МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХЕРСОНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ БІЗНЕСУ І ПРАВА
КАФЕДРА НАЦІОНАЛЬНОГО, МІЖНАРОДНОГО ПРАВА ТА ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ В РОБОТУ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), АВТОМАТИЗОВАНИХ СИСТЕМ, КОМП'ЮТЕРНИХ МЕРЕЖ ЧИ МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

Кваліфікаційна робота (проєкт)
на здобуття ступеня вищої освіти «магістр»

Виконала: студентка 2 курсу 12-282 групи
Спеціальності 081 Право
Освітньо-професійної програми
«Право»
Волковська Євгенія Геннадіївна

Керівник: к.ю.н., доцент **Проценко М.В.**
Рецензент: в.о. доцентки кафедри адміністративного права та адміністративного процесу Херсонського державного аграрно-економічного університету
к.ю.н. **Шевченко Н.Л.**

Херсон – 2021

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Одна з основних функцій України як держави полягає у тому, щоб забезпечити інформаційну безпеку, оскільки благополуччя нації безпосередньо залежить від інформаційного елемента. Сьогоднішня криміногенна ситуація в країні потребує розробки та адаптації належних заходів, аби запобігати вчиненню кримінальних правопорушень на об’єкти у «сфері використання електронно-обчислювальних машин (ЕОМ), систем та комп’ютерних мереж і мереж електрозв’язку». У зв’язку з чим, протиправність використання електронно-обчислювальної техніки, а також циркулюючої в ній інформації і характеризує серйозну суспільну небезпеку.

Взагалі комп’ютерним злочинам (кіберзлочинам) притаманна значна суспільна небезпечність. Наведене викликане вагомістю об’єкта посягання, його значимістю, цінністю та суттєвою вразливістю комп’ютерної інформації.

В контексті поставленого питання на розгляд в дослідженні, а саме особливостей розслідування ст. 361 Кримінального кодексу України (КК України): «несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку», до криміналістичних особливостей виявлення та розкриття даного злочинного діяння слід відносити високу латентність та труднощі виявлення фактів вчинення такого злочину; специфічність контингенту осіб, якими вчиняється дане злочинне діяння; невпинно прогресивний розвиток інформаційних технологій; низку криміналістично значущих ознак; труднощі підбору кваліфікованих спеціалістів з метою залучення допомоги при проведенні окремих слідчих (розшукових) дій; відсутність чітко встановленої програми щодо протидії такій категорії злочинних діянь; складність

процедури розкриття цього злочину, збирання і створення доказової системи, тощо.

Окрім цього, однією із причин низького рівня ефективності при розкритті та розслідуванні цього злочину є те, що переважна більшість працівників слідчих та оперативних підрозділів наразі не відповідають тому рівню підготовки, щоб дієво розкривати та розслідувати подібного роду злочини. Тобто ними в недостатній мірі використовуються спеціальні знання, невдало визначається предмет цього злочину та елементи, що підлягають доказуванню. Адже проблематика розслідування злочину, передбаченого ст. 361 КК України, перш за все обумовлюється потребою використовувати спеціальні знання, засоби, методи збирання та дослідження слідової «картини», що формується в межах електронних засобів ЕОМ та їх системах, відображаючи віртуальне середовище.

З наведеного випливає актуальність порушеної проблематики окресленого питання, зокрема в контексті прояву криміналістичного аспекту.

Теоретичне підґрунтя дослідження представлене науковими працями видатних вчених різних галузей права, які займалися висвітленням комп'ютерних злочинів загалом та в аспекті застосування криміналістичних засад, зокрема: Д.С. Азарова, Ю.М. Батуріна, П.Д. Біленчука, А.С. Білоусова, В.В. Василевича, А.Ф. Волобуєва, В.Д. Гавловського, В.А. Губановим, О.В. Демешко, М.В. Карчевським, О.І. Котляревським, В.Г. Лукашевичем, С.А. Кузьміною, О.В. Мазоліною, Т.В. Михальчуком, О.І. Мотляхом, В.Ю. Рогозіна, С.А. Смірнова, О.П. Снігерьова, О.А. Самойленка, М.І. Хавронюка, В.Б. Харченка, В.С. Цимбалюка, Н.Г. Шурухнова, О.М. Яковлєва, Н.М. Ярмиша та інших.

Водночас, не дивлячись на значний масив теоретичних напрацювань, слід вказати, що на сьогоднішній день фактично не існує

комплексних досліджень з виявлення проблематики розслідування даної категорії злочинів, деякі питання піддавались розкриттю лише фрагментарно. Наведене обумовлює актуальність та значимість окресленої тематики дослідження, вказуючи на необхідність приділення уваги саме на висвітлення питання щодо особливостей розслідування злочину, передбаченого ст. 361 КК України.

Зв'язок роботи з науковими програмами, планами, темами. Кваліфікаційну роботу виконано згідно з розробленим кафедрою національного, міжнародного права та правоохоронної діяльності факультету бізнесу і права ХДУ планом проведення актуальних наукових досліджень та у відповідності до ініціативної теми кафедри («Теорія та практика реформування галузевого законодавства України», № 0118U006817).

Мета та завдання дослідження. Мета кваліфікаційної роботи полягає у тому, щоб шляхом аналізу теоретичних напрацювань та чинного кримінального процесуального законодавства виявити існуючі криміналістичні засади, необхідні для з'ясування особливостей розслідування несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Досягнення поставленої мети передбачає вирішення наступних **завдань**:

– розглянути поняття та виокремити види комп'ютерних злочинів;

– виявити способи, обстановку та слідову картину комп'ютерних злочинів;

– надати характеристику особі злочинця, якою вчиняються комп'ютерні злочини;

– дослідити організаційні і тактичні особливості розслідування несанкціонованого втручання в роботу електронно-обчислювальних

машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку.

Об’єкт дослідження – суспільні відносини, що виникають у процесі застосування криміналістичних засад під час розслідування несанкціонованого втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку.

Предмет дослідження – особливості розслідування несанкціонованого втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку.

Методи дослідження. Методологічна основа кваліфікаційної роботи представлена загальнонауковими та спеціально-юридичними методами. Діалектичний метод сприяв наданню загальної характеристики комп’ютерним злочинам. Системно-структурний метод дозволив визначити логіку взаємозв’язків за системою елементів криміналістичної характеристики комп’ютерних злочинів. Порівняльний метод допоміг виявити місце методики розслідування окресленого злочину в межах дослідження. Метод системного аналізу дозволив зосередити увагу не проблемах та недоліках під час виявлення особливостей розслідування окресленого злочину в межах дослідження.

Наукова новизна одержаних результатів полягає в тому, що на базі опанування спеціальної літератури та чинного кримінального процесуального законодавства, було всебічно та комплексно проаналізовано категоріально-понятійний апарат комп’ютерних злочинів; виявлено класифікацію видів комп’ютерних злочинів; надано криміналістичну характеристику комп’ютерних злочинів, в тому числі щодо злочину, передбаченого ст. 361 КК України, виступаючого основним для дослідження в межах теми кваліфікаційної роботи; досліджено організаційно-тактичні особливості розслідування злочину,

передбаченого ст. 361 КК України. Крім того, звернено прискіпливу увагу на труднощі, які виникають під час розслідування злочину, передбаченого ст. 361 КК України.

Практичне значення одержаних результатів полягає в тому, що надані в роботі висновки, пропозиції та рекомендації можна використовувати для подальшого розкриття даної тематики, практичній діяльності, а окремі положення та висновки роботи – під час підготовки і проведення практичних занять з курсу «Криміналістика», «Кримінальний процес», «Методика розслідування окремих видів злочинів» та інших дисциплін кримінального процесуального спрямування.

Апробація результатів дослідження. Основні положення дослідження були представленні на V-ій Всеукраїнській мультидисциплінарній науково-практичній інтернет-конференції «Міждисциплінарний підхід до наукових досліджень» (26 листопада 2021 р., м. Одеса).

Структура роботи обумовлена метою, задачами, об’єктом та предметом дослідження й складається зі вступу, двох розділів, висновків, списку використаних джерел.

Повний обсяг роботи становить 76 сторінок: основний текст – 67 сторінок, обсяг, що займає список використаних джерел і літератури (70 найменувань) – 9 сторінок.

РОЗДІЛ 1
КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА КОМП'ЮТЕРНИХ ЗЛОЧИНІВ (КІБЕРЗЛОЧИНІВ)

1.1. Поняття, види комп'ютерних злочинів

Початок нашого дослідження пропонуємо розпочати з дослідження такої категорії як «комп'ютерні злочини» (кіберзлочини). В сучасному світі мільярди осіб розташовують можливістю доступу до мережі «Інтернет». З регулярним зростанням її користувачів, збільшується також і кількість осіб, які сприймають глобальну мережу як майданчик для вчинення протиправних діянь. Системи комп'ютерного та телекомунікаційного характеру відкривають не лише унікальну можливість, аби задовольняти найбільш широкі запити людини за усіма сферами її життєдіяльності, але й формують сприятливі умови з приводу вчинення різних злочинних дій. Починають з'являтися цілі організовані групи, мета яких – створювати злочинний бізнес, базисом якого виступає шахрайство у сфері новітніх технологій, за рахунок чого отримуються колосальні прибутки. В результаті виокремлюється окрема категорія комп'ютерних злочинів, вчинюваних за допомогою цифрових технологій.

Слід вказати, що комп'ютерні злочини є порівняно новим явищем в аспекті дослідження наукою кримінального права та криміналістики. В Україні перший комп'ютерний злочин зафіксовано у 1990 році. Так, програмою для електронно-обчислювальної машини (ЕОМ), якою здійснювався перерахунок комсомольських внесків працівників одного з промислових підприємств до розрахункового рахунку районного комітету комсомолу, мало місце її перепрограмування, щоб відраховувати відповідні грошові суми не тільки із заробітної плати членів комсомолу, а й усіх інших працівників підприємства [1, с. 76].

Саме після цього випадку категорію комп'ютерних злочинів поступово починають замінювати вживанням поняття «кіберзлочинність (кіберзлочини)».

В контексті наведеного зазначимо, що наразі ні в документах міжнародного зразку, ні за вітчизняним законодавством не розроблено єдиної термінології та підходу з приводу поняття кіберзлочинності, застосовуваного у прив'язці з поняттям комп'ютерна злочинність. Проте саме поняття кіберзлочинності є ширшим, ніж комп'ютерна злочинність, яке більш детально розкриває природу такого глобального явища, як злочинність за інформаційним простором. Якщо термін кіберзлочинності є співвідносним як із використанням комп'ютерів та інформаційних технологій (глобальних мереж), то в поняття комп'ютерної злочинності вкладається осмислення злочинів, здійснюваних проти електронних пристроїв та даних, які в них містяться.

Опубліковані теоретичні джерела продовжують проводити дискусії щодо визначення підходів поняття «кіберзлочини». По суті дане питання в переважній більшості розкривається кримінологами або фахівцями в галузі права [2, с. 55]. Відсутність повноцінного понятійного-категоріального апарату, яким забезпечується сфера окреслених злочинів, зайвий раз доводить про відсутність осмисленого розуміння змісту цієї проблеми, її актуальність та спостережливість як зі сторони вченої спільноти, так і з сторони громадянського суспільства щодо нових погроз зростаючих масштабів злочинності.

Продовжуючи, зазначимо, що існування різноманіття з приводу трактування окресленої категорії зводиться декількома основними підходами. Згідно з першим під кіберзлочином вважається протиправне діяння, вчинене через використання комп'ютерних пристроїв (незаконність зберігання та/або поширення інформації з використанням комп'ютерних технологій). В цілому, за цим підходом кіберзлочини

пов’язані з різними правопорушеннями, які вчиняються в рамках електронних мереж [3, с. 26].

Другий підхід відносить кіберзлочини до протиправних діянь, що вчиняються через комп’ютерний та мобільний зв’язок в інформаційних мережах, насамперед в Інтернеті, а також за рахунок їх програмних складових щодо інформації, яка розміщується в межах віртуального простору Інтернет. Даний підхід слід відмічати як вузький, що концентрується виключно на злочинних діяннях в рамках електронних мереж [3, с. 27].

Третій підхід ще прийнято називати інтеграційним, за яким об’єднують два окреслених вище підходи. За даним підходом кіберзлочини вважаються суспільно небезпечними діяннями, вчинювані через використання засобів та способів комп’ютерного і мобільного зв’язку, в яких електронний пристрій характеризується знаряддям кримінальних посягань в межах віртуального простору. В контексті вказаного, з позиції кримінального права кіберзлочин – це винне суспільно небезпечне, кримінально каране втручання в роботу комп’ютерів (програм, мереж) та інші протиправні діяння, вчинювані через комп’ютери, їх мережі та програми з метою отримання доступу до віртуального простору [3, с. 28-29].

Говорячи про визначення, представлені науковою спільнотою, виокремимо деякі. Певними фахівцями вважається, що «комп’ютерні злочини – це всі злочинні дії, при яких комп’ютер є знаряддям, засобом чи метою їх здійснення» [4, с. 31]. Інше визначення під терміном комп’ютерних злочинів об’єднує «всі протизаконні дії, які завдають збитки майну і пов’язані з електронним опрацюванням даних» [5, с. 12]. Третім визначенням комп’ютерних злочинів висвітлюються наступні основоположні види протиправних дій, зокрема: «1) комп’ютерні майнові злочини (наприклад, комп’ютерне шахрайство, саботаж, промисловий шпіонаж); 2) комп’ютерні злочини проти прав особи;

3) правопорушення проти громадських і суспільних правових цінностей (наприклад, проти національної безпеки)» [6, с. 87].

Враховуючи наведені визначення, юридична література надає характерні ознаки комп'ютерної злочинності, які на наш погляд, є досить вдалими, а саме: 1) притаманність міжнародного характеру злочину; 2) складність визначення «місцезнаходження злочину»; 3) слабкий зв'язок між ланками за системою доказів; 4) неможливість візуального спостереження та фіксування доказів; 5) широкий спектр використання шифрованої інформації злочинцями [7, с. 13].

Комп'ютерні злочини є якісно новим видом злочинності в Україні, що не скажеш про світову практику, де їх діапазон неймовірних масштабів. Практично навіть дилетанти, так і досвідчені злочинці, на сьогоднішній день можуть знайти доступ проникнення до різноманітних комп'ютерних систем та їх даних. Даний вид суспільно небезпечного діяння нині, як вже зазначалось вище, недостатньо досліджений.

З метою продовження розкриття змісту комп'ютерних злочинів саме як кіберзлочинів, нас може зацікавити міжнародний аспект використання такої термінології. Наприклад в Конвенції про кіберзлочинність від 23 листопада 2001 року, до таких діянь відносяться: незаконний доступ до комп'ютерних систем (ст. 2); нелегальне перехоплення даних, передача яких реалізується через цифрові канали зв'язку (ст. 3); втручання в дані, які зберігаються за комп'ютерними системами або передаються через електронні канали зв'язку (ст. 4); втручання в комп'ютерні системи (ст. 5); зловживання комп'ютерними пристроями (ст. 6); здійснення підробок, пов'язаних з комп'ютерами (ст. 7); шахрайські дії, які пов'язуються з комп'ютерами (ст. 8) [8] тощо.

У 2013 році Управління ООН по боротьбі з наркозлочинністю опубліковало Звіт, яким поняття кіберзлочинності поставили в залежність від контексту та мети вживання даної дефініції. Окрім цього, Звітом зазначається, що до переліку комп'ютерних злочинів

включаються не лише злочинні діяння проти конфіденційності, цілісності та доступності даних, але й інші дії, цілеспрямовані на протизаконне отримання прибутку в кіберпросторі. Серед іншого, як вказувалось авторами Звіту – створювати якесь універсальне визначення кіберзлочинності немає сенсу, оскільки, враховуючи аспект міжнародної співпраці під час розслідування злочинів, набагато важливішим є гармонізація норм, які мають безпосереднє відношення до збору та надання електронних доказів. Відтак, такий штучний термін як «кіберзлочин» не може обмежити таку необхідність, тому що на електронних носіях та комунікаціях може зберігатись інформація, що належить до будь-якого виду кримінальних правопорушень, вчинюваних в межах як кіберпростору, так і поза ним [9].

Ширше кіберзлочини розглядали автори «Модельного закону» про кіберзлочинність Міжнародного союзу електрозв'язку, взаємопов'язуючи їх з незаконними діями, вчинюваними в сфері кіберпростору, а до предмету злочинних відносили: «комп'ютери, комп'ютерні системи, мережі, їх комп'ютерні програми, комп'ютерні дані, дані контенту, рух даних і користувачі» [10].

Далі слід вказати на основоположний Розділ XVI Кримінального кодексу України «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» [11] (далі – КК України), в якому міститься ряд норм, які передбачають кримінальну відповідальність за вчинення злочинних діянь у сфері використання комп'ютерних технологій. Перелічувати усі норми глави не будемо, а виокремимо лише ключову в межах нашого дослідження ст. 361 КК України, в якій викладено наступне: «несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації,

спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, – карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, – караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років» [11]. Застосування цієї спеціальної норми під час кваліфікації комп'ютерних злочинів полягає не лише у кримінально-правовій функції, але й у здійсненні ряду криміналістичних функцій, у тому числі – забезпеченні напрацювань з приводу методики виявлення та розкриття злочинів, їх профілактичних засобів, тощо. Також додамо, що в процесі подальшого дослідження, аби постійно не дублювати досить об'ємну назву вищенаведеної статті, будемо просто оперувати ст. 361 КК України.

Отже, враховуючи теоретичні напрацювання, на цій підставі сформулюємо поняття комп'ютерних злочинів під якими потрібно осмислювати суспільно небезпечну діяльність, здійснювану шляхом використання сучасних інформаційних технологій та засобів комп'ютерної техніки з ціллю спричинення збитків майнового або суспільного інтересу держави, а також порушення прав певної особи.

Наведене визначення дає можливість констатувати, що комп'ютерні злочини є складним, відносно новим явищем кримінально-правової практики, яке вимагає більш досконалого спеціального та систематичного опанування.

Для ефективної протидії злочинів у сфері використання комп'ютерних систем, важливим моментом є виявлення

криміналістичної суті видів розглядуваного злочину, що в свою чергу викликає потребу їх наукової класифікації.

Зазначимо, що переважною більшістю фахівців комп'ютерні злочини представлені двома типами:

1) злочини, об'єкт здійснення яких виступає ЕОМ, за якими: знешкоджуються або замінюються дані, програмне забезпечення та обладнання; розкрадаються вхідні, вихідні дані, програмне забезпечення та обладнання; відбувається економічне шпигунство та розголошуються відомості, які становлять державну та/або комерційну таємницю (придбання за допомогою протиправних засобів або викриття, переміщення чи використання комерційної таємниці без відповідного дозволу чи інших підстав законного характеру з ціллю – нанести економічну шкоду особі, допущеної до таємниці, або отримати протизаконну економічну вигоду для інших осіб);

2) протизаконні акції, для реалізації яких ЕОМ використовують як знаряддя для досягнення злочинної цілі, зокрема: комп'ютерний саботаж (ліквідації або фальсифікації інформації, пошкодження засобів інформаційної техніки через проникнення до комп'ютерних мереж з ціллю перешкоджання функціонування комп'ютерних систем); вимагання та шантаж; розтрата; розкрадання коштів, тощо [4, с. 55-58].

Значний вклад щодо криміналістичної кваліфікації розглядуваної категорії злочинів зробили ведучі промислово розвинутих держав світу, представивши так званий «мінімальний список порушень» та «необов'язковий список порушень», прийнятих державами-членами Європейського співтовариства [12, с. 61].

«Мінімальний список порушень» складається з таких видів комп'ютерних злочинів: «комп'ютерне шахрайство, підробка комп'ютерної інформації, ушкодження даних ЕОМ або програм ЕОМ, комп'ютерний саботаж, несанкціонований доступ, несанкціоноване

перехоплення даних, несанкціоноване використання захищених комп'ютерних програм, несанкціоноване відтворення схем» [12, с. 64].

«Необов'язковий список» складається з таких видів комп'ютерних злочинів: «зміна даних ЕОМ або програм ЕОМ, комп'ютерне шпигунство, несанкціоноване використання ЕОМ, несанкціоноване використання захищеної програми ЕОМ» [12, с. 66].

Далі зробимо акцент на одну із найбільш поширених класифікацій комп'ютерних злочинів, базисом якої є кодифікатор робочої групи Інтерполу, який взяли за основу у процесі розробки автоматизованої інформаційно-пошукової системи 90-хх рр. Згідно з названим кодифікатором класифікація комп'ютерних злочинів мала наступний вигляд:

– несанкціонований доступ та перехоплення відмічається комп'ютерним абордажем; перехопленням; крадіжкою часу;

– зміна комп'ютерних даних відмічається логічною бомбою; троянський конем; комп'ютерним вірусом; комп'ютерним черв'яком;

– комп'ютерне шахрайство відмічається шахрайством з банкоматами; комп'ютерною підробкою; шахрайством з ігровими автоматами; маніпуляціями з програмами вводу-виводу; шахрайством з платіжними коштами; телефонним шахрайством;

– незаконне копіювання відмічається комп'ютерними іграми; іншим програмним забезпеченням; типологією напівпровідникових пристроїв;

– комп'ютерний саботаж вчиняється через апаратне та програмне забезпечення;

– інші комп'ютерні злочини відмічаються використанням комп'ютерних на табло оголошень; передачею інформації, яка є обов'язковою в судовому порядку [13, с. 110-112].

Виходячи з наведеної класифікації, можна зрозуміти обґрунтовані позиції багатьох криміналістів з приводу того, що криміналістична

класифікація слугує фундаментом побудови не лише криміналістичної характеристики, але і системи криміналістичних методик розслідування комп'ютерних злочинів.

У зв'язку з наведеним, в контексті використання криміналістичного аспекту в межах нашого дослідження, вбачаємо за доцільне запропонувати наступний підхід класифікації комп'ютерних злочинів:

1) ліквідація (руйнація) інформації;

2) незаконне заволодіння інформацією або порушення права її використання, що може мати прояв у: неправомірному заволодінні інформації як комплексу відомостей (документів) щодо порушення прав володіння; неправомірному заволодінні інформації як алгоритму; неправомірному заволодінні інформацією як товаром;

3) дія або бездіяльність стосовно генерації інформації з заданими властивостями, а саме: поширення інформаційно-обчислювальних мереж інформації через телекомунікаційні канали, наносячи збиток абонентам; виготовлення та розповсюдження комп'ютерних вірусів для ЕОМ;

4) неправомірна модифікація інформації, яка характеризується комплексом фактів та відомостей; алгоритмом; товаром з ціллю використання її корисних властивостей.

На нашу думку, наданий підхід класифікації комп'ютерних злочинів дає можливість більш прозоро осмислити механізм вчинення таких злочинних діянь, а також відобразити виключно криміналістичні особливості, оскільки його підґрунтям виступають злочинні дії та механізм утворення слідів, тобто весь комплекс дій, завдяки яким визначаються вектори під час розслідування комп'ютерних злочинів, в тому числі, передбаченого ст. 361 КК України.

На підставі вищевикладеного можна зробити наступні висновки. Здійснивши аналіз теоретичних напрацювань щодо визначення поняття

комп’ютерних злочинів (кіберзлочинів), нами було сформульовано власне поняття комп’ютерних злочинів під якими потрібно осмислювати суспільно небезпечну діяльність, здійснювану шляхом використання сучасних інформаційних технологій та засобів комп’ютерної техніки з ціллю спричинення збитків майнового або суспільного інтересу держави, а також порушення прав певної особи.

Наведене визначення дало можливість констатувати, що комп’ютерні злочини є складним, відносно новим явищем кримінально-правової практики, яке вимагає більш досконалого спеціального та систематичного опанування.

Встановлено, що для ефективної протидії злочинів у сфері використання комп’ютерних систем, важливим моментом є виявлення криміналістичної суті видів розглядуваного злочину, що в свою чергу викликало потребу їх наукової класифікації, на підставі якої нами в контексті використання криміналістичного аспекту в межах нашого дослідження, запропоновано власний підхід класифікації комп’ютерних злочинів.

1.2. Способи, обстановка та слідова картина комп’ютерних злочинів

Протидія комп’ютерних злочинам вимагає використання дієвих механізмів боротьби із злочинностю з метою розкриття та розслідування конкретних кримінальних правопорушень у «сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку» [11]. Проте це потребує наявності сучасних методик розслідування, для виявлення яких в даному підрозділі дослідження насамперед потрібно приділити увагу кожному елементу, зокрема: способам, обстановці та слідовій картині комп’ютерних злочинів.

1. Розглядаючи способи комп'ютерних злочинів, попередньо відзначимо, що вони є практично недослідженими в межах даної категорії.

Розкриваючи способи комп'ютерних злочинів, передбачених розділом XVI КК України, слід вказати, що їх можливо вчиняти з використанням засобів комунікацій віддаленого доступу, без потреби присутності правопорушення на місці вчинення злочину (йдеться про загальне розуміння). Протягом останнього часу можемо спостерігати тенденцію, коли комп'ютерна злочинність зрощується з традиційною організованою злочинністю, тим самим, доволі частими є випадки несанкціонованого проникнення в банківські кредитно-розрахункові комп'ютерні системи, торгівлю через мережу Інтернет, тощо [14, с. 89].

Також комп'ютерні злочини, передбачені розділом XVI КК України, характеризуються тим, що більша їх частина (в тому числі злочину, передбаченого ст. 361 КК України), не піддається виявленню без використання спеціальних заходів практичного спрямування. На прикладі ст. 361 КК України можна відзначити, що зловмисником, яким здійснено несанкціоновану копію інформації з жорсткого диску ЕОМ на USB-носій – практично не залишається слідів (в плані фіксування поетапності своїх дій на комп'ютері). Подібне можна пояснити тим, що першочергово операція з копіювання інформації з USB-носія на USB-носій створювалась як функціонально необхідна в ЕОМ, а відтак, не передбачалось ніяких заходів з приводу її авторизації [14, с. 89].

Слід відмітити і те, що специфічність вчинення комп'ютерних злочинів, передбачених розділом XVI КК України – встановлює їх високий рівень латентності. При цьому латентність, враховуючи специфіку вчинення та фіксації кримінальних правопорушень володіє природним характером. Штучна латентність, за ініціативою правоохоронних органів, практично відсутня, бо більшість існуючих

злочинів, передбачених розділом XVI КК України, як правило, мають суттєвий суспільний резонанс, однак з іншої сторони – власники комп'ютерних систем не квапляться повідомляти третім особам про успішні атаки на їх системи [15, с. 13-14].

Останнім способом вчинення комп'ютерних злочинів, передбачених розділом XVI КК України, можна вважати використання зі злочинною ціллю шкідливих програмних продуктів. Так, заражені так звані «комп'ютери-жертви» без згоди на це їх власників являються учасниками botnet-мереж. Відбувається крадіжка особистих персональних та комерційних даних користувачів, їх конфіденційна інформація, ключі захисту, а також використовується апаратний ресурс «комп'ютера-жертви» з подальшим проведенням DDoS-атак, несанкціонованих розсилок повідомлень, тощо [16, с. 551].

2. Наступним елементом є обстановка комп'ютерних злочинів. Обстановка з точки зору криміналістики «вивчає середовище, в якому вчинюється злочин» [16, с. 563]. Відмітимо, що під час розслідування будь-якого злочину (в тому числі комп'ютерного) органом досудового розслідування – спочатку відбувається сприйняття та аналіз обстановки. Виявлення обстановки злочинного діяння дає можливість слідчому відтворити уявлення щодо механізму здійснення злочину та ймовірного місця пошуку слідів, особи злочинця, а також деяких аспектів способу його вчинення.

Зауважимо, що вченими-криміналістами не надається єдиного розуміння стосовно тлумачення обстановки злочинів. Зокрема, Т.С. Анненкова під обстановкою вчинення злочину осмислює «систему взаємопов'язаних і взаємообумовлених елементів в просторових межах яких, здійснюється взаємодія учасників злочину, а також інших різних обставин об'єктивного середовища, що впливають на формування слідів злочину, його розслідування та розкриття» [17, с. 55]. На думку М.П. Яблокова, під обстановкою вчинення злочину потрібно сприймати

«систему різного роду взаємодіючих між собою до та в момент вчинення злочину об’єктів, явищ та процесів, що характеризують місце, час, матеріальні, природно-кліматичні, виробничі, побутові та інші умови навколишнього середовища, а також інші фактори об’єктивної реальності, що визначають можливість, умови та інші обставини скоєння злочину» [18, с. 36].

На наш погляд, більш поглиблено досліджував дане питання В.Ф. Єрмолович, яким цілком правильно пропонувалось у криміналістичному аспекті розуміти саме обстановку злочину, якій притаманно три самостійні ланки: «обстановка, яка передувала скоєнню злочину; обстановка скоєння злочину; обстановка, яка склалася після скоєння злочину» [19, с. 181]. Вчений додає, що «цим зумовлюється трактування обстановки злочину як системи умов та обставин, сформованих взаємодією між собою до, під час і після скоєння злочину об’єктів, явищ, процесів в певному часі та місці, а також суб’єктів злочину з іншими особами, що впливають на настання злочинного результату» [19, с. 182].

Говорячи про поняття обстановки комп’ютерного злочину, то тут слід відмітити, що юридична література також не пропонує конкретного трактування. Доречно зауважує Л.П. Звернявська: «такі злочини здійснюються у певному, особливому середовищі – кіберпросторі. Значущою інформацією для криміналістичної оцінки буде те, як був захищений предмет злочину, яким чином були задіяні учасники, в яких географічних та часових умовах здійснювався злочин» [20, с. 39].

В контексті наведеного слід зауважити, що під кіберпростором осмислюють «інформаційне середовище (простір), яке виникає (існує) за допомогою технічних (комп’ютерних) систем при взаємодії людей між собою, взаємодії технічних (комп’ютерних) систем та управлінні людьми цими технічними (комп’ютерними) системами» [21, с. 65].

На нашу думку, брати до уваги таку специфічну ознаку як кіберпростір є правильним, проте потрібно враховувати й інші не менш важливі ознаки матеріального (реального) середовища, які є суттєвими у процесі розслідування подібних злочинів.

Тож, на підставі наведеного, вбачаємо за доцільне в обстановці комп'ютерних злочинів виокремлювати такі складники: 1) кіберпростір, за яким відбувається електронний процес (до, в момент та після вчинення кримінального правопорушення, що відмічається місцем, часом та взаємодією у віртуальному просторі учасників діяння); 2) матеріальний (фізичний) простір – комплекс умов та обставин, взаємодіючих між собою (до, в момент та після вчинення кримінального правопорушення щодо об'єктів, процесів, що відмічають місце, час та фактичний взаємозв'язок учасників діяння).

Продовжуючи, зазначимо, що у процесі розслідування комп'ютерних злочинів вагоме значення відводиться інформації з приводу ймовірного місця та часу його вчинення. Для слідчого важливо встановити місце скоєння злочину. Взагалі установлення місця вчинення злочинного діяння сприяє встановленню місцезнаходження можливих доказів та осіб, які можуть бути причетними до нього. Конкретно час вчинення комп'ютерного злочину дає змогу з'ясувати послідовність та тривалість вчинюваних злочинних дій. Прикладом може послугувати, коли особи домовились вчинити DoS-атаку в конкретний день та часовий проміжок, використовуючи допоміжні програми, за якими узгоджували свої дії (Instagram, Telegram, Viber, тощо).

Аналізуючи місце вчинення злочину, необхідно зробити акцент на тому, що воно обирається суб'єктами злочинного діяння аж ніяк не випадково. Тобто, здійснивши попередню оцінку з різних сторін про ймовірне місце, суб'єктом воно використовується в якості засобу, аби реалізувати свій злочинний намір [22, с. 744]. В свою чергу, піддаючи аналізу час вчинення злочину, принагідно сказати, що він не завжди

обмежений астрономічними характеристиками (секунда, хвилина, година, місяць, рік). Тобто час в даному випадку може пов'язуватись з сезонністю, коли настає темна чи світла доба, час відпочинку, тощо [22, с. 746].

Враховуючи специфічність комп'ютерних злочинів, в тому числі, передбачених розділом XVI КК України, до місця їх вчинення слід виокремлювати: електронне середовище (вузли мережі), за якими розташовуються (програмно-технічні засоби, які піддались злочинному впливу, а також точки їх доступу до відповідних мереж; програмно-технічні засоби, які використовувались злочинцем опосередковано, а також точки їх доступу до відповідних мереж; мережні вузли каналів зв'язку, при використанні яких відбувався обмін інформацією між програмно-технічними засобами злочинця та потерпілою особою) [23, с. 72-73].

Говорячи про вибір фізичного середовища злочинцем, доречно буде погодитись з позицією О.І. Мотляха, який зазначав, що злочинцями даного злочину обираються, як правило, наступні місця:

– приміщення адміністративного та службового типу суб'єктів господарювання (підприємства, організації, компанії, тощо), які використовують, аби проводити свою виробничу діяльність електронних пристроїв;

– власні та орендовані житлові приміщення (офіси, квартири, кімнати, тощо), в межах яких встановлюються електронні пристрої з можливістю виходу до мережі Інтернет;

– приміщення комунальної власності (цокольні, напівпідвальні, тощо), які на правах власності або оренди можуть бути задіяні у вигляді комп'ютерних клубів [24, с. 64].

Акцентуючи більш прискіпливу увагу на основне електронне середовище як місце комп'ютерного злочину, тут доцільно підтримати

Л.П. Зверянську, яка конкретизувала місця вчинення комп'ютерних злочинів, а саме:

– робоча станція як місце для обробки інформації, яка стала предметом злочинного посягання;

– місце з постійним зберіганням та/або інформації – сервер;

– місце з використанням технічних засобів для несанкціонованого доступу до комп'ютерної інформації, що перебуває в межах іншої точки (як приклад, злам через зовнішній віддалений мережевий доступ);

– місце, де відбувається підготовка злочинів (розробка вірусів, програм зламу, підбір паролів, тощо) або місце безпосереднього використання інформації (копія, поширення, ліквідація, тощо) щодо несанкціонованого доступу до даних, розташованих на пристрої [25, с. 40].

З метою продовження важливо вказати, характерною особливістю комп'ютерних злочинів є те, що для них не властиве просторове обмеження і вчинення кримінального правопорушення може виходити за межі однієї держави. Тобто злочинне діяння відбулось в межах однієї держави, а негативні наслідки настали в іншій. Саме тому таким злочинам притаманний транснаціональний характер (наявність іноземної складової в криміналістичній характеристиці та в кримінально-процесуальних відносинах при його розслідуванні) [26, с. 56].

Серед іншого, з'ясування часу вчинення комп'ютерних злочинів не передбачає особливих проблем, тому що операційна система електронного пристрою деталізовано простежує практично кожну важливу операцію, інформаційні дані щодо якої відображаються в межах статистичних файлів. З врахуванням програм загальносистемного призначення вбачається за можливе з'ясувати поточний час функціонування комп'ютерної системи. Це дозволяє за тією чи іншою командою вивести на екран дисплею інформацію з приводу секунди,

хвилини, години та ін., стосовно якої виконувалась відповідна операція [27, с. 101].

Насамкінець додамо, що бувають ситуації, при яких час вчинення комп'ютерного злочину з'ясувати не видається за можливе. Наведене можна обумовлювати технічними факторами (перезавантажується електронний пристрій; обнуляються або стираються інформаційні дані, тощо). У зв'язку з цим, час вчинення потрібно з'ясовувати через проведення комп'ютерно-технічної експертизи. Між тим, час вчинення комп'ютерного злочину можливо з'ясувати і при проведенні окремих слідчих (розшукових) дій (про це поговоримо в наступному розділі дослідження).

3. Останнім елементом криміналістичної характеристики комп'ютерних злочинів є слідова картина. Завдяки слідовій картині можливо виявити механізм скоєного злочинного діяння у віртуальному середовищі.

Перш за все слід вказати, що термін «слід» вживається як у процесуальному, так і криміналістичному значенні. Процесуальне значення відмічається таким: «отримана з його допомогою інформація використовується для формування доказової бази і згодом відображається в процесуальних документах» [20, с. 47]. Криміналістика ж «слід» викладає як «будь-які зміни в середовищі, що виникають внаслідок вчинення злочинної діяльності. Сліди є носіями певної сукупності інформації, яка може бути використана як для розшукових дій, так і для висування версій, визначення напряму дій слідчого» [28, с. 102].

Тож, з наведеного можна явно прослідкувати, що комп'ютерним злочинам властива специфічна картина слідів. Зокрема, на місці події повинні бути віртуальні сліді, розташованих в пам'яті електронних пристроїв. Взагалі віртуальні сліди характеризуються слідами вчинення

будь-яких дій в межах інформаційного простору комп'ютерних та інших цифрових пристроїв, їх мереж та систем [29, с. 519].

Зауважимо, що теорія криміналістики має різні точки дотику щодо розуміння віртуальних слідів: «1) віртуальні сліди як зміна автоматизованої інформаційної системи; 2) віртуальні сліди з точки зору фізичної і квантової теорії; 3) віртуальні сліди як результат логічних і математичних операцій з двійковим кодом і багато інших» [30, с. 167].

Окрім наведених визначень вкажемо на те, що першим хто запропонував в криміналістиці поняття «віртуальні сліди» є В.О. Мещеряков, який під ними осмислював «будь-яку зміну стану автоматизованої інформаційної системи, пов'язану з подією злочину і зафіксовану у вигляді комп'ютерної інформації. Такі сліди займають умовно проміжну позицію між матеріальними та ідеальними слідами» [31, с. 266]. П.Д. Біленчук підтримував аргументи вченого та виокремлював віртуальні сліди за самостійною групою нарівні з ідеальними та матеріальними. «В результаті електронно-цифрового відображення на матеріальному носії фіксується образ з цифрових значень параметрів формальної математичної моделі спостережуваного реального фізичного явища», – вважає вчений [32, с. 215]. Подібна позиція представлена іншою групою авторів (В.О. Давидовим та А.Ю. Головіним), які під віртуальними слідами розуміли «зафіксовану у вигляді цифрового способу формальної моделі зміну стану інформації в пам'яті абонентських електронних пристроїв (терміналів, білінгових систем тощо), викликану алгоритмом встановленого програмного забезпечення і пов'язану з подією злочину (що має кримінально-релевантне значення)» [33, с. 255].

Встановивши, що собою являють віртуальні сліди, не потрібно забувати, що комп'ютерні мережі – це складні системи взаємодії різноманітного технічного обладнання, в межах якого відбувається неймовірне різноманіття віртуальних слідів.

Беручи до уваги наведене, класифікація віртуальних слідів під час вчинення комп'ютерних злочинів має наступний вигляд:

1) за походженням: електронна інформація, реалізована ЕОМ під час свого функціонування; електронна інформація, реалізована під час діяльності людини; похідна електронна інформація, реалізована комп'ютером, виходячи з введених даних користувачем або інформація, реалізована з даних, які генерувались безпосередньо комп'ютерною системою;

2) за формою подання: інформація, яка доступна для сприйняття людиною; інформація, яка представлена у вигляді машинного коду;

3) за місцем зберігання: а) дані, збережені в комп'ютерних системах (ЕОМ, сервери, локальні та глобальні мережі); б) дані, які підлягали копіюванню або переміщенню користувачем на електронні носії; в) паперові копії (листування, скріншоти та ін.);

4) за формою: вихідні дані; коди шифрування; різні види програмного забезпечення; комп'ютерні системи (ЕОМ, сервери, локальні та глобальні мережі) [34, с. 302-303].

В свою чергу, Л.Б. Краснова пропонувала класифікувати віртуальні сліди, виходячи з механізму їх утворення – на первинні та вторинні. «Первинні формують безпосередній вплив користувача з використанням будь-якої інформаційної технології, а вторинні – в результаті впливу технологічних процесів без участі людини», – вказує вчена [35, с. 11].

На нашу думку, віртуальні сліди характеризуються цифровим образом, електронними сигналами, що залишають в пам'яті електронних пристроїв та які передаються через заданий алгоритм. Окрім цього, будь-які дії з використанням високоточних пристроїв залишають свій слід в їх пам'яті. Найбільш явними в даному аспекті є сліди пам'яті комп'ютера (сліди включення/виключення; сліди різноманітних

операцій із вмістом пам’яті; сліди дій з програмами та відомостями про роботу в мережі Інтернет) [29, с. 520].

В цілому віртуальні сліди виступають доказовою базою вчинення або планування злочину відповідною особою (групою осіб). На початковому етапі виявлення віртуальних слідів проводиться опис відомостей в протоколі стосовно пристрою, в пам’яті якого знайдено віртуальні сліди; відомостей того, кому належить пристрій; чи є можливість даного пристрою до виходу у мережу Інтернет; коли конкретно файл було створено або змінено. Після чого фотографується екран з подальшим виведенням інформації про характерні властивості аналізованих файлів та в результаті відбувається їх вилучення, щоб дослідити даний об’єкт з віртуальними слідами.

Таким чином, протидія комп’ютерним злочинам вимагає використання дієвих механізмів протидії із злочинності з метою розкриття та розслідування конкретних кримінальних правопорушень, передбачених розділом XVI КК України. Проте це потребує наявності сучасних методик розслідування, для виявлення яких було приділено увагу кожному елементу, зокрема:

1) способам комп’ютерних злочинів, до яких слід відносити (вчинення з використанням засобів комунікацій віддаленого доступу; переважна більшість комп’ютерних злочинів не піддається виявленню без використання спеціальних заходів практичного спрямування; використання зі злочинною ціллю шкідливих програмних продуктів);

2) обстановці комп’ютерних злочинів, яка характеризується тим, що у процесі розслідування комп’ютерних злочинів вагоме значення відводиться інформації з приводу ймовірного місця та часу його вчинення;

3) слідовій картині, завдяки якій можливо виявити механізм скоєного злочинного діяння у віртуальному середовищі. Коректне виявлення та вивчення віртуальних слідів органами досудового

розслідування сприяють ефективно з’ясовувати факти розповсюдження інформації щодо злочину, передбаченого ст. 361 КК України.

1.3. Характеристика особи злочинця, якою вчиняються комп’ютерні злочини

Особа злочинця – центральний елемент криміналістичної характеристики злочину, передбаченого ст. 361 КК України, тому що предмет злочинного посягання, його спосіб та слідова картина завжди пов’язуються з особистісними рисами такої особи, а також закономірностями її поведінки. Аналіз особи злочинця дозволяє провести оптимізацію процесу висунення слідчих версій та забезпечити обрання найбільш раціональних тактичних прийомів, аби провести окремі слідчі (розшукові) дії під час розслідування комп’ютерних злочинів взагалі та злочину, передбаченого ст. 361 КК України, зокрема. Тож, з врахуванням дослідження поведінки та психології особи злочинця, виявляється за можливе з’ясувати дійсні причини та умови вчинення комп’ютерного злочину; оцінити суспільну небезпеку злочинця; надати коректну кримінально-правову кваліфікацію та в результаті призначити обґрунтоване і справедливе покарання.

Насамперед принагідно відмітити, що в юридичній літературі існують різні точки зору стосовно змістовного наповнення такого елементу криміналістичної характеристики як особа злочинця. Однією групою вчених особу злочинця розуміють як «соціально-біологічну систему, властивості та ознаки якої відображаються у матеріальному середовищі та використовують для розкриття та розслідування злочинів (до таких властивостей відносяться: фізичні, біологічні та соціальні)» [36, с. 112]. З позиції інших: «особа злочинця – це поняття, що виражає сутність особи, яка вчинила злочин, а до системи ознак особи злочинця включають дані демографічного характеру, деякі моральні властивості і

психологічні особливості» [37, с. 278-279]. Третьою ж групою, з-поміж існуючої інформації про особу злочинця, яка відображає його характеристику, додають «всі ті дані, які можуть визначати ефективні шляхи розшуку та викриття злочинця, і пов'язані із цим, завдання розслідування» [38, с. 99].

Отже, враховуючи наведені підходи, бачимо, що більша частина вчених до характеристики особи злочинця відносить такі складові: 1) соціальні (освіта, сімейний стан, соціальний статус, тощо); 2) психологічні (переконання, звички, емоції, темперамент, тощо); 3) фізіологічні (ознаки анатомічного та функціонального характеру, біохімічні властивості крові, слини, тощо).

Також принагідно зазначити, що характерною особливістю комп'ютерних злочинців є їх вік. Фахівцями по-різному розділялись подібного роду групи осіб. Одними виділялись дві групи осіб «у віці від 14 до 20 років; у віці від 21 року і старші» [39, с. 69], іншими такі особи характеризувались «віком від 15 до 45 років, з яких 33 % віком до 20 років, 54 % були у віці від 20 до 40 років; 13 % осіб були старшими 40 років» [40, с. 253].

В контексті наведеного, особливостями вчинення комп'ютерних злочинів особами віком до 20 років є: відсутність продуманої підготовки до злочинного діяння; відсутність оригінальних способів вчинення злочинного діяння; використання побутових технічних засобів як знарядь злочину; відсутність необхідних заходів, аби приховати злочин; проявлення необґрунтованого бешкетництва [39, с. 71].

В свою чергу, особам віком від 20 років, які вчинили комп'ютерний злочин, як правило, притаманний усвідомлений корисливий характер. Дана категорія злочинців відмічається стійкими злочинними навичками: відносяться до організованих злочинних груп; володіють серйозними професійними навиками; володіють необхідною оперативною технікою. Окрім цього, злочини, які характеризуються

серійністю та вчиняються неодноразово, завжди супроводжуються відповідними діями, щоб приховати такі злочини [39, с. 73].

Продовжуючи, зазначимо, що «професійні» звички та почерк такої категорії злочинців проявляється за певними способами, методами та прийомами вчинення комп'ютерного злочину. Так, залишені та знайдені на місці злочинного діяння сліди дають можливість встановити соціально-психологічний портрет конкретної особи, вказуючи на досвід, вік, стать, професійні навики, тощо. Як правило, такі злочини вчиняються особами з високою кваліфікацією, особливо щодо злочину, передбаченого ст. 361 КК України. Це потребує досить складних заходів технологічного та інформаційного спрямування, адже чим «хитріший» спосіб несанкціонованого доступу, тим вужче коло ймовірних злочинців [24, с. 142].

Пропонуємо виокремити ще дві досить цікаві групи можливих злочинців, які вчиняють комп'ютерні злочини.

До представників першої групи слід відносити працівників служби безпеки та інженерно-технічний персонал. Певною частиною програмістів, інженерів та операторів вчиняються несанкціоновані доступи до інформаційних систем. Значної загрози варто очікувати від працівників організацій по сервісному обслуговуванню та ремонту комп'ютерної техніки, у яких є усі важелі впливу для використання добутої ними інформації з подальшим вчиненням комп'ютерних злочинів.

До представників другої групи слід відносити осіб, які мають необхідний масив знань у сфері інформаційних технологій та які в більшості ситуацій оперують корисливими мотивами; особи, якими здійснюється перевірка фінансово-господарської діяльності підприємств, установ, організацій [41, с. 85-86].

Тож, підсумовуючи окреслені вище напрацювання, до осіб, якими можуть вчинятись комп'ютерні злочини, потрібно відносити: 1) осіб,

якими вчиняються операційні злочинні діяння (оператори, за рахунок яких забезпечується робота комп'ютерів); 2) осіб, які під час вчинення комп'ютерного злочину залучають програмне забезпечення (системні та прикладні комп'ютерні програмісти; спеціалісти по захисту інформації); 3) осіб, які проводять обслуговування апаратної частини (системні та електронні інженери); 4) осіб, які проводять організаційну роботу стосовно інформаційних систем (керівники підприємств, установ та організацій, з наявністю в їх розташуванні комп'ютерів; адміністратори комп'ютерних мереж та баз даних).

Зауважимо, що під час розслідування злочину, передбаченого ст. 361 КК України, необхідно з'ясувати наявність спеціального суб'єкта – особи з правом доступу до комп'ютерної інформації. Принагідно додати, що під час несанкціонованого доступу до ЕОМ – поширення дисків, USB-носіїв, в яких містяться шкідливі програми, зазвичай, відбувається у процесі реалізації піратського програмного забезпечення, представлених наборами програм, чітко спрямованих на «зламування» інформаційних систем [41, с. 87].

Також під час з'ясування криміналістичної характеристики особи комп'ютерного злочинця вбачається за необхідне мати на увазі можливі схеми дій злочинців, використовуваних для віддаленого проникнення до комп'ютерних систем. В даному контексті фахівцями до таких груп злочинців відносяться: хакер-одинак; об'єднана хакерська група; конкурентне підприємство; представники певних державних структур [39, с. 83]. Охарактеризуємо кожну групу злочинців більш детальніше.

Як відмічають фахівці, у розпорядженні хакера-одинака стандартний персональний комп'ютер з модемним виходом до мережі Інтернет або через WI-FI. Така особа, як правило, фінансово обмежена, оскільки не є обов'язковим фактором володіти глибокими знаннями у сфері комп'ютерних програм та сценаріїв, доступних в Інтернеті, щоб реалізувати задумані загрози. Даний тип злочинців в принципі може не

володіти достатніми знаннями про побудову комп'ютерної системи. Спектр їх дій здебільшого носить експериментальний характер, тобто у них не має прагнення отримати доступ до відповідної інформації з ціллю одержання вигоди. Для них цікавий сам процес з проведення окремих дій щодо комп'ютерних систем, які є недоступними для простих користувачів. Дії таких злочинців мають скритий характер. Також додамо, що вони найчастіше призупиняють свою «діяльність» після того, як провели перший успішний вплив. Цікаво, що найбільш масовою причиною спроб злому є вчинення несанкціонованого доступу з використанням інформаційних технологій [41, с. 102].

До більш небезпечного типу злочинців відноситься об'єднана хакерська група. Вони, зазвичай, є скутими у своїм фінансових можливостях, а відтак, в переважній більшості ситуацій не володіють обчислювальними ресурсами на рівні великого підприємства та пропускних каналів в мережі Інтернет. Водночас, необхідно враховувати й той факт, що існують хакерські групи, які навпаки мають значні фінанси, щоб придбати дорогу техніку. Такі злочинці залучають різноманітні прийоми з метою організації сканування комп'ютерних систем з ціллю – виявити нові уразливі місця з врахуванням методів реалізації загроз, шляхом виокремлення уже відомих лазівок. Ними можуть реалізовуватись комп'ютерні програми, використовувані для виявлення уразливостей (віруси та інші програмні засоби).

Для подальшої реалізації своїх злочинних намірів, вони можуть вмонтувати шкідливі програми до комп'ютерних систем майбутніх «потерпілих» з метою отримання доступу до переважної більшості комп'ютерних ресурсів великих відомств. Окреслені дії дають можливість їм вчиняти серйозні атаки на комп'ютерні та інформаційні системи в мережі Інтернет. Їх дії мають цілеспрямований характер з проявом певних зусиль, щоб мати уявлення стосовно принципів функціонування системи захисту тієї чи іншої організації.

Цілеспрямованість дій окресленої групи злочинців полягає у тому, щоб підробляти кошти на рахунках (модифікувати дані) та отримувати/знищувати важливі дані за замовленням. Під час планування своїх дій, хакерська група прибігає до вжиття усіх можливих зусиль, аби приховати сам факт несанкціонованого доступу. Зазвичай, хакерській групі притаманний стиль не зупинятися ні перед чим аж до моменту реалізації поставленої цілі або у разі зіткнення з непереборними перепонами, не дозволяючи тим самим проводити подальший несанкціонований доступ до інформаційних та комп'ютерних систем [41, с. 104].

Характеризуючи конкурентне підприємство, зауважимо, що воно передбачає модель, при якій мають місце бути власні потужні комп'ютерні мережі та канали передачі даних з притаманною високою пропускною здатністю для того, щоб вийти в мережу Інтернет. Враховуючи те, що така група злочинців, як правило, має значні фінансові можливості та високий рівень знань комп'ютерних фахівців, у такому разі доволі частими є ситуації підкупу працівників служби безпеки та/або інші дії у сфері соціальної інженерії. Конкурентами можуть прикладатись вагомі зусилля, щоб отримати відомості стосовно функціонування системи інформаційного захисту, у тому числі залучити свого представника служби безпеки чи адміністрування комп'ютерної системи. Ціль такого полягає у: блокуванні функціонування комп'ютерної системи конкурента; доступі до чужої інформації; нанесенні підриву іміджу; деструктивних діях, спрямованих на завдання непоправного збитку конкурентові, аж до моменту його руйнації та фактичного банкрутства. Наведене передбачає використання витончених методів проникнення до інформаційних та комп'ютерних систем, впливаючи на потоки їх даних. Діям конкурентів притаманний демонстративний характер скритого та відкритого типу. Як правило, під

час здійснення намірів, сторона-конкурент, в переважній більшості випадків досягає поставленої цілі [41, с. 106].

Остання група злочинців, на яку звернемо увагу, відмічається представниками певних державних структур. Слід зазначити, що корумповані представники різноманітних структур практично необмежені в комп'ютерних та фінансових можливостях, а також є повністю незалежними в плані регулювання та контролю трафіку в мережі Інтернет. До найманих працівників даної категорії злочинців відносяться високопрофесійні та освічені фахівці. Додамо, що в деяких зарубіжних країнах бували випадки, коли замість позбавлення волі, відомих хакерів брали на службу в структурні органи національної безпеки. Тож, такі фахівці займаються розробкою стандартів з безпеки інформації, мережних протоколів та загалом максимально володіють можливостями та недоліками комп'ютерних і мережних технологій. Ціль даної групи злочинців неоднозначна, тобто її неможливо встановити заздалегідь. При цьому, такі злочинці можуть залучатись підтримкою нормативно-правових актів та органів влади [41, с. 108].

Беручи до уваги розбір найбільш поширених типів злочинців, якими вчиняються комп'ютерні злочини, насамкінець необхідно визнати доречну думку Н.С. Постіля, який вказував, що «аномальні зміни психіки накладають відбиток на особистісні якості суб'єкта, що може послужити поштовхом до вчинення комп'ютерного злочину. Зокрема, Всесвітня організація охорони здоров'я, проаналізувавши і узагальнивши матеріали щодо впливу комп'ютерів на здоров'я людини, зробила висновок, що тривала робота з комп'ютером несе негативні наслідки для здоров'я користувача» [42, с. 237].

Як підсумок підрозділу, виокремимо основні постулати. Особа злочинця – центральний елемент криміналістичної характеристики злочину, передбаченого ст. 361 КК України, тому що предмет злочинного посягання, його спосіб та слідова картина завжди

пов’язуються з особистісними рисами такої особи, а також закономірностями її поведінки.

Зосереджено прискіпливу увагу на розборі типології злочинців, якими можуть вчинятись комп’ютерні злочини.

Виявлено, що ефективна протидія комп’ютерним злочинам передбачає опанування низки специфічних питань, які безпосередньо відносяться до криміналістичної характеристики даної категорії злочинів. Також під час встановлення особи злочинця потрібно враховувати різноманітні чинники: тип доступу до комп’ютерних систем та інформації; складність обрання способу вчинення злочинного діяння; соціально-психологічний портрет особи злочинця, тощо.

В цілому аналіз особи злочинця дозволяє провести оптимізацію процесу висунення слідчих версій та забезпечити обрання найбільш раціональних тактичних прийомів, аби провести окремі слідчі (розшукові) дії під час розслідування комп’ютерних злочинів взагалі та злочину, передбаченого ст. 361 КК України, зокрема.

РОЗДІЛ 2
ОРГАНІЗАЦІЯ І ТАКТИЧНІ ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ В РОБОТУ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), АВТОМАТИЗОВАНИХ СИСТЕМ, КОМП'ЮТЕРНИХ МЕРЕЖ ЧИ МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

2.1. Типові слідчі ситуації під час розслідування несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку

Переходячи безпосередньо до аналізу основного питання дослідження, а саме організаційно-тактичним особливостям розслідування «несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку» [11] (ст. 361 КК України), традиційно слід розпочинати його розгляд з виявлення типових слідчих ситуацій під час розслідування даного злочину.

Першочергово пропонуємо охарактеризувати, що собою становить типова слідча ситуація крізь призму криміналістичної науки.

Серед вчених-криміналістів по сей день продовжують відбуватись дискусії стосовно окресленої категорії. Однією групою вчених обґрунтовується, що вчення про слідчі ситуації пов'язується з аналізом проблем криміналістичної методики, тим самим, вони її розглядають як конструктивний елемент відповідних методик розслідування. Так, Н.А. Селіванов відмічав, що «слідча ситуація здійснює значний безпосередній вплив на методику розслідування злочину, ніж криміналістична характеристика. Цей факт потрібно враховувати в процесі планування проведення розслідування» [43, с. 57]. Є.С. Хижняк

запевняв, що «слідча ситуація, як і криміналістична характеристика, є одним із визначальних інструментів слідчого, що надає можливість максимально збільшити ефективність розслідування злочинів, а володіння типовими слідчими ситуаціями дозволяє слідчому виявити коло пріоритетних завдань, мінімізувати вплив чи уникнути нецільової витрати часу й сил. На основі порівняння типової слідчої ситуації та ситуації, що сталася під час розслідування конкретного злочину, використовуючи взаємозв'язки між елементами криміналістичної характеристики цієї групи злочинів, слідчий зможе оптимально спланувати процес розслідування та найефективніше розв'язати завдання встановлення особи, яка вчинила злочин» [44, с. 198].

Інша група вчених була переконана, що слідча ситуація – це категорія криміналістичної тактики. Наприклад, В.К. Весельський стверджував: «слідча ситуація належить до кола понять криміналістичної тактики й у такій ролі реалізується в криміналістичній методиці» [45, с. 195]. Дане твердження цим же вченим аргументується тим, що «саме слідча ситуація зумовлює тактику конкретних слідчих дій» [45, с. 195]. В свою чергу В.В. Кікінчук пропонує під формулюванням «типова слідча ситуація» осмислювати «сукупність умов, даних та інших факторів, що безпосередньо чи опосередковано впливають на особу, яка наділена правовим статусом, у певний момент розслідування нею окремого виду злочину й диктують чітку послідовність інтелектуальної діяльності як закономірного й властивого кожному розумового процесу (інколи на підсвідомому рівні), котрий знаходить своє відбиття в прийнятті відповідних процесуально обґрунтованих рішень» [46, с. 132]. В.А. Журавель надав таке поняття типовій слідчій ситуації як «наукова абстракція, яка сформована на підставі апріорних знань, є результатом узагальнення та аналізу значного емпіричного матеріалу й в якій відбиті найзагальніші риси, що характеризують перебіг і стан розслідування на певному етапі

(вихідному, початковому, наступному)» [47, с. 106]. В.М. Шевчук до типових слідчих ситуацій відносив «ті ситуації, з якими стикається слідчий на початковому чи наступному етапі розслідування злочину залежно від повноти вихідних даних. Типові слідчі ситуації суттєво відрізняються від того, за яких умов здійснено злочин – очевидності чи неочевидності. Виокремлення типових слідчих ситуацій можливе за умови, якщо в основі типізації закладено ставлення підозрюваного до повідомлення про підозру» [48, с. 126]. Р.Л. Степанюк стверджував, що «типова слідча ситуація може бути визначена як сформульована на підставі аналізу практики розслідування певної категорії злочинів, абстрагована штучна модель, що відбиває стан наявної в слідчого інформації про обставини злочину й обставини, що склалися на певному етапі розслідування» [49, с. 111]. С.С. Чернявський вбачає в типовій слідчій ситуації «інформаційну модель із найважливішими властивостями й ознаками процесу розслідування в кримінальних провадженнях щодо злочинів певної категорії» [50, с. 405]. І.В. Калініна розуміла типову слідчу ситуацію як «сукупність об’єктивних положень, що виникають передусім на початковому етапі розслідування в разі незначного обсягу інформації та часто дублюються в практиці розслідування. Інформація про типові слідчі ситуації є результатом узагальнення практики розслідування певного виду злочинів» [51, с. 215].

На підставі наведених позицій, представлених наукою криміналістики, констатуємо, що типовим слідчим ситуаціям відводиться провідне інформаційне та організаційно-методичне навантаження під час встановлення методики розслідування злочину, передбаченого ст. 361 КК України. Основними типовими слідчими ситуаціями є початковий та подальший етап розслідування, які взаємопов’язані між собою.

Продовжуючи та перед тим як перейти до аналізу основного питання підрозділу, зауважимо, що при вчиненні комп'ютерних злочинів, аби досягнути злочинний результат – важливим є обстановка кіберпростору, що обумовлює потребу застосовувати комплекс методів, засобів і прийомів задля розв'язання практичних задач на початковому та наступному етапі розслідування [52, с. 82].

Так як типова слідча ситуація є науковою абстракцією, створеною на підставі апріорних знань, значить її високий ступінь обумовлює фундаментальне теоретичне та методичне значення, щоб розробити спектр питань криміналістики. Відтак, якщо конкретна ситуація відображає стан досудового розслідування відповідного кримінального провадження, то типова слідча ситуація відображає результат наукового узагальнення слідчої практики [53, с. 212].

Втім, наразі можна говорити про принципово новий відтінок діяльності слідчого як на початковому, так на наступному етапі розслідування, в межах злочину, передбаченого ст. 361 КК України, оскільки він пов'язується із сучасною інформаційною моделлю злочинного діяння, якому властиві усі риси багатоепізодної злочинної діяльності, необхідність встановлення злочинного наміру злочинця, а також характерна специфіка розподілу ролей учасників при здійсненні несанкціонованого доступу. Між іншим, здійснивши власний аналіз матеріалів практики щодо розслідування комп'ютерних злочинів, доводимо про те, що вони викликають складнощі та є трудомісткими під час досудового розслідування.

В контексті наведеного, законодавець з приводу досудового розслідування чітко розмежовує розшукову та слідчу діяльність, що проявляється у неможливості одержати відомості про злочин та особу, яка його вчинила, в межах іншого способу, ніж проведення негласних слідчих (розшукових) дій.

З метою продовження слід зазначити, що для злочину, передбаченого ст. 361 КК України властива двовекторна типізація тактичних задач розслідування, що обумовлює існування слідчо-розшукової та слідчої моделі типових ситуацій розслідування. З цього приводу справедливо відмічає В.А. Журавель: «одним із суттєвих критеріїв типізації слідчих ситуацій є саме ступінь їх впливу на процес формування стратегічних і тактичних завдань розслідування й визначення оптимальної послідовності проведення слідчих дій або тактичних операцій, що спрямовані на виконання цих завдань» [47, с. 107].

Переходячи безпосередньо до слідчо-розшукової моделі ситуації, відмітимо, що вона характеризується наявністю фактичних даних про злочинні наміри особи (групи осіб) стосовно вчинення злочину. При такій моделі для слідчого встановлюються відповідні напрями діяльності (виявлення, викриття та документування злочинної діяльності особи (групи осіб)). Як результат – слідчому необхідно оперувати конкретною сукупністю слідчих (розшукових) дій. Далі слід відмітити, що типовим слідчим-розшуковим ситуаціям початкового та наступного етапів розслідування характерна певна динаміка, а тому, невиконання хоча б однієї із тактичних задач в межах слідчо-розшукової ситуації початкового етапу розслідування призводить до появи ідентичної моделі ситуації на наступному етапі.

Отже, в межах слідчо-розшукової ситуації злочину, передбаченого ст. 361 КК України, вбачається за можливе виокремити низку типових тактичних задач (властивих як початковому, так і наступному етапу розслідування), а саме:

– документування мотиву злочинної діяльності злочинця;

– виявлення осіб, які діяли в групі та не знали про вчинення злочину (як приклад, займались виконанням дій, які не заборонені законом, виконуючи функції технічного або адміністративного

спрямування, як-от розробка сайту, надання послуг з його розміщення та ін.);

– встановлення зв’язків між учасниками групи, а також виявлення причинно-наслідкового зв’язку, що засвідчує існування корупційного складника злочинної діяльності;

– виявлення функцій кожного учасника групи (тобто конкретизується роль);

– встановлення методів, за якими відбувається конспірація злочинної діяльності групи, методів підтримки для досягнення авторитетності її керівників з метою формування у співучасників упевненості щодо можливості не бути притягнутими до відповідальності за скоєння несанкціонованих доступів до комп’ютерних мереж, тощо [52, с. 136-137].

В свою чергу, слідчій моделі ситуації притаманна наявність фактичних даних стосовно вчинення злочину та особи злочинця. При такій моделі слідчий в межах злочину, передбаченого ст. 361 КК України має можливість забезпечити повноцінне розслідування (доказувати події злочину; довести винуватість конкретної особи; виявляти інші обставини, які характеризуються релевантним значенням, що відповідають пошуковій задачі слідчого, аби з’ясувати ознаки складу даного злочину) [52, с. 138].

Надалі принагідно додати, що стан розслідування злочину, передбаченого ст. 361 КК України зумовлений рівнем вирішення тактичних задач початкового етапу розслідування, тобто в момент реєстрації в Єдиному реєстрі досудових розслідувань (ЄРДР) інформації стосовно пред’явлення певній особі обґрунтованої та законної підозри у вчиненні комп’ютерного злочину. Стан розслідування повинен оцінюватись з ціллю встановлення моделі ситуації, при якій слідчий має почати наступний етап розслідування, щоб конкретизувати обумовлені

динамікою початкового етапу розслідування обставини, які мають вагоме значення для майбутньої слідчої ситуації.

У контексті вищесказаного, видається за можливе виокремити дві типові слідчі ситуації розслідування в межах злочину, передбаченого ст. 361 КК України, зокрема:

1) сприятлива слідча ситуація розслідування, якій притаманна повнота вирішення тактичних задач та конкретизація зайнятих позицій кожним із підозрюваних в межах кримінального провадження. Додамо, що під час розслідування злочину, передбаченого ст. 361 КК України, для окресленої слідчої ситуації характерним є поширення її різновидів:

а) неускладнена сприятлива ситуація, яка має місце бути у разі збігу позицій підозрюваних осіб та сприяння їх слідству;

б) ускладнена сприятлива ситуація, яка може бути у разі розбіжності позицій декількох підозрюваних. Якщо говорити з позиції тактики, дана ситуація вимагає вирішення відповідних тактичних задач розслідування (подолати протидію розслідування; усунути суперечності між джерелами з доказовим значенням; забезпечити збереження вже одержаних джерел доказів) [52, с. 140].

Окрім цього, при сприятливій слідчій ситуації розслідування, до основоположних задач слідчого належать: повідомлення підозрюваного щодо проведення окремих слідчих (розшукових) дій; проведення одночасних допитів кількох осіб, аби подолати суперечності у показаннях; здійснення організаційних заходів, спрямованих на збирання необхідних матеріалів, що відображають особу підозрюваного; проведення додаткових допитів підозрюваних [52, с. 141].

2) несприятлива слідча ситуація розслідування. Для неї характерним є здійснення пізнавальних задач розслідування та невизначеність зайнятої позиції підозрюваними особами в межах кримінального провадження. Для даної слідчої ситуації розслідування злочину, передбаченого ст. 361 КК України, суттєвими факторами є:

– опитування підозрюваних осіб до того, як їм оголошено підозру (слідчий повинен відповісти, чи не буде негативних наслідків щодо активної протидії розслідуванню у разі попереднього опитування підозрюваної особи);

– вибрана слідчим поетапність оголошення підозри співучасникам злочину (йдеться про можливість одночасного повідомлення підозри усім співучасникам, коли слідчий, виходячи з особистісних характеристик організатора, виконавця, пособника, приймає рішення з приводу того, хто з учасників групи отримає оголошення про підозру першим, а хто останнім) [52, с. 143].

Підсумовуючи, зазначимо, що типовим слідчим ситуаціям відводиться провідне інформаційне та організаційно-методичне навантаження під час встановлення методики розслідування злочину, передбаченого ст. 361 КК України. Основними типовими слідчими ситуаціями є початковий та подальший етап розслідування, які взаємопов’язані між собою.

Виявлено, що для злочину, передбаченого ст. 361 КК України властива двовекторна типізація тактичних задач розслідування, що обумовлює існування слідчо-розшукової та слідчої моделі типових ситуацій розслідування.

Також встановлено, у разі виконання усіх постановлених тактичних задач на початковому етапі розслідування, наступний етап розслідування злочину, передбаченого ст. 361 КК України відбуватиметься з використанням двох типових слідчих ситуацій, зокрема: 1) сприятлива слідча ситуація розслідування; 2) несприятлива слідча ситуація розслідування.

2.2. Проведення окремих слідчих (розшукових) дій під час розслідування несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку

На сьогоднішній день робота переважної більшості установ, організацій та підприємств організовується за рахунок комп'ютерів, комп'ютерних систем та мереж (електрозв'язку), внаслідок чого несанкціонований доступ в їх роботу виступає впливовим чинником для України як держави, що є сучасною, демократичною та правовою. Між тим, не дивлячись на беззаперечність розвитку та поширення сучасних інформаційних технологій, створюються передумови для зростання злочинних дій, пов'язаних із несанкціонованим доступом до комп'ютерних мереж та/або несанкціонованим одержанням інформації.

Враховуючи специфіку комп'ютерних злочинів, в тому числі злочину, передбаченого ст. 361 КК України, нагадаємо, що вони характеризуються високим рівнем латентності та низьким рівнем розкриття. З-поміж цього, внаслідок швидких темпів комп'ютеризації суспільства, працівники правоохоронних органів зіштовхуються з труднощами, які виникають по причині відсутності комплексної обґрунтованої методики розслідування комп'ютерних злочинів та складнощами під час проведення окремих слідчих (розшукових) дій, в особливості таких як допиту та слідчий огляд, про які і буде зосереджуватись увага в даному підрозділі під час розслідування злочину, передбаченого ст. 361 КК України.

Починаючи з характеристики допиту, зазначимо, що йому відводиться значна роль під час розслідування злочину, передбаченого ст. 361 КК України. Адже у процесі розслідування слідчий, як і раніше, не може обходитись без інформації, отриманої від інших осіб (підозрюваних, потерпілих, свідків). Враховуючи те, що комп'ютерний

злочинець, як нам доводилось говорити в попередньому розділі дослідження, є особою, яка має спеціальні знання та навички, а також відмічається високим інтелектом, тактика допиту окресленої категорії осіб в цьому сенсі є більш ніж значима та особлива.

Зауважимо, що виявлення комп'ютерного злочину відбувається шляхом повідомлення про нього від фізичних чи юридичних осіб, а от що стосується виявлення ознак даного злочину, то вони є дуже рідкісними. Тож, провідне значення на початковій стадії розслідування відводиться саме роботі з особами, що повідомили про комп'ютерний злочин [54, с. 91].

В контексті наведеного цікавим може послугувати підхід, який пропонував Є.С. Шевченко, згідно з яким «слідчі дії під час розслідування кіберзлочинів слід поділити на вербальні та невербальні» [55, с. 200]. Призначення вербальних слідчих дій полягає у тому, щоб одержати інформацію з приводу події злочину, а от за допомогою невербальних слідчих дій з'ясовується об'єктивна сторона комп'ютерного злочину, необхідної для встановлення його повноцінної картини.

В свою чергу, основу вербальної слідчої дії в розслідуванні комп'ютерних злочинів становить допит, який проводиться за загальними правилами, передбаченими ст. 224 Кримінального процесуального кодексу України (КПК України) [56].

В юридичній літературі допит розуміється 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» [57, с. 153]. Отже, не дивлячись на існування загальних вимог до проведення допиту, практика їх застосування завжди повинна враховувати специфічність тієї чи іншої

справи, особливо під час розслідування злочину, передбаченого ст. 361 КК України.

Продовжуючи характеристику допиту, відмітимо про його труднощі, які виникають при допиті однієї та двох (більше) осіб. Так, пропонуємо виділити низку тактичних проблем, підлягаючих вирішенню у процесі підготовки та при проведенні допиту:

1) потреба залучати спеціалістів, що володіють спеціальними знаннями. Зокрема, у процесі розслідування комп'ютерних злочинів потребуються відповідні знання у сфері телекомунікаційних систем, комп'ютерних технологій та техніки. Між тим, далеко не кожному слідчому властиві подібні знання, у зв'язку з чим і виникає необхідність залучення спеціалістів при підготовці до допиту, сприяння якого дає можливість чітко сформулювати питання та надати всебічне усвідомлення і правильну фіксацію слідчого стосовно відповідей на них. Однак, в цьому аспекті може мати місце проблема можливої інтелектуальної протидії зі сторони злочинця, саме тому і потребується використання спеціальних знань та навичок, на які зверне увагу тільки спеціаліст;

2) слідчий під час розслідування має здійснити аналіз значного масиву даних, які відображені в електронному вигляді та частина з яких складає предмет слідчої дії, а інша підлягає конкретизації при допиті;

3) при допиті необхідно застосовувати знання юридичної психології;

4) обмеженість тривалості допиту. Нагадаємо, що чинним КПК України допит в цілому може тривати до 8 годин. Без сумніву, цього часу, як здається на перший погляд, повинно вистачити, однак враховуючи об'єктивний часовий фактор та динаміку електронного середовища, які впливають на дієвість розслідування злочину, передбаченого ст. 361 КК України – слідчому може потребуватись значно більше часу, щоб провести допит підозрюваної особи [52, с. 149].

До інших важливих питань на стадії підготовки до проведення допиту в межах злочину, передбаченого ст. 361 КК України слід відносити: необхідність провести інформаційне забезпечення допиту; дослідити особистість обвинуваченого та планування його допиту. Розкриємо ці питання більш ґрунтовніше.

1. Інформаційне забезпечення – це важлива складова на стадії підготовки допиту обвинуваченого в межах злочину, передбаченого ст. 361 КК України, тому що за рахунок усіх зібраних матеріалів справи та допоміжної інформації технічного «відтінку», гарантується контроль ситуації при проведенні допиту. Серед іншого, інформаційне забезпечення потрібно для того, щоб ліквідувати помилки при кваліфікації скоєного злочинного діяння. Ще одна із умов інформаційного забезпечення допиту у процесі розслідування злочину, передбаченого ст. 361 КК України – наявність знань комп'ютерних технологій та законодавчої бази, за допомогою яких регулюється галузь порушених цим злочином прав та законних інтересів.

В контексті наведеного слід вказати, що при виборі тактики допиту щодо злочину, передбаченого ст. 361 КК України – важливо також попередньо виявити певний набір інформації про подію злочину, що одержується з різноманітних джерел, а також про характерні особливості його механізму та застосовуваних знарядь у вигляді технічних засобів [58, с. 47].

2. З-поміж опанування технічної сторони питання, при підготовці допиту потрібно брати до уваги й характер особистості допитуваної особи.

Взагалі джерелами інформації про особу, виходячи з криміналістичної науки відносяться «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.)» [30, с. 325].

Однак, в межах розглядуваного нами злочину до джерел інформації потрібно відносити профіль такої особи в соціальних мережах, а також історію відвідування електронних сторінок, відображених у відповідному браузері. Тут доцільно зупинити свою увагу на певний психологічний феномен, який має враховувати слідчий при підготовці допиту щодо злочину, передбаченого ст. 361 КК України. Так, зрозуміло, що проблемність одержання інформації з приводу особистісних характеристик злочинця можуть викликати складність у зв'язку з відсутністю джерел такої інформації. Однак, на підставі особливостей поведінки особи в аспекті «тут і зараз», видається за можливе встановити відношення такої особи до злочину, тобто його суб'єктивність. Після виявлення типу комп'ютерного злочинця значно легше з'ясувати його ціль та відношення до злочину [59, с. 93].

Особливо важливим в межах злочину, передбаченого ст. 361 КК України є виявлення попередньої діяльності обвинуваченого. В результаті проведеного аналізу різної інформації про допитуваного при підготовці до самого допиту – повинно стати з'ясування слідчим рівня знань та інформації стосовно комп'ютерних технологій, якими володіє злочинець, а також з'ясувати, з чим пов'язане вчинення такого злочину, чи могла взагалі допитувана особа його вчинити чи ні. Саму ж інформацію потрібно одержувати з результатів дослідження інформації, яка є у відкритому доступі про особу в мережі Інтернет. До подібного роду інформації може належати та, що вказується нею при реєстрації в соціальних мережах, в тому числі враховуються відомості про її життя, які вона розміщує у процесі користування (як приклад facebook/instagram). До того ж, при дослідженні профілю особи в соціальних мережах виникає можливість виявити професійні інтереси допитуваної особи в ролі обвинуваченого.

Отже, роблячи проміжний висновок стосовно допиту в межах розглядуваного злочину, передбаченого ст. 361 КК України, слід відмітити перш за все його характерні особливості, зокрема: 1) високий інтелектуальний рівень та психологічний аспект допитуваних осіб, в особливості злочинця; 2) обсяг питань, що підлягають виявленню при проведенні допиту, відмічаються складним технічним характером. Враховуючи зазначене, слідчому потрібно бути особливо ретельним при підготовці та проведенні допиту, щоб забезпечити максимально результативне «вилучення» необхідної інформації, потребуючої для розслідування злочину, передбаченого ст. 361 КК України.

З метою продовження та переходячи безпосередньо до аналізу наступної слідчої (розшукової) дії – слідчого огляду, насамперед зазначимо, що ефективність протидії злочину, передбаченого ст. 361 КК України залежить від того, наскільки слідчі готові працювати з віртуальною інформацією в електронному середовищі, виявляти та фіксувати її, що в сукупності відображає чинники організаційно-правового спрямування та вбачає наявність належного матеріально-технічного оснащення.

У процесі розслідування комп'ютерного злочину – проведення слідчого огляду відбувається у місцях збереження та обробки комп'ютерної інформації, яка піддалась злочинному впливу (як приклад, знищення, блокування, шифрування, тощо), знаходження комп'ютерного обладнання, використовуваного в момент вчинення злочину (як приклад, поширювався комп'ютерний вірус після несанкціонованого проникнення до комп'ютерної мережі); місцях збереження інформації, одержаної незаконним шляхом (як приклад, відбулось несанкціоноване заволодіння інформацією в електронному вигляді), тощо [60, с. 30].

Зазначимо, що дієвість слідчого огляду в межах розглядуваного злочину, передбаченого ст. 361 КК України залежить від вирішення

наступних завдань: 1) опанування обстановки на місці, щоб з'ясувати суть та обставини події, які дають підстави здійснювати подальше досудове розслідування; 2) одержати первинну інформацію для висунення версій про механізм здійснення злочину, передбаченого ст. 361 КК України, особу злочинця та наявності співучасників (якщо вони є); 3) зібрання відомостей для організації розшуку злочинця по «гарячим слідам», а також проведення оперативно-розшукових заходів, аби встановити злочинця та затримати його; 4) виявлення слідів злочину, предметів, залишених комп'ютерним злочинцем, які можуть мати вагому доказову значущість, тощо [61, с. 90].

Сам процес здійснення слідчого огляду умовно можна поділити на такі етапи: підготовчий, робочий та заключний. Пропонуємо змістовно проаналізувати кожен етап з прив'язкою до злочину, передбаченого ст. 361 КК України.

1. Підготовчий етап. Його початок датується моментом прийняття відповідного рішення щодо його проведення та підготовки до робочого етапу.

Зазначимо, що до того як прибути на місце проведення огляду, слідчим вирішується низка організаційних питань (перелічувати їх не будемо, щоб не виходити за межі дослідження), а також документально фіксуються підстави та законність окресленої процесуальної дії.

Завершення даного етапу відбувається після прибуття на місце події та вирішення наступних дій: підтвердження часу прибуття на місце проведення огляду та часу початку слідчої дії; при проведенні огляду у власності потерпілої особи, одержати в присутності понятих згоди щодо проведення огляду місцевості, приміщення та ін.; виявлення місць з зовнішнім підключенням до будівлі електропостачання, комунікаційних та мережевих кабелів, проведення організаційних заходів з приводу їх охорони на час проведення огляду; зібрання попередніх відомостей від осіб, які знаходяться на місці події з метою врахування обставин, які

можуть становити вагомість для проведення огляду; усунення з місця події усіх сторонніх осіб; здійснення пошуку та залучення понятих (не менше двох осіб), виходячи з розрахунку приміщень, в яких розташовуються певні елементи комп'ютерної системи (важливо відмітити, що поняті мають бути обізнаними у комп'ютерній техніці та процесах роботи з електронною інформацією з метою фактичного підтвердження усвідомлення і ними суті дій як учасників слідчої групи); проведення інструктажу учасників огляду з відповідним роз'ясненням їх прав та обов'язків; проведення інших невідкладних дій та заходів, необхідних для ефективності умов огляду (забезпечити штучне освітлення, тощо) [62, с. 41-42].

2. Робочий етап характеризується безпосереднім проведенням огляду, який з ціллю охоплення усіх можливих слідчих версій вчинення злочину передбачає здійснення огляду місцевості, приміщення та предметів (комп'ютерна техніка; електронні документи).

За цим етапом в першу чергу проводиться загальний огляд місця події, відповідно до якого визначаються територіальні межі місця проведення огляду; зіставляються плани-схеми (розташування об'єктів, що підлягають огляду, мережевих з'єднань комп'ютерів та серверів, тощо); виявляються вихідні точки та спосіб огляду; визначаються точки орієнтирів та обирається позиція для орієнтуючої і оглядової фото- та відеофіксації [63, с. 102].

Наступний крок – статичне фіксування комп'ютерних пристроїв, існуючих мережевих підключень, схем взаємного розташування пристроїв, зовнішнього вигляду пристроїв, що в сукупності є необхідним в момент проведення огляду. Знову ж таки, усі окреслені дії супроводжуються криміналістичною фото- та відеофіксацією, а також складанням плану приміщення та схеми розташування комп'ютерного обладнання і локальних мереж, підключених до мережі Інтернет. Суттєвий момент полягає у тому, щоб унеможливити фізичний доступ

до комп’ютерної техніки осіб, працюючих з нею та у разі необхідності врахувати вжиття спеціальних заходів, щоб блокувати можливі спроби здійснення віддаленого доступу [63, с. 103].

Після того як закінчено процедуру загального огляду, слідчим здійснюється перехід до динамічної стадії – детальний огляд. Динаміка викликана тим, що предмети, які складають певні об’єкти огляду, можуть зрушуватись з місця. Такі об’єкти огляду по вказівці слідчого прискіпливо досліджує спеціаліст-криміналіст на предмет слідів пальців рук, нігтів та ін., з метою їх фіксування та подальшого вилучення. Такий підхід типовий для фіксування слідів злочину, проте в межах розглядуваного злочину потрібно брати до уваги той факт, що можуть виявлятись відшарування порошків, фарби та інших мікроелементів на поверхнях комп’ютерної техніки. У разі аналізу однієї з версій, а саме несанкціонованого втручання через фізичне підключення до комп’ютерної техніки, потрібно зробити акцент на наявність нашарувань пилу на поверхнях, які можуть свідчить про те, що окремі пристрої пересувались або зрушувались з місця. Окрім цього, не зайвим є залучення працівника оперативно-технічного забезпечення, щоб той оглянув точки мережевого підключення та електропостачання на предмет втиснення, а також здійснив перевірку стану кабелів стосовно ймовірних слідів припаювання, тощо. В завершення, після того як вилучено дрібні предмети для здійснення судового експертного аналізу, їх кладуть до окремого поліетиленового пакету, герметично закриваючи та опечатуючи биркою [63, с. 104-105].

По результатам огляду та аналізу матеріальної частини місця злочину, необхідно концентрувати увагу на роботі з інформацією, представленою електронною формою. Як вже доводилось казати, участь спеціаліста в цьому випадку вважається одним із основоположних моментів, який обов’язково потрібно враховувати та забезпечити при огляді комп’ютерної техніки. Адже з позиції програмно-технічного

аспекту – елементи, які є невід'ємною складовою комп'ютерної системи, у процесі аналізу на місці потребують дуже обережного поводження, оскільки передбачено значний масив інформації в електронній формі; існування права інтелектуальної власності на певну частину інформації, яка підлягає огляду; наявність прихованих даних, доступу до яких у звичайних користувачів немає.

Беручи до уваги вищенаведене та враховуючи специфічність злочину, передбаченого ст. 361 КК України, можемо прослідувати, що для реалізації задач кримінального провадження тільки речових доказів замало, а тому суттєвою є процесуально грамотна та технічно відточена фіксація інформації в комп'ютерних мережах та системах. Наведене на нашу думку обґрунтовує обов'язковість залучення спеціаліста, завдяки якому буде забезпечено комплексне проведення пошуку електронних доказів з подальшим збереженням та документуванням доказової інформації.

У зв'язку з наведеним, завершальний крок робочого огляду передбачає документування внутрішніх слідів злочину, передбаченого ст. 361 КК України (які залишили в електронній формі). В межах цього кроку спеціаліст документує несанкціоноване втручання в комп'ютери, автоматизовані системи та комп'ютерні мережі, виконуючи наступні завдання:

– діагностує апаратні засоби (комп'ютери, ноутбуки, планшети, мобільні пристрої, тощо);

– визначає функціональне призначення, характеристики, алгоритм роботи та структурні особливості стану виявленого програмного забезпечення;

– здійснює проведення пошуку, аналізу та оцінювання цифрових даних, які виготовлялись користувачем або створювались прикладними програмами, щоб реалізувати інформаційні процеси у комп'ютерній системі;

– ідентифікує електронні файли/каталоги, а також ототожнює їх з файлами/каталогами на інших носіях інформації [63, с. 109-110].

Виходячи з результатів проведення огляду комп'ютера, комп'ютерної мережі, віддаленого інформаційного ресурсу, в протокол огляду долучається таке: робочий та контрольний примірник криміналістичних програмних засобів, застосованих з метою з'ясування, копіювання та збереження інформації в іншому носії; контрольний примірний файл (еталонний); контрольний примірник носія, в якому збережено файли та інформацію, які становлять доказову базу [63, с. 110].

3. Заключний етап проведення слідчого огляду полягає у тому, щоб визначити успішність його проведення, для якого необхідно враховувати вимоги, додержання яких дасть можливість забезпечити ефективне судово-експертне дослідження вилучених об'єктів в рамках проведення відповідних експертиз (про них поговоримо детальніше в кінцевому підрозділі дослідження). Окрім цього, важливо враховувати правильність завершення всіх працюючих програмних засобів, що убезпечить від потенційної втрати важливої доказової інформації [63, с. 113].

Отже, роблячи проміжний висновок щодо проведення слідчого огляду в межах злочину, передбаченого ст. 361 КК України, констатуємо, що для здійснення такої процесуальної дії необхідною умовою є наявність належної нормативної та технічної готовності слідчих до роботи з інформацією, представленою в електронній формі. Інший суттєвий аспект полягає у тому, щоб нормативно-правове забезпечення діяльності правоохоронних органів повністю відповідало сьогоднішнім реаліям, в першу чергу в частині науково-дослідної роботи та щодо прийняття відповідних розпорядчих актів, інструкцій методичного спрямування, за допомогою яких регламентується проведення слідчого огляду в межах розглядуваного нами злочину.

На підставі вищевикладеного, охарактеризувавши встановлені точки дотику стосовно проведення окремих слідчих (розшукових) дій, пропонуємо зробити узагальнені підсумки.

Виявлено, що допиту як слідчій (розшуковій) дії – відводиться значна роль під час розслідування злочину, передбаченого ст. 361 КК України. Адже у процесі розслідування слідчий, як і раніше, не може обходитись без інформації, отриманої від інших осіб (підозрюваних, потерпілих, свідків). Враховуючи те, що комп'ютерний злочинець, є особою, яка має спеціальні знання та навички, а також відмічається високим інтелектом, тактика допиту окресленої категорії осіб в цьому сенсі є більш ніж значима та особлива.

Зосереджено увагу на низці тактичних проблем, підлягаючих вирішенню у процесі підготовки та при проведенні допиту, а також зроблено акцент на інші не менш важливі питання, які виникають на стадії підготовки до проведення допиту, зокрема (необхідність провести інформаційне забезпечення допиту; дослідити особистість обвинуваченого та планування його допиту).

З'ясовано, що ефективність такої слідчої (розшукової) дії як слідчий огляд щодо злочину, передбаченого ст. 361 КК України залежить від того, наскільки слідчі готові працювати з віртуальною інформацією в електронному середовищі, виявляти та фіксувати її, що в сукупності відображає чинники організаційно-правового спрямування та вбачає наявність належного матеріально-технічного оснащення.

Визначено особливості процесу здійснення слідчого огляду в межах злочину, передбаченого ст. 361 КК України, який здійснюється за трьома етапами: підготовчий, робочий та заключний.

2.3. Використання спеціальних знань під час розслідування несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку

Кінцевий для розгляду підрозділ дослідження полягає у виявленні спеціальних знань під час розслідування злочину, передбаченого ст. 361 КК України. Основною процесуальною формою використання спеціальних знань є судова експертиза.

Перш ніж перейти до розгляду ключового питання, вважаємо за необхідне з'ясувати теоретико-прикладні категорії в межах даного підрозділу.

Насамперед, у Великому енциклопедичному юридичному словнику судова експертиза розглядається як «дослідження спеціалістом-експертом матеріальних об'єктів, явищ і процесів, які містять інформацію про обставини справи, що перебуває у провадженні органів дізнання, досудового слідства або суду» [64, с. 263]. В свою чергу, відомий криміналіст Р.С. Бєлкін вважає, що «судова експертиза – це родове поняття досліджень, що їх проводить відповідно до кримінально-процесуального або цивільно-процесуального закону особа, яка має спеціальні пізнання в науці, техніці, мистецтві, ремеслі, з метою з'ясувати обставини (фактичні дані), що мають значення для справи» [65, с. 93]. О.І. Жеребко осмислює судову експертизу як «слідчу дію з організації й тактики використання спеціальних знань з метою здобуття доказової інформації методами наукового дослідження, яку виконують за дорученням слідчих і судових органів та відображають у висновку експерта» [66, с. 53].

Отже, оперуючи наведеними міркуваннями та враховуючи, що експерти є обізнаними особами, а значить і носіями спеціальних знань,

пропонуємо сформулювати їх визначення в межах розглядуваного нами злочину.

Під спеціальними знаннями при виявленні та розслідуванні злочину, передбаченого ст. 361 КК України, слід розуміти знання за різними галузями науки (техніка, мистецтво та ремесло) щодо комп'ютерної інформації та високих технологій, здобутих під час професійної освіти (діяльності), яким притаманні теоретичні навички та уміння, які застосовуються учасниками кримінального судочинства, аби з'ясувати підлягаючі доказуванню обставини, керуючись чинним кримінальним процесуальним законодавством України.

Тож, переходячи безпосередньо до ключового питання підрозділу, зазначимо, що висновки судових експертів переважної більшості кримінальних проваджень займають місце найсуттєвіших доказів, без наявності яких вирішити відповідну справу (особливо з приводу комп'ютерного злочину) практично неможливо [67, с. 315].

Залежно від конкретних обставин розслідування злочину, передбаченого ст. 361 КК України вбачається за доцільне призначення та проведення відповідних судових експертиз. Виокремимо на нашу думку ключові та охарактеризуємо їх.

1. Посилена увага при фіксуванні злочинних дій за ст. 361 КК України зосереджується на можливостях проведення експертизи біологічних слідів людини.

Під час розслідування злочину, передбаченого ст. 361 КК України, типовою виступає судово-медична експертиза речових доказів. Залежно від того, який вид речових доказів біологічного походження, судово-медична експертиза здійснюється окремим спеціалізованим відділом бюро судово-медичних експертиз, згідно до передбачених правил «Інструкцією про проведення судово-медичної експертизи», затвердженою Наказом від 17 січня 1995 року № 6 [68] (далі – Інструкція).

З огляду на типові слідчі ситуації розслідування злочину, передбаченого ст. 361 КК України, речовими доказами біологічного походження слід вважати: волосся, сліди крові, шкірний епітелій, слина, слізна рідина, тощо.

Алгоритмом дій при дослідженні окреслених речових доказів є опис, фотографування, вилучення та пакування слідів; з'ясування наявності крові у вилучених експертних матеріалах або інших рідин та тканин; визначення видової, статевої та групової приналежності слідів (імунні системи); виключення або встановлення приналежності слідів біологічного походження за конкретною особою [69, с. 120].

Досліджуючи сліди біологічного походження, застосовують методологію, затверджену Наказом [68]. Сам же перелік орієнтованих питань, винесених для вирішення судово-медичної експертизи, нормативним рівнем не передбачається. Проте, виходячи з результатів співробітництва слідчих та судово-медичних експертів при розслідуванні злочинів, виникає можливість сформулювати варіацію типових питань, які виносяться на вирішення судово-медичної експертизи речових доказів. Так, судово-медична експертиза слідів крові при розслідуванні злочину, передбаченого ст. 361 КК України, повинна дати відповіді на наступні питання: чи була кров на об'єкті; яка група крові; стать людини, до якої належить кров (дитина або доросла людина); регіональність походження крові; давність плям крові; можливість походження крові від певної людини [69, с. 120].

Здійснивши власний аналіз слідчої практики, було встановлено, що досить частими є випадки, коли вилучається та досліджується волосся, знайдене в місцях фізичного доступу до апаратних складових комп'ютерів або серверів. Подібні об'єкти надсилають, щоб провести судово-медичну (цитологічну) експертизу. Так, відділами судово-медичної цитології проводяться дослідження з ціллю встановлення в слідах і речових доказах клітини тканин людини, з'ясовуючи їх

приналежність до виду, групи, статі. До основних питань, які підлягають вирішенню в межах цієї експертизи є наступні: чи відноситься наданий об'єкт до волосся (якщо так, то з'ясуванню підлягає питання кому саме, людині або тварині); походженням якої частини тіла є волосся (з'ясувати, які саме були механічні пошкодження); за яким способом видалялось волосся (випало, вирване або розірване); чи має волосся характерні риси хімічної або термічної дії; чи можна вважати таке волосся з ймовірними захворюваннями; приналежність волосся до статі, тощо. У разі необхідності проводиться комплексне дослідження, з можливістю застосування аналізу ДНК [69, с. 121].

2. Суттєве значення під час розслідування злочину, передбаченого ст. 361 КК України відводиться комп'ютерно-технічній експертизі (далі – КТЕ) та експертизі телекомунікаційних систем і засобів. Проведення окреслених досліджень здійснюються за правилами, встановленими «Інструкцією про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень», затвердженої Наказом Міністерства юстиції України 8 жовтня 1998 року № 53/5 [70] (далі – Інструкція).

У процесі дослідження наукових джерел, нами було виявлено підвиди КТЕ, зокрема: 1) апаратний аналіз (вивчаються технічні засоби та комп'ютери); 2) програмний аналіз (вивчаються алгоритми, які застосовують в пристроях, необхідних для забезпечення їх функціонування); 3) інформаційний аналіз (виявляються та аналізуються файли, якими оперує користувач, а також оцінюється функціональність даних, їх призначення та ідентифікація).

До основних завдань КТЕ слід відносити наступні: встановити, чи в робочому стані комп'ютерно-технічні засоби; встановити обставини, які прямо відносяться до використання комп'ютерно-технічних засобів, інформації та програмного забезпечення; виявити інформацію та

програмне забезпечення, що знаходиться на комп’ютерних носіях; встановити відповідність програмних продуктів на предмет версій чи вимог стосовно його розроблення [69, с. 122].

Конкретизуючи експертизу телекомунікаційних систем і засобів, відмітимо, що її формування відбувалось у процесі вдосконалення та поглиблення методик КТЕ. Це відбулось у результаті прогресивного розвитку видів та форм передання даних між тими чи іншими комп’ютерами. Після того, як суспільство почало масово підключатись до глобальної мережі Інтернет, комунікаційних модулів WI-FI – в цей же період визначились із загальноприйнятною формою функціоналу комп’ютера [69, с. 122]. Відтак, у зв’язку з необхідністю піддавати аналізу маршрути та способи передання інформації, сформовано основні завдання для експертизи телекомунікаційних систем і засобів: «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; визначення якості надання телекомунікаційних послуг на рівні їх споживання; встановлення конфігурації та робочого стану телекомунікаційних систем та засобів; встановлення типу, марки, моделі та інших класифікаційних категорій телекомунікаційних систем та засобів; дослідження алгоритмів обробки інформації та її захисту у сфері телекомунікацій» [70] (п. 14.2 Інструкції).

Оперуючи положенням Інструкції, «об'єктами експертизи телекомунікаційних систем та засобів є телекомунікаційні системи, засоби, мережі і їх складові частини та інформація, що ними передається, приймається та обробляється» [70] (п. 14.1).

До основних питань, поставлених на вирішення відносяться такі: «які тип, марка, модель телекомунікаційного засобу (системи); чи в робочому стані знаходиться телекомунікаційний засіб (об'єкт); які

характеристики підключень до мережі має телекомунікаційний засіб;чи змінювались користувачем телекомунікаційної мережі налаштування окремих пристроїв, у який час, які їх значення; який загальний характер підключень до телекомунікаційної мережі виконував об'єкт (телекомунікаційна система, засіб); за допомогою яких програмних засобів здійснювалось підключення до телекомунікаційної мережі; яка топологія апаратних засобів, об'єднаних у телекомунікаційну систему; чи відповідає функціонування телекомунікаційного засобу (системи) технічній документації; які технічні характеристики (параметри) має телекомунікаційний засіб (система); чи мав місце факт доступу до телекомунікаційної системи та в який спосіб; чи мало місце використання ресурсів та інформації в телекомунікаційній системі та в який спосіб; чи мав місце факт передачі (отримання) інформації в телекомуніка ційній системі та в який спосіб; чи є ознаки втручання в роботу телекомунікаційної системи; чи могли апаратні засоби об'єднуватись у телекомунікаційну мережу та за якими ознаками; які шляхи маршрутизації даних у телекомунікаційній системі; чи можливо використання телекомунікаційного засобу (обладнання) для вказаних цілей» [70] (п. 14.3 Інструкції).

З приводу наведеного переліку питань додамо, що він є орієнтовним, оскільки залежно від обставин розслідуваного злочину, передбаченого ст. 361 КК України, може виникнути потреба коригування, конкретизації та доповнення певних питань, враховуючи при цьому консультативну допомогу спеціаліста та експерта, яким проводитиметься експертиза.

Насамкінець слід вказати, що доволі часто охарактеризовані експертизи застосовуються комплексно щодо злочину, передбаченого ст. 361 КК України. Обґрунтовується це наявністю у Реєстрі методик проведення судових експертиз відповідної методики стосовно експертного дослідження.

Підсумовуючи наведене вище, робимо висновок про те, що використання спеціальних знань під час розслідування злочину, передбаченого ст. 361 КК України відмічається основною процесуальною формою їх використання – судовою експертизою.

З'ясовано, що залежно від конкретних обставин розслідування злочину, передбаченого ст. 361 КК України вбачається за доцільне призначати та проводити відповідні судові експертизи. Конкретно нами було проаналізовано судово-медичну експертизу; комп'ютерно-технічну експертизу та експертизу телекомунікаційних систем і засобів. Зазначимо, що це неповний перелік судових експертиз, які можуть проводитись в межах розглядуваного злочину.

В цілому, проведення судових експертиз є дуже важливим моментом під час розслідування не тільки означеного нами злочину, а й взагалі при виявленні різного роду комп'ютерних злочинів (кіберзлочинів) в Україні.

ВИСНОВКИ

На основі аналізу теоретичних напрацювань та чинного кримінального процесуального законодавства виявлено існуючі криміналістичні засади, необхідні для з'ясування особливостей розслідування несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Отримані під час дослідження результати, виходячи з реалізованої мети та завдань кваліфікаційної роботи (проєкту) дали підстави для надання наступних висновків:

1. Здійснивши аналіз теоретичних напрацювань щодо визначення поняття комп'ютерних злочинів (кіберзлочинів), нами було сформульовано власне поняття комп'ютерних злочинів під якими потрібно осмислювати суспільно небезпечну діяльність, здійснювану шляхом використання сучасних інформаційних технологій та засобів комп'ютерної техніки з ціллю спричинення збитків майнового або суспільного інтересу держави, а також порушення прав певної особи.

Наведене визначення дало можливість констатувати, що комп'ютерні злочини є складним, відносно новим явищем кримінально-правової практики, яке вимагає більш досконалого спеціального та систематичного опанування.

Встановлено, що для ефективної протидії злочинів у сфері використання комп'ютерних систем, важливим моментом є виявлення криміналістичної суті видів розглядуваного злочину, що в свою чергу викликало потребу їх наукової класифікації, на підставі якої нами в контексті використання криміналістичного аспекту в межах нашого дослідження, запропоновано власний підхід класифікації комп'ютерних злочинів.

На підставі наданого підходу класифікації комп'ютерних злочинів запропоновано, що він дає змогу більш прозоро осмислити механізм вчинення таких злочинних діянь, а також відобразити виключно криміналістичні особливості, оскільки його підґрунтям виступають злочинні дії та механізм утворення слідів, тобто весь комплекс дій, завдяки яким визначаються вектори під час розслідування комп'ютерних злочинів, в тому числі, передбаченого ст. 361 КК України.

2. Протидія комп'ютерним злочинам вимагає використання дієвих механізмів протидії із злочинності з метою розкриття та розслідування конкретних кримінальних правопорушень, передбачених розділом XVI КК України. Проте це потребує наявності сучасних методик розслідування, для виявлення яких було приділено увагу кожному елементу, зокрема:

1) способам комп'ютерних злочинів, до яких слід відносити (вчинення з використанням засобів комунікацій віддаленого доступу; переважна більшість комп'ютерних злочинів не піддається виявленню без використання спеціальних заходів практичного спрямування; використання зі злочинною ціллю шкідливих програмних продуктів);

2) обстановці комп'ютерних злочинів, яка характеризується тим, що у процесі розслідування комп'ютерних злочинів вагоме значення відводиться інформації з приводу ймовірного місця та часу його вчинення;

3) слідовій картині, завдяки якій можливо виявити механізм скоєного злочинного діяння у віртуальному середовищі. Коректне виявлення та вивчення віртуальних слідів органами досудового розслідування сприяють ефективно з'ясовувати факти розповсюдження інформації щодо злочину, передбаченого ст. 361 КК України.

3. Особа злочинця – центральний елемент криміналістичної характеристики злочину, передбаченого ст. 361 КК України, тому що предмет злочинного посягання, його спосіб та слідова картина завжди

пов’язуються з особистісними рисами такої особи, а також закономірностями її поведінки.

Зосереджено прискіпливу увагу на розборі типології злочинців, якими можуть вчинятись комп’ютерні злочини.

Виявлено, що ефективна протидія комп’ютерним злочинам передбачає опанування низки специфічних питань, які безпосередньо відносяться до криміналістичної характеристики даної категорії злочинів. Також під час встановлення особи злочинця потрібно враховувати різноманітні чинники: тип доступу до комп’ютерних систем та інформації; складність обрання способу вчинення злочинного діяння; соціально-психологічний портрет особи злочинця, тощо.

В цілому аналіз особи злочинця дозволяє провести оптимізацію процесу висунення слідчих версій та забезпечити обрання найбільш раціональних тактичних прийомів, аби провести окремі слідчі (розшукові) дії під час розслідування комп’ютерних злочинів взагалі та злочину, передбаченого ст. 361 КК України, зокрема.

4. Типовим слідчим ситуаціям відводиться провідне інформаційне та організаційно-методичне навантаження під час встановлення методики розслідування злочину, передбаченого ст. 361 КК України. Основними типовими слідчими ситуаціями є початковий та подальший етап розслідування, які взаємопов’язані між собою.

Виявлено, що для злочину, передбаченого ст. 361 КК України властива двовекторна типізація тактичних задач розслідування, що обумовлює існування слідчо-розшукової та слідчої моделі типових ситуацій розслідування.

Також встановлено, у разі виконання усіх постановлених тактичних задач на початковому етапі розслідування, наступний етап розслідування злочину, передбаченого ст. 361 КК України відбуватиметься з використанням двох типових слідчих ситуацій,

зокрема: 1) сприятлива слідча ситуація розслідування; 2) несприятлива слідча ситуація розслідування.

5. Виявлено, що допиту як слідчій (розшуковій) дії – відводиться значна роль під час розслідування злочину, передбаченого ст. 361 КК України.

Характерними особливостями допиту в межах розглядуваного злочину є: 1) високий інтелектуальний рівень та психологічний аспект допитуваних осіб, в особливості злочинця; 2) обсяг питань, що підлягають виявленню при проведенні допиту, відмічаються складним технічним характером. Враховуючи зазначене, слідчому потрібно бути особливо ретельним при підготовці та проведенні допиту, щоб забезпечити максимально результативне «вилучення» необхідної інформації, потребуючої для розслідування злочину, передбаченого ст. 361 КК України.

Зосереджено увагу на низці тактичних проблем, підлягаючих вирішенню у процесі підготовки та при проведенні допиту, а також зроблено акцент на інші не менш важливі питання, які виникають на стадії підготовки до проведення допиту, зокрема (необхідність провести інформаційне забезпечення допиту; дослідити особистість обвинуваченого та планування його допиту).

З’ясовано, що для проведення такої слідчої (розшукової) дії як слідчий огляд, в межах злочину, передбаченого ст. 361 КК України – необхідною умовою є наявність належної нормативної та технічної готовності слідчих до роботи з інформацією, представленою в електронній формі. Інший суттєвий аспект полягає у тому, щоб нормативно-правове забезпечення діяльності правоохоронних органів повністю відповідало сьогоднішнім реаліям, в першу чергу в частині науково-дослідної роботи та щодо прийняття відповідних розпорядчих актів, інструкцій методичного спрямування, за допомогою яких

регламентується проведення слідчого огляду в межах розглядуваного нами злочину.

Визначено особливості процесу здійснення слідчого огляду в межах злочину, передбаченого ст. 361 КК України, який здійснюється за трьома етапами: підготовчий, робочий та заключний.

6. Використання спеціальних знань під час розслідування злочину, передбаченого ст. 361 КК України відмічається основною процесуальною формою їх використання – судовою експертизою.

З'ясовано, що залежно від конкретних обставин розслідування злочину, передбаченого ст. 361 КК України вбачається за доцільне призначати та проводити відповідні судові експертизи. Конкретно нами було проаналізовано судово-медичну експертизу; комп'ютерно-технічну експертизу та експертизу телекомунікаційних систем і засобів. Зазначимо, що це неповний перелік судових експертиз, які можуть проводитись в межах розглядуваного злочину.

В цілому, проведення судових експертиз є дуже важливим моментом під час розслідування не тільки означеного нами злочину, а й взагалі при виявленні різного роду комп'ютерних злочинів (кіберзлочинів) в Україні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Азаров Д.С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження): [монографія] К. : Атіка, 2007. 304 с.

2. Римарчук Г.С. Юридична природа кіберзлочинів. *Науковий вісник Ужгородського національного університету. Серія ПРАВО*. 2013. Вип. 24. Т. 4. С. 54–57.

3. Біленчук П.Д., Зубань М.А. Комп'ютерні злочини: соціально-правові та кримінолого-криміналістичні аспекти: Навч. посіб. К.: Українська академія внутрішніх справ, 1994. 72 с.

4. Комп'ютерна злочинність: Навчальний посібник / П.Д. Біленчук, Б.В. Романюк, В.С. Цимбалюк та ін. К.: Атіка, 2012. 240 с.

5. Селюк А.В. Розслідування комп'ютерних злочинів. Наук.-метод. посіб.: Вид-во НА СБУ, 2010. 124 с.

6. Лісовий В.В. «Комп'ютерні» злочини: питання кваліфікації. *Право України*. 2002. № 2. С. 86–88.

7. Голубєв В. Комп'ютерна злочинність. *Юридичний вісник України*. 2012. № 6 (9). С. 12–16.

8. Конвенція про кіберзлочинність від 23 листопада 2001 року Офіційна інтернет-сторінка Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 25.10.2021).

9. Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector. URL : https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_ 2_E.pdf (дата звернення: 25.10.2021).

10. ITU Model Cybercrime Legislation: Project Overview. URL : http://www.itu.int/ITU-D/cyb/cybersecurity/docs/model-cybercrime-lawproject-overview.pdf (дата звернення: 25.10.2021).

11. Кримінальний кодекс України: Закон України від 5 квітня 2001 року № 2341-III Офіційна інтернет-сторінка Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 25.10.2021).

12. Колесник В.А. Розслідування комп'ютерних злочинів. Наук.-метод. посіб. К.: Вид-во НА СБУ, 2012. 188 с.

13. Біленчук П.Д. Комп'ютерна злочинність. Навч. посіб. К.: Атіка, 2012. 240 с.

14. Поливода О.Ю. Боротьба з комп'ютерною злочинністю в Україні: проблемні питання. *Взаємодія правоохоронних органів з провайдерами та операторами зв'язку в боротьбі з комп'ютерними злочинами: матеріали регіонального наук.-практ. семінару*, м. Донецьк, 12 грудня 2008 р. / Донецький юрид. ін.-т ЛДУВС ім. Е.О. Дідоренка. Донецьк: ДЮІ ЛДУВС, 2009. С. 88–91.

15. Бєлей К.В. Актуальні проблеми виявлення латентних комп'ютерних злочинів. *Взаємодія правоохоронних органів з провайдерами та операторами зв'язку в боротьбі з комп'ютерними злочинами: матеріали регіонального наук.-практ. семінару*, м. Донецьк, 12 грудня 2008 р. / Донецький юрид. ін.-т ЛДУВС ім. Е.О. Дідоренка. Донецьк: ДЮІ ЛДУВС, 2009. С. 12–16.

16. Криминалистика: учебник / Т.В. Аверьянова, Р.С. Белкин, Ю.Г. Корухов, Е.Р. Россинская / под ред. Р.С. Белкина. М.: Норма, 2001. 990 с.

17. Анненкова Т.С. Обстановка совершения преступления и криминалистические методы её исследования: дис. канд. юрид. наук: 12.00.09. Саратов, 2007. 225 с.

18. Яблоков Н.П. Криминалистика: учебник. 2-е изд., перераб. и доп. М., 2008. 400 с.

19. Ермолович В.Ф. Криминалистическая характеристика преступлений М., 2001. 304 с.

20. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій: [наук.-прак. посіб.] / [Б.В. Романюк, В.Д. Гавловський, М.В. Гуцалюк, В.М. Бутузов]; за ред. проф. Я.Ю. Кондратьєва. К. : Вид. Паливода А. В., 2004. 144 с.

21. Шевченко В.Ф., Суслов С.О. Розкриття та розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Бюлетень МВС по обміну досвідом роботи*. 2003. № 135. С. 60–76.

22. Криминалистика: учебник для бакалавров / В.П. Антонов, И.И. Белозерова, Л.В. Бертовский, С.А. Боринская, ред.: Л.В. Бертовский. М., 2018. 961 с.

23. Бутузов В.М. Документування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку при проведенні дослідчої перевірки: науково-практичний посібник. Київ, 2010. 245 с.

24. Мотлях О.І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій: дис. … канд. юрид. наук: 12.00.09. Київ, 2013. 221 с.

25. Проблемы выявления и расследования киберпреступлений: монография / Л.П. Зверянская. Красноярск, 2016. 176 с.

26. Злобін Д.Л. Способи вчинення комп'ютерних злочинів у сфері високих технологій та заходи протидії. *Актуальні питання юридичної науки: теорія та практика: матеріали міжнар. наук.-практ. конф.*, м. Кіровоград, 11 грудня 2013 р. / Кіровоградський ін-т. держ та муніц. упр. КПК. Кіровоград: КІДМУ КПУ, 2013. С. 55–60.

27. Голубєв В.О. Інформаційна безпека: проблеми боротьби з кіберзлочинами: Монографія. Запоріжжя, 2003. 250 с.

28. Криміналістика: навч. посіб. / В.В. Кір'яков, Н.Є. Маковецька; Львів. держ. ун-т внутр. справ. Львів, 2015. 407 с.

29. Постіл Н.С. Виявлення слідів комп'ютерних атак. *Проблеми впровадження інформаційних технологій в економіці: тези доповідей V Міжнародної науково-практичної конференції* (Ірпінь, травень 2004 р.). Ірпінь, 2004. С. 518–522.

30. Криміналістика: підручник / В.В. Пясковський, Ю.М. Чорноус, А.В. Іщенко, О.О. Алексєєв та ін. К.: Центр учбової літератури, 2015. 544 с.

31. Мещеряков В.А. Следы преступлений в сфере высоких технологий. *Библиотека криминалиста*. 2013. № 5 (10). С. 265–269.

32. Біленчук П.Д. Криміналістична тактика і методика розслідування окремих видів злочинів: [навч. посіб.] / П.Д. Біленчук, А.П. Гель, Г.С. Семаков. К. : МАУП, 2007. 512 с.

33. Давыдов В.О., Головин А.Ю. Значение виртуальных следов в расследовании преступлений экстремистского характера. *Известия Тульского государственного университета. Экономические и юридические науки*. 2016. № 2(3). С. 254–259.

34. Білоусов А.С. Комп'ютерні об'єкти та їх значення в криміналістичній характеристиці злочинів. *Вісник Запорізького юридичного інституту*. 2007. № 3. С. 301–306.

35. Краснова Л.Б. Компьютерные объекты в уголовном процессе и криминалистике : автореф. дис. канд. юрид. наук. Воронеж, 2005. 17 с.

36. Салтевський М.В. Навчально-довідковий посібник з криміналістики / М.В. Салтевський, В.Г. Лукашевич, В.М. Глібко. Київ: Рад. шк., 1994. 180 с.

37. Криміналістика: підручник / В.Ю. Шепітько, В.О. Коновалова, В.А. Журавель та ін.; за ред. В.Ю. Шепітька. 5-е вид., перероб. і доп. Х.: Право, 2011. 464 с.

38. Ермолович В.Ф. Криминалистическая характеристика преступлений Мн.: Амалфея, 2001. 194 с.

39. Голубєв В.О. Розслідування комп'ютерних злочинів: [монографія] Запоріжжя: Гуманітарний університет «ЗІДМУ», 2003. 296 с.

40. Козак Н.С. Криміналістичні аспекти виявлення комп'ютерних злочинів. *Науковий вісник Національного університету ДПС України*. 2010. № 4(51). С. 252–258.

41. Актуальні питання розслідування кіберзлочинів: матеріали Міжнар. наук. – практ. конф., м. Харків, 10 груд. 2013 р. / МВС України, Харк. нац. ун-т внутр. справ. Х.: ХНУВС, 2013. 272 с.

42. Постіл Н.С. Сутність і підслідність комп'ютерних злочинів. *Науковий вісник Національної академії ДПС України*. 2005. № 1(28). С. 234–243.

43. Селиванов Н.А. Криминалистические характеристики преступлений и следственные ситуации в методике расследования преступлений. *Социалистическая законность*. 1977. № 2. С. 56–59.

44. Хижняк Є.С. Типові слідчі ситуації при розслідуванні окремих видів злочинів. *Південноукраїнський правничий часопис*. 2012. № 4. С. 197–199.

45. Весельський В.К. Слідча ситуація як категорія криміналістичної тактики. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2011. № 25. С. 193–199.

46. Кікінчук В.В. Типові слідчі ситуації початкового етапу розслідування. *Право і безпека*. 2013. № 2 (49). С. 131–135.

47. Журавель В.А. Ситуаційний підхід до формування окремих криміналістичних методик розслідування злочинів. *Теорія і практика судової експертизи і криміналістики*. 2008. Вип. 8. С. 102–108.

48. Шевчук В.М. Слідчі ситуації та їх вплив на розробку тактичних операцій. *Науковий вісник Міжнародного гуманітарного університету*. 2013. № 6–3. Т. 2. С. 125–129.

49. Степанюк Р.Л. Ситуаційний підхід у формуванні методик розслідування злочинів, вчинених у бюджетній сфері України. *Право і безпека*. 2013. № 3 (50). С. 110–115.

50. Чернявський С.С. Теоретичні та практичні основи методики розслідування фінансового шахрайства: дис. ... д-ра юрид. наук: 12.00.09. Київ, 2010. 610 с.

51. Калініна І.В. Ситуаційна обумовленість розслідування окремих видів злочинів. Вчені записки Таврійського національного університету ім. В.І. Вернадського. 2013. Том 26 (65). С. 212–217.

52. Ахтирська Н.М. Актуальні проблеми розслідування кіберзлочинів: навч. посіб. Київ: ВПЦ «Київський університет», 2018. 229 с.

53. Розслідування окремих видів злочинів: навч. посібник / О.В. Бишивець, М.А. Погорецький, Д.В. Сергєєва та ін.; за ред. М.А. Погорецького та Д.Б. Сергєєвої. Київ: Алерта, 2015. 563 с.

54. Протидія злочинам, що вчиняються у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж: науково-практичний посібник / [С.І. Ніколаюк, Д.Й. Никифорчук, О.В. Тихонова, С.В. Шутенко, Я.Ю. Липчей]. К.: КНТ, 2007. 196 с.

55. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: дис. … канд. юрид. наук: 12.00.09, Москва, 2016. 249 с.

56. Кримінальний процесуальний кодекс України: Закон України від 13 квітня 2012 року № 4651-VI Офіційна інтернет-сторінка Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 25.10.2021).

57. Гресь Ю.О. Допит: визначення тактичного та технологічного аспектів. *Науковий вісник Міжнародного гуманітарного університету: Сер. Юриспруденція*. 2016. № 20. С. 152–155.

58. 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.

59. Косенков А.Н., Чёрный Г.А. Общая характеристика психологии киберпреступника. *Криминологический журнал БГУЭП*. 2012. № 3(21). С. 91–104.

60. Зачек О.І., Захарова О.В., Навроцька В.В., Федчак І.А. Особливості розкриття та розслідування кіберзлочинів Методичні рекомендації – Львів: Львівський державний університет внутрішніх справ, 2010. 60 с.

61. Ніколайчук С.І., Никофорчук Д.Й., Семчук А.Г., Шутенко С.В., Липчей. Протидія злочинам, що вчиняються у сфері використання ЕОМ, систем і комп'ютерних мереж. // Науково-практичний посібник. К.:КНТ, 2007. 57 с.

62. Салтевський М.В. Основи методики розслідування злочинів, скоєних з використанням ЕОМ. Навч. Посібник. Харків: Нац. юрид акад. України. 2000. 135 с.

63. Теплицький Б.Б., Шарай Л.Г., Ковальов К.М., Кузьмін С.А. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: спеціальні питання кваліфікації, проведення слідчих (розшукових) дій,

призначення комп'ютерно-технічних судових експертиз: наук.-практ. посіб. Київ: Паливода А.В., 2019. 168 с.

64. Велика українська юридична енциклопедія: у 20 т.: Т. 20: Криміналістика, судова експертиза, юридична психологія / Авдєєва Г.К. та ін.; редкол.: В.Ю. Шепітько (голова) та ін.; Нац. акад. прав. наук України, Ін-т держави і права ім. В.М. Корецького НАН України, Нац. юрид. ун-т ім. Ярослава Мудрого. Харків: Право, 2018. 951 с.

65. Основи судової експертизи: навчальний посібник / авт.-уклад.: Л.М. Головченко, А.І. Лозовий, Е.Б. Сімакова-Єфремян та ін. Х. : Право, 2016. 928 с.

66. Судова експертологія: курс лекцій для слухачів магістратури юридичних вузів / Тертишник В.М., Варава В.В., Сачко О.В. / За заг. ред. д.ю.н, професора В.М. Тертишника. Дніпро: ЛІРА, 2021. 208 с.

67. Клименко Н.І. Судова експертологія: курс лекцій: навч. посіб. для студ. юрид. спец. вищ. навч. закл. К.: Видавничій дім «Ін Юре», 2007. 528 с.

68. Інструкція про проведення судово-медичної експертизи: Наказ Міністерства охорони здоров'я України від 17 січня 1995 року № 6 Офіційна інтернет-сторінка Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/z0254-95#Text (дата звернення: 25.10.2021).

69. Козак Н.С. Використання спеціальних знань при розкритті й розслідуванні комп'ютерних злочинів. *Вісник Луганського державного університету внутрішніх справ. Спеціальний випуск*. 2014. № 2. Частина 3. С. 119–126.

70. 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: Наказ Міністерства юстиції України від

8 жовтня 1998 року № 53/5 Офіційна інтернет-сторінка Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#n14 (дата звернення: 25.10.2021).