УДК 343.9.024:004.056.5
DOI https://doi.org/10.32782/2524-0374/2022-2/42

ФОРМУВАННЯ ТА РЕАЛІЗАЦІЯ КРИМІНАЛІСТИЧНИХ КОМПЛЕКСІВ НА ПОЧАТКОВОМУ ЕТАПІ РОЗСЛІДУВАННЯ ЗЛОЧИННОЇ ДІЯЛЬНОСТІ ЕКОНОМІЧНОЇ СПРЯМОВАНОСТІ, ВЧИНЕНОЇ ІЗ ВИКОРИСТАННЯМ КІБЕРПРОСТОРУ

FORMATION AND IMPLEMENTATION OF CRIMINAL COMPLEXES AT THE INITIAL STAGE OF INVESTIGATING ECONOMIC CRIMINAL ACTIVITIES COMMITTED WITH THE USE OF CYBER SPACE

Куліуш В.М., аспірант кафедри кримінального процесу
Одеський державний університет внутрішніх справ

У статті наголошено, що протиправні практики у сфері економіки, які вчиняються із використанням кіберпростору мають усі ознаки складної злочинної діяльності. Наголошено на необхідності розроблення відповідних криміналістичних комплексів для оптимізації початкового етапу розслідування таких злочинів, а також визначено чинники, які впливають на формування таких комплексів. Охарактеризовано відповідний криміналістичний комплекс, який пов'язаний із організацією слідчим аналітичної роботи на початковому етапі розслідування. Виокремлено та охарактеризовано блоки завдань, які вирішуються у ході реалізації такого комплексу. Наголошено, що основним завданням реалізації такого комплексу є встановлення сутності події з метою забезпечення правильної кваліфікації злочину. Також, окремо проаналізовано роботу слідчого щодо аналітичної оцінки якості попереднього документування злочинної діяльності. Визначено структурні елементи злочинної діяльності, які підлягають обов'язковому документуванню у межах роботи оперативних підрозділів до початку кримінального провадження.

Крім того, виокремлено та охарактеризовано криміналістичний комплекс пов'язаний із встановленням особи злочинця. Наголошено, що цей комплекс крім слідчих (розшукових) та негласних слідчих (розшукових) дій включає відповідну систему агентурно-оперативних заходів. Визначено основні елементи аналітичної роботи, які передують формуванню такого комплексу. Виокремлено особливості формування типового портрету (моделі) особи, яка здійснює таку злочинну діяльність. Окреслено можливі моделі поведінки, спрямовані на протидію розслідуванню.

Детальна увага приділена аналізу криміналістичного комплексу щодо виявлення та фіксації цифрових доказів. У межах дослідження цих питань проаналізована сутність цифрових слідів, а також особливості формування цифрових доказів. Звернута увага на особливості коректної фіксації цифрових доказів та їх специфічні ознаки.

Ключові слова: криміналістичний комплекс, кіберпростір, злочинна діяльність, аналітична робота, цифрові докази.

The article emphasizes that illegal practices in the economic sphere, which are committed using cyberspace, have all the signs of complex criminal activity. The need to develop appropriate forensic complexes to optimize the initial stage of investigation of such crimes is emphasized, and the factors influencing the formation of such complexes are also determined. The corresponding forensic complex is characterized, which is related to the organization of analytical work by the investigator at the initial stage of the investigation. Blocks of tasks, which are solved during the implementation of such a complex, have been singled out and characterized. It is emphasized that the main task of implementing such a complex is to establish the essence of the event in order to ensure the correct qualification of the crime. Also, the work of the investigator regarding the analytical assessment of the quality of preliminary documentation of criminal activity was analysed separately. The structural elements of criminal activity have been determined, which are subject to mandatory documentation within the scope of work of operational units before the start of criminal proceedings.

In addition, the forensic complex associated with establishing the identity of the criminal is singled out and characterized. It was emphasized that this complex, in addition to investigative (search) and covert investigative (search) actions, includes a corresponding system of agent-operational measures. The main elements of analytical work that precede the formation of such a complex are defined. The peculiarities of the formation of a typical portrait (model) of a person who carries out such criminal activity are highlighted. Possible models of behaviour aimed at countering the investigation are outlined.

Detailed attention is paid to the analysis of the forensic complex for the detection and recording of digital evidence. Within the framework of the study of these issues, the essence of digital traces is analysed, as well as the peculiarities of the formation of digital evidence. Attention is drawn to the features of correct recording of digital evidence and their specific features.

Key words: forensic complex, cyberspace, criminal activity, analytical work, digital evidence.

Вивчення матеріалів оперативно-розшукових справ, кримінальних проваджень та аналітичних матеріалів підрозділів кіберполіції свідчить, що протиправна діяльність у сфері економіки, яка здійснюється із використанням кіберпростору є складною та доволі структурованої формою протиправної соціальної практики, фактично у даному випадку можна говорити про злочинну діяльність. У той же час, слушно зауважити, що досліджуючи проблему злочинності у кіберпросторі науковці, як правило, як сукупність одиничних злочинів, що і зумовлює вибір відповідної методології наукового пізнання проблеми та структуру відповідних практичних рекомендацій. У той же час, на нашу думку, аналізуючи це явище крізь призму категорії "злочинна діяльність" можливо використати більш комплексні та складні теоретико-методологічні конструкції, спрямовані на оптимізацію слідчої діяльності щодо розслідування таких злочинів.

Зважаючи на викладене, вважаємо, що наразі існує теоретико-методологічна необхідність обґрунтування відповідних криміналістичних комплексів, які спрямовані на вирішення комплексних завдань розслідування на відповідних етапах. При цьому, слушно наголосити, що такі криміналістичні комплекси знаходяться у прямій залежності від: *по-перше,* підстав для початку кримінального провадження; *по-друге,* типової слідчої ситуації, яка склалась на відповідному етапі розслідування злочинної діяльності економічної спрямованості, вчиненої із використанням кіберпростору.

Вивчення практики роботи підрозділів кіберполіції свідчить, що кримінальні провадження щодо злочинної діяльності економічної спрямованості, яка здійснюється із використанням кіберпростору у переважній більшості випадків розпочинається за матеріалами оперативних підрозділів, які здійснювали попереднє документування злочинної діяльності, а якість таких матеріалів значним чином залежить від того чи залучався на етапі роботи за оперативно-розшуковою справою слідчий для надання методичної допомоги.

Загалом, необхідно зауважити, що за наявності такої форми початку кримінального провадження перед слідчим постає завдання щодо реалізації певної групи криміналістичних комплексів, які з одного боку є системою завершених дій, а з іншого перебувають відповідних взаємозв'язках між собою. Так, першим таким комплексом є *"Аналітичне опрацювання та оцінка отриманих матеріалів"*. Незважаючи на те, що під час такої діяльності слідчим не проводиться відповідна система слідчих (розшукових) та негласних слідчих (розшукових) дій, у той же час використовуються тактичні прийоми та аналітичні методи спрямовані на оцінку отриманих матеріалів, прийняття первинних тактичних рішень та визначення загальної стратегії розслідування кримінального провадження. Саме тому, на нашу думку, цей організаційно-тактичний блок діяльності слідчого можна визначити як самостійний криміналістичний комплекс. Необхідно наголосити, що незважаючи на зростання ролі комплексної роботи з інформацією під час здійснення досудового розслідування, питання аналітичної роботи слідчого залишається майже недослідженим у межах вітчизняної криміналістичної науки, а аналізується, як правило, крізь призму інформаційно-аналітичного забезпечення розслідування загалом та використання інформаційних систем правоохоронних органів під час досудового розслідування кримінальних правопорушень.

Продовжуючи, на нашу думку, слушно виокремити основні блоки завдань, які вирішуються слідчим під час реалізації вказаного криміналістичного комплексу, зокрема:

по-перше, визначення сутності кримінально-релевантної події, яка охарактеризована у матеріалах оперативного підрозділу. Аналіз практики роботи підрозділів кіберполіції свідчить, що у 87% випадків, направляючи матеріали слідчому працівник оперативного підрозділу вказує відповідну норму кримінального закону та кримінальне правопорушення, задокументоване ним. У той же час, слідчому із метою належної попередньої кваліфікації злочину як такого, що вчинений із використанням кіберпростору слушно проаналізувати наявні матеріали з метою визначення: а) технології злочинної діяльності; б) обстановки вчинення злочину; в) знарядь та засобів, які використовувались для здійснення злочинної діяльності. Зважаючи на складність досліджуваної нами категорії злочинної діяльності здійснюючи попередню діагностику сутності події, слідчому поряд із нормами кримінального закону слушно працювати й з іншими джерелами правової та іншої інформації із використанням аналітичної методології, яка включає використання таких методів як: порівняння, екстраполяція, аналіз, синтез тощо, а додатковими інформаційними джерелами для аналітичного опрацювання є: матеріали архівних та поточних кримінальних проваджень щодо злочинів цієї категорії, а також судова практика у частині кваліфікації різних форм злочинної діяльності економічної спрямованості, яка здійснюється із використанням кіберпростору.

по-друге, встановлення якості попереднього документування злочинної діяльності. Згідно із положеннями відомчих нормативно-правових актів, у ході оперативної розробки забезпечується збір інформації про причетність особи або групи осіб, у тому числі невстановлених, до підготовки вчинення злочину, інші обставини та відомості, що мають значення для попередження і припинення злочину. Також підлягають документуванню виявлені під час оперативної розробки інші злочини, при цьому, крім причетності до його вчинення конкретної особи або групи осіб, фіксується: *по-перше,* час, місце, спосіб учинення злочину; *по-друге,* місцезнаходження знарядь злочину, здобутого злочинним шляхом майна, товарно-матеріальних цінностей, грошей тощо; *по-третє,* місця приховування викрадених документів, майна, предметів, речовин тощо; *по-четверте,* розмір шкоди, заподіяної злочином; *по-п'яте,* інші обставини (спосіб приховування слідів злочину, мотив тощо).

Науковці, аналізуючи особливості оперативної розробки і документування злочинів у сфері економіки, відзначають, що правопорушення цієї категорії відзначаються значною складністю розкриття, тому, що в процесі документування необхідно встановлювати: а) способи вчинення злочинів; б) коло причетних до вчинення злочину осіб, які беруть участь в економічних операціях; в) зв'язок із працівниками фінансово-банківських структур, співробітниками з інших галузей господарювання; г) місце приховування цінностей, коштів, які нажиті злочинним шляхом, забезпечення їх вилучення з метою відшкодування збитків. До основних напрямів документування вказані науковці відносять: а) виявлення предметів і документів, які після проведення у майбутньому процесуальних дій будуть джерелами доказів і забезпечення їх зберігання до моменту початку кримінального провадження; б) встановлення осіб, які мають відомості про протиправні дії розроблюваних і можуть бути допитані як свідки у кримінальному провадженні; в) фіксація протиправних і злочинних дій розроблюваних у процесі їх діяльності[4]. Підтримуючи такий підхід, наголосимо, що під час вирішення цього завдання слідчим з'ясовується рівень попереднього документування відповідної системи обставин, які підлягають встановленню під час розслідування даного виду злочинної діяльності. Аналізуючи якість попереднього документування злочинної діяльності економічної спрямованості, яка вчиняється із використанням кіберпростору, з метою якісного подальшого планування розслідування слідчому слушно акцентувати увагу на таких аспектах: а) документуванні усієї технології злочинної діяльності; б) встановленні під час документування конкретного різновиду апаратних засобів та програмного забезпечення, яке використовувалось для злочинної діяльності. Наголосимо, що особливо вагоме значення встановлення таких даних має у разі документування фактів протиправної діяльності невстановленої особи (групи осіб);

по-третє, виокремлення обставин злочинної діяльності, які потребують першочергової фіксації за допомогою проведення слідчих (розшукових) та негласних слідчих (розшукових) дій. У контексті цього слушно наголосити, що під час такого аналізу та планування основна увага слідчого акцентується на якнайшвидшій фіксації цифрових слідів злочинної діяльності, що зумовлено специфічною природою цифрової інформації та можливістю її безповоротної втрати у разі початку протидії досудовому розслідуванню з боку злочинців та/або їх зв'язків.

Іншим криміналістичним комплексом є *"Встановлення особи злочинця"*, реалізація слідчим якого розпочинається після внесення відомостей до ЄРДР та початку кримінального провадження. Наголосимо, що практика роботи підрозділів кіберполіції, які у своїй оперативно-розшуковій роботі також керуються відповідним спеціальним принципом оперативно-розшукової діяльності – наступальності, свідчить, що і до початку кримінального провадження оперативними підрозділами реалізуються відповідні оперативно-тактичні комплекси, які спрямовані на встановлення осіб причетних до злочинної діяльності економічної спрямованості, яка здійснюється із використанням кіберпростору. Як правило, такі оперативно-тактичні комплекси включають у себе систему агентурно-оперативних та оперативно-технічних заходів, які можуть здійснюватися оперативними підрозділами до початку кримінального провадження.

Водночас, опрацювання матеріалів кримінальних проваджень свідчить, що на початковому етапі розслідування правоохоронним органам невідомі точні установчі дані осіб, які причетні до такої злочинної діяльності, а лише відомі нікнейми, котрі особи використовують для самоідентифікації у кіберпросторі.

Слушно зауважити, що розроблення слідчим внутрішньої структури такого криміналістичного комплексу передує аналітична робота щодо встановлення можливих кореляційних залежностей між: а) технологією злочинної діяльності – особою злочинця; б) предметом злочинного посягання – особою злочинця; в) знаряддями та засобами злочинної діяльності – особою злочинця. Проведення такої аналітичної роботи вирішує декілька завдань на початковому етапі розслідування, зокрема:

по-перше, формування типового портрету (моделі) особи (групи осіб), які могли вчинити таке кримінальне правопорушення. Як відзначає Н.А. Жерж, моделювання властивостей невідомого злочинця, або складання психологічного портрета, здійснюється в умовах гострого дефіциту інформації, на основі поведінкового аналізу наявних слідів і відомих обставин скоєння злочину. Такі моделі дозволяють також на основі відомих взаємозв'язків і кореляційних залежностей прогнозувати і не встановлені властивості, і особливості розшукуваних злочинців, для того щоб зробити портрет більш детальним. Деякі науковці, що займалися проблемою розробки типових моделей створення пошукового портрета злочинця, наводять відомості про його структуру і елементний склад. Структура за пропонованих моделей може мати невеликі відмінності, але практично всі дослідники цього питання виділяють ознаки, що характеризують біологічні, психічні та соціальні складові розшукуваної особи[3].

по-друге, звуження кола осіб, серед яких необхідно здійснювати пошукові заходи та слідчі дії;

по-третє, прогнозування можливих моделей протидії досудовому розслідуванню, зокрема: а) приховування невстановлених епізодів злочинної діяльності; б) знищення елементів слідової картини встановлених фактів злочинної діяльності.

Опрацювання матеріалів кримінальних проваджень щодо злочинної діяльності економічної спрямованості, яка здійснюється із використанням кіберпростору свідчить, що вказаний криміналістичний комплекс поєднує відповідну систему таких слідчих дій як: а) допит; б) огляд; в) тимчасовий доступ до речей та документів; г) зняття інформації з електронних інформаційних систем. Наразі, під час характеристики структури криміналістичних комплексів, ми не акцентуємо увагу на організаційно-тактичних особливостях проведення вказаних слідчих дій, оскільки останні будуть проаналізовані нами у наступних підрозділах дослідження.

Логіка системного розслідування кримінальних проваджень щодо злочинної діяльності економічної спрямованості, яка вчиняється із використанням кіберпростору свідчить, що поряд із вищеописаним криміналістичним комплексом на початковому етапі розслідування першочерговій реалізації підлягає криміналістичних комплекс *"Фіксація цифрових слідів та формування цифрових доказів".* Аналіз наявних монографічних досліджень свідчить, що вченими не приділяється достатньо уваги аналізу сутності цифрових слідів та цифрових доказів, тому, на нашу думку, перед визначенням структури та особливостей реалізації такого криміналістичного комплексу слушно звернути увагу на наявні наукові та практичні підходи щодо сутності цифрових слідів та цифрових доказів. У контексті цієї проблематики, необхідно звернути увагу, що наразі у межах криміналістики не досягнуто доктринальної єдності щодо вибору термінологічної конструкції для позначення специфічних слідів, які утворюються під час злочинної діяльності у кіберпросторі, зокрема на шпальтах наукових видань для позначення цієї категорії використовуються такі термінологічні конструкції, які позначають один і той же об'єкт: "віртуальні сліди", "цифрові сліди", "електроні сліди" тощо. Дослідники звертають увагу, що кіберзлочини характеризуються специфічною картиною слідів. На місці події одночасно зі звичайними слідами мають бути віртуальні сліди, що залишаються у пам'яті електронних пристроїв. Віртуальні сліди являють собою сліди вчинення будь-яких дій в інформаційному просторі комп'ютерних та інших цифрових пристроїв, їх систем та мереж. У теорії криміналістики є різні думки про те, що варто розуміти під віртуальними слідами: 1) віртуальні сліди як зміна автоматизованої інформаційної системи; 2) віртуальні сліди з точки зору фізичної та квантової теорії; 3) віртуальні сліди як результат фізичних та логічних операцій з двійковим кодом тощо[6]. У свою чергу, Н.М. Ахтирська зазначає, що сліди вчинення кіберзлочинів можуть знаходитись не лише безпосередньо в комп'ютерній техніці, на флеш-носіях, а й у кіберпросторі – середовищі (віртуальному просторі), яке надає можливості для здійснення комунікації та реалізації соціальних відносин, комунікаційних систем та забезпечення електронної комунікації з використанням мережі Інтернет, або інших глобальних мереж передачі даних[2].

Як відзначають вчені, електронні сліди – це матеріальні, невидимі сліди, що можуть бути виявлені, зафіксовані та вивчені за допомогою цифрових електронних пристроїв та які містять будь-яку криміналістично-значиму інформацію (відомості, дані), зафіксовану в електронній цифровій формі на матеріальних носіях. Специфічними властивостями електронних слідів є: а) відсутність нерозривного зв'язку із матеріальним носієм; б) динамічність, можливість миттєвого перенесення у просторі; в) можливість зміни й знищення інформації будь-якого обсягу інформації у короткі проміжки часу (також за допомогою віддаленого доступу); г) ідентичність оригіналу інформації та усіх її копій незалежно від виду носія[1].

Як відзначає О.П. Метелев, цифровий слід може складатися з великої кількості окремих інформаційних компонентів, записаних на одному чи кількох машинних носіях (локальних або мережевих), тобто він не має фізично цілісної структури. Також його відображення в кожний конкретний проміжок часу залежить від технічних характеристик пристрою (його апаратне наповнення, операційна система, файлова система тощо), за допомогою якого цей цифровий слід інтерпретується у прийнятний для людини вигляд. Цифрові сліди не належать до матеріальних слідів, адже не мають фізичних властивостей, і не охоплюються поняттям ідеальних слідів, адже вони існують не у свідомості людини, а на певних матеріальних носіях, які можна дослідити тільки за допомогою спеціальних апаратно-програмних комплексів. Таким чином, цифровий слід суттєво відрізняється від традиційних матеріальних слідів, насамперед через свій багатокомпонентний характер. У процесі електронно-цифрового відображення механізм формування цифрового сліду включає дві основні групи компонентів: діяльність людини або обчислювального процесу й апаратно-програмного середовища. Крім того, у цифрових слідах відсутня фізично цілісна структура, вони мають складну інформаційну будову, специфічний механізм слідоутворення, а також сталий зв'язок із матеріальним носієм, на якому містяться. Отже, цілком доцільно було б розглядати цифрові сліди як окрему категорію[5].

Зауважимо, що ми повністю поділяємо підхід щодо необхідності виокремлення цифрових слідів у самостійну категорію поряд з матеріальними та ідеальними слідами, які тривалий час досліджуються та ґрунтовно досліджені у межах криміналістичної науки.

Підсумовуючи викладене, необхідно зауважити, що на початковому етапі розслідування злочинної діяльності економічної спрямованості, вчиненої із використанням кіберпростору доцільним є застосування криміналістичних комплексів варіативність та структура яких залежить від підстав початку кримінального провадження та вихідної слідчої ситуації розслідування, що забезпечує системне та всебічне збирання доказової інформації на початковому етапі розслідування складних форм злочинної діяльності.

ЛІТЕРАТУРА

1. Авдєєва Г.К., Стороженко С.В. Електронні сліди: поняття та види. *Вісник ЛДУВС ім. Е.О. Дідоренка.* 2017. № 1. С. 168-175.
2. Ахтирська Н.М. Актуальні проблеми розслідування кіберзлочинів: навчальний посібник. К. 2018. 229 с.
3. Жерж Н.А. Пошуковий портрет злочинця: зарубіжний та вітчизняний досвід. *Науковий вісник Національного університету ДПС України.* № 2. 2014. С. 172-179.
4. Захаров В.П. Особливості оперативного документування злочинів у сфері економіки: навчально-методичний посібник. Львів. Львівський державний університет внутрішніх справ. 2008. 200 с.
5. Метелев О.П. Гносеологічна і правова природа цифрових доказів у кримінальному процесі. *Правова позиція.* № 1. 2018. С. 75-86.
6. Нейдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. *Підприємництво, господарство і право.* 2019. № 5. С. 304-307.