УДК 343.985.7
DOI https://doi.org/10.32849/2663-5313/2020.7.61

Ярослав Неділько,
аспірант кафедри правосуддя
юридичного факультету
Київського національного університету імені Тараса Шевченка

ОБСТАНОВКА ТА «СЛІДОВА КАРТИНА» ЯК ЕЛЕМЕНТИ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ КІБЕРЗЛОЧИНІВ

Стаття присвячена актуальним питанням розслідування кіберзлочинів, а саме розгляду питання виявлення криміналістично значущих слідів, що свідчать про вчинення кіберзлочину, та встановлення обстановки, за якої скоєння стає можливим. Офіційно поступ до інформаційного суспільства був проголошений Комісією Європейського Союзу у 1993 році. Із 1995 року почала роботу міжнародна Комісія з Глобальної інформаційної інфраструктури, що координує розвиток національних інфраструктур країн світу у створені глобальної взаємодії інформаційних потоків у діловій та інформаційній сфері на основі Інтернету. Інформатизація та використання відповідних технічних засобів не забезпечило повний захист від злочинних посягань, що призвело до нових викликів та загроз у виді кіберзлочинів. Статистичні показники, що характеризують кіберзлочинність в Україні, підкреслюючи нагальну потребу сучасного підходу до розробки методик розслідування злочинів «нового покоління». Ситуація вчинення цього виду злочинів є відмінною від інших кримінальних правопорушень, оскільки кіберзлочини вчиняються дистанційно. Тому ситуацію необхідно аналізувати з погляду знаходження інформаційного ресурсу, який є об'єктом посягання, місця перебування злочинця, та локалізації настання негативних наслідків. А середовище, в якому вчиняються кіберзлочини. автор поділяє на фізичне та електронне.

Особливості притаманні й «слідовій картині», оскільки при дослідженні виявляють «віртуальні сліди», «інформаційні сліди», «нетрадиційні сліди», «електронні сліди» тощо. Електронна інформація не відноситься в чистому вигляді до матеріальних слідів, а також і до ідеальних. Хоча електронна інформація і «матеріальний» слід, оскільки вона зберігається в пам'яті машини та може бути вилучена звідти, а принцип дії комп'ютера має схожість з принципом діяльності мозку людини, але відрізняється від нього тим, що складається не з нейронів, а з електронних схем. Притаманні електронній інформації також певні ознаки «ідеального» сліду, вона невидима, не сприймається ні за допомогою людських органів (зору, слуху), ані за допомогою спеціальних засобів посилення сприйняття (збільшувальні прибори, спеціальні порошки тощо).

Ключові слова: розслідування кіберзлочинів, інформаційні сліди, цифрова криміналістика, електронна інформація.

Постановка проблеми. Розкриття кіберзлочинів є досить важким та непростим завданням органу досудового розслідування. Це пов'язано із наявністю у злочинців спеціальних знань та технічних засобів, які вони використовують для скоєння кіберзлочину, а також проблемою виявлення, фіксацією та використанням електронних слідів. Так, за статистичними даними Генеральної прокуратури України, у 2019 році зареєстровано 2204 злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (361-363^{-1} КК України), у 1481 кримінальному провадженні особам вручено повідомлення про підозру, у 63 – кримінальне провадження зупинено у зв'язку з тим, що знаходження підозрюваного невідомо, з обвинувальним актом до суду направлено 1259 проваджень [1]. За даними Судової адміністрації України, в 2019 році засуджено за ст.ст. 361-363^{-1} КК України – 50 осіб (з яких два іноземних громадянина) [2], що свідчить про не якісне досудове розслідування, а також, невизнання судами електронних (цифрових) доказів, які були отримані із порушенням процесуального законодавства.

Обстановку та «слідову картину» як елементи криміналістичної характеристики досліджували такі вчені як: Н.М. Ахтирська, В.Ф. Єрмолович, В.О. Коновалова, М.А. Погорецький, М.В. Салтевський, М.І. Скригонюк, В.Ю. Шепітько, М.П. Яблоков та інші.

Мета статті – на базі теоретичних досліджень визначити особливості обстановки та «слідової картини» як елементів криміналістичної характеристики кіберзлочинів та запропонувати авторське визначення даних понять.

Виклад основного матеріалу. Обстановка злочину є предметом дослідження різних юридичних наук. Кримінальне право розглядає обстановку як елемент кримінально-правової характеристики злочинів; кримінологія – з точки зору запобігання злочинності; кримінальне процесуальне право з боку доказування. Криміналістична наука розглядає обстановку як елемент криміналістичної характеристики, який вивчає середовище, в якому вчинюється злочин.

Розслідування злочину органом досудового розслідування, в більшості випадків, розпочинається зі сприйняття і дослідження обстановки, в якій воно було вчинено. З'ясування обстановки вчинення злочину допомагає сформулювати слідчому уявлення про механізм здійснення злочину, ймовірні місця пошуку слідів злочину, суб'єкта (суб'єктів) вчинення злочину, мотив та мету, а також деякі аспекти способу його вчинення.

Серед учених-криміналістів немає одностайності щодо тлумачення ситуації вчинення злочинів.

Зокрема, Т.С. Анненкова під обстановкою вчинення злочину розуміє 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 [3, с. 55].

На думку М.П. Яблокова, під обстановкою вчинення злочину слід розуміти 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 [4, с. 36].

На нашу думку, більш глибше дослідив це питання В.Ф. Єрмолович, який цілком доречно пропонує у криміналістичному аспекті розглядати саме обстановку злочину, яку складають три самостійні і в той же час взаємопов'язані ланки: «обстановка, яка передувала скоєнню злочину», «обстановка скоєння злочину», «обстановка, яка склалася після скоєння злочину» [5, с. 181]. 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 [5, с. 180].

Що стосується поняття обстановка кіберзлочину, то у юридичній літературі не існує конкретного його визначення.

Слушно зазначає Л.П. Зверянська, що обстановка вчинення кіберзлочину має свою специфіку. 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 [6, с. 39].

Слід зауважити, що під кіберпростором розуміють 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 [7].

Враховувати таку специфічну ознаку як кіберпростір (віртуальний простір) є цілком доречним, однак не слід забувати і про інші ознаки матеріального (реального) середовища, які є вагомими для розслідування та розкриття даних злочинів. Проаналізувавши вищенаведені теоретичні погляди вчених, а також зважаючи на особливості кіберзлочинів, на наш погляд, в обстановці кіберзлочину слід виділяти: 1) кіберпростір – в якому здійснюється електронний процес, до, в момент та після вчинення злочину, що характеризується місцем, часом, віртуальною взаємодією учасників злочину; 2) матеріальний (фізичний) простір – систему умов та обставин, що взаємодіють між собою до, в момент та після вчинення злочину об'єктів, процесів, що характеризують місце, час та реальну взаємодію учасників злочину, а також інші обставини скоєння кіберзлочину (соціально-психологічні, економічні, без пекові, політичні тощо).

Під час розслідування кіберзлочинів велике значення має інформація про ймовірне місце та час його вчинення. Для слідчого є важливим встановлення місця скоєння даного злочину. Насамперед, установлення місця вчинення злочину допомагає встановити місцезнаходження можливих доказів та коло осіб причетних до вчинення злочину. Час вчинення кіберзлочину дозволяє встановити в якій саме послідовності здійснювались злочинні дії та їх тривалість.

Натомість, серед науковців не існує одностайності в визначенні поняття місця та часу вчинення кіберзлочинів.

Досліджуючи місце вчинення злочину, необхідно звернути увагу на те, що воно обирається суб'єктами злочину не випадково. Попередньо, з різних сторін оцінивши ймовірне місце, суб'єкт фактично використовує його в якості засобу реалізації свого злочинного наміру. Місце вчинення злочину розглядається як визначена географічна точка (територія, приміщення тощо), яке тісно пов'язане з іншими елементами обстановки злочину [8, с. 744].

Аналізуючи час вчинення злочину, доречно зауважити, що час не обмежується астрономічними властивостями (рік, місяць, дата, години, хвилини, секунди). Це може бути час пов'язаний з сезонністю, з настанням темноти чи світлого часу доби, часом відпочинку та часом відсутності потерпілих в місцях проживання, годиною «пік», час, який пов'язаний з певною періодичністю тощо [8, с. 743–744].

Враховуючи специфіку кіберзлочинів, можна виокремити місця їх вчинення: фізичне середовище (ділянки місцевості) та електронне середовище (вузли мережі), де розташовані:

– програмно-технічні засоби (носії інформації), що зазнали злочинного впливу, та точки їхнього доступу до певних мереж;

– програмно-технічні засоби, які злочинець використовував опосередковано, та точки їх доступу до певних мереж;

– мережні вузли каналів зв'язку, з використанням яких відбувався обмін інформацією між програмно-технічними засобами злочинця та потерпілого [9, с. 72–73].

Що стосується вибору фізичного середовища злочинцем, то слід погодитися з думкою О.І. Мотляха, що злочинці переважно обирають наступні місця:

– адміністративні та службові приміщення різного типу суб'єктів господарювання (підприємств, організацій, компаній, фірм тощо), які використовують у своїй виробничій діяльності електронні пристрої;

– власні та орендовані житлові приміщення (офіси, квартири, кімнати та інше), в яких встановлені електронні пристрої, що забезпечені виходом до всесвітньої мережевої системи Інтернет;

– приміщення комунальної власності або ж споріднені з ними (цокольні, напівпідвальні чи ті, що примикають до житлових будинків приміщення), котрі на правах власності чи оренди можуть використовуватися під комп'ютерні клуби, Інтернет-кафе тощо [10, с. 64].

Переходячи до дослідження електронного середовища (кіберпростору, як головного місця вчинення кіберзлочину), слід погодитися з Л.П. Зверянською, що при здійсненні даних злочинів може бути декілька місць їх вчинення, а саме:

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

– місце постійного зберігання або резервування інформації – сервер або стример (пристрій запису та зберігання даних на магнітній стрічці);

– місце використання технічних засобів для неправомірного доступу до комп'ютерної інформації, що знаходиться в іншій точці, при цьому місце використання може збігатися з робочим, але перебувати поза організацією (наприклад при зломі шляхом зовнішнього віддаленого мережевого доступу);

– місце підготовки злочину (розробка вірусів, програм злому, підбору паролів) чи місце безпосереднього використання інформації (копіювання, поширення, спотворення), отриманої в результаті неправомірного доступу до даних, що містяться на пристрої [6, с. 40].

Необхідно зазначити, що суттєвою особливістю кіберзлочинів є те, що для них відсутнє просторове обмеження і вчинення злочину може виходити за рамки однієї держави. Злочин вчиняється в одній державі, а негативні наслідки настають в іншій. Такі злочини набувають транснаціонального характеру. Тобто, для них є властивим наявність іноземного елемента в криміналістичній характеристиці та в кримінально-процесуальних відносинах під час його розслідування [11, с. 873–874].

Встановлення часу вчинення кіберзлочинів не складає великих проблем, оскільки операційна система електронного пристрою детально стежить практично за кожною важливою операцією, інформація про які відображається в статистичних файлах. За допомогою програм загальносистемного призначення можна встановити поточний час роботи комп'ютерної системи. Це дозволить за відповідною командою вивести на екран дисплею інформацію про день, години, хвилини та секунди виконання тієї або іншої операції [12, с. 101].

Не відкидаються випадки, коли час вчинення злочину установити неможливо. Це може бути зумовлено технічними причинами, зокрема під час перезавантаження електронного пристрою повністю або частково обнуляються чи стираються дані тощо. Тому в таких випадках час вчинення необхідно встановлювати шляхом проведення

судової комп'ютерно-технічної експертизи. Крім того, час вчинення кіберзлочину можна встановити проведенням слідчих (розшукових) дій. Також слід звертати увагу чи час виставлений на електронному пристрою співпадає з поточним і чи не корегувався він.

Варто зауважити, що під віртуальною взаємодією учасників кіберзлочину слід розуміти їх спільні дії у кіберпросторі. Наприклад, особи домовилися вчинити DoS-атаку у відповідний день та час, використовуючи при цьому допоміжні програми, в яких узгоджують свої дії (Telegram, Viber, Discord тощо). Під реальною взаємодією учасників кіберзлочину розуміється їх контакт у фізичному середовищі.

Безумовно, елементи обстановки залишають різного роду сліди, які можуть бути виявлені при криміналістичному аналізі злочину в процесі його розслідування [13, с. 68].

Сліди злочину – це результат взаємодії об'єктів живої і неживої природи, що опинилися в сфері злочинної діяльності [14, с. 89].

Ми підтримуємо точку зору О.О. Безсонова, який у своєму дисертаційному дослідженні стверджує, що існує закономірний зв'язок між обстановкою злочину з іншим елементом криміналістичної характеристики злочину – слідами злочину («слідовою картиною» злочину) [15, с. 164–165]. Тому у криміналістичній характеристиці кіберзлочинів слід виділяти такий елемент як «слідова картина» кіберзлочину, оскільки він допоможе зрозуміти слідчому, де знаходяться сліди злочинного діяння, що допоможе в розслідуванні даних злочинів та доведенні вини особи.

Водночас у криміналістичній літературі є різні думки вчених стосовно трактування слідів злочину, як елемента криміналістичної характеристики, а також понять «слідова обстановка», «слідовий вібавід», «слідова картина» злочину. Деякі науковці виокремлюють поняття «слідова обстановка» злочину під яким розуміють час, місце, обставини, обстановку вчинення злочину. В своїй основі «слідова обстановка» концентрує проблематику ідеальних та матеріальних слідів [16, с. 250]. М.І. Скригонюк пропонує використовувати поняття «слідовий вібавід», обґрунтовуючи це тим, що саме слово «вібавід» складається утворюється з абревіатури трьох слів-компонентів: ві – відображення, ба – бачення, від – відтворення [16, с. 250].

На нашу думку, не слід поєднувати два елемента криміналістичної характеристики (обстановка злочину та сліди злочину) в один (слідова обстановка). Такий підхід створить важкість тлумачення даного поняття та плутанину серед практиків. Що стосується застосування терміну «вібавід», то воно є досить складним для вживання і навряд чи набуде практичного значення як елемент криміналістичної характеристики. Більш практичним є поняття «слідова картина» злочину, що увійшло в науковий обіг із практики оперативно-розшукової діяльності та має певний інформаційний зміст [17, с. 12].

На думку О.І. Дикунова «слідова картина» злочину це сукупність джерел речової інформації, що залучена для вирішення конкретних оперативно-розшукових чи слідчих завдань, які мають дані підтвердити чи спростувати версії обставин злочину [17, с. 154]. Слід погодитися з В.О. Коноваловою, яка під «слідовою картиною» злочину розуміє комплекс слідів, які відображають картину події злочину та поведінку суб'єкта на місці злочину, дозволяє висунути найбільш обґрунтовані версії щодо його вчинення [18, с. 25].

У криміналістичній літературі прийнято поділяти сліди на матеріальні та ідеальні, що відбиває два боки пізнання – інформаційний і доказовий. Ідеальні сліди – це відображення події або її елемента у пам'яті людини, уявний образ сприйнятого, характер якого залежить від стану органів чуття особи, її пам'яті, рівня інтелекту тощо. Матеріальні сліди – це відображення механізму події та її результатів на об'єктах матеріального світу [19, с. 138].

Виходячи із наведеного базового визначення, розглядається і «слідова картина» кіберзлочинів. Матеріальними слідами цієї категорії злочинів, слушно зазначає А.І. Кунтій, необхідно вважати: сліди-відображення зовнішнього фізичного впливу на комп'ютерні системи, периферійні пристрої та мережі (сліди рук, ніг, знарядь злому тощо); сліди-речовини: у вигляді витратних матеріалів (тонерів, фарб, різних мастил, що використовуються в комп'ютерних системах, їх мережах та периферійних пристроях); сліди-предмети: змінні диски та стрічки, пристрої дистанційного зняття інформації, роздруківки на паперових носіях та документи на електронних носіях, кабелі та роз'єми, пристрої фізичного знищення комп'ютерів і їх мереж [20, с. 876–877].

Доречно зауважити, що у кіберзлочинах, необхідно виділяти третій вид слідів. При їх дослідженні науковці використовують різні поняття, зокрема: «віртуальні сліди», «інформаційні сліди», «нетрадиційні сліди», «електронні сліди» тощо.

Наприклад, В.О. Мещеряков називає їх «віртуальними» від латинського virtualis – можливий, який може або має проявитися за певних умов [21, с. 109]. Пропонує визна-

чення віртуального сліду як будь-яких криміналістичних змін стану автоматизованої інформаційної системи (утвореного нею кібернетичного простору), що пов'язані з подією злочину і зафіксовані у вигляді комп'ютерної інформації на матеріальному носієві, у тому числі і в електромагнітному полі [22, с. 104].

Термін «інформаційні сліди» використовує Ю.В. Гаврілін, який вважає, що злочини даної категорії майже завжди пов'язані з неправомірним доступом злочинця до комп'ютерної інформації і поділяє сліди на два види: традиційні сліди, що вивчаються трасологією, і нетрадиційні – інформаційні сліди. Зазначає, що інформаційними їх називати слід тому, що утворюються вони в результаті впливу злочинця (знищення, модифікації, копіювання, блокування тощо) на комп'ютерну інформацію шляхом доступу до неї і становлять собою будь-які зміни комп'ютерної інформації, пов'язані з подією злочину [23, с. 32].

Слушною є думка В.Б. Вехова, який пропонує розглядати «електронний цифровий слід», під яким слід розуміти будь-яку криміналістично значущу комп'ютерну інформацію, тобто свідчення (повідомлення, дані), що знаходяться в електронно-цифровій формі, зафіксовані на матеріальному носієві або такі, що передаються каналами зв'язку за допомогою електромагнітних сигналів. Ці сліди є матеріальними невидимими слідами. Слідами предметами (частинами предметів) та одночасно типовими матеріальними носіями електронно-цифрових слідів варто вважати машинні носії інформації, інтегральні мікросхеми, мікроконтролери, пластикові картки та інші комбіновані документи, ЕОМ та інші комп'ютерні пристрої [24, с. 30].

Повною мірою поділяємо позицію Н.М. Ахтирської, яка розглядає «електронний слід». Насамперед, вона зазначає, що електронна інформація не відноситься в чистому вигляді до матеріальних слідів, а також і до ідеальних. Хоча електронна інформація і «матеріальний» слід, оскільки вона зберігається в пам'яті машини та може бути вилучена звідти, а принцип дії комп'ютера має схожість з принципом діяльності мозку людини, але відрізняється від нього тим, що складається не з нейронів, а з електронних схем. Притаманні електронній інформації також певні ознаки «ідеального» сліду, вона невидима, не сприймається ні за допомогою людських органів (зору, слуху), ані за допомогою спеціальних засобів посилення сприйняття (збільшувальні прибори, спеціальні порошки тощо) [25, с. 136–137].

Прикладом електронних слідів можна вважати:

1) інформація, яка міститься в журналах операційних систем та окремих програмних продуктів;

2) дані електронного листування, за допомогою яких можна встановити дату та час, адресу відправника тощо;

3) дії на різних сайтах (Facebook, Twitter тощо), які залишають електронні сліди у вигляді повідомлень, пошукових запитів, фотознімків тощо [26, с. 171].

Не менш важливим при розслідуванні кіберзлочинів є дослідження слідів даного злочину.

Стосовно цього, цілком вірно висловилась Н.М. Ахтирська, яка зауважує, що сліди вчинення кіберзлочинів можуть знаходитись не лише безпосередньо в комп'ютерній техніці, на флеш-носіях, а і в кіберпросторі – середовищі (віртуальному просторі), яке надає можливості для здійснення комунікацій та реалізації суспільних відносин, комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет або інших глобальних мереж передачі даних [25, с. 138].

Проте, при розслідування кіберзлочинів не слід нехтувати матеріальними слідами (сліди пальців рук, сліди виділень тощо), що залишені на електронних пристроях.

Таким чином, «слідова картина» кіберзлочину становить сукупність матеріальних, ідеальних та електронних слідів кіберзлочину, які дозволяють слідчому встановити картину даного злочину. При цьому обстановка та «слідова картина» як криміналістичні елементи кіберзлочину взаємопов'язані між собою та мають певну специфіку, опанування якими має важливе як теоретичне так і практичне значення для ефективного розслідування та розкриття злочинів даної категорії.

Список використаних джерел:

1. Статистика Генеральної прокуратури України. URL: https://old.gp.gov.ua/ua/statinfo.html (дата звернення 18.05.2020).

2. Статистика Судової влади України. URL: https://court.gov.ua/inshe/sudova_statystyka/analit_tabl_19 (дата звернення 18.05.2020).

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

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

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

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

7. Текст лекції з дисципліни «Організаційне забезпечення технічного захисту інформації. Розробники: Ю.М. Онищенко, В.В. Носов. Харків, 2016. URL: http://lib.univd.edu.ua/?controller=service&action=downloadRep&id=97504 (дата звернення 18.05.2020).

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

9. 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. К., 2010. 245 с.

10. Мотлях О.І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій: дис. ... канд. юрид. наук: 12.00.09. Київ, 2005. 221 с.

11. Криміналістика : підручник / за заг. ред. Є.В. Пряхіна. Львів, 2016. 948 с.

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

13. Криминалистика: Учебник / Отв. ред. Н.П. Яблоков. 3-е изд., перераб. и доп. М., 2005. 781 с.

14. Салтевский М.В. Криміналістика (у сучасному викладі): Підручник. Київ. 2006. 588 с.

15. Бессонов А.А. Частная теория криминалистической характеристки преступлений : дис. док. юрид. наук : 12.00.12 / Бессонов Алексей Александрович. Элиста. 2017. 456 с.

16. Скригонюк М.І. Криміналістика: Підручник. К., 2005. 496 с.

17. Дикунов А.И. Криминалистический анализ следовой картины расследуемого события с признаками преступления : дис... канд. юрид. наук 12.00.09 / Александр Иванович Дикунов. Москва. 2005. 186.

18. Коновалова В.О. Вбивство: мистецтво розслідування : монографія. К., 2001. 311 с.

19. Криміналістика : підручник / за ред. В.В. Тіщенка. Одеса, 2017. 556 с.

20. Криміналістика : підручник / за заг. ред. Є.В. Пряхіна. Львів, 2016. 948 с.

21. Словник іншомовних слів / уклад.: С.М. Морозов, Л.М. Шкарапута. К., 2000. 680 с.

22. Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж, 2002. 408 с.

23. Гаврилин Ю.В. Расследование неправомерного доступа к компьютерной информации / под ред. Н.Г. Шурухнова. М., 2001. 88 с.

24. Вехов В.Б. Криминалистическое учение о компьютерной информации и средствах ее обработки: автореф. дис. ... докт. юрид. наук: 12.00.09. Волгоград, 2008. 45 с.

25. Ахтирська Н.М. Актуальні проблеми розслідування кіберзлочинів : навчальний посібник. К., 2018. 229 с.

26. Авдєєва Г.К., Стороженко С.В. Електронні сліди: поняття та види. URL: http://dspace.nlu.edu.ua/bitstream/123456789/13283/1/Avdeeva_168-175.pdf (дата звернення 19.05.2020). bitstream/123456789/13283/1/Avdeeva_168-175.pdf (дата звернення 19.05.2020).

Yaroslav Nedilko. Situation and trace as elements of the criminalistic characteristics of cybercrime

The article is devoted to topical issues of cybercrime investigation, namely the consideration of the issue of detecting forensic traces that indicate the commission of a cybercrime, and the establishment of the situation in which the commission becomes possible. Accession to the information society was officially announced by the European Commission in 1993. Since 1995, the International Commission on Global Information Infrastructure has been working to coordinate the development of national infrastructures of the world in creating a global interaction of information flows in business and information in the Internet. Informatization and the use of appropriate technical means did not provide full protection against criminal encroachments, which led to new challenges and threats in the form of cybercrime. Statistical indicators characterizing cybercrime in Ukraine, emphasizing the urgent need for a modern approach to the development of methods for investigating crimes of the "new generation". The situation of committing this type of crime is different from other criminal offenses, as cybercrimes are committed remotely. Therefore, the situation must be analyzed in terms of finding the information resource that is the object of encroachment, the location of the offender, and the location of the negative consequences. And the environment in which cybercrimes are committed. the author divides into physical and electronic.

Peculiarities are also inherent in the "trace picture", because the study reveals "virtual traces", "information traces", "non-traditional traces", "electronic traces" and so on. Electronic information does not belong in its pure form to material traces, as well as to the ideal. Although electronic information and "material" should be, because it is stored in the memory of the machine and can be extracted from there, and the principle of the computer is similar to the principle of the human brain, but differs from it in that it consists not of neurons but from electronic circuits. Electronic information also has certain features of an "ideal" trace, it is invisible, it is not perceived either by human organs (sight, hearing) or by special means of enhancing perception (magnifying devices, special powders, etc.).

Key words: cybercrime investigation, information traces, digital forensics, electronic information.