank electronic payments. The legal conflict regarding granting the right of an investigator to carry out investigative actions is analyzed. The signs of a crime in the field of bank electronic payments are investigated. The signs of such an offense include: self-interest; illegal actions and behavior (action) prohibited by law; royalty-free appropriation; seizure and (or) appeal for the benefit of the perpetrator or other persons of the stolen money; damnification of the owner; legal protection of information accessed by third parties; the fact of unlawful access to information with the possibility of obtaining information and its use; modifying or copying information. The objective and subjective factors influencing investigative situations of this category of crime are determined. The formation of investigative situations in the investigation of this type of crime is influenced by both objective and subjective factors, which depend on a number of factors, namely:

– the need to involve persons with special knowledge in the field of computer technologies and knowledge of the procedure and rules for accounting for financial and business operations carried out in an automated way, including the procedure and rules for the use of electronic payment facilities and systems, during the conduct of investigators (detective) actions and operational-search activities;

– the need for studying in the process of revealing this type of crime a large amount of data, which is mainly in electronic form; in this regard, special importance is given to data and registers about the transmission and reception of electronic means, other sources of information on the transfer or exchange of such means;

– a shortage of time and dynamism of the situation in the network environment, due to the limited storage of server memory, which does not allow to keep technical information on network interactions of computers, other information of evidence and orientation; the high variability of individual types of evidence in an electronic form (for example, many arrays of official information are organized in such a way that new information overwrites the old in a continuous cycle);

– an elimination of counteraction to an investigation in which criminals carry out actions to conceal traces of a crime which are in electronic form.

An important role in the formation of investigative situations of objective factors is noted, since they can not be eliminated by the actions of investigators or operational units.

The findings are practically significant in the investigation of crimes committed in the field of banking electronic payments and payments and can help law enforcement officers to deal effectively with organizational issues related to the investigation of crimes in this category.

Keywords: electronic money, pre-trial investigation, signs of a crime, payments, crime detection, investigative (search) actions, investigative situations.

Отримано 13.03.2018