should ensure the completeness of the investigation of the mechanism of the traffic accident. As well as in establishing the causes and links to the incident of any actions or inaction of the participants in the traffic accident.

Key words: auto-technical examination, administrative offense, traffic accident.

DOI: https://doi.org/10.33994/kndise.2020.65.45
УДК 343.98

Олексій Сергійович Омельян
аспірант

E-mail: mailto:omelan_ssu@ukr.net

Національна академія Служби безпеки України

ПОНЯТТЯ ТА ОЗНАКИ ЦИФРОВИХ СЛІДІВ, ЩО УТВОРЮЮТЬСЯ ПІД ЧАС ВЧИНЕННЯ КІБЕРЗЛОЧИНІВ

В статті розглянуто наукові погляди щодо термінології у сфері криміналістичного і судово-експертного забезпечення розслідування кіберзлочинів та, з урахуванням специфіки використання інформаційно-телекомунікаційних технологій в судовій експертизі, обґрунтовано коректність вживання терміну «цифрові сліди». Запропоновано авторське визначення поняття цифрових слідів, які утворюються під час вчинення кіберзлочинів, наведено і проаналізовано їх специфічні ознаки та властивості.

Ключові слова: *цифрові сліди, кіберзлочини, інформаційно-телекомунікаційні технології, спеціальні знання, судова експертиза.*

Прогрес у сфері інформаційно-телекомунікаційних технологій обумовлює появу нових видів кіберзлочинів, а також способів їх вчинення та приховування. Водночас, розвиток цифрових технологій дозволяє знаходити й ефективні рішення у сфері протидії кіберзлочинності.

Однією з актуальних проблем, що виникає протягом розслідування кіберзлочинів, є виявлення, фіксація, вилучення та збереження значної кількості цифрових слідів, які утворюються під час вчинення правопорушення та залишаються в пам'яті атакованого комп'ютера та/чи комп'ютера зловмисника, а також у мережевому обладнанні, через яке здійснювалась кібератака тощо. У зв'язку з цим, відсутність розуміння особливостей утворення і відображення цифрових слідів та їх природи може спричинити повну втрату або знецінення доказової бази стосовно зазначених правопорушень.

Акцентуємо увагу на тому, що без розуміння сутності та ознак цифрових слідів є неможливим ефективний пошук та збирання доказів в рамках розслідування кіберзлочинів, а також подальше проведення судових експертиз. А від цього, у свою чергу, залежить успішність

доказування у кримінальному процесі. Доводиться визнати, що на сьогоднішній день в теорії криміналістики та судової експертології фактично відсутні теоретичні і методичні основи з отримання та дослідження таких доказів, що б цілком відповідали сучасним вимогам. Існують лише розрізнені та переважно вже застарілі рекомендації. Найбільш розробленим в цій сфері можна вважати методичне забезпечення судової комп'ютерно-технічної експертизи, але й воно охоплює лише вирішення окремих завдань, що не задовольняє всі потреби вітчизняного судочинства. Також залишається не до кінця вирішеним і проблемне питання щодо коректності використання нових «технологічних» термінів у галузі судової експертизи.

Згідно з положеннями Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року № 96, одним із пріоритетних заходів для розвитку потенціалу сектору безпеки і оборони є проведення наукових досліджень у галузі кібербезпеки та кіберзахисту для потреб національної безпеки.

Досліджуваним у цій статті проблемним питанням присвячували свої праці такі науковці, як Г. К. Авдєєва, В. Ю. Агібалов, В. Д. Басай, О. Г. Волеводз, Г. Л. Грановський, Є. П. Іщенко, А. В. Касаткін, В. А. Мещеряков, Я. Найдьон, Ю. Ю. Нізовцев, О. А. Парфило, О. Р. Россинська, О. В. Ростовцев, І. А. Рядовский, А. І. Семикаленова, О. Б. Смушкін, Є. С. Хижняк, Д. М. Цехан, А. К. Шеметов, та інші.

Метою дослідження є удосконалення понятійно-категоріального апарату у сфері криміналістичного та судово-експертного забезпечення розслідування кіберзлочинів, теоретичне визначення поняття цифрових слідів, дослідження їх сутності та значення у процесі розслідування кримінальних правопорушень.

Для досягнення поставленої мети визначено такі завдання:

– дослідити сучасні наукові підходи до визначення криміналістично значимої інформації, що виникає внаслідок вчинення кіберзлочинів за допомогою інформаційно-телекомунікаційних технологій та комп'ютерної техніки;

– визначити поняття та проаналізувати специфічні ознаки і властивості цифрових слідів, що утворюються під час вчинення кіберзлочинів;

– встановити види спеціалізованих засобів для виявлення та аналізу цифрових слідів кіберзлочинів;

– проаналізувати значення цифрових слідів у процесі розслідування кіберзлочинів.

Варто зауважити, що термін «кіберзлочин» в даному дослідженні вживається не в кримінально-правовому аспекті, де це лише може ускладнити кваліфікацію діяння, а в криміналістичному, оскільки він пов'язаний не з кваліфікацією, а саме з місцем, способами та засобами вчинення правопорушення і, відповідно, з методикою його розкриття та розслідування.

У сучасних наукових джерелах використовуються різні терміни для визначення об'єктів, що мають відношення до інформаційно-

телекомунікаційних технологій: віртуальні сліди, електронні сліди, двійкові/бінарні сліди, цифрові сліди тощо. Такої ж думки дотримується й Г.К. Авдєєва, яка зазначає, що «учені дискутують не лише щодо сутності цифрових слідів злочинів, а й стосовно їх найменування (комп'ютерні сліди, віртуальні сліди, електронно-цифрові, інформаційні, комп'ютерно-технічні, електронні, цифрові сліди тощо)» [1, с. 91]. Хоча за контекстом зазвичай зрозуміло, про що саме йде мова, таке розмаїття термінів може вносити певну плутанину. Негативні наслідки такої невизначеності ще значніші при використанні вказаних термінів в офіційних документах і матеріалах практики. Спробуємо проаналізувати найчастіше вживані терміни та визначити найбільш відповідний з них.

Словосполучення «віртуальні сліди», яке нерідко використовується багатьма вченими-криміналістами [2, с. 305; 3, с. 161], на наш погляд є невдалим з точки зору семантики слів «віртуальний», «віртуальність». Досліджуючи еволюцію смислового значення поняття «віртуальна реальність», Ю. Шадських доходить висновку, що уявність, неспостережуваність, а потім і ілюзорність стають пріоритетними сенсами не лише по відношенню до віртуальних часток у фізиці, але і при застосуванні терміну «віртуальне» в таких галузях знання, як обчислювальна техніка і інформатика. Наприклад, термін «віртуальне» застосовується у словосполученнях «віртуальна пам'ять», «віртуальна машина», що інтерпретується як створення деякої ілюзії реальної машинної пам'яті або самої машини [4, с.75-76].

Якщо звернутися до словника, можна зрозуміти семантичне значення слова віртуальний. Віртуальність (від лат. virtualis – можливий, спроможний, здатний) – характеристика квазіреальності деяких об'єктів та їх властивостей, що використовується для пояснення, опису й аналізу як об'єктивно існуючих предметів, так і штучно створених сучасними інформаційними технологіями, зокрема комп'ютерною технікою [5, с. 92-93]. Або іншими словами, віртуальність – об'єкт або стан, які реально не існують, але можуть виникнути за певних умов [6, с. 395]. Ще одне джерело дає наступне визначення: віртуальність – вигаданий, уявний об'єкт, суб'єкт, категорія, ставлення, дія тощо, не присутні в цей час у реальному світі, а створені лише грою уяви людської думки, або зімітовані за допомогою інших об'єктів [7].

Отже, семантично віртуальні сліди – це сліди, які реально не існують, вигадані сліди. Але те, що не існує, не може бути досліджено слідчим, захисником, експертом чи іншими учасниками досудового розслідування та судового розгляду, а отже, не може бути визнано доказом. Тим більше не може бути доказом вигадана інформація, оскільки це суперечить вимогам ст. 84 КПК України.

Більш вдалим, на наш погляд, є термін «електронні сліди». В цьому разі доречно згадати, що споріднені терміни вже використовуються у законодавстві. Мова йде про «електронний документ», який, відповідно до чинного вітчизняного законодавства, є документом, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа [8]. Дійсно, у багатьох випадках інформація у комп'ютерних

системах зберігається, обробляється та передається саме в електронному вигляді. Але не завжди, наприклад, на дисках для оптичних систем зчитування (CD, DVD, Blu-ray тощо) чи в оптоволоконних телекомунікаційних системах для зберігання та, відповідно, передавання інформації використовуються властивості світлового потоку. Крім того, електроніка є як цифрова, так і аналогова, а отже, є значна кількість електронних пристроїв, які не є обчислювальними машинами, вони не зберігають, не оброблюють і не передають «комп'ютерну» інформацію. Іншими словами, «комп'ютерна» інформація не завжди зберігається чи передається в електронному вигляді та не кожен електронний пристрій містить «комп'ютерну» інформацію. Таким чином, вказаний термін – «електронні сліди» – також не є досконалим. Схожа ситуація стосується і «електронно-цифрових слідів», за тим винятком, що там завідомо мова не йде про аналогову електроніку.

Наступним розглянемо термін «комп'ютерні сліди» (в окремих джерелах використовується схожий термін «комп'ютерно-технічні сліди»). На перший погляд цей термін здається правильним. Адже він охоплює «комп'ютерну» інформацію як в електронному вигляді, так і в іншому (наприклад, оптичному). Але слід згадати, що комп'ютерні технології наразі набули такого розповсюдження та інтеграції у різноманітні прилади (зокрема, побутові), що нерідко важко впізнати комп'ютер у, наприклад, звичайному холодильнику. Разом з тим, ці «розумні» побутові прилади все частіше стають «жертвами» або «співучасниками» кібератак [9]. Не слід також забувати і про допоміжні вузькоспеціалізовані пристрої, які хоч і забезпечують роботу комп'ютерів та їх мереж, але за своїми можливостями не дотягують до повноцінних комп'ютерів (наприклад, маршрутизатори). Отже, якщо мова йде про «розумні» прилади, які в цілому отримали назву IoT (англ. Internet of Things – інтернет речей), або допоміжні пристрої, використання терміну «комп'ютерні сліди» є не зовсім коректним, оскільки звужує рамки до меж лише самих комп'ютерів.

Невдалим, на нашу думку, є також термін «інформаційні сліди», оскільки будь-які сліди (у тому числі, трасологічні, дактилоскопічні, балістичні тощо) містять певну інформацію і саме в цьому їх цінність для слідства. Зрозуміло, що у значній частині випадків для отримання вказаної інформації необхідним є залучення компетентної особи – судового експерта, який зможе дослідити сліди, «прочитати» приховану в них інформацію та надати її у зрозумілому для учасників розслідування вигляді. Тобто, термін «інформаційні сліди» є занадто широким та неконкретним.

Зважаючи на зазначене, найбільш вдалим, на нашу думку, є термін «цифрові сліди». Це пояснюється тим, що у всіх перелічених вище пристроях і приладах інформація зберігається, обробляється та передається саме у цифровому вигляді.

Зокрема, цифровими слідами в криміналістиці, на думку Г. К Авдєєвої, «є матеріальні невидимі сліди, які містять криміналістично-значущу інформацію (відомості, дані), зафіксовану в цифровій формі на

матеріальних носіях і можуть бути виявлені, зафіксовані й досліджені за допомогою певних цифрових пристроїв» [1, с. 91].

В цьому контексті слід звернути увагу на визначення О. Р. Россинської та І. А. Рядовского, які вважають, що «...цифровий слід являє собою криміналістично значиму комп'ютерну інформацію про події або дії, що відображені в матеріальному середовищі, в процесі її виникнення, обробки, зберігання та передачі» [10, с. 8].

В цілому погоджуючись з позицією вчених-криміналістів Г. К. Авдєєвої [1], О. Р. Россинської, І. А. Рядовского [10], О. В. Ростовцева [11], А. І. Семикаленової [12] та проаналізувавши зарубіжні англомовні наукові джерела [13; 14] вважаємо, що при формулюванні поняття цифрового сліду в криміналістиці та судовій експертизі слід виходити з таких характеристик цього явища. По-перше, це інформація, що зафіксована у цифровому вигляді, тобто у форматі, зрозумілому для електронно-обчислювальних машин.

По-друге, ця інформація міститься в різного роду цифрових пристроях зі створення, обробки, збереження та передачі цієї інформації (комп'ютерах, носіях інформації, комунікаційних системах тощо).

По-третє, цифровий слід відображає злочинну діяльність, так як причинно пов'язаний з подією кіберзлочину і дозволяє встановити як обставини вчиненого правопорушення, так і особу кіберзлочинця.

З огляду на вищенаведене пропонуємо для практичного використання в тому числі і в судово-експертній практиці наступне визначення. *Цифрові сліди, що утворюються під час вчинення кіберзлочинів – це інформація, яка зафіксована у цифровому форматі, міститься в різного роду цифрових пристроях зі створення, обробки, збереження та передачі цієї інформації, причинно пов'язана з подією кіберзлочину та дозволяє встановити як обставини вчиненого правопорушення, так і особу кіберзлочинця.*

Цифрові сліди можуть міститися у різного роду об'єктах, як то лог-файли, дампи оперативної пам'яті, дампи мережевих трафіків, інші файли або їх частини (у разі пошкодження), як наявні, так і видалені, а також службовій інформації про ці файли тощо. Вказані об'єкти зазвичай розташовуються на матеріальних носіях інформації у вигляді цифрових кодованих послідовностей або спеціально записуються (копіюються) на матеріальні носії інформації для подальшого використання у процесі доказування. Крім того, можна проаналізувати діяльність користувача ЕОМ і отримати інформацію про операції, які здійснювалися з певними файлами і програмами (встановлення, видалення, зміна), про роботу в локальній мережі або мережі Інтернет.

Доступна сприйняттю людиною така інформація тільки за допомогою використання спеціалізованих програмних і апаратних засобів, що здійснюють декодування і візуалізацію в звичній графічній, текстовій або звуковій формі. Тут важливо відзначити, що зважаючи на свою рухливість і складну структуру зберігання подібного роду дані можуть бути отримані та інтерпретовані в повному обсязі і без зміни змісту тільки з використанням спеціальних знань [12, с.116].

Звертаємо увагу, що обсяг спеціальних знань у сфері інформаційних технологій при розслідуванні кіберзлочинів є значно ширшим за обсяг «звичайних» спеціальних комп'ютерних знань, що використовуються під час досудового розслідування інших злочинів. У даному випадку ефективність пошуку, виявлення, фіксації та вилучення цифрових слідів правопорушення потребує також досконалого знання способів вчинення кіберзлочинів.

Крім теоретичних знань у сфері комп'ютерних технологій необхідні й практичні навички роботи з комп'ютерним і телекомунікаційним обладнанням, а також спеціалізованим програмним забезпеченням. Крім того необхідні знання способів та методів реалізації кібератак. Це дозволить найбільш ефективно застосовувати спеціалізовані криміналістичні програмно-апаратні засоби для пошуку, фіксації, вилучення та подальшого дослідження і зберігання цифрових слідів кіберзлочину.

До спеціалізованих засобів для виявлення та аналізу цифрових слідів кіберзлочинів можна віднести:

– експертне програмне забезпечення для криміналістичного дослідження комп'ютерних носіїв інформації, наприклад «Forensic Toolkit», «EnCase Forensic», «X-Ways Forensics», «Belkasoft Evidence Center»;

– мобільні комплекси, що дозволяють добувати, декодувати та аналізувати цифрову інформацію, отриману з мобільних пристроїв, зокрема «Cellebrite UFED Touch 2», «MSAB XRY Field», «MOBILedit Forensic Express Pro»;

– програмне забезпечення з відновлення комп'ютерних даних «R-Studio», «UFS Explorer» тощо.

Оскільки якісна робота із вказаними програмними та апаратно-програмними засобами потребує високої кваліфікації, її, зазвичай, виконує спеціаліст або судовий експерт (конкретний статус залежить від процесуальної дії, в рамках якої відбувається пошук цифрових слідів). Наведемо низку прикладів вдалих дій спеціаліста та експерта щодо виявлення цифрових слідів під час розслідування кіберзлочинів.

Сайт організації «П» перестав бути доступним для користувачів. Під час огляду серверу слідчий за допомогою спеціаліста вилучив лог-файли роботи сервера, які згодом надіслав на телекомунікаційну експертизу з метою встановлення ознак втручання в роботу вказаного серверу. Під час проведення експертизи було виявлено цифрові сліди віддаленого втручання в роботу сервера шляхом розподіленої атаки на відмову в обслуговуванні (англ. DDoS – Distributed Denial of Service) у вигляді значної кількості http-запитів від 4-х IP-адрес. Згодом шляхом проведення слідчих (розшукових) дій було встановлено власників вказаних IP-адрес, які зізналися у спланованій атаці на сайт організації «П».

Сервер підприємства «І», що працював під керуванням операційної системи Linux CentOS, був «зламаний» невідомою особою. Хоча значної шкоди від цих дій компанія не зазнала, сервер було досліджено на предмет наявності цифрових слідів, що міг залишити зловмисник. В історії команд терміналу було виявлено порядок дій зловмисника, який зміг підібрати пароль адміністратора та завантажив на сервер новітній на той час шкідливий програмний засіб, що був відсутній у всіх антивірусних базах.

Серед команд, набраних зловмисником, було виявлено адресу джерела (ресурсу) розповсюдження шкідливої програми. Дані передані відповідним правоохоронним органам, а системний адміністратор підприємства замінив пароль сервера на більш складний.

З огляду на результати аналізу наукових джерел та матеріалів судово-експертної практики спробуємо виділити специфічні ознаки та властивості цифрових слідів, зокрема:

– технологічність (така властивість формування цифрових слідів обумовлена специфікою реалізації інформаційно-телекомунікаційних технологій, оскільки для перетворення цифрових слідів в доступну для сприйняття форму також використовуються зазначені технології);

– висока швидкість трансформації (за певних умов цифрові сліди легко знищуються чи модифікуються, саме тому навіть незначне зволікання з фіксацією виявлених цифрових слідів може спричинити їх втрату);

– неможливість безпосереднього сприйняття органами чуття, а тільки за допомогою використання спеціалізованих програмних і апаратних засобів;

– здатність до відтворення та поширення (цифрові сліди можуть бути представлені практично нескінченною кількістю ідентичних копій, легко можуть бути передані через комп'ютерні мережі та бути доступними в будь-якій точці, де є підключення до мережі Інтернет);

– багатокомпонентність та складність інформаційної структури;

– можливість підтвердження контрольними числами (хеш-сумами) або іншими даними, що свідчать про їх цілісність.

Підсумовуючи вищенаведене вважаємо, що внаслідок специфічного механізму слідоутворення, пошук та виявлення цифрових слідів при проведенні огляду або обшуку потребує використання спеціальних знань (як теоретичної підготовки так і практичних навиків) у сфері інформаційно-телекомунікаційних технологій, а вилучення цифрових слідів можливе лише за допомогою спеціальних програмно-технічних засобів. Оскільки будь-які неточні маніпуляції можуть призвести до безповоротних змін в інформації, і, таким чином, до знищення цифрових слідів. Саме тому, на наш погляд, необхідно вже зараз розробляти концепцію цифрових слідів, досліджувати нові, відмінні від традиційних, способи, методи і засоби їх виявлення, фіксації, аналізу та забезпечення зберігання.

Перелік посилань

1. *Авдєєва Г. К.* Сутність цифрових слідів в криміналістиці. *Актуальні питання судової експертизи та криміналістики*: зб. матеріалів міжнар. наук.-практ. конфер., присвяч. 95-річчю створення ХНДІСЕ ім. засл. проф. М. С. Бокаріуса (Харків, 10–11 жовт. 2018 р.). Харків, 2018. С. 90-93. URL: http://dspace.nlu.edu.ua/bitstream/123456789/ 15677/1/Avdeeva_90-93.pdf

References

1. *Avdieieva, H. K.* (2018). The essence of digital prints in forensics. *Topical issues of forensic science and criminalistics*: conference proceedings of the international scientific and practical conference dedicated to the 95th anniversary of the establishment of Hon. Prof. M.S. Bokarius Kharkiv Research Institute of Forensic Examinations. Kharkiv. P. 90-93. Retrieved from http://dspace.nlu.edu.ua/bitstream/123456789/15677/1/Avdeeva_90-93.pdf. (in Ukrainian).

2. *Найдьон Я.* Поняття та класифікація віртуальних слідів кіберзлочинів. *Підприємництво,господарство і право*. 2019. № 5. С. 304-307.

3. *Хижняк Є.С.* Поняття віртуальних слідів та їх значення у процесі розслідування злочинів. *Актуальні проблеми держави і права:* зб. наук. праць. 2017. № 79. С. 159-166.

4. *Шадських Ю.* Еволюція смислового значення поняття “віртуальна реальність” *Вісник Національного університету "Львівська політехніка"*. 2012. № 723: Філософські науки. С. 73–78. URL: http://ena.lp.edu.ua:8080/bitstream/ntb/13679/1/14_73-78_Vis723Filosofiya.pdf

5. *Філософський енциклопедичний словник*: енциклопедія / НАН України, Ін-т філософії ім. Г. С. Сковороди ; голов. ред. В. І. Шинкарук. Київ: Абрис, 2002. 742 с.

6. *Рузавин Г.И.* Виртуальность. *Новая философская энциклопедия* / Ин-т философии РАН; Нац. обществ.-науч. фонд; 2-е изд., испр. и доп. Москва: Мысль, 2010. Т. 1: А-Д. 741 с.

7. *Віртуальність* / Вікіпедія. URL: https://uk.wikipedia.org/wiki/Віртуальність.

8. *Про електронні документи* та електронний документообіг: закон України 22 травня 2003 року № 851-IV. База Законодавство України». URL:https://zakon.rada.gov.ua/laws/show/851-15.

9. *Холодильник атакует:* как киберпреступники используют бытовую технику. РБК. URL: https://www.rbc.ru/technology_and_media/13/11/2 016/5825cf889a79475b671ff971.

10. *Россинская Е. Р., Рядовский И. А.* Концепция цифровых следов в криминалистике // *Аубакировские чтения*: материалы Междунар. науч.-практ. конф. (19 февраля 2019 г.). Алматы, 2019. С. 6-8.

2. *Naidon, Ya.* (2019). The concept and classification of virtual traces of cybercrime. *Entrepreneurship, economy and law*. No 5. P. 304-307. (in Ukrainian)

3. *Khyzhniak, Ye. S.* (2017). The concept of virtual traces and their significance in the process of investigation of crimes. *Topical problems of the state and law:* proceedings of papers. No 79. P. 159-166. (in Ukrainian).

4. *Shadskykh, Yu.* (2012). The evolution of the semantic meaning of the concept of “virtual reality”. *Bulletin of the National University “Lviv Polytechnic”*. No. 723: Philosophical Sciences. P. 73–78. Retrieved from http://ena.lp.edu.ua:8080/bitstream/ntb/13679/1/14_73-78_Vis723Filosofiya.pdf (in Ukrainian).

5. *Shynkaruk, V. I. (Ed.).* (2002). *Philosophical Encyclopedic Dictionary.* Encyclopedia / NAS of Ukraine, H. Skovoroda Institute of Philosophy. Kyiv: Abrys. 742 p. (in Ukrainian).

6. *Ruzavin, H. I.* (2010). Virtuality. *New Philosophical Encyclopedia*/ Institute of Philosophy of the Russian Academy of Sciences; National Social Science Foundation; 2nd edition, revised and supplemented. Moscow: Vol. 1: A-D. 741 p. (in Russian)

7. *Virtuality* / Wikipedia. *Ret*rieved from https://uk.wikipedia.org/wiki/Virtualnist (in Ukrainian).

8. *On electronic documents* and electronic document management: Law of Ukraine on May 22, 2003 No. 851-IV. Base Legislation of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/851-15 (in Ukrainian).

9. *Attacks of refrigerator*: how cybercriminals use home appliances. RBK Retrieved from https://www.rbc.ru/technology_and_media/13/11/2016/5825cf889a79475b671ff971 (in Russian).

10. *Rossynskaia, E. R., Riadovskii, Y. A.* (2019). The concept of digital traces in forensics // *Aubakirov’s readings*: materials of the International scientific and practical conference. (February 19,). Almaty. P. 6-8. (in Russian)

11. *Ростовцев А. В.* Особенности судебно-экспертного исследования «цифровых следов». *Сетевое издание «Академическая мысль»*. 2019. № 3(8). С. 71-73.

11. *Rostovtsev, A. V.* (2019). Features of a forensic study of “digital traces”. *Network publication “Academic Thought”*. No 3(8). P. 71-73. (in Russian)

12. *Семикаленова А. И.* Цифровые следы: назначение и производство экспертиз. *Вестник Университета им. О. Е. Кутафина (МГЮА)*. 2019. № 5(57). С. 115-120.

12. *Semikalenova, A. I.* (2019). Digital traces: appointment and production of examinations. *Courier of the Kutafin Moscow State Law University (MSAL).* No 5(57). P. 115-120. (in Russian)

13. *Antwi-Boasiako, Albert and Hein Venter.* (2017). A Model for Digital Evidence Admissibility Assessment. G. Peterson and S. Shenoi. (eds.). Advances in Digital Forensics P. 23-38.

13. *Antwi-Boasiako, Albert and Hein Venter.* (Eds.). (2017). A Model for Digital Evidence Admissibility Assessment. G. Peterson and S. Shenoi. Advances in Digital Forensics. P. 23-38. (in English).

14. *Whitcomb C. M.* A Historical Perspective of Digital Evidence: A Forensic Scientist’s View. *International Journal of Digital Evidence Spring*. 2002. Vol. 1, Is. 1. URL:www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

14. *Whitcomb, C. M* (2002). A Historical Perspective of Digital Evidence: A Forensic Scientist’s View. *International Journal of Digital Evidence Spring*. Vol. 1, Is. 1. Retrieved from www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf (in English).

ПОНЯТИЕ И ПРИЗНАКИ ЦИФРОВЫХ СЛЕДОВ, ОБРАЗУЮЩИХСЯ ВО ВРЕМЯ СОВЕРШЕНИЯ КИБЕРПРЕСТУПЛЕНИЙ

А. С. Омельян

В статье рассмотрены некоторые аспекты применения терминологии в области криминалистического и судебно-экспертного обеспечения расследования киберпреступлений.

С учетом специфики использования информационно-телекоммуникационных технологий, обоснована целесообразность употребления термина «цифровые следы» в судебной экспертизе.

Предложено авторское определение понятия цифровых следов, которые образуются во время совершения киберпреступлений, приведены и проанализированы их специфические признаки и свойства. Отмечена необходимость использования специальных знаний и соответствующего экспертного оборудования для поиска, обнаружения и фиксации цифровых следов. Подчеркнуто значение оперативности обнаружения и исследования цифровых следов в процессе расследования киберпреступлений. Обоснована необходимость разработки концепции цифровых следов, исследования новых, отличных от традиционных, способов, методов и средств их обнаружения, фиксации, анализа и обеспечения сохранности.

Ключевые слова: цифровые следы, киберпреступления, информационно-телекоммуникационные технологии, специальные знания, судебная экспертиза.

CONCEPT AND SIGNS OF DIGITAL TRACES THAT FORM DURING CYBERCRIMES

O. Omelian

The article considers scientific views on terminology in the field of forensics and forensic examination for the investigation of cybercrime, as well as taking into account the specific use of information and telecommunication technologies in forensics, the validity of the term's use "digital traces" is substantiated.

The author's definition of the concept of digital traces that are formed during the commission of cybercrimes is proposed. Its specific signs and properties are presented and analyzed as well. The necessity of using special knowledge and appropriate expert equipment to search for, detect and record digital tracks has been noted. It is emphasized the importance of the speed of detection and investigation of digital traces in the process of investigating cybercrimes. The necessity of developing the concept of digital tracks, research of new, different from traditional methods, methods and means of their detection, fixation, analysis and preservation is substantiated.

***Key words**:* digital traces, cybercrime, information and telecommunication technologies, special knowledge, forensic examination.