**УДК 343.9**

***Довженко О. Ю.,***
*аспірант кафедри кримінального процесу*
*Одеського державного університету внутрішніх справ*

# ДО ПИТАННЯ ПРО ТАКТИКУ ДОПИТІВ У СПРАВАХ ПРО КІБЕРЗЛОЧИНИ

**Анотація.** У статті розглядаються деякі питання призначення і проведення допитів під час розслідування кіберзлочинів. Аналізується сучасний стан правового регулювання даного питання. Наводяться рекомендації щодо постановки питань слідчим у процесі призначення та проведення допиту у справах про кіберзлочини.

**Ключові слова:** допит, очна ставка, кіберзлочини, комп'ютерні злочини, розслідування кіберзлочинів.

**Постановка проблеми.** Допит відіграє значну роль у розслідуванні великої кількості злочинів. Це стосується і розслідування нової категорії кіберзлочинів, тобто злочинів, що здійснюються за допомогою можливостей комп'ютерної техніки та мереж, злочинів у «кіберсвіті». Під час їх розслідування слідчий, як і раніше, не може обійтись без інформації, що може бути надана безпосередньо іншими особами (підозрюваним, потерпілим, свідком). Комп'ютерний злочинець, як правило, є особою, яка володіє набором спеціальних знань та навичок і, зазвичай, високим інтелектом, що зумовлює особливості допиту даної категорії осіб.

**Аналіз останніх досліджень і публікацій.** До проблематики допитів у справах про кіберзлочини зверталося чимало дослідників. Слід виділити роботи М.М. Єнікєєва та Є.С. Шевченко, присвячені особливостям психологічної підготовки та проведення допиту кіберзлочинців. Із технічної точки зору допит у справах про кіберзлочини розглядали І.Г. Смірнова, В.В. Коломинов. Водночас ця тема потребує постійної наукової уваги, адже саме досліджуване явище продовжує розвиватися, виникають нові види взаємодії людей у кіберсвіті, а отже, і потреба в нових способах дослідження цієї взаємодії, зокрема через допит.

**Метою** цієї статті є запропонувати відповіді на деякі новітні питання проведення допиту у справах про кіберзлочини. Зокрема, розглядаються сучасні рекомендації щодо проведення.

**Виклад основного матеріалу.** Специфічний віртуальний характер кіберзлочинів визначає і особливості тактики слідчо-розшукових дій із їх розслідування. На початковій стадії вирішальне значення має встановлення самої події кіберзлочину, його характеристик та визначення кола версій, що дозволить вести подальшу дослідну роботу, переважно експертного характеру, спрямовану на встановлення істини та розкриття злочину. Саме початковий етап визначає весь подальший хід розслідування. Виявлення кіберзлочину відбувається зазвичай завдяки повідомленням від фізичних чи юридичних осіб, а випадки безпосереднього виявлення ознак злочину вкрай рідкісні. Отже, вирішальне значення на первинній стадії розслідування має саме робота з особами, що повідомили про злочин, (можливими) жертвами злочину, а також особами, які в силу своїх службових обов'язків можуть володіти інформацією, необхідною для розслідування злочину (як свідками, так і особами, що мають технічні знання в певних питаннях).

Інтерес становить підхід, запропонований Є.С. Шевченко, відповідно до якого слідчі дії під час розслідування кіберзлочинів слід поділити на вербальні та невербальні [1, с. 200]. Вербальні призначені для отримання інформації щодо події злочину та передують діям невербальним, які призначені для з'ясування об'єктивної сторони кіберзлочину, встановлення його повної картини.

Основною вербальною слідчою дією в розслідуванні кіберзлочинів є допит. Допит, зокрема одночасний допит (очна ставка) (ст. 224 КПК України), проводяться у відповідності до загальних правил проведення слідчих (розшукових) дій, визначених статтею 223 КПК України. Щодо окремих слідчих дій можуть встановлюватися спеціальні вимоги, прикладом чого є стаття 226 КПК України (особливості допиту малолітньої або неповнолітньої особи).

Допит є головним способом отримання вербальної інформації під час проведення слідчих дій у розслідуванні кіберзлочинів. Необхідно відзначити, що український законодавець розглядає одночасний допит двох чи більше осіб (очну ставку) як різновид допиту, що підтверджується встановленням порядку одночасного допиту у статті 224 КПК України, яка присвячена допитам взагалі, на відміну від попереднього радянського підходу [2], який зберігся, наприклад, у російській доктрині [3, с. 100], де очна ставка розглядається як самостійна слідча дія. Однак незалежно від виділення очної ставки в окрему слідчу дію чи її розгляду як різновиду допиту зберігається основна функція цих слідчих дій у криміналістичному забезпеченні кримінального провадження: за їх допомогою вирішується тактичне завдання з перевірки слідчих версій, здійснюється виявлення неправдивих показань, розпізнання позицій допитуваних, виявлення раніше невідомих обставин тощо [4, с. 265].

У літературі допит розглядається як одна з найскладніших слідчих дій, що складається з технічних, психологічних та процесуальних компонентів. Тактика проведення допиту повинна бути гнучкою, враховувати особу допитуваної особи, її професійну підготовку, а також відштовхуватися від здібностей слідчого в розслідуванні певних діянь. Таким чином, хоча й існують загальні вимоги до проведення такої слідчої дії, як допит, практика застосування цих вимог щоразу має відповідати специфіці конкретної справи [5, с. 153].

З огляду на складність допиту однієї особи та двох чи більше осіб слід виділити ряд тактичних проблем, які підлягають розв'язанню під час підготовки до допиту та під час його проведення. По-перше, це необхідність залучення спеціалістів, які володіють спеціальними знаннями, під час проведення слідчих дій, що розглядаються. Зокрема, під час розслідування кіберзлочинів необхідні знання в галузі телекомунікаційних систем, комп'ютерних технологій та комп'ютерної техніки. Разом із тим не кожний слідчий володіє такими знаннями, або володіє ними в недостатньому обсязі, у зв'язку із чим під час підготовки до допиту слід розв'язати питання про необхідність залучення спеціаліста, допомога якого уможливить точне формулювання питань, а також усебічне й повне розуміння слідчим відповідей на них та їх вірну фіксацію. Пов'язана із цим і проблема можливої інтелектуальної протидії з боку злочинця, для чого ним можуть використовуватися спеціальні знання та навички, на які також може звернути увагу залучений спеціаліст. По-третє,

слідчий у ході розслідування повинен дослідити значний обсяг даних, що існують, як правило, в електронному вигляді, частина з яких складатиме власне предмет слідчої дії, а частина підлягатиме уточненню в ході допиту. По-четверте, під час допиту мають застосовуватися знання юридичної психології. По-п'яте, чинним КПК встановлюються обмеження тривалості допиту. Вони, разом з об'єктивним часовим фактором, який впливає на ефективність розслідування злочинів у динамічному електронному середовищі (наприклад, короткотривалість існування програм, можливість автоматичного знищення даних тощо), визначає необхідність для слідчого бути готовим проводити слідчі дії (зокрема допит) в найкоротший можливий строк.

На стадії підготовки до допиту у справах про кіберзлочини необхідно провести інформаційне забезпечення допиту, дослідження особистості обвинуваченого та планування допиту. Інформаційне забезпечення є важливою складовою частиною на стадії підготовки допиту підозрюваного (обвинуваченого) за кібезрлочином, адже високий рівень знань слідчого та володіння ним всіма зібраними щодо справи матеріалами та допоміжною інформацією технічного характеру гарантує контрольованість ситуації на допиті. Крім того, інформаційне забезпечення необхідно для виключення помилки під час кваліфікації скоєного злочину. Ще однією умовою інформаційного забезпечення допиту під час розслідуванні кіберзлочинів є наявність знань комп'ютерних технологій, а також нормативно-правової бази, що регулює галузь порушених злочином прав та законних інтересів. Мова тут іде не тільки про знання кримінального закону, але й про розуміння слідчим сутності охоронюваних цим законом суспільних відносин [6, с. 163]. Наприклад, це може бути розуміння комп'ютерної програми як об'єкта права власності та авторського права, що має ідеальний віртуальний характер, однак посягання на неї наносять матеріальну шкоду.

На етапі підготовки допиту для більш глибокого розуміння обставин кіберзлочину слідчому доцільно ознайомитись зі спеціальною літературою, присвяченою технологіям, що було ймовірно використано під час підготовки кіберзлочину, довідниками з комп'ютерної тематики, провести консультації зі спеціалістами. Важко не погодитися з М.М. Менжегою в тому, що слідчому, який не володіє, щонайменше на базовому рівні, необхідними знаннями, буде важко усвідомити саму подію злочину (наприклад, відрізнити технічний збій чи випадкову помилку від злочинного посягання), виявити суперечності та брехню в показаннях допитуваних. Крім того, під час розгляді ряду технічних питань, зокрема того, чи проводилося копіювання або зміна інформації під час виконання певних дій, важко обійтися без допомоги спеціаліста [7, с. 117].

Під час вибору тактики допиту у справах щодо кіберзлочинів важливим є попереднє виявлення певного набору інформації про подію злочину, що отримуються з різних джерел, а також про особливості механізму злочину, про застосовані знаряддя та технічні засоби [8, с. 47]. За таких умов відсутність у слідчого спеціальних знань може викликати складнощі під час розв'язання основних завдань допиту, таких як виявлення елементів складу кіберзлочину, встановлення його обставин, способу, мотивів, супутніх обставин, виділення ознак кіберзлочину, встановлення способу його приховування тощо.

Можна виділити такі способи приховування інформації, що стосується кіберзлочину, як: шифрування (електронної пошти, файлів), видалення інформації з пам'яті комп'ютера чи машинних носіїв, встановлення паролю, зберіганні інформації, що стосується кіберзлочину, в мережі Інтернет (на так званих «хмарних» серверах), встановлення програм видаленого користування, програм захисту інформації від несанкціонованого доступу, використання шкідливих програм для видалення файлів, використання недостовірної електронної адреси чи анонімної електронної пошти, використання програми заміни або приховування IP-адреси. Ці прийоми є найбільш простими та очевидними, в той час як злочинці, які володіють великим обсягом знань та навичок, можуть суттєво розширити даний злочинний арсенал. Із цього випливає висновок, що необхідна присутність під час здійснення слідчих дій, а особливо під час допиту, спеціаліста в галузі комп'ютерних технологій, який вже на стадії підготовки до слідчої дії зможе пояснити слідчому складні технічні терміни, призначення вилучених технічних засобів, способи скоєння злочинів, тощо.

Окрім вивчення матеріальної технічної сторони питання, під час підготовки до допиту необхідно враховувати характер особистості допитуваної особи. До джерел інформації про особу у криміналістичній науці можна віднести наявні біографічні дані, дослідження й порівняння відомостей про особу з різних джерел, збір і співставлення незалежних характеристик, аналіз трудової (учбової) діяльності особи, призначення судово-психологічних експертиз та врахування їх висновків, безпосереднє спостереження за особою (емоції, мова та ін.) [9, с. 28]. До джерел інформації про особу можна віднести також профіль цієї особи в соціальних мережах, історію відвідування особою електронних сторінок, що відображається у браузері.

Тут слід особливо зупинитися на певному психологічному феномені, що повинен бути взяти до уваги слідчим у розслідуванні кіберзлочинів (та може стати у пригоді в розслідуванні будь-яких злочинів) під час підготовки до слідчих дій з допиту. Зрозуміло, що проблема отримання інформації про особисті характеристики злочинця може бути складною через відсутність джерел такої інформації. Тим не менш, на підставі особливостей поведінки особи «тут і зараз» можна визначити ставлення цієї особи до злочину, тобто його суб'єктивну сторону. Одні з перших у світі дослідників злочинної поведінки, американські фахівці Д. Айков, К. Сейгер та У. Фонсторх, запропонували поділ комп'ютерних злочинців на три категорії в залежності від мотивів, якими скеровані їхні дії: зломщики (головний мотив – проникнення до захищеної системи), злочинці (головний стимул – матеріальна вигода) та вандали (що прагнуть до простого нанесення шкоди чи прославлення власного діяння) [10, с. 90]. Ці характеристики визначаються загальними підвалинами особистості, а отже, їх можна визначити шляхом спостереження за особою «тут і зараз», особливо коли до такого спостереження залучено психолога. Після встановлення типу комп'ютерного злочинця легшим стає виявлення його мети, ставлення до злочину, отримує пояснення характер злочинного впливу тощо.

Психологічна характеристика окремих кібезлочинців виявилась настільки важливою характеристикою кіберзлочинів, що в літературі було запропоновано ряд нових їхніх класифікацій. Зокрема, було запропоновано класифікацію, що ґрунтується на рівні комп'ютерних навичок злочинців: 1. Злочинці, що цілеспрямовано спеціалізуються на кіберзлочинах, скоюють їх самостійно й мають професійні технічні знання, необхідні для скоєння злочинів такого роду; 2. Злочинці загального злочинного типу, що скоюють злочини за допомогою електронних пристроїв; 3. Злочинці, що скоюють злочини, неспецифічні для кіберпростору, користуючись під час цього знаннями, які стали їм відомі випадково (на приклад, паролі), або такими, що включать у себе лише поверхневе розуміння комп'ютерної науки [11, с. 92].

Оскільки умови кіберпростору суттєво відрізняються від реальних, для встановлення процесу виникнення злочинного задуму, його природи та ступеня суспільної небезпеки злочинця виникає також необхідність класифікації злочинців у залежності від локалізації їхньої злочинної діяльності. Цей критерій

також є важливим для локалізації самого кіберзлочину та встановлення його місця як важливої обставини справи. Виходячи із цього, кіберзлочинців можна поділити на таких, що ведуть основну злочинну діяльність виключно в кіберпросторі, таких, що ведуть злочинну діяльність як у кіберпросторі, так і в реальному житті, а також осіб, що ведуть злочинний спосіб життя та для яких кіберзлочин є лише одним із різновидів злочинних посягань, які злочинець принципово не відрізняє від злочинного посягання в реальному світі.

Інформацію щодо особистості підозрюваного (обвинуваченого) можна отримати й традиційними для слідства способами: з даних криміналістичного обліку та від інших осіб (знайомих, родичів). Можуть бути з'ясовані спеціальні та професійні навички підозрюваного, схильність до скоєння злочинів, коло спілкування, наявні в підозрюваного засоби комп'ютерної техніки та місця їх зберігання, можливі цілі й мотиви скоєння злочину тощо.

Особливо важливими для даної категорії справ уявляються аналіз попередньої діяльності підозрюваного (трудової та учбової), призначення судово-психологічних та судово-психіатричних експертиз та врахування їх висновків, безпосереднє спостереження. Результатом аналізу різноманітної інформації про допитуваного під час підготовки до допиту має стати встановлення слідчим рівня знань та інформації про комп'ютерні технології, якими володіє злочинець, із чим було пов'язано злочин, чи могла допитувана особа вчинити цей злочин або ні.

Фактичну інформацію доцільно отримувати з аналізу відкритої інформації про особу, що стає доступною з дослідження активності цієї особи в мережі Інтернет. До такої інформації належить така, що вказується особою під час реєстрації в соціальних мережах, а також відомості про життя особи, що розміщуються нею добровільно під час користування сайтами. Це прізвище, дата й місце народження і проживання, стать, освіта та в яких закладах освіти вона була отримана, рік їх закінчення, сімейний стан, місце роботи, контактна інформація, соціальні зв'язки. До того ж, дослідження профілю особи в соціальних мережах дозволяє встановити професійні інтереси, зацікавлення і хобі допитуваного. В.О. Голубєв вказує на важливість отримання в підозрюваного інформації про те, до якої інформації він мав або повинен був мати доступ у силу своїх посадових обов'язків [12, с. 140].

Чималий масив інформації можна встановити з дописів і коментарів особи в соціальних мережах. Це, наприклад, ставлення особи до певних соціальних явищ, зокрема схвалення певної злочинної поведінки (особи, що займаються зламом комп'ютерних мереж та викраденням інформації, в тому числі з порушенням авторського права, схильні виправдовувати свої дії міркуваннями абсолютної «свободи в мережі» та, нерідко, анархістськими політичними переконаннями). У деяких випадках можна встановити важливі технічні дані, такі як інформація про електронні прилади особи, оскільки деякі сайти вимагають від користувача обов'язкового зазначення електронної адреси, номеру мобільного телефону тощо. Дана інформація може бути використана для встановлення часу й місця доступу до певної інформації та здійснення дій та сприяти визначенню того, чи могли ці дії бути скоєні відповідною особою.

**Висновки.** Можна виділити дві основні особливості допиту у справах про кіберзлочини. По-перше, це високий інтелектуальний рівень та певний психологічний склад допитуваних осіб, зокрема злочинця. По-друге, це складний технічний характер питань, що підлягають з'ясуванню під час проведення допиту. З урахуванням цього від слідчого вимагається особливо ретельна підготовка до проведення допиту у справах про кіберзлочини. У деяких випадках може вимагатися залучення спеціаліста (психолога чи фахівця з комп'ютерної техніки). Це має забезпечити успішність та максимальну інформаційну цінність допиту у справах про кіберзлочин.

***Література:***


1. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений : див. … канд. юрид. наук : 12.00.09, Москва, 2016. 249 с.
2. Кримінально-процесуальний кодекс України від 28.12.1960. URL : https://zakon.rada.gov.ua/laws/show/1001-05/ed19601228 (дата звернення : 02.01.2019). Глава XV.
3. Яковлев А.Н., Олиндер Н.В. Особенности расследования преступлений, совершённых с использованием электронных платёжных средств и систем : науч.-метод. пособие. Москва, 2012. 259 с.
4. Еникеев М.И. Юридическая психология. Москва : Норма, 2005. 419 с.
5. Гресь Ю.О. Допит: визначення тактичного та технологічного аспектів. *Науковий вісник Міжнародного гуманітарного університету: Сер. Юриспруденція*. 2016. № 20. С. 152–155.
6. Шевченко Е.С. Социально-технологические детерминанты следственных действий при расследовании киберпреступлений. *Актуальные проблемы российского права*. 2016. № 10. С. 160–169.
7. Менжега М.М. Криминалистические проблемы расследования создания использования и распространения вредоносных программ для ЭВМ : дис. … канд. юрид. наук. Саратов. 2005. 238 с.
8. Смирнова И.Г., Коломинов В.В. Тактические особенности производства допроса по делам о преступлениях в сфере компьютерной информации. *Известия Иркутской государственной экономической академии (БГУЭП)*. 2015. № 3. С. 44–50.
9. Питерцев С.К., Степанов А.А. Тактика допроса. Санкт-Петербург : Питер, 2001. 220 с.
10. Айков Д., Сейгер К., Фонсторх У. Компьютерные преступления : Руководство по борьбе с компьютерными преступлениями. Москва : Мир, 1999. 351 с.
11. Косенков А.Н., Чёрный Г.А. Общая характеристика психологии киберпреступника. *Криминологический журнал БГУЭП*. 2012. № 3(21). С. 91–104.
12. Голубєв О.В. Розслідування комп'ютерних злочинів : монографія. Запоріжжя : Гуманітарний університет «ЗІДМУ», 2003. 296 с.


**Довженко А. Ю. К вопросу о тактике допросов в делах о киберпреступленях**


**Аннотация.** В статье рассматриваются некоторые вопросы назначения и проведения допросов при расследовании киберпреступлений. Анализируется современное состояние правового регулирования данного вопроса. Приводятся рекомендации относительно постановки вопросов следователям при назначении и проведении допросов в делах о киберепреступлениях.



**Ключевые слова:** допрос, очная ставка, киберпреступления, компьютерные преступления, расследование киберпреступлений.


**Dovzhenko O. Concerning the tactics of interrogation in the cases on cybercrimes**


**Summary.** The article considers some aspects of appointment and arrangement of questioning in investigation of cybercrimes. It analyzes the contemporary state of legal regulation of the matter. It offers some recommendations concerning formulation of questions by the investigator at the appointment and running of questioning in the cases on cyber-crimes.



**Key words:** questioning, cybercrimes, computer crimes, investigation of cybercrimes.