– по-друге, реалізацію можливостей такої системи в повсякденній практиці розкриття й розслідування злочинів, що забезпечується результатами формування цієї системи, її станом.

Таким чином, практична реалізація можливостей криміналістичного забезпечення припускає системність підходу до формування його організаційно-правового механізму, здійснення цілеспрямованої, планомірної діяльності з забезпечення державної безпеки. У свою чергу, така діяльність не може бути успішною без її відповідного методичного забезпечення, без теоретичних та практичних розробок проблем криміналістичного забезпечення.

Список використаних джерел

1. Ануфрієв М.І. Службова підготовка працівників органів внутрішніх справ: навч.-метод. посіб. Київ: РВВ МВС України, 2003. 440 с.

2. Бандурка О.М. Оперативно-розшукова діяльність. Частина І: підруч. Харків: НУВС, 2002. 336 с.

3. Бесчастний В.М. Механізми державного управління розвитком вищих навчальних закладів системи МВС України: теорія, методологія та практика: монографія. Донецьк: Юго-Восток, 2009. 458 с.

4. Ківалов С.В., Дрьомін В.Н. Кримінологічна політика у сфері боротьби з організованою злочинністю. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2001. № 4. С. 28–33.

Курилін Іван Ростиславович,
доцент кафедри криміналістики та судової медицини Національної академії внутрішніх справ, кандидат юридичних наук, доцент;
Атаманчук Володимир Миколайович,
старший слідчий в особливо важливих справах Головного слідчого управління Національної поліції України, кандидат юридичних наук

ТАКТИЧНІ ОСОБЛИВОСТІ ДОПИТУ В ПРОВАДЖЕННЯХ ПРО КІБЕРЗЛОЧИНИ

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 [2].

Допит при розслідуванні кіберзлочинів можна віднести до одних із найважливіших та найважчих слідчих (розшукових) дій. Така ситуація зумовлена особливостями вчинення кіберзлочинів. До таких можна віднести: спосіб вчинення злочинів; місце вчинення злочину; особу-злочинця, яка володіє спеціальними знаннями; розмір нанесеної шкоди; організованість вчинення кіберзлочинів та інші.

Слідчі які розслідують кіберзлочини 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 [2].

Тактика здійснення допиту при розслідуванні кіберзлочинів залежить від механізму їх вчинення. Аналіз практики розслідування вчинених зазначених злочинів показав, що при здійсненні допиту виникають такі труднощі: проблеми з термінологією, вибором тактичних прийомів взаємодії та встановлення контакту [9].

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'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.

– брак спеціальних знань у слідчого дає можливість кіберзлочинцю цим користуватися в процесі допиту;

– 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 (розшуковою) 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. [9].

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 [6].

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 [6].

Важливим у процесі здійснення допиту є його планування, що відображається в тактичній побудові зазначеної слідчої 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 [9].

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 дії.

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

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 [3].

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.

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

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 зацікавленість 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 [6].

В тому випадку, якщо потерпілою є юридична особа, то тактика допиту слідчим повинна будуватися 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 [7].

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 [4].

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.

Список використаних джерел

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

2. Borges E. Cyber Crime Investigation Tools and Techniques Explained [Електронний ресурс] / E. Borges. – 2016. – Режим доступу до ресурсу : https://securitytrails.com/blog/cyber-crime-investigation.

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

4. Hutchings A. Interviewing cybercrime offenders [Електронний ресурс] / Hutchings A., Holt T. J. // Journal of Qualitative Criminal Justice and Criminology. – 2019. – Режим доступу до ресурсу: https://doi.org/10.17863/CAM.24191.

6. Polivanyuk V. Interrogation of Suspects in Investigating Computer Crime [Електронний ресурс] / V. Polivanyuk – Режим доступу до ресурсу: http://www.crime-research.org/library/Polivan1003eng.html.

7. Смирнова И. Г. Тактические особенности производства допроса по делам о преступлениях в сфере компьютерной информации [Електронний ресурс] / И. Г. Смирнова, В. В. Коломинов // 2015. – № 3. – Режим доступу до ресурсу: https://bit.ly/3oKfVDi.

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

Курята Леонід Леонідович,
здобувач кафедри криміналістики та судової медицини Національної академії внутрішніх справ

ОБСТАВИНИ, ЯКІ ПІДЛЯГАЮТЬ ВСТАНОВЛЕННЮ ПІД ЧАС РОЗСЛІДУВАННЯ ШАХРАЙСТВА

Об’єктивними факторами погіршення криміногенної ситуації у сфері економічної діяльності можна визначити: підвищення рівня корупції; послаблення державного контролю в сфері економіки;маскування злочинцями своїх неправомірних дій під цивільно-правові відносини; нестабільна економічна ситуація, в тому числі зумовлена подіями, пов’язаними із введенням обмежень у період із пандемії; ускладнення правила ведення підприємницької діяльності; постійне оновлення нормативної бази у сфері фінансово-господарської діяльності; тощо. Саме тому, дедалі частішими є факти виявлення непоодиноких шахрайських дій у різних сферах, а проблема боротьби із шахрайством є однією із найбільш актуальних у сучасних умовах.

Дослідженням актуальних положень методики розслідування шахрайства, займались такі вчені як: С.М. Астапкина, В.П. Бахін, Д.В. Березін, А.Ф. Волобуєв, О.В. Волохова, В.Ю. Голубовський, О.В. Журавльов, О.Н. Колісниченка, В.Є. Коновалова, В.П. Лавров, В.Д. Ларичев, О.І. Лученка, Г.А. Матусовський, О.С. Овчинський, В.І. Отряхин, Т.А. Пазинич, М.В. Салтевський, Р.С. Сатуєв, С.С. Чернявський, С. Ю.Шаров, В.Ю. Шепітько, та ін.

Методика розслідування шахрайства структурно поєднує у собі систему елементів, які містять суттєві ознаки, відомості, прийоми та методи, спрямовані на отримання криміналістично значущої інформації під час кримінального провадження.

До структури методики розслідування шахрайства, на нашу думку, доцільно включити наступні елементи

– криміналістична характеристика шахрайства та її типові елементи;