УДК 343.985

МІСЦЕ КІБЕРПРОСТОРУ У СИСТЕМІ ОБСТАНОВКИ ЗЛОЧИНУ

Динту В.А., к. ю. н.,
доцент кафедри криміналістики
Інститут кримінальної юстиції
Національного університету «Одеська юридична академія»

У статті автор досліджує кіберпростір як частину обстановки злочину. Розглядає структурні елементи кіберпростору як системи відповідного середовища, де вчиняються дії з підготовки, реалізації та приховування злочину. Наводить свої міркування щодо алгоритмізації дій слідчого при дослідженні кіберпростору у кримінальному провадженні та пропонує відповідні засоби його пізнання.

Ключові слова: *кіберпростір, обстановка злочину, криміналістична характеристика злочинів, слідчі (розшукові) дії.*

В статье автор исследует киберпространство как часть обстановки преступления. Рассматривает структурные элементы киберпространства как системы соответствующей среды, где совершаются действия по подготовке, реализации, сокрытию преступления. Анализирует необходимость алгоритмизации действий следователя при исследовании киберпространства в уголовном производстве и предлагает соответствующие средства его познания.

Ключевые слова: *киберпространство, обстановка преступления, криминалистическая характеристика преступлений, следственные (розыскные) действия.*

Dyntu V.A. CIBERSPACE AS CRIME SITUATION

The article explores cyberspace as part of the crime situation, considering the structural elements of cyberspace as systems where particular actions are committed, namely preparation, implementation and concealing the crime.The author introducces observations on the proper algorithm of actions and suggests eligible methodsfor the conduction of criminal investigation.

Key words: *cyberspace, situation of crime, criminological characteristics of crime, investigative actions.*

Постановка проблеми. Кримінальні правопорушення є найбільш негативним, аморальним і загально небезпечним явищем у житті сучасного суспільства. Вони спричиняють деструктивні наслідки для держави, суспільства та окремо взятої людини. Злочинна діяльність значно впливає, тією чи іншою мірою, на всі соціальні інститути, детермінуючи тим самим дисфункцію останніх. Соціальна та економічна криза, що спостерігається останнім часом в Україні, зумовила появу ряду факторів, що призвели до стійкої тенденції зростання кількості кримінальних правопорушень, внаслідок чого питання боротьби зі злочинністю набули особливої актуальності.

Вказані фактори зумовлюють необхідність подальшого глибокого вивчення злочинної діяльності, що дає змогу підвищити ефективність рекомендацій з її виявлення, розслідування та запобігання.

Ступінь розробленості проблеми. Розробками проблем поняття та значення обстановки злочину займалися такі вчені, як Т.С. Аннєнкова, С.І. Аннєнков, О.В. Жоголєва, І.М. Букаєва, В.Ф. Єрмолович, В.І. Куліков, Л.О. Щербич та ін.

Проте на теперішній час у криміналістиці відсутнє комплексне дослідження саме кіберпростору як обстановки злочину і потужного та змістовного джерела криміналістично значущої інформації у відповідному кримінальному провадженні.

Мета дослідження: визначення місця кіберпростору у системі обстановки злочину та способи і засоби його ефективного пізнання.

Виклад основного матеріалу. Слід зазначити, що розвиток комп'ютерних технологій впливає на появу нових форм взаємодії між членами суспільства. З'являється простір, у якому людина отримує доступ до безмежних інформаційних потоків, тим самим розширюючи можливість вчинення нових форм та видів злочинів як одного із проявів людської діяльності, що реалізується у відповідному інформаційному просторі – кіберпросторі.

Указом Президента України від 15 березня 2016 року «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України (далі – Стратегія)» передбачено необхідність створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Таким чином, наразі на законодавчому рівні визначено наявність такого середовища людської діяльності, як кіберпростір, та сформульовано загальні завдання, з якими законодавець пов'язує забезпечення безпеки функціювання та використання кіберпростору. Зокрема, Стратегія передбачає посилення спроможностей суб'єктів сектору безпеки та оборони для забезпечення ефективної боротьби із кіберзлочинністю. Отож, законодавець в кіберпросторі вбачає певне середовище, в якому можуть бути вчинені відповідні кримінальні правопорушення, та визначає необхідність його використання.

Слід зазначити, що кіберпростір не варто ототожнювати із поняттям Інтернет. Відповідно до ст. 1 Закону України «Про телекомунікації» Інтернет – всесвітня інформаційна система загального доступу, яка логічно пов'язана глобальним адресним простором

та базується на Інтернет-протоколі, визначеному міжнародними стандартами.

З наведеного вище вбачається, що кіберпростір утворюється за допомогою технічних систем, в ньому циркулюють або зберігаються відповідні дані. Таким чином, кіберпростір може утворюватись як за допомогою Інтернет-мережі та безпосередньо у ній функціонувати, так і бути автономною системою, яка не пов'язана із глобальною мережею.

Наразі кіберпростір у певних сферах людської діяльності використовується як середовище для реалізації кримінальних правопорушень і потребує ретельного вивчення крізь призму його розуміння у якості обстановки злочину.

Обстановка злочину є одним із основних елементів криміналістичної характеристики злочинів, оскільки вона суттєво впливає на поведінку злочинця та вибір ним об'єкту злочину, способу та засобів його вчинення. Говорячи про місце обстановки злочину в системі криміналістичної характеристики злочинів, слід відзначити методологічний принцип взаємної детермінації обстановки та інших елементів криміналістичної характеристики злочинів.

Розуміння обстановки злочину можна здійснювати на теоретичному та практичному рівнях. На теоретичному рівні поняття обстановки злочину є системою типових даних стосовно факторів об'єктивної реальності, що визначають сукупність умов, в яких відбувався процес підготовки, реалізації та приховування кримінального правопорушення, та які знаходять своє відображення й оцінку у системі криміналістичної характеристики злочинів. На практичному рівні обстановка злочину – це середовище, в якому вчинялися дії з підготовки, реалізації та приховування злочину, яке має бути дослідженою, проаналізованою та зафіксованою з метою забезпечення швидкого, повного та ефективного розслідування кримінальних правопорушень.

Спираючись на дані узагальнення слідчої практики, можна констатувати, що між обстановкою злочину та іншими елементами криміналістичної характеристики злочинів (особа злочинця, об'єкт злочину, спосіб злочину) наявні причинно-наслідкові, функціональні, ймовірнісні, а також кореляційні зв'язки. Це дає змогу обґрунтовано конструювати версії щодо особи злочинця та обставин кримінального правопорушення, цілеспрямовано здійснювати пошук слідів та інших доказів та їх джерел, приймати правильне рішення тактичного і процесуального характеру.

Вбачається, що дослідження обстановки злочину надає можливість виявити, зібрати, зафіксувати та оцінити доказову інформацію з метою її використання у процесі розслідування злочину. Вона є одним із першоджерел для процесуальних джерел доказів у формі речових доказів, документів, показань, висновків експертів. За допомогою доказової інформації, яку містить обстановка злочину, стає можливим встановити обставини, що підлягають доказуванню у кримінальному проваджені та закріплені у кримінальному процесуальному законодавстві.

За своєю природою кіберпростір відповідає ознакам обстановки злочину, що визначається як система факторів об'єктивної реальності, в якій відбувався процес підготовки, вчинення та приховування злочину.

Оскільки кіберпростір може бути визнаний у якості матеріального середовища, що слугує відповідним «майданчиком» для реалізації кримінальних правопорушень, то доцільно було б розглянути питання можливості його дослідження у рамках відповідного кримінального провадження як обстановки злочину.

Вбачається, що кіберпростір може виступати як обстановка одного акту реалізації злочинного діяння, тобто бути або місцем, де відповідний злочин готувався, або місцем безпосереднього його вчинення, або приховування слідів вчинення злочину. Також може зустрічатись структура із двоелементного складу реалізації злочинного діяння, тобто кіберпростір може бути середовищем, де відбувалась підготовка та вчинення злочину; вчинення та приховування злочину, або підготовка та приховування.

Існування кіберпростору пов'язане із фізичними мережевими об'єктами (комп'ютерами, серверами, мережевим обладнанням). При розслідуванні злочину, що був реалізований у кіберпросторі, вказані вище об'єкти будуть виступати у якості носіїв матеріально-фіксованих слідів злочину. Таким чином, обстановка кіберпростору включає в себе матеріальне середовище, тобто сукупність пов'язаних між собою об'єктів, явищ і процесів матеріального світу, в яких вчинялись дії з підготовки, реалізації та приховування злочину.

До структури матеріального середовища кіберпростору можна віднести наступні елементи:

– інформаційно-обчислювальні системи, сервери, засоби підтримки їх належного функціонування;

– безпосередньо самі обчислювальні машини та їх відповідні системи, різноманітні гаджети, смартфони, технічні засоби, що застосовуються для зберігання, резервного копіювання, переносу і обміну відповідними даними (USB флеш-накопичувач, зовнішній жорсткий диск та ін.);

– канали передачі даних;

– сама інформація у формі сигналу або комплексу сигналів, що можуть бути сприйняті відповідними системами для їх використання за функціональним призначенням тощо.

Вважається доцільним розглянути можливість комбінованої обстановки злочину, у структуру якої буде входити кіберпростір та об'єктивна матеріальна обстановка. Тобто для вчинення злочину злочинець використовує об'єкти реального світу, поєднуючи їх із відповідним кіберпростором.

Слід зазначити, що за допомогою кіберпростору виникло нове соціальне середовище, яке для комунікації використовує технічні системи та мережу Інтернет (наприклад, соціальні мережі VK, Facebook та ін.). Соціальні мережі призначені для формування та організації соціальних взаємозв'язків в Інтернеті. Тобто, розглядаючи соціальні мережі як фор-

му комунікації відповідних соціальних груп, можна говорити про те, що за їх допомогою також можуть вчинятися відповідні злочини.

Обстановка кіберпростору включає в себе і мікросоціальне середовище, тобто певну інфраструктуру, що являє собою безпосереднє соціальне оточення кримінального правопорушення на стадії його готування, реалізації та приховування.

При здійсненні комунікації між суб'єктами у мікросоціальному середовищі кіберпростору виникають певні психологічні стани, формується відповідний настрій, налагоджуються стосунки. Слід зазначити, що інформація, яка міститься у кіберпросторі, може впливати на психічний стан особи, яка у ньому знаходиться, та координувати її поведінкові акти. Тобто у кіберпросторі може бути реалізований відповідний психологічний вплив, тиск, а також маніпулювання як однією особою, так і відповідними людськими групами.

Вказане вище дає змогу прийти до висновку, що у обстановці кіберпростору також простежується наявність морально-психологічного середовища, яке проявляється у сукупності психологічних та моральних станів, настроїв, стосунків між користувачами кіберпростору у період підготовки, вчинення або приховування злочину.

З наведеного вбачається, що кіберпростір є обстановкою злочину, структура якої складається із матеріального, мікросоціального та морально-психологічного середовища, у якому вчинялись дії із підготовки, реалізації, приховування злочину. Дослідження кіберпростору у процесі розслідування може надати слідчому комплекс криміналістично значущої та доказової інформації для ефективного та оперативного розслідування та встановлення фактичних обставин певного кримінального провадження.

Основним джерелом інформації, що міститься в обстановці злочину, є слід. Дослідження кіберпростору як одного із структурних елементів обстановки злочину детермінує необхідність у відокремленні слідової картини, що у ньому міститься.

Аналіз слідової картини при реалізації злочину у кіберпросторі надає можливість визначити появу нового виду сліду, носієм якого не є матеріальні об'єкти або свідомість та пам'ять людини; він відображається у відповідному технічному засобі (комп'ютер, гаджет, смартфон та ін.), програмі, системі, мережі тощо. Вказаний вид сліду у науковій літературі прийнято називати «віртуальним слідом». Віртуальні сліди розглядаються як будь-яка зміна стану автоматизованої інформаційної системи (утвореного нею «кібернетичного простору»), пов'язана з подією злочину та зафіксована у вигляді комп'ютерної інформації (тобто інформації у вигляді, придатному для машинної обробки) на матеріальному носії, у тому числі й на електромагнітному полі [5, с. 21].

Слід зазначити, що «віртуальні сліди» є досить складним об'єктом, який має бути досліджений в результаті здійснення слідчим пізнавальної діяльності в рамках відповідного кримінального провадження. Тому слідчому доцільно використовувати нові підходи у реалізації слідчих (розшукових) та негласних слідчих (розшукових) дій та конструювати відповідні програми, спрямовані на алгоритмізацію прийняття тактичних та процесуальних рішень, з метою ефективного та оперативного виявлення, фіксації, аналізу інформації, що міститься у кіберпросторі, та має криміналістично-значиме або доказове значення.

Так, до програми дослідження кіберпростору доцільно включити традиційні слідчі (розшукові) дії.

Для дослідження матеріального середовища кіберпростору слідчий може використовувати огляд. У ході проведення огляду мають бути проаналізовані всі наявні елементи матеріального середовища: комп'ютери, гаджети, що містять інформацію про кримінальне правопорушення, сервери, системи, програмне забезпечення, соціальні мережі, канали зв'язку та ін.

Слід зазначити, що для огляду кіберпростору слідчому обов'язково необхідно залучати спеціаліста у галузі комп'ютерних технологій.

Не останню роль у дослідженні кіберпростору відіграє огляд документів, оскільки наявні форми передачі інформації передбачають можливість використання електронного документообігу. Також у ст. 99 КПК України передбачено, що до документів можуть належати, зокрема, матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі електронні). Таким чином, матеріали фотозйомки, звукозапису, відеозапису, що містяться в кіберпросторі, мають бути досліджені як документи, та виявлена інформація, у відповідній формі зафіксована і долучена до матеріалів кримінального провадження.

За допомогою допиту учасників кримінального правопорушення також можна певною мірою дослідити кіберпростір як складову частину обстановки відповідного злочину.

Наприклад, адміністратор відповідної групи у соціальній мережі може надати відомості щодо інформації, яка надсилалась користувачами групи, часу їх спілкування, моменту появи та реакції користувачів на відповідне повідомлення тощо.

Для дослідження кіберпростору доцільно використовувати відповідні негласні слідчі (розшукові) дії, функціональна спрямованість яких буде орієнтована на отримання криміналістично-значимої або доказової інформації для відповідного кримінального провадження стосовно злочину, що розслідується.

Так, доцільно здійснювати зняття інформації з транспортних телекомунікаційних мереж, оскільки великий обсяг інформації у кіберпросторі передається саме за допомогою телекомунікаційних мереж.

Важливе місце у дослідженні кіберпростору має пошук, виявлення і фіксація відомостей, що містяться в електронній інформаційній системі або їх частин, що може бути реалізовано за допомогою негласної (розшукової) дії у формі зняття інформації з електронних інформаційних систем.

Не останнє місце у програмі дій слідчого, спрямованих на дослідження кіберпростору,

мають відігравати і відповідні експертизи з метою з'ясування обставин, що мають значення для кримінального провадження та для отримання яких необхідні спеціальні знання. Для дослідження відповідних об'єктів при дослідженні кіберпростору слідчому доцільно призначати такі види експертиз:

1) авторознавча експертиза. Перед експертом можуть ставитись наступні запитання: чи є певна особа автором наданого на дослідження тексту; чи є певна особа автором декількох різних текстів; чи є автор та виконавець тексту однією або різними особами; чи даний текст складений кількома авторами. Експертизою можуть вирішуватися також інші питання;

2) також інформація, що міститься у електронному документі, може бути досліджена за допомогою семантико-текстуальної експертизи писемного мовлення. Орієнтовний перелік питань, що слідчим можуть бути поставлені перед експертом: які значення мають слова, словосполучення, фрази, зафіксовані в досліджуваному тексті; яким є об'єктивний зміст досліджуваного словосполучення, речення, тексту, групи текстів; чи містяться у тексті висловлювання, виражені у формі закликів до певних дій (вказати, яких саме); якщо так, то чи є ці заклики публічними (або який характер та форму мають ці заклики).

Вказану експертизу доцільно призначати для дослідження інформації, наявної у відповідних групах соціальних мереж (Vk, Facebook та ін.), повідомлень, в яких містять заклики, наприклад, до участі у масових заворушеннях, терористичних актах тощо.

Для дослідження відео– або аудіоматеріалів, що містяться у кіберпросторі, можуть використовуватись різноманітні лінгвістичні експертизи мовлення. Об'єктом дослідження лінгвістичної експертизи будуть продукти мовленнєвої діяльності людини, відображені в усній формі і зафіксовані у фоно(відео)грамі.

За допомогою цифрових фотокамер та відеокамер наразі в кіберпросторі міститься великій обсяг інформації, який виражений у цифровому файлі та є відповідним фото– або відеозображенням. Для його дослідження може бути призначена фототехнічна експертиза.За її допомогою можна здійснити ідентифікацію предметів, приміщень та ділянок місцевості, відображених на знімках та відеозаписах, або визначити розмірні характеристики зображень на фотознімках (кінокадрах, відеокадрах).

Також при дослідженні фото– або відеозображень, що містяться у кіберпросторі, може бути призначена портретна експертиза для ідентифікації особи (трупа) за фотознімком (фотокарткою, негативом) та відеозаписом.

Із комплексу інженерно-технічних експертиз можуть бути призначені: експертиза комп'ютерної техніки і програмних продуктів, а також експертиза телекомунікаційних систем та засобів.

До основних завдань експертизи комп'ютерної техніки і програмних продуктів належить, зокрема, установлення робочого стану комп'ютерно-технічних засобів; установлення обставин, пов'язаних з використанням комп'ютерно-технічних засобів, інформації та програмного забезпечення; виявлення інформації та програмного забезпечення, що містяться на комп'ютерних носіях; установлення відповідності програмних продуктів певним версіям чи вимогам на його розробку тощо.

Основними завданнями експертизи телекомунікаційних систем та засобів є, зокрема, визначення характеристик та параметрів телекомунікаційних систем та засобів; встановлення фактів та способів передачі (отримання) інформації в телекомунікаційних системах; встановлення фактів та способів доступу до систем, ресурсів та інформації у сфері телекомунікацій тощо.

Висновки. З наведеного вище вбачається, що кіберпростір є складною динамічною системою, яка може використовуватись для здійснення злочинної діяльності. Для її дослідження та встановлення фактичних обставин кримінального правопорушення, що було вчинено у ній, або реалізовано за її допомогою, необхідна ефективна система слідчих (розшукових) та негласних (слідчих) розшукових дій, яка надасть можливість отримати криміналістично-значиму та доказову інформацію. Також наявність у провадженні об'єкту дослідження у формі кіберпростору як обстановки злочину потребує обов'язкового залучення до пізнання обставин провадження спеціалістів у сфері комп'ютерних технологій та експертів.

ЛІТЕРАТУРА:

1. Кримінальний процесуальний кодекс України : Закон України № 4651-VI від 13 квітня 2012 р. // Офіційний вісник України. – 2012. – № 37. – С. 11. – Ст. 1370.

2. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України. Указ Президента України» [Електронний ресурс] : Режим доступу : http://zakon5.rada.gov.ua/laws/show/96/2016.

3. Закон України «Про телекомунікації» від 18.11.2003р. – № 1280-IV [Електронний ресурс]. – Режим доступу : http://zakon0.rada.gov.ua/laws/show/1280-15.

4. Наказ Міністерства юстиції України від 08.10.98 № 53/5 «Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень» [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/z0705-98/page.

5. Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации : автореф. дис. на соискание учен. степени доктора юрид. наук : спец. 12.00.09 «Уголовный процесс ; криминалистика и судебная экспертиза ; оперативно-розыскная деятельность» / В.А. Мещеряков. – Воронеж, 2001. – 39 с.