УДК 343.98.06
DOI https://doi.org/10.32849/2663-5313/2019.8.41

***Олена Самойленко,***
*канд. юрид. наук, доцент,*
*доцент кафедри криміналістики*
*Національного університету «Одеська юридична академія»*

# ВІДКРИТТЯ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ ЩОДО ЗЛОЧИНІВ, ВЧИНЕНИХ У КІБЕРПРОСТОРІ

*У статті з позицій криміналістичної науки характеризуються чотири форми початку кримінального провадження щодо злочинів, що вчиняються у кіберпросторі, зокрема:*

*1) кримінальне провадження розпочинають в результаті отримання заяви потерпілого / повідомлення особи про кримінальне правопорушення;*

*2) кримінальне провадження розпочинають в результаті ознайомлення з матеріалами оперативного підрозділу щодо перевірки оперативної інформації;*

*3) кримінальне провадження розпочинають в результаті роботи за оперативно-розшуковою справою (ОРС);*

*4) кримінальне провадження розпочинають в результаті виявлення безпосередньо слідчим іншого кримінального правопорушення під час здійснення досудового розслідування в уже дорученому для здійснення розслідування кримінальному провадженні. Перша форма властива кожній класифікаційній підгрупі злочинів, вчинених у кіберпросторі. Окрема увага приділяється другій та третій з указаних форм початку кримінального провадження як таким, що свідчать про ключову роль взаємодії слідчого і спеціалізованих оперативних підрозділів у визначенні оптимального моменту початку досудового розслідування. Внесення інформації про злочин до Єдиного реєстру досудових розслідувань цілком залежить від майстерності слідчого / прокурора оцінювати матеріали первинної перевірки. Тому слідчому необхідно орієнтуватися в умовах оперативної обстановки в кіберпросторі для того, щоб рекомендації слідчого можна було реалізувати оперативному співробітнику. Наголошується на проблемі фактичного позбавлення можливості здійснювати оперативно-розшукових заходів під час перевірки оперативної інформації щодо вчинення невеликої або середньої тяжкості злочинів.*

*У результаті розгляду форм автор висновує про те, що більшість випадків кримінальних проваджень даної категорії злочинів відкриваються саме за матеріалами оперативно-розшукової діяльності. Сформульовані автором положення свідчать про потребу поглибленого розгляду питань здійснення оперативно-розшукової діяльності щодо визначеної категорії злочинів та розуміння слідчим специфіки такої діяльності.*

**Ключові слова:** злочин, інформація, кримінальне провадження, кіберзлочин, кіберпростір, оперативно-розшукова діяльність, початок провадження, форма.

**Постановка проблеми.** Специфічність механізму вчинення злочинів у кіберпросторі, зокрема, особливості їх слідів, які можуть бути легко фальсифіковані або взагалі знищені, зумовлює й особливості початку кримінального провадження щодо цих злочинів. У чинному КПК України (ч. 1 ст. 214) визначена правова процедура початку досудового розслідування [1], однак конкретизація специфіки відкриття кримінального провадження щодо певного виду злочинів надасть можливість ефективно використовувати результати оперативно-розшукової діяльності як докази, забезпечить повноту досудового слідства та перспективу судового розгляду матеріалів таких кримінальних проваджень.

**Аналіз останніх досліджень і публікацій з даної теми.** В.А. Журавель відзначає потребу у виділенні самостійного етапу розслідування «відкриття кримінального провадження» [2, с. 141]. Однак більшість науковців, що досліджують методики розслідування окремих видів злочинів, намагаються уникати розгляду питань початку кримінального провадження, не висвітлюючи завдань слідчого з виявлення кримінального правопорушення, сучасних реалій реформування правоохоронних органів і перспектив діяльності «детективів» у структурі Національної поліції України.

**Мета даної статті** полягає у характеристиці основних форм початку кримінального провадження щодо злочинів, вчинених у кіберпросторі.

**Виклад основного матеріалу.** З огляду на особливий комплексний і транснаціо-

нальний характер злочинної діяльності в кіберпросторі, спираючись на класифікаційні підгрупи таких злочинів, на підставі аналізу матеріалів слідчо-судової практики виділимо чотири форми початку кримінального провадження щодо злочинів, вчинених у кіберпросторі.

*1. Кримінальне провадження розпочинають в результаті отримання заяви потерпілого / повідомлення особи про кримінальне правопорушення.* Типова заява складається власником певного інформаційного продукту / майна, особи, що став предметом злочинного посягання, жертвою насильницько-дискримінаційних дій у кіберпросторі, повідомлення особи про кримінальне правопорушення – представником установи-жертви, Інтернет-сервісу, власником вебсайту, що зазнав злочинного впливу. В арсеналі способів дії слідчого є опитування, огляд місця події та організаційні заходи у формі звернення до відкритих джерел інформації з метою підтвердження отриманих відомостей.

Така форма властива кожній класифікаційній підгрупі злочинів, вчинених у кіберпросторі, зокрема: інтелектуальному піратству та злочинам, пов'язаним із комунікаційними діями (90% аналізованих проваджень); злочинам, пов'язаним із насильницько-егоїстичними діями (70%); злочинам, пов'язаним з анархістськими діями в кіберпросторі (40%); злочинам, що спрямовані на заволодіння чужим майном, і пов'язаним із ними злочинам у сфері функціонування електронних розрахунків (40%); злочинам, що пов'язані з насильницько-дискримінаційними діями (40%); злочинам, що порушують механізми захисту від монополізму та недобросовісної конкуренції (25%); злочинам, що порушують встановлений порядок обігу певних речей (10%), і злочинам, що пов'язані з антидержавницькими діями (10%).

Акцентуємо, що під час організації розслідування на підставі неперевіреної, первинної, інформації про злочин слідчому вкрай потрібні знання основ оперативної роботи, адже це, по суті, «безальтернативний» для слідчого шлях розпочати провадження. Часто після відкриття кримінального провадження за ознаками тяжкого або особливо тяжкого злочину, вчиненого в кіберпросторі, суб'єкт, який зазнав шкоди, через небажання розголошувати свою неспроможність захистити інформацію, перспективу втратити довіру клієнтів не бажає співпрацювати зі слідчим. Аналогічно й потерпілі, які на момент подання заяви про кримінальне правопорушення не були обізнані, що «близька» людина (чоловік (дружина), інший член сім'ї), найманий працівник учинили тяжкий злочин проти них. Це провокує створення потужних важелів протидії розслідуванню, для подолання яких слідчий використовує арсенал засобів оперативно-розшукової діяльності.

*2. Кримінальне провадження розпочинають в результаті ознайомлення з матеріалами оперативного підрозділу щодо перевірки оперативної інформації.* Аналіз матеріалів слідчо-судової практики дає підстави для визначення специфіки цієї форми початку кримінального провадження щодо злочинів, вчинених у кіберпросторі. З одного боку, можливість встановлення первинної кваліфікації події за результатами ознайомлення з матеріалами оперативного підрозділу щодо перевірки оперативної інформації надали можливість слідчому внести відповідні дані до ЄРДР і розпочати розслідування щодо: 40% злочинів, що спрямовані на заволодіння чужим майном, і пов'язаних із ними злочинів у сфері функціонування електронних розрахунків; 40% злочинів, пов'язаних з анархістськими діями в кіберпросторі (розділ XVI КК України); 10% злочинів, що порушують встановлений порядок обігу певних речей, і злочинів, пов'язаних із насильницько-егоїстичними діями (ст. 301 КК України); 10% злочинів, пов'язаних із насильницько-егоїстичними діями (ст. 301 КК України). З іншого боку, ці показники поширеності форми мають бути вищими за рахунок показників безальтернативної форми початку провадження, адже в половині аналізованих матеріалів кримінальних проваджень констатовано формалізовану наявність повідомлення про вчинення злочинів, попередження, виявлення та припинення яких належить до завдань Департаменту кіберполіції Національної поліції України. Більшість практиків визначають складність реалізації матеріалів перевірки щодо нетяжких і середньої тяжкості злочинів, вчинених у кіберпросторі. Зазначене зумовлено декількома чинниками.

По-перше, у регіонах України досі немає слідчих або прокурорів, які були б спроможні оцінити достовірність інформації, отриманої під час реалізації заходів ініціативного пошуку в кіберпросторі, що, власне, й здійснюють перевірку оперативної інформації. Спеціалізація слідчих щодо розслідування злочинів цієї категорії регламентована лише на рівні Головного слідчого управління НП України.

По-друге, в умовах надмірного навантаження слідчого / прокурора суб'єкт початку провадження не має часу на пізнання сутності джерела оперативної інформації в кіберпросторі. Тому він з підстав «неможливості здійснити первинну кваліфікацію події» повертає такі матеріали в оперативний

підрозділ з вказівками щодо конкретизації певних обставин події (особи злочинця та мотиву, наслідків вчинення правопорушення, розміру шкоди тощо).

По-третє, оскільки оперативні підрозділи фактично позбавлені можливості здійснювати оперативно-розшукові заходи під час перевірки оперативної інформації щодо вчинення невеликої або середньої тяжкості злочинів, а попередження, виявлення та припинення більшості таких злочинів належать саме до завдань Департаменту кіберполіції, то повернення матеріалів перевірки інформації про них дедалі частіше зводиться до віднесення їх до категорії «латентна злочинність».

Внесення відповідної інформації до ЄРДР цілком залежить від майстерності слідчого / прокурора оцінювати матеріали первинної перевірки. Тому слідчому необхідно орієнтуватися в умовах оперативної обстановки в кіберпросторі для того, щоб рекомендації слідчого можна було реалізувати оперативному співробітнику. Із цих позицій важливим є значення Закону України «Про внесення змін до деяких законодавчих актів України щодо спрощення досудового розслідування окремих категорій кримінальних правопорушень». Із 1 січня 2020 року кримінальні правопорушення поділятимуть на кримінальні проступки і злочини, невеликої та середньої тяжкості злочини буде об'єднано в нову кримінально-правову категорію – «нетяжкі кримінальні правопорушення». Згідно із змінами ст. 12 КК України кримінальним проступком буде дія чи бездіяльність, за вчинення якої передбачено основне покарання у виді штрафу в розмірі не більше ніж три тисячі неоподатковуваних мінімумів доходів громадян або інше покарання, не пов'язане з позбавленням волі. Такі правопорушення розслідуватимуть за спрощеною процедурою здійснення досудового розслідування.

Це нововведення призначене розвантажити слідчих правоохоронних органів, адже провадження щодо проступків здійснюватиме спеціальний суб'єкт – дізнавач, який буде співробітником новоствореного органу дізнання або іншого підрозділу Національної поліції, уповноваженим на здійснення дізнання. З метою спрощення процесу розслідування буде логічним уповноважити на це співробітника оперативного підрозділу, який виявив відповідний факт вчинення проступку та знає обставини його події краще, ніж будь-хто з працівників правоохоронного органу. Однак аналіз санкцій статей КК України засвідчує, що злочини, попередження, виявлення та припинення яких належать до завдань Департаменту кіберполіції, не будуть проступками, більшість із них визначатимуться як «нетяжкі злочини». Тому вони не будуть підслідні суб'єкту здійснення дізнання.

Розв'язанню окресленої вище проблеми реалізації цієї форми початку провадження щодо виявлених кіберполіцейськими злочинів могла б сприяти новація законодавця щодо створення можливостей здійснення розслідування у формі дізнання не лише стосовно проступків, а й щодо нетяжких злочинів. Адже за такої умови кіберполіцейський щодо виявлених ним нетяжких злочинів буде вправі відкривати кримінальне провадження та здійснювати розслідування у формі дізнання.

*3. Кримінальне провадження розпочинають в результаті роботи за оперативно-розшуковою справою (ОРС).*

Робота слідчого в межах ОРС здійснюється в умовах викриття 90% злочинів, вчинених у кіберпросторі з антидержавно-політичних мотивів, 40% злочинів, що порушують встановлений порядок обігу певних речей, і 10% злочинів, пов'язаних з анархістськими діями в кіберпросторі (ч. 2 ст. 361, ч. 3 ст. 362 КК України) та з насильницько-егоїстичними діями (ч. 3 ст. 120; ч. 3–5 ст. 301 КК України). Матеріали оперативно-розшукових заходів слідчий використовує надалі як докази. Це дає підстави стверджувати, що, крім слідчих (розшукових) дій, до комплексу пізнавальних засобів слідчого під час розслідування тяжких та особливо тяжких злочинів, вчинених у кіберпросторі, належатимуть й оперативно-розшукові заходи. Знання оперативних можливостей дасть змогу слідчому на практиці оцінити наявну на момент початку кримінального провадження оперативну ситуацію, обґрунтовано обрати найбільш доцільні комплекси слідчих (розшукових) дій та організаційних заходів на криміналістичних етапах розслідування злочинів, вчинених у кіберпросторі.

*4. Кримінальне провадження розпочинають в результаті виявлення безпосередньо слідчим іншого кримінального правопорушення під час здійснення досудового розслідування в уже дорученому для здійснення розслідування кримінальному провадженні.*

Лише 16% кримінальних проваджень щодо досліджуваної категорії злочинів відкриває слідчий унаслідок здійснення розслідування в іншому кримінальному провадженні, зазвичай випадково, під час виявлення ознак вчинення злочину іншої кваліфікації, під час провадження обшуку, в результаті отримання результатів судової експертизи (зокрема, так виявляються 50% злочинів, що

порушують механізми захисту від монополізму та недобросовісної конкуренції, або злочини, пов'язані з насильницько-дискримінаційними діями; 20% злочинів, що спрямовані на заволодіння чужим майном, і пов'язаних із ними злочинів у сфері функціонування електронних розрахунків; 10% злочинів, що порушують встановлений порядок обігу певних речей, злочинів, пов'язаних із насильницько-егоїстичними діями, і злочинів, пов'язаних з анархістськими діями в кіберпросторі). Тому таку форму початку кримінального провадження складно вважати типовою стосовно злочинів, вчинених у кіберпросторі. З огляду на те, що фактично в кіберпросторі триває багатоепізодна злочинна діяльність, така ситуація спричинена формальним ставленням слідчих до планування розслідування, незалученням до цього процесу потенціалу оперативних підрозділів або перекладанням своїх повноважень щодо здійснення слідчих (розшукових) дій у таких справах на оперативного працівника. Останній часто не втрачає можливості, отримавши за дорученням слідчого інформацію про «можливий» новий епізод злочинної діяльності, перевірити його, що звісно позначається на статистичному показнику щодо суб'єкту виявлення злочину.

Така форма початку провадження реалізується в межах одного з основних завдань розслідування – виявлення всієї сукупності епізодів злочинної діяльності в кіберпросторі, яке виконують шляхом здійснення комплексу слідчих (розшукових) дій та організаційних заходів. Зазначене призводить до реєстрації додаткових епізодів кримінального правопорушення певної правової кваліфікації (залежно від типового поєднання злочинів у злочинну технологію або всієї множини одиничних схожих злочинів).

**Висновки.** Наведені форми початку кримінального провадження щодо злочинів, вчинених у кіберпросторі, свідчать про ключову роль взаємодії слідчого і спеціалізованих оперативних підрозділів у визначенні оптимального моменту початку досудового розслідування. Значною мірою це зумовлено тим, що здебільшого кримінальні провадження цієї категорії відкриваються саме за матеріалами оперативно-розшукової діяльності.

**Список використаних джерел:**

1. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/ laws/ show/4651-17

2. Журавель В. Проблеми періодизації досудового розслідування. *Вісник Національної академії правових наук України*. 2014. № 2 (77). С. 136–143.

*From the standpoint of forensic science, the article describes four forms of commencement of criminal proceedings regarding crimes committed in cyberspace, in particular:*

*1) the criminal proceedings begin as a result of the receipt of the application of the victim / the message of the person about the criminal offense;*

*2) criminal proceedings are initiated as a result of familiarization with the materials of the operational unit for checking operational information;*

*3) criminal proceedings begin as a result of work on the operational-search case;*

*4) criminal proceedings are initiated as a result of the discovery by the investigator of another criminal offense during the conduct of the pre-trial investigation in the criminal proceedings already entrusted for the investigation.*

*The first form is inherent in each classification subgroup of crimes committed in cyberspace. Special attention is paid to the second and third of these forms of commencement of criminal proceedings. They indicate the key role of interaction between the investigator and specialized operational units in determining the optimal moment of the start of the pre-trial investigation. Inclusion of information about a crime in the Unified Register of Pre-Trial Investigations completely depends on the skill of the investigator / prosecutor to evaluate the materials of the primary check. Therefore, the investigator needs to be guided in the operational environment in cyberspace. Names with the recommendations of the investigator can be implemented operational staff. The problem of actual deprivation of the possibility to carry out operational-search measures when checking operational information about the commission of a small or medium gravity of crimes is emphasized.*

*As a result of the examination of the forms, the author comes to the conclusion that most cases of criminal proceedings of this category of crimes are opened precisely from the materials of the operational-search activity. The provisions formulated by the author indicate the need for in-depth consideration of the issues of the implementation of operational-search activities for a certain category of crimes and for the investigator to understand the specifics of such activities.*

**Key words:** crime, information, criminal proceedings, cyberspace, operational-search activity, commencement of production, form.