КРИМІНАЛЬНИЙ ПРОЦЕС ТА КРИМІНАЛІСТИКА; СУДОВА ЕКСПЕРТИЗА; ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ

УДК 343.1
DOI https://doi.org/10.32840/pdu.3-2.9

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

ОСОБЛИВОСТІ ПРОВЕДЕННЯ ДОПИТУ У СПРАВАХ ПРО КІБЕРЗЛОЧИНИ

У статті розглядаються теоретичні та прикладні особливості проведення слідчої дії допиту у процесі розслідуванні злочинних посягань у кіберсфері. Досліджується специфіка допиту в кримінальних провадженнях щодо кіберзлочинів, яка полягає в тому, що допитувані особи, особливо підозрювані, відрізняються високим розумовим та професійним рівнем, який дозволяє ним чинити суттєвий інтелектуальний спротив слідчому під час проведення допиту, заважати у встановленні істини в справі, спрямовувати слідство невірним шляхом тощо. Ці особливості варто враховувати і під час допиту інших осіб (потерпілих, свідків), адже через складність кіберсфери та особливостей мислення осіб, які працюють у кіберсфері, можливе специфічне розуміння ними слідчих дій, невірне уявлення про сутність кримінальних проваджень, що може призводити до приховування ними інформації. Також варто брати до уваги особливості психіки та професійного розвитку осіб, які працюють у кіберсфері, звичні для них способи надання інформації про себе та події навколо себе, наявність у них особливих уявлень про навколишній світ.

Встановлюється, що визначальним для успіху допиту як процесуальної дії при розслідуванні кіберзлочинів є підготовка слідчого. Її основним елементом має бути збирання інформації про особу допитуваного, встановлення його характеру, за допомогою чого можна побудувати найбільш ефективну тактику допиту. Для збору інформації доцільно використовувати не тільки традиційні для криміналістики джерела, такі як бази даних, але й будь-яку інформацію про особу, яку можна встановити з відкритих електронних джерел, таких як соціальні мережі.

Робиться висновок про наявність спеціальних знань у слідчого у процесі проведення допиту в кримінальних провадженнях про кіберзлочини. З огляду на це, доцільним є залучення фахівців у галузі комп'ютерних технологій на етапі підготовки до допиту, а також ретельна самопідготовка слідчого. Крім того, особливе значення має попередній збір інформації про допитувану особу, зокрема про її суб'єктивні уявлення, які проявляються в інформації, яку особа поширює про себе в електронних мережах. Така інформація має використовуватися поряд з інформацією з «традиційних» для слідчого джерел, таких як бази даних, картотеки тощо.

Ключові слова: *допит, кіберзлочин, розслідування кіберзлочинів, провадження у справах про кіберзлочини, допит підозрюваного, допит свідка, допит потерпілого.*

Постановка проблеми. Специфічний віртуальний характер кіберзлочинів визначає і особливості тактики слідчо-розшукових дій з їхнього розслідування. На початковій стадії вирішальне значення має встановлення самої події кіберзлочину,

його характеристик та визначення кола версій, що дасть змогу 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 з огляду на свої службові обов'язки можуть володіти інформацією, необхідною для розслідування злочину (як свідками, так і особами, що мають технічні знання в певних питаннях).

Аналіз останніх досліджень і публікацій. Дослідження особливостей проведення допиту у справах про кіберзлочини слід проводити, враховуючи як криміналістичні техніки, так і напрацювання в галузі кримінальної психології. Прикладом перших є дисертаційне дослідження Є.С. Шевченко, других – робота з юридичної психології Є.М. Анікеєва. Серед українських авторів вказаної проблеми торкався Ю.О. Гресь.

Виклад основного матеріалу. Допит є головним способом отримання вербальної інформації у процесі проведення слідчих дій під час розслідування кіберзлочинів. Необхідно зазначити, що український законодавець розглядає одночасний допит двох чи більше осіб (очну ставку) як різновид допиту, що підтверджується встановленням порядку одночасного допиту в ст. 224 КПК України, яка присвячена допитам взагалі, на відміну від попереднього радянського підходу [1, глава XV], який зберігся, наприклад, у російській доктрині [2, с. 265], 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, виявлення неправдивих показань, розпізнання позицій допитуваних, виявлення раніше невідомих обставин тощо.

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 по справі матеріалами та допоміжною інформацією технічного характеру гарантує контрольованість ситуації на допиті. Крім того, інформаційне забезпечення необхідне для виключення помилки у процесі кваліфікації скоєного злочину. Ще однією умовою інформаційного забезпечення допиту при розслідуванні кіберзлочинів є наявність знань комп'ютерних технологій, а також нормативно-правової бази, що регулює галузь порушених злочином прав та законних інтересів. Мова тут йде про знання не тільки кримінального закону, але й про розуміння слідчим сутності охоронюваних цим законом суспільних відносин [3, 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 завдають матеріальної шкоди.

На етапі підготовки допиту для більш глибокого розуміння обставин кіберзлочину слідчому доцільно ознайомитись зі спеціальною літературою, присвяченою технологіям, що було, імовірно, використано у процесі підготовки кіберзлочину, довідниками з комп'ютерної тематики, провести консультації зі спеціалістами. Важко не погодитися з М.М. Менжегою у 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, у процесі розгляду технічних питань, зокрема, того чи проводилося копіювання або зміна інформації

при виконанні певних дій, важко обійтися без допомоги спеціаліста [4, с. 117].

У процесі вибору тактики допиту по справах по кіберзлочинах важливим є попереднє виявлення певного набору інформації про подію злочину, що отримуються з різних джерел, а також про особливості механізму злочину, застосовані знаряддя та технічні засоби [5, с. 47]. За таких умов відсутність у слідчого спеціальних знань може викликати складнощі при розв'язанні основних завдань допиту, таких як виявлення елементів складу кіберзлочину, встановлення його обставин, способу, мотивів, супутніх обставин, виділення ознак кіберзлочину, встановлення способу його приховування тощо.

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 залежно від локалізації їхньої злочинної діяльності. Цей критерій також є важливим для локалізації самого кіберзлочину та встановлення його місця як важливої обставини справи. З огляду на це 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.

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

Особливо важливими для цієї категорії справ видаються аналіз попередньої діяльності підозрюваного (трудової та учбової), призначення судово-психологічних та судово-психіатричних експертиз та врахування їхніх висновків, безпосереднє спостереження. Результатом аналізу різноманітної інформації про допитуваного при підготовці 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 особи вчинити цей злочин.

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 їхнього закінчення, сімейний стан, місце роботи, контактна інформація, соціальні зв'язки. До того ж дослідження профілю особи в соціальних мережах дає змогу 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 з огляду на свої посадові обов'язки [6, с. 140].

Чималий масив інформації можна встановити з дописів і коментарів особи в соціальних мережах. Це, наприклад, ставлення особи до певних соціальних явищ, як-то схвалення певної злочинної поведінки (зокрема, 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. Ця 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.

Додатковим джерелом інформації про особу можуть стати результати судово-психологічних й судово-психіатричних експертиз. Відомо, що найбільш «віртуозні» кіберзлочини вчиняють особи, які мають технічну освіту й тривалий досвід роботи в галузі інформаційних технологій. Це програмісти, оператори терміналів, системні адміністратори тощо. Однак левову частку кіберзлочинів становлять ті, що важко назвати віртуозними, і для їхнього скоєння достатньо базових технічних навичок. Відповідно, здебільшого необхідно встановити не стільки теоретичну здатність особи до скоєння злочину, скільки її психологічний стан та готовність використати свої знання зі злочинною метою. Отриманню саме цієї інформації і слугують судово-психологічні та судово-психіатричні експертизи.

Окрім безпосереднього отримання вербальної інформації від допитуваної особи, допит може також непрямим чином сприяти виявленню додаткової орієнтуючої інформації, що отримується з невербальних комунікацій. Слідчому варто брати до уваги, що кіберпростір справляє значну дію на свідомість особи, що взаємодіє з ним, призводячи до певної деформації.

Американський дослідник Р. Спінелло наголошує, що в умовах кіберпростору змінюється психологічний зміст взаємозв'язків між злочинцем, предметом злочину та потерпілим. Замість безпосереднього контакту відбувається зв'язок злочинця з електронним пристроєм, який призводить до впливу на предмет злочинного посягання та шкоди для потерпілого. Таким чином, зв'язок між злочинцем і злочином втрачає безпосередність [7, p. 24]. Кіберпростір створює в злочинця ілюзію вседозволеності та можливості ухилитися від покарання. Дж. Сулер називає цей феномен «ефектом онлайндезингибиції» [8, p. 20].

Зрештою, анонімність у мережі дає змогу злочинцю створити власний образ, що не відповідає реальності, та залишатися при цьому неідентифікованим. У зв'язку з цим у кіберзлочинців можуть розвиватися певні особливості поведінки, такі як інтернет-залежність, тривожні розлади, дисоціативні розлади особистості. Кіберзлочини можуть скоюватися особами, що мають відповідні особливості (розлади) поведінки. Їхня наявність може опосередковано свідчити про залучення особи до «кіберсвіту», наявність у неї знань та навичок щодо його особливостей. Успішність розслідування можна підвищити шляхом використання слідчим цих специфічних рис особистості допитуваної особи. Зокрема, слідчий може розробляти та використовувати нові тактичні рухи та їхні комбінації, що ґрунтуються на знанні психологічних закономірностей поведінки допитуваного, застосовувати традиційні прийоми з урахуванням індивідуальних особливостей конкретного обвинуваченого у справі.

Цікавою є думка, висловлена Є.С. Шевченко, що у процесі вибору тактики проведення допиту особи, підозрюваної у скоєнні кіберзлочину, слід мати на увазі, що такі особи, як правило, не мають антисоціальної настанови в поведінці [3, с. 167]. Отже, під час допиту у процесі розслідування кіберзлочинів можна широко застосовувати метод переконання, який полягає в доведенні до підозрюваного злочинної сутності певних дій, поясненні йому наслідків діянь у кіберсвіті тощо.

Висновки і пропозиції. З урахуванням наведеного слідчі ситуації, що складаються під час допиту, можна умовно поділити на безконфліктні (прості), коли слідчий має докази та конфліктні (складні), коли він не має доказів та веде допит, сподіваючись на їхнє отримання. У процесі проведення допиту як початкової слідчої дії логічним виглядає припущення, що більшість допитів будуть проходити у «складній» формі. Допитувані можуть відмовлятися від показань, надавати неправдиві свідчення, применшувати свою провину або взагалі заперечувати участь у злочині. Цю поведінку варто розглядати в поєднанні з характером кіберзлочину як такого, що зазвичай характеризується спланованістю та усвідомленням злочинцем сутності інформації, яка перебуває в розпорядженні слідчого, іноді краще за самого слідчого. Відповідно, злочинець має змогу скористатися

своїми технічними знаннями й продумати правдоподібну неправдиву версію. Окрім того, злочинці можуть використовувати тактику надмірного ускладнення показань спеціальними термінами, які можуть не стосуватися сутності справи, чим суттєво ускладнює роботу слідчого з виявлення брехні. Отже, слідчому треба заздалегідь ретельно продумати тактику допиту та фіксації його результатів.

Список використаної літератури:

1. Кримінально-процесуальний кодекс України від 28.12.1960 р. URL: https://zakon.rada.gov.ua/laws/show/1001-05/ed19601228 (дата звернення: 02.01.2019).
2. Яковлев А.Н., Олиндер Н.В. Особенности расследования преступлений, совершённых с использованием электронных платёжных средств и систем : науч.-метод. пособие. Москва, 2012. 259 с.
3. Шевченко Е.С. Социально-технологические детерминанты следственных действий при расследовании киберпреступлений. *Актуальные проблемы российского права*. 2016. № 10. С. 160-169.
4. Менжега М.М. Криминалистические проблемы расследования создания использования и распространения вредоносных программ для ЭВМ : дис. … канд. юрид. наук. Саратов, 2005. 238 с. 117.
5. 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.
6. Голубєв О.В. Розслідування комп'ютерних злочинів : Монографія. Запоріжжя : Гуманітарний університет «ЗІДМУ», 2003. 296 с.
7. Spinello R. Cyberethics: Morality and Law in Cyberspace. Jones & Bartlett Learning. 2010. 256 p. P. 71.
8. Suler J. Psychology of Cyberspace. Rider University, 2000. 284 p. P. 20.

Dovzhenko O. Peculiarities of interview in cyber-crime cases

The article deals with theoretical and applied peculiarities of investigation of interrogation in the investigation of criminal offenses in the cyber sphere. The specificity of the interrogation in criminal proceedings concerning cybercrime is investigated, which consists in the fact that the interviewed persons, especially suspects, have a high mental and professional level, which allows them to make significant intellectual resistance to the investigator during the interrogation, to interfere with the establishment of truth in the case. The wrong way, etc. You should also take into account the peculiarities of the psyche and professional development of persons working in the cybersphere, the usual ways for them to provide information about themselves and events around them, the presence of specific ideas about the world around them.

It is established that the decisive factor for the success of the interrogation as a procedural action in the investigation of cybercrime is the preparation of the investigator. Its main element should be to gather information about the person of the interviewee, to establish his character, by which it is possible to build the most effective tactics of the questioning. Not only traditional criminal sources, such as databases, but also any personally identifiable information that can be retrieved from open electronic sources, such as social networks, is useful for gathering information.

It is concluded that there is a special knowledge of the investigator during the interrogation in criminal proceedings on cybercrime. Against this background, it is advisable to involve computer experts in the pre-interrogation phase as well as thorough investigator self-training. In addition, the pre-gathering of information about the interviewee, in particular about his/her subjective perceptions, which is reflected in the information that the person disseminates about himself/herself via electronic networks is of particular importance. Such information should be used in conjunction with information from "traditional" sources such as databases, filing cabinets, etc.

Key words: *interrogation, cybercrime, investigation of cybercrime, proceedings in cybercrime cases, interrogation of a suspect, interrogation of a witness, interrogation of a victim.*