УДК 343.9.024:004.056.5
DOI https://doi.org/10.32850/sulj.2023.1.14

ХАРАКТЕРИСТИКА СТРУКТУРНИХ ЕЛЕМЕНТІВ ЗЛОЧИННОЇ ДІЯЛЬНОСТІ ЕКОНОМІЧНОЇ СПРЯМОВАНОСТІ, ЯКА ЗДІЙСНЮЄТЬСЯ ІЗ ВИКОРИСТАННЯМ КІБЕРПРОСТОРУ

Куліуш В. М.

У статті надана характеристика елементів злочинної діяльності економічної спрямованості, яка вчиняється із використанням кіберпростору. Звернута увага на наявні дискусійні положення щодо її структурних елементів. Обґрунтовано, що в окремих методиках розслідування використання криміналістичної характеристики є необґрунтованим, а злочину діяльність доцільно аналізувати крізь призму характеристики її структурних елементів. Виокремлено та охарактеризовано типові ознаки злочинної діяльності. Сформульовано визначення економічної злочинної діяльності, яка вчиняється із використанням кіберпростору. На підставі аналізу матеріалів практики, виокремлено структурні елементи злочинної діяльності економічної спрямованості, яка вчиняється із використанням кіберпростору.

Детальна увага приділена стадії формування у особи задуму і умислу на здійснення злочинної діяльності із використанням кіберпростору. Визначено чинники, які впливають на формування умислу і задуму та надано їх детальну характеристику. Охарактеризовані етапи формування умислу та задуму на вчинення злочинів цієї категорії. Визначено важливість аналізу стадії формування умислу та задуму для своєчасного виявлення та припинення такої злочинної діяльності. Ґрунтовно проаналізовано стадію підготовки до здійснення такої злочинної діяльності, зокрема окрема увага звернута на форми та способи залучення фахівців у галузі високих інформаційних технологій до вчинення таких злочинів, а також особливості підбору знарядь та засобів злочинної діяльності. Окремо проаналізовано формування злочинних груп спрямованих на здійснення злочинної діяльності економічної спрямованості із використанням кіберпростору. Детально досліджено стадію приховування вказаної злочинної діяльності, а також окремі елементи протидії її виявленню та розслідуванню.

Окрема увага звернута на те, що злочинці з високим рівнем підготовки використовують універсальні способи приховування злочинної діяльності та надано характеристику таких способів.

Ключові слова: *злочинна діяльність, кіберпростір, злочини економічної спрямованості, структура злочинної діяльності, спосіб вчинення злочину, приховування злочину, високі інформаційні технології.*

Kaliush V. M. Characteristics of the structural elements of criminal activities of economic direction which is carried out with the use of cyber space

The article provides a description of the elements of criminal activity of economic orientation, which is committed using cyberspace. Attention is drawn to the existing debatable provisions regarding its structural elements. It is substantiated that in some methods of investigation, the use of forensic characteristics is unfounded, and it is advisable to analyse the activity of a crime through the prism of the characteristics of its structural elements. Typical signs of criminal activity are identified and characterized. The definition of economic criminal activity, which is committed using cyberspace, is formulated. Based on the analysis of practice materials, the structural elements of criminal activity of an economic orientation, which is committed using cyberspace, are singled out.

Detailed attention is paid to the stage of formation of a person's plan and intent to carry out criminal activity using cyberspace. The factors that influence the formation of intention and intention are determined and their detailed characteristics are provided. The stages of forming the intention and plan to commit crimes of this category are characterized. The importance of analysing the stage of formation of intent and design for the timely detection and termination of such criminal activity is determined. The stage of preparation for carrying out such criminal activity is thoroughly analysed, in particular, special attention is paid to the forms and methods of involving specialists in the field of high information technologies to commit such crimes, as well as the peculiarities of the selection of tools and means of criminal activity. The formation of criminal groups aimed at carrying out economic-oriented criminal activities using cyberspace is separately analysed. The stage of concealment of the specified criminal activity, as well as individual elements of countermeasures against its detection and investigation, were investigated in detail.

Particular attention is paid to the fact that criminals with a high level of training use universal methods of concealing criminal activity, and a description of such methods is given.

Key words: *criminal activity, cyberspace, crimes of economic orientation, structure of criminal activity, method of committing a crime, hiding a crime, high information technologies.*

Постановка проблеми. Необхідно зауважити, що у сучасній криміналістичній доктрині криміналістична характеристика злочинів розглядається як невід'ємна складова методики розслідування та має у відповідній методиці розслідування своє функціональне призначення. Так, професор В.В. Тіщенко в структуру окремих методик розслідування пропонує включати такі елементи: 1) криміналістичну класифікацію злочинів конкретної категорії; 2) криміналістичну характеристику таких злочинів; 3) обставини, що підлягають установленню; 4) особливості початкового етапу розслідування та типові вихідні слідчі ситуації; 5) типові стратегічні й тактичні завдання та слідчі версії на початковому етапі розслідування; типові програми розслідування, що містять засоби й методи розв'язання поставлених завдань і перевірки версій, форми взаємодії з оперативними підрозділами; 6) типові слідчі ситуації та програми розслідування на його наступному й завершальному етапах; 7) організаційно-тактичні й техніко-криміналістичні особливості проведення слідчих дій і тактичних операцій у розслідуванні злочинів відповідної категорії [6].

Зауважимо, що дана наукова категорія безумовно є ефективною під час формування видових методик розслідування злочинів. У той же час, наголосимо, що в окремих випадках, зокрема й під час розроблення методик розслідування високотехнологічних злочинів, доволі складно системно та об'єктивно описати усі структурні елементи криміналістичної характеристики у контексті її традиційного розуміння у науковій доктрині.

Зважаючи на це, на нашу думку, у межах нашого дослідження доцільно використати інший методологічний підхід та розкрити сутність досліджуваної нами форми злочинної діяльності крізь призму аналізу її етапної структури.

Аналіз останніх досліджень та публікацій. Останніми роками питання структури злочинної діяльності у кіберпросторі досліджували Р. В. Бараненко, І. О. Воронов, В. Д. Гавловський, М.О. Кравцова, О.А. Самойленко, М.І. Саєнко, В.В. Сеник, О.С. Тарасенко, С.О. Харін, Д.М. Цехан, Ю.Є. Якубівська та інші науковці. У той же час, необхідно відзначити, що структура злочинної діяльності економічної спрямованості, яка здійснюється із використанням кіберпростору не досліджена вченими на достатньому рівні і потребує додаткового аналізу.

Мета статті. Метою статті є формування на основі наукових джерел та матеріалів практики типової структури злочинної діяльності економічної спрямованості, яка вчиняється із використанням кіберпростору на характеристика її структурних елементів.

Виклад основного матеріалу. Так, перш за все, спираючись на теоретичні положення, а також матеріали практики, на нашу думку, слушно виокремити типові ознаки злочинної діяльності, які відрізняють останню від одиничного злочину. Так, вважаємо, що до типових ознак злочинної діяльності потрібно відносити такі:

по-перше, наявність прямого умислу, попереднього задуму та повноструктурного способу (технології) досягнення злочинної мети;

по-друге, вчинення на різних стадіях реалізації злочинного умислу дій, які утворюють самостійні склади злочинів. У контексті цього, необхідно відзначити, що такі дії можуть бути вчиненими не безпосередньо суб'єктом, а й іншими особами, але вони мають бути спрямованими на забезпечення реалізації злочинного задуму суб'єкта у межах здійснення конкретної форми злочинної діяльності;

по-третє, систематичне вчинення конкретних дій для досягнення злочинного результату та їх відтворення у разі успіху;

по-четверте, наявність у суб'єкта стратегічної злочинної мети на яку спрямована злочинна діяльність, наприклад побудова кримінальної кар'єри та досягнення відповідного статусу у злочинному середовищі. Принагідно відзначити, що загалом концепт побудови кримінальної кар'єри досліджувався лише крізь призму загальнокримінальної злочинності, зокрема діяльності рецидивістів та лідерів кримінального середовища. Водночас, вивчення практики протидії злочинності, яка вчиняється у кіберпросторі свідчить, що для осіб, які здійснюють таку злочинну діяльність також є прагнення до побудови кримінальної кар'єри у своєму середовищі про що свідчить наявність "рейтингів" хакерів тощо;

по-п'яте, створення інфраструктури для забезпечення своєї злочинної діяльності, зокрема встановлення корумпованих зв'язків тощо;

по-шосте, вчинення злочинної діяльності групою осіб. У той же час, необхідно зауважити, що дана ознака може розглядатись як факультативна, оскільки автономна злочинна діяльність у кіберпросторі є доволі розповсюдженою.

Зважаючи на викладене, на нашу думку, *економічна злочинна діяльність у кіберпросторі* – це систематична, багатоетапна протиправна діяльність особи (групи осіб), яка здійснюється за допомогою використання високих інформаційних технологій, забезпечується створенням необхідної інфраструктури і спрямована проти функціонування фінансово-економічної системи держави, фінансової діяльності юридичних та фізичних осіб.

Вважаємо, що подальший аналіз досліджуваної нами злочинної діяльності слушно здійснювати крізь призму характеристики її етапі, зокрема: *по-перше*, формування задуму щодо здійснення злочинної діяльності; *по-друге*, підготовка до здійснення злочинної діяльності; *по-третє*, безпосереднє здійснення злочинної діяльності; *по-четверте*, приховування слідів злочинної діяльності.

Опрацювання матеріалів практики свідчить, що ***формування у особи задуму та умислу*** на здійснення злочинної діяльності із використанням кіберпростору перебуває у прямій залежності із такими чинниками:

по-перше, рівень професійних знань та навичок особи щодо організації фінансово-економічних процесів у кіберпросторі та можливостей використання кіберпростору як інфраструктурної складової для здійснення злочинної діяльності;

по-друге, можливість застосування особою наявних у нього знань та навичок у легальній сфері. У даному випадку необхідно звернути увагу на наявність прямої залежності між рівнем кваліфікації та рівнем оплати праці;

по-третє, становище особи у професійній спільноті та входження до груп, які керуються відповідною субкультурою.

Так, проведене нами дослідження свідчить, що формування задуму на вчинення злочинної діяльності економічної спрямованості із використанням кіберпростору як система мислинєво-конклюдентних актів охоплює:

а) формування установки на вчинення діяння, відповідальність за яке передбачена за законодавством. У даному випадку мова йде про формування у особи загальної установки щодо можливості порушення закону як прийнятної форми соціальної практики;

б) розумова оцінка своїх компетентностей та реальної можливості здійснення злочинної діяльності економічної спрямованості із використанням кіберпростору;

в) оцінка ризиків та переваг від здійснення злочинної діяльності економічної спрямованості із використанням кіберпростору;

г) остаточне формування умислу та задуму (моделі) подальшої злочинної діяльності економічної спрямованості із використанням кіберпростору.

Аналіз практики роботи підрозділів кіберполіції свідчить, що розуміння структури формування у особи умислу та задуму на вчинення злочинів економічної спрямованості із використанням кіберпростору має важливе значення у контексті виявлення таких осіб у межах організації оперативного обслуговування окремих напрямів та ліній роботи, а також оперативного (ініціативного) пошуку, оскільки формування умислу та задуму злочинної діяльності доволі часто крім психологічно-мисленої діяльності супроводжується вчиненням певних конклюдентних дій особи у відповідному середовищі.

Продовжуючи аналіз, необхідно звернути детальну увагу також ***на стадію підготовки*** до здійснення злочинної діяльності економічної спрямованості із використанням кіберпростору. Необхідно зауважити, що у межах криміналістики питання підготовки до вчинення злочину досліджені на теоретичному рівні значно ґрунтовніше аніж проблематика формування злочинного задуму, зокрема й щодо злочинів, які вчиняються із використанням можливостей кіберпростору крізь призму аналізу способів вчинення таких злочинних діянь [5; 2; 1; 3; 7].

Так, першим структурним елементом злочинної діяльності економічної спрямованості, яка вчиняється із використанням кіберпростору є вибір об'єкта злочинного посягання, що передбачає детальне вивчення інфраструктури його обслуговування. Необхідно зауважити, що на цій стадії особами можуть додатково залучатись й інші фахівці у сфері високих інформаційних технологій, якщо у суб'єкта (суб'єктів) злочинної діяльності недостатньо власних компетенцій для вирішення цього завдання. Опрацювання матеріалів практики свідчить, що існує декілька типових способів залучення фахівця на даній стадії:

- фахівець у сфері високих інформаційних технологій надаючи консультативні послуги не знає, що приймає участь у підготовці вчинення злочинів;

- фахівець у сфері високих інформаційних технологій надаючи консультаційні послуги знає, що приймає участь у підготовці злочину.

Вивчення матеріалів практики та спеціалізованих видань свідчить, що пошук потенційного об'єкта злочинного посягання відбувається шляхом сканування мережі Інтернет за допомогою спеціалізованого програмного забезпечення. При цьому, як свідчить опитування працівників оперативних підрозділів у 92% випадків виявити підготовчі дії щодо вчинення злочину за допомогою технічних засобів фактично неможливо і тому у даному випадку ефективним є проведення традиційних оперативно-розшукових заходів.

У типовий набір фахівця у сфері високих інформаційних технологій, який використовується під час вивчення об'єкта злочинного посягання входять: сканери телефонних ліній; зломувачі та генератори паролів, засоби шифрування, а також цілі програмні пакети, які комплексно автоматизують операції зломів (наприклад, CiberKit). Традиційно злочинцями для визначення апаратних засобів, які мають модемний вхід використовується спеціалізоване програмне забезпечення (PhoneSweep, Tolenoc), які поступово встановлюють зв'язок з телефонними номерами, які знаходяться у відповідному діапазоні. Номери на які відкликається модем реєструються у відповідному файлі (аналогічні методи використовуються для виявлення уразливих місць комп'ютерів, які підключені до Інтернету). Досить часто з цією метою використовуються стандартні програми пошуку уразливості мережі і скануючі програми, які поступово підбирають усі можливі точки доступу до системи з метою визначення найоптимальнішого варіанту проникнення.

Серед найпоширеніших інструментів необхідно також виділити сканери портів комп'ютера, які в автоматичному режимі запитують кожен порт комп'ютера з'ясовуючи, який з них є відкритим. У даному випадку комп'ютер автоматично відправляє звіт, надаючи необхідну для аналізу інформацію. Таке "зондування" портів дозволяє виявити ті з них, які є найуразливішими для атак.

Наступним етапом є ***формування групи та підготовка засобів***. Аналізуючи цей етап, особливої уваги заслуговує методика втягнення у злочинну діяльність персоналу установ чи організацій, де планується вчинення злочину. Вивчення кримінальних проваджень свідчить, що залучення персоналу до злочинної діяльності відбувається з використанням: погроз (застосування фізичного насильства, оприлюднення компрометуючих матеріалів тощо); підкуп (традиційно використовується стосовно працівників професійної ланки, які мають відповідний доступ, а також осіб, у яких є фінансові проблеми); інші чинники (інтимні стосунки зі злочинцем, помста керівництву, самоствердження тощо).

Вважаємо, що способи сприяння персоналу установи (організації) злочинцям можна згрупувати у три блоки: умисне невжиття заходів щодо збереження паролів, іншої конфіденційної інформації та розголошення відомостей, щодо конфіденційної інформації, яка знаходиться у мережі; невиконання належних заходів захисту, зокрема допуск до роботи у локальних мережах сторонніх осіб; неповідомлення керівництву чи правоохоронним органам про виявленні ознаки злочинної активності у мережі.

Безперечно, що основним етапом є ***безпосередня реалізація злочинного задуму***. Зважаючи на те, що спектр розглядуваних діянь є досить широким, проаналізуємо типові способи реалізації найбільш типових форм злочинної діяльності економічної спрямованості, яка здійснюється із використанням кіберпростору.

Аналіз матеріалів практики свідчить, що у моделі, які застосовуються злочинцями для приховування злочинної діяльності економічної спрямованості, яка вчиняється із використанням кіберпростору значною мірою корелює із рівнем кваліфікації злочинців. Так, особи які мають високий рівень підготовки та компетентностей використовуються *універсальні способи* приховування злочинної діяльності сутність який полягає у приведенні відповідної інформаційної системи та середовища вчинення злочину до попереднього стану. Такі способи приховування характерні для злочинів під час яких відбувається незаконне заволодіння невеликими по відношенню до обігу фінансової установи сумою коштів та спрямовуються на: а) суттєве відтермінування виявлення злочину, оскільки незаконне заволодіння такими сумами у разі продовження нормально функціонування інформаційної системи залишається непомітним; б) забезпечення можливості у разі не виявлення факту вчинення злочину в подальшому вчинити новий злочин у вказаній інформаційній системі; в) фактичне знищення усіх слідів злочинної діяльності. Використання таких універсальних способів приховування злочинної діяльності економічної спрямованості супроводжується, як правило, застосуванням спеціалізованого програмного забезпечення – rootkit, яке може використовуватися й на інших стадіях злочинної

діяльності. Характерною особливістю способів приховування (маскування) злочинної діяльності економічної спрямованості, яка вчиняється із застосуванням кіберпростору є застосування електронного блокування, яке може використовуватись і під час безпосереднього вчинення злочинних дій і спрямовується на відволікання служб захисту інформації від основного задуманого кримінального правопорушення. Сутність таких дій полягає в одночасному блокуванні системи значною кількістю користувачів із різних місць, тому, як правило, використання такого способу приховування та маскування характерне для злочинної діяльності, яка вчиняється в організованій формі.

У контексті цього слушно також підтримати позицію О.С. Тарасенка, який відзначає, що на заключній стадії злочинної діяльності використовуються способи зачистки до яких дослідник відносить: а) способи видалення змін у системі: використання програм віддаленого адміністрування комп'ютерної системи; використання виявлених під час підготовки та вчинення злочину "потайних ходів" в системі для доступу для необхідних ресурсів; б) способи руйнації комп'ютерної інформації: використання руйнівних програмних вірусів; використання програм форматування носіїв інформації [4].

Висновки. Підсумовуючи викладене, необхідно відзначити, що, на нашу думку, використання методологічного підходу щодо аналізу злочинної діяльності економічної спрямованості, яка вчиняється із використанням кіберпростору крізь призму структури останньої є ефективнішим ніж використання криміналістичної характеристики як інформаційної моделі для опису цього явище. Типова структура злочинної діяльності економічної спрямованості охоплює такі етапи: *по-перше*, формування задуму щодо здійснення злочинної діяльності; *по-друге*, підготовка до здійснення злочинної діяльності; *по-третє*, безпосереднє здійснення злочинної діяльності; *по-четверте*, приховування слідів злочинної діяльності. Вказані етапи перебувають у кореляційних залежностях між собою, а їх внутрішня структура зумовлюється видом злочинної діяльності.

Література

1. Кримський Т.С. Способи вчинення злочинів, пов'язаних із несанкціонованим доступом до комп'ютерних мереж та мереж електрозв'язку. *Юридична наука*. 2020. №7. С. 331-338;

2. Марков В.В. Про механізми скоєння злочинів у кіберпросторі та особливості їх кваліфікації. *Південноукраїнський правничий часопис*. 2013. №1. С. 112-115;

3. Пушина Н.Л. Способи вчинення незаконних операцій із використанням платіжних карток та інших засобів доступу до банківських ресурсів, електронних грошей, обладнання для їх виготовлення. *Науковий вісник Ужгородського національного університету*. 2020. Серія. Право. Випуск. 61. Том. 2. С. 112-115

4. Тарасенко О.С. Теорія та практика протидії кримінальним правопорушенням, пов'язаним з обігом протиправного контенту у мережі Інтернет : монографія. Одеса : Видавничий дім «Гельветика». 2021. 426 с.

5. Телійчук В.Т. Способи вчинення злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку і засади протидії. *Держава та регіони*. Сер. Право. 2014. №2. С. 31-37;

6. Тіщенко В.В. Структура окремих криміналістичних методик. Криміналістика : підручник. Одеса : Видавничий дім "Гельветика". 2017. С. 352-361

7. Фінагеєв В.О. Способи вчинення злочинів, пов'язаних з використанням засобів доступу до банківських ресурсів. *Науковий вісник Національної академії внутрішніх справ*. №1. 2016. С. 63-82;

Куліуш В. М.,
аспірант кафедри кримінального процесу
Одеського державного університету
внутрішніх справ