УДК 343.9

Курилін Іван Ростиславович
кандидат юридичних наук,
доцент кафедри криміналістики та судової медицини
Національна академія внутрішніх справ
Курилин Иван Ростиславович
кандидат юридических наук,
доцент кафедры криминалистики и судебной медицины
Национальная академия внутренних дел
Kurilin Ivan
PhD (Law), Associate Professor of Department of
Criminalistics and Forensic Medicine
National Academy of Internal Affairs
ORCID: 0000-0002-5672-3959

DOI: 10.25313/2520-2308-2020-9-6275

ТАКТИКА ДОПИТУ ПРИ РОЗСЛІДУВАННІ КІБЕРЗЛОЧИНІВ

ТАКТИКА ДОПРОСА ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

INTERROGATION TACTICS IN THE INVESTIGATION OF CYBERCRIME

Анотація. *У статті досліджується тактика допиту при розслідуванні кіберзлочинів. Зокрема з'ясовано проблемні питання, які можуть виникати при проведенні допиту кіберзлочинців до яких належить: необхідність залучення спеціаліста, недостатні спеціальні знання у слідчого, часові обмеження у зберіганні електронних доказів. З'ясовано основні тактичні завдання, які потрібно розв'язати при здійсненні допиту. Встановлено основні тактичні етапи підготовки до проведення допиту: постановка завдань допиту; вивчення особи-злочинця; визначення переліку запитань; інформаційне забезпечення проведення допиту; визначення доцільності залучення спеціаліста; технічна підготовка до допиту; визначення часу, способу та місця здійснення зазначеної слідчої (розшукової) дії. Доведено важливість наявність спеціальних знань у слідчого при розслідуванні кіберзлочинів, а зокрема в проведенні допиту злочинців, що вчинили кіберзлочини. Виділено особливості кіберзлочинності: спосіб вчинення злочинів; територіальні межі; місце скоєння злочину; особа-злочинець, яка володіє спеціальними знаннями; розмір шкоди; організованість вчинення кіберзлочинів та інші, що утрудняють розслідування кіберзлочину, зокрема проведення допиту. Доведено, що важливим у побудові тактики допиту є встановлення характеристики особи, яка планується допитувать. Досліджено особливості тактики допиту свідків та потерпілих від кіберзлочинів. Виділено основні завдання допиту потерпілого та свідків: з'ясувати правдивість інформації, яка дає підстави вважати потерпілих та свідків такими, а також, іншу інформацію стосовно події злочину. Встановлено особливості тактичної побудови допиту у розслідуванні кіберзлочинів. Доведено важливість налагодження особистого контакту з особою, яка допитується.*

Ключові слова: *кіберзлочин, комп'ютерний злочин, допит, тактика допиту, розслідування злочину.*

Аннотация. *В статье исследуется тактика допроса при расследовании киберпреступлений. В частности установлено проблемные вопросы, которые могут возникать при проведении допроса киберпреступников к которым относится: необходимость привлечения специалиста, недостаточны специальные знания у следователя, временные ограничения в хранении электронных доказательств. Выяснены основные тактические задачи, которые нужно решить при осуществлении допроса. Установлены основные тактические этапы подготовки к проведению допроса: постановка задач допроса;*

изучение личности-преступника; определение перечня вопросов; информационное обеспечение проведения допроса; определение целесообразности привлечения специалиста; техническая подготовка к допросу; определение времени, способа и места осуществления указанного следственного действия. Доказана важность наличие специальных знаний у следователя при расследовании киберпреступлений, а в частности в проведении допроса преступников, совершивших киберпреступления. Выделены особенности киберпреступности: способ совершения преступлений; территориальные границы; место совершения преступления; лицо-преступник, обладающий специальными знаниями; размер ущерба; организованность совершения киберпреступлений и другие, затрудняющие расследование киберпреступлений, включая проведение допроса. Доказано, что важным в построении тактики допроса является установление характеристики лица, которое планируется допрашивать. Исследованы особенности тактики допроса свидетелей и потерпевших от киберпреступлений. Выделены основные задачи допроса потерпевшего и свидетелей: выяснить правдивость информации, дает основания считать потерпевших и свидетелей такими, а также другую информацию о преступлении. Установлены особенности тактического построения допроса в расследовании киберпреступлений. Доказано важность налаживания личного контакта с лицом, которое допрашивается.

Ключевые слова: *киберпреступление, компьютерное преступление, допрос, тактика допроса, расследование преступления.*

Summary. *The article examines the tactics of interrogation in the investigation of cybercrime. In particular, the problematic issues that may arise during the interrogation of cybercriminals, which include: the need to involve a specialist, insufficient special knowledge of the investigator, time constraints in the storage of electronic evidence. The main tactical tasks that need to be solved during the interrogation are clarified. The main tactical stages of preparation for the interrogation are established: setting the tasks of the interrogation; study of a criminal; determining the list of questions; information support of the interrogation; determining the feasibility of involving a specialist; technical preparation for interrogation; determination of the time, method and place of implementation of the specified investigative action. The importance of the investigator's special knowledge in the investigation of cybercrimes, and in particular in the interrogation of criminals who have committed cybercrimes, has been proven. Features of cybercrime are highlighted: the method of committing crimes; territorial boundaries; crime scene; a criminal person who has special knowledge; the amount of damage; organization of cybercrime and others that complicate the investigation of cybercrime, including interrogation. It is proved that it is important to establish the characteristics of the person to be interrogated in the construction of interrogation tactics. Peculiarities of tactics of interrogation of witnesses and victims of cybercrimes are investigated. The main tasks of the interrogation of the victim and witnesses are highlighted: to find out the veracity of the information that gives grounds to consider the victims and witnesses as such, as well as other information about the crime. The peculiarities of tactical construction of interrogation in the investigation of cybercrimes are established. The importance of establishing personal contact with the interrogated person is proved.*

Key words: *cybercrime, computer crime, interrogation, interrogation tactics, crime investigation.*

Постановка проблеми. Кіберзлочинність є відносно новою темою для кримінологічних досліджень, причому більшість опублікованих робіт з'явилися протягом першого десятиліття 21 століття. Розслідування зазначеної категорії злочинів є складним, так як особливістю їх є територіальні масштаби вчинення злочину, їх організованість та велика шкода. Допит як слідча дія, яка проводиться безпосередньо зі злочинцем або носієм інформації, яка є корисною з точки зору розкриття злочину, є надважливим доказом. Тому, від тактично правильної побудови допиту, залежить повнота отриманої інформації від її носія.

Аналіз останніх досліджень та публікацій. Дослідження проблематики тактики допиту при розслідування кіберзлочинів здійснювали вітчизняні та зарубіжні науковці: Айков Д., Сейгер К., Фонсторх У. [1], Биков В. М. [2], Borges E. [3], Верхов В. Б. [4], Hutchings A., Holt T. J. [5], Lynch W. [6], Polivanyuk V. [7], Смірнова І. Г. [8], Хахановський В. Г. [9], Шевченко Е. С. [10] та інші.

Формування цілей статті (постановка завдання). Ціллю статті є встановлення основних тактичних етапів підготовки до проведення допиту. З'ясування проблемних питань, які можуть виникати при проведенні допиту кіберзлочинців. Встановити особливості тактичної побудови допиту у розслідуванні кіберзлочинів.

Виклад основного матеріалу. Розслідування кіберзлочинності — це процес розслідування, аналізу та відновлення критично важливих криміналістичних цифрових даних із мереж, що беруть участь у нападі — це може бути Інтернет та (або) локальна мережа — з метою встановлення авторів цифрових злочинів та їхні справжні наміри [3].

Кіберзлочинність або, як ще називають, «цифровий злочин» — це злочин, який передбачає викори-

стання комп'ютера, телефону чи будь-якого іншого цифрового пристрою, підключеного до мережі [3].

Стандартне розслідування кіберзлочинів включає низку перевірених методів розслідування, кожен призначений для відстеження та захоплення кіберзлочинців. При виявленні кіберзлочинності органи влади часто беруть участь в особистих співбесідах, допитуючи залучені сторони, щоб зібрати якомога більше інформації про справу. Ці перші співбесіди встановлюють, чи був скоєний злочин та як найкраще розпочати розслідування злочину. Записані показання свідків є важливими не лише у формуванні розслідування, а й у розбудові судової справи щодо можливих підозрюваних [6].

Допит при розслідуванні кіберзлочинів можна віднести до одних із найважливіших та найважчих слідчих дій. Така ситуація зумовлена особливостями вчинення кіберзлочинів. До таких можна віднести: спосіб вчинення злочинів; територіальні межі; місце скоєння злочину; особа-злочинець, яка володіє спеціальними знаннями; розмір шкоди; організованість вчинення кіберзлочинів та інші.

Слідчі з питань кіберзлочинності повинні бути експертами в галузі інформатики, розуміючи не тільки програмне забезпечення, файлові системи та операційні системи, а й те, як працюють мережі та обладнання. Вони повинні бути достатньо обізнаними, щоб визначити, як відбувається взаємодія між цими компонентами, отримати повне уявлення про те, що сталося, чому це сталося, коли це сталося, хто саме вчинив кіберзлочин і як жертви можуть у майбутньому захиститися від цих типів кіберзагроз [3].

Тактика здійснення допиту в розслідуванні кіберзлочинів залежить від механізму вчинення кіберзлочинів. Аналіз практики розслідування вчинених зазначених злочинів показав, що при здійсненні допиту виникають такі труднощі: проблеми з термінологією, вибором тактичних прийомів взаємодії та встановлення контакту [10, с. 162].

Отже, можна виділити основні проблеми, які можуть виникати при здійсненні допиту кіберзлочинців:

– залучення спеціалістів при проведенні допиту. Такий підхід зумовлений браком спеціальних знань в слідчих. Так, при здійсненні допиту кіберзлочинців потрібні знання в програмному забезпеченні комп'ютерної техніки, комп'ютерних технологіях, телекомунікаційних мереж та інші. Такими знаннями володіє спеціаліст, який може надати консультативну допомогу у роз'ясненні термінів, побудові запитань, встановити логічний зв'язок між здійсненими особою операціями та вчиненим злочином та інші. Однак, потрібно врахувати той факт, що присутність спеціаліста на допиті носить двоякий результат — з однієї сторони, присутність спеціаліста не впливає на особу кіберзлочинця ніяким чином і допит проводиться в звичному для слідчого режимі, з іншої — присутність спеціаліста негативно впливає на допитуваного, так як виникає недовіра щодо професіоналізму слідчого або присутність третьої особи. Попри це, присутність спеціаліста на допиті приносить більшу користь, аніж негатив;
– брак спеціальних знань у слідчого дає можливість кіберзлочинцю цим користуватися в процесі допиту;
– слідчий повинен орієнтуватися в способі вчинення конкретного злочину із залученням комп'ютерних технологій, так як в процесі допиту можливе уточнення по окремих діях або способах;
– важливість проведення повноти допиту, так як докази, які в більшості зберігаються в електронному вигляді можуть мати часові обмеження або піддаватися змін.

З криміналістичної точки зору, допит є слідчою дією, яка вирішує ряд тактичних завдань: викриття особи в брехні, яка протидіє слідству; перевірка висунутих версій; розпізнання міцності позицій допитуваного; з'ясування раніше невідомих обставин і т.д. [10, с. 163].

В. Поляник в своїй науковій праці зазначає про такі основні тактичні завдання допитів в сфері кіберзлочинності:

– розкриття складових злочину;
– встановлення обставин, місця та часу дій, важливих для розслідування; шляхи та мотиви їх виконання та одночасні, особливості осіб, які беруть у ньому участь;
– визначення предмета кримінального правопорушення;
– визначення розміру заподіяної шкоди;
– встановлення інших свідків та осіб, причетних до злочинів [7].

На початковому етапі розслідування незаконного доступу необхідно допитувати громадян різних категорій (операторів комп'ютерів, програмістів, службовців, відповідальних за інформаційну безпеку, менеджерів, службовців, зайнятих сервісом, керівників комп'ютерних центрів або підприємств (організацій). Є певна тема допиту для кожної з цих категорій [7].

Важливим у процесі здійснення допиту є його планування, що відображається в тактичній побудові зазначеної слідчої (розшукової) дії. Ключовим є той факт, що допит, здійснений на стадії досудового розслідування не є доказом на етапі судового

розгляду, а тому, слідчий повинен опиратися на мету проведення допиту та шляхи досягнення ефективного результату.

Є. С. Шевченко до стадій підготовки до допиту підозрюваного в кіберзлочинності відносить: інформаційне забезпечення допиту, вивчення особи підозрюваного і планування допиту [10, с. 163].

Доцільно дещо розширити перелік стадій підготовки. Так, тактика проведення допиту учасників кримінального провадження у вчиненні кіберзлочину повинна включати такі етапи підготовки:
- постановка завдань допиту;
- вивчення особи-злочинця;
- визначення переліку запитань;
- інформаційне забезпечення проведення допиту;
- визначення доцільності залучення спеціаліста;
- технічна підготовка до допиту;
- визначення часу, способу та місця здійснення зазначеної слідчої (розшукової) дії.

Д. Айков, К. Сейгер, У. Фонсторх поділяють комп'ютерних злочинців на три категорії взалежності від мотивів вчинення злочинів: взломщики (головне переконання — проникнення в систему), злочинці (головне переконання — вигода), вандали (головне переконання — нанесення шкоди) [1, с. 42].

В. Б. Вєхов виділяє такі три групи комп'ютерних злочинців: особи, особливістю яких є стійке сполучення професіоналізму у сфері комп'ютерної техніки та програмування з елементами своєрідного фанатизму та винахідливості; особи, які страждають на новий вид психічних захворювань — інформаційні хвороби (комп'ютерні фобії); професійні комп'ютерні злочинці з яскраво вираженою корисливою метою [4, с. 38–39].

Якщо особа, яка вчинила кіберзлочин має певні психічні захворювання, вона потребує призначення психіатричної експертизи та особливий процес здійснення допиту.

Тому, слідчий повинен розробити перелік стандартних питань допиту осіб, віднесених до всіх трьох груп. Для розуміння до якої групи особа належить слід зібрати максимально багато інформації, яка характеризує особу та поставити стандартні запитання в сфері кіберзлочинності, такі як: наявність освіти в сфері комп'ютерних технологій; рівень комп'ютерних навиків; рівень технічної підготовки; наявність психічних захворювань або про такі в минулому; мотиви вчинення кіберзлочину; наявність інформації в соціальних мережах, їх актуальність і правдивість; кількість та тривалість вчинення кіберзлочинів.

Важливим є факт визнання або ж невизнання підозрюваним вини. Так як, слідчий повинен врахувати цей факт та розробити декілька тактичних варіантів побудови допиту.

Вторгнення в комп'ютерні мережі потерпілих ззовні організацій становлять половину комп'ютерних злочинів. Тому на допитах підозрюваного (обвинуваченого) дуже важливо вказати «технологію» скоєного злочину, отримати доступні дані або електронні та будь-які матеріальні сліди вчиненого, коли це можливо, знайти інформацію, цікаву для розслідування [7].

Допит потерпілих та свідків становить найбільше джерело інформації про вчинений злочин. Тому, допит зазначених осіб є найбільш інформативний канал, який допомагає встановити найбільш реальну версію вчинення кіберзлочину, можливий спосіб та інструменти вчинення такого злочину, часткову характеристику особу-злочинця, логічні зв'язки між отриманою в ході розслідування інформацією та інше.

Для побудови тактики допиту потерпілого та свідка, як і підозрюваного, необхідно встановити особу-потерпілого, свідка та їх характеристику.

Виокремлюють три головні групи потерпілих від таких злочинів: клієнти, які користуються їх послугами; власники комп'ютерної системи; інші особи [9].

В. М. Биков відмічає, що тактика допиту повинна будуватися з врахуванням характеристики потерпілих. Науковець останніх типізує на: активних і неактивних добросовісних потерпілих, неврівноважених, а також недобросовісних [2, с. 28].

Етапи допиту потерпілих та свідків не відрізняються від етапів допиту підозрюваного запропонованих вище.

Основними завданнями допиту потерпілого та свідків є: з'ясування правдивості інформації, яка дає підстави вважати потерпілих та свідків такими, а також, іншу інформацію стосовно події злочину.

Для вирішення зазначених завдань слідчий під час допиту потерпілих та свідків повинен з'ясувати, чи:
- хтось виявляв інтерес до комп'ютерної інформації, програмного забезпечення, комп'ютерних засобів даного підприємства, організації, установи чи компанії;
- сторонні особи мали доступ до кімнат, де розташовані комп'ютерні засоби;
- випадки зловживання службовим становищем мали місце;
- мали місце збої в роботі програмного забезпечення;
- сталося викрадення носіїв даних та інших комп'ютерних пристроїв;
- мали місце збої в роботі обладнання, мереж, засобів комп'ютерного захисту інформації [7].

В тому випадку, якщо потерпілою є юридична особа, то тактика допиту слідчим повинна будувати-

ся з врахуванням того факту, що працівники або особи, які надають послуги пов'язані з комп'ютерною технікою, програмним забезпеченням цій юридичній особі можуть бути причетні до кіберзлочинності.

Науковцями пропонується перелік питань, які повинен з'ясувати слідчий у свідків, які мають відношення до потерпілої юридичної особи:

- вид діяльності і місцезнаходження юридичної особи;
- наявність реєстраційних документів, ліцензій;
- режим роботи юридичної особи (наявність охорони, засобів сигналізації, спостереження, пропускного режиму; вимоги внутрішнього трудового розпорядку, штатного кадрового розкладу; посадових інструкцій та інше);
- об'єм роботи, характер і наявність укладених договорів, їх види, зміст і умови, найменування та місцезнаходження контрагентів;
- сутність і об'єм інформації, що зберігається в комп'ютері, наявність доступу до неї, кодів та паролей;
- документальне підтвердження наявності, характер і об'єм спричиненого злочином шкоди, умови його спричинення;
- хто із співробітників вступав в контакт з потенційними злочинцями;
- думка кожної категорії допитуваних про механізм вчиненого злочину, а також причинах і умовах настання злочинного результату [8].

При допиті будь-якої категорії осіб важливим є встановлення психологічного контакту з допитуваною особою. Такий можливий лише при особистому допиті. Враховуючи особливість кіберзлочину, що місцем вчинення може бути навіть інша країна, а потерпілі можуть бути громадяни інших держав, не завжди слідчий може провести його особисто.

На особистих допитах набагато легше налагодити контакт з людина, це особлива форма спілкування, простіше посередницької діяльності, і кіберзлочинці дещо віддаляються від звичної маріонетки маніпулювання інформаційним середовищем, до якого вони звикли. Особисті співбесіди дуже вигідні, оскільки вони виводять учасника за межі типового середовища, до якого вони звикли [5].

Висновки і перспективи подальших досліджень. Отже, допит як елемент тактичного механізму розслідування кіберзлочинності характеризується багатогранністю дій слідчого. Важливою особливістю, яка відрізняє розслідування кіберзлочинності від інших є наявність спеціальних знань в IT-технологіях та масштабність вчинення зазначеного злочину. У зв'язку з чим, здійсненню допиту повинно передувати ґрунтовна тактична підготовка.

Тактика допиту залежить від багатьох чинників, основними з яких є: механізм вчинення злочину; характеристика особи-злочинця, потерпілого, свідка; наявність у слідчого достатніх спеціальних знань; визнання вини підозрюваним; місце вчинення кіберзлочину; кількість суб'єктів, що вчинили злочин; потерпілим є фізична особи чи юридична та інші.

Тому, вважаємо, що слідчий повинен мати набір стандартних запитань, відповідно до конкретної групи осіб (підозрюваного, потерпілого, свідка) з врахуванням зазначених вище чинників.

Проблематика тактики допиту в розслідуванні кіберзлочинності є динамічною і потребує постійного дослідженні та оновлення, так як IT-технології розвиваються, відповідно виникають нові напрямки кіберзлочинності, які потребують ефективного розслідування.

Література

1. Айков Д. Компьютерные преступления: Руководство по борьбе с компьютерными преступлениями / Д. Айков, К. Сейгер, У. Фонсторх. Москва: Мир, 1999. 90 с.

2. Быков В. М. Допрос потерпевшего / В. М. Быков. // Законность. 2014. № 6. С. 27–32.

3. Borges E. Cyber Crime Investigation Tools and Techniques Explained / E. Borges. 2016. URL: https://securitytrails.com/blog/cyber-crime-investigation.

4. Верхов В. Б. Компьютерные преступления. Способы совершения, методики расследования / В. Б. Верхов. Москва: Право и закон, 1996. 182 с.

5. Hutchings A. Interviewing cybercrime offenders / Hutchings A., Holt T. J. // Journal of Qualitative Criminal Justice and Criminology. 2019. URL: https://doi.org/10.17863/CAM.24191.

6. Lynch W. Cyber Crime Investigative Techniques / W. Lynch. URL: https://itstillworks.com/advantages-disadvantages-using-camera-wire-tap-surveillance-24039.html.

7. Polivanyuk V. Interrogation of Suspects in Investigating Computer Crime / V. Polivanyuk. URL: http://www.crime-research.org/library/Polivan1003eng.html.

8. Смирнова И. Г. Тактические особенности производства допроса по делам о преступлениях в сфере компьютерной информации / И. Г. Смирнова, В. В. Коломинов // 2015. № 3. URL: file:///C:/Users/Lenovo/Downloads/takticheskie-osobennosti-proizvodstva-doprosa-po-delam-o-prestupleniyah-v-sfere-kompyuternoy-informatsii.pdf.

9. Хахановський В. Г. Особливості криміналістичної характеристики кіберзлочинів / В. Г. Хахановський. 2011. URL: file:///C:/Users/Lenovo/Downloads/aymvs_2011_1(1)__13.pdf

10. Шевченко Е. С. Социально-технологические детерминанты следственных действий при расследовании киберпреступлений / Е. С. Шевченко // Актуальные проблемы российского права. 2016. № 10. С. 160–169.

References

1. Ajkov D. Komp'yuternыe prestupleny'ya: Rukovodstvo po bor'be s komp'yuternыmy' prestupleny'yamy' [Computer Crime: A Guide to Combating Computer Crime]. My'r. Moskva. 1999. 90 s.

2. Выkov V. M., Dopros poterpevshego [Interrogation of the victim]. Zakonnost'. 2014. № 6. S. 27–32.

3. Borges E. Cyber Crime Investigation Tools and Techniques Explained. 2016. URL: https://securitytrails.com/blog/cyber-crime-investigation.

4. Verxov V. B. Komp'yuternye prestupleny'ya. Sposobы soversheny'ya, metody'ky' rasledovany'ya [Computer crimes. Methods of commission, methods of investigation]. Moskva. Pravo y' zakon. 1996. 182 s.

5. Hutchings A., Holt T. J. Interviewing cybercrime offenders // Journal of Qualitative Criminal Justice and Criminology. 2019. URL: https://doi.org/10.17863/CAM.24191.

6. Lynch W. Cyber Crime Investigative Techniques. URL: https://itstillworks.com/advantages-disadvantages-using-camera-wire-tap-surveillance-24039.html.

7. Polivanyuk V. Interrogation of Suspects in Investigating Computer Crime. URL: http://www.crime-research.org/library/Polivan1003eng.html.

8. Smy'rnova Y'. G. Takty'chesky'e osobennosty' proy'zvodstva doprosa po delam o prestupleny'yax v sfere komp'yuternoj y'nformacy'y' [Tactical features of interrogation in cases of crimes in the field of computer information]. 2015. URL: file:///C:/Users/Lenovo/Downloads/takticheskie-osobennosti-proizvodstva-doprosa-po-delam-o-prestupleniyah-v-sfere-kompyuternoy-informatsii.pdf.

9. Xaxanovs'ky'j V. G. Osobly'vosti kry'minalisty'chnoyi haraktery'sty'ky' kiberzlochy'niv [Features of forensic characteristics of cybercrimes]. 2011. URL: file:///C:/Users/Lenovo/Downloads/aymvs_2011_1(1)__13.pdf

10. Shevchenko E. S. Socy'al'no-texnology'chesky'e determy'nanty sledstvennyh dejstvy'j pry' rassledovany'y' ky'berprestupleny'j [Socio-technological determinants of investigative actions in the investigation of cybercrimes] // Aktual'nye problemy rossy'jskogo prava. 2016. № 10. S. 160–169.