Технічні науки

УДК 004.02

Пилипенко Олександр Вадимович

судовий експерт

Харківський науково-дослідний експертно-криміналістичний центр

Міністерства внутрішніх справ України

Пилипенко Александр Вадимович

судебный эксперт

Харьковский научно-исследовательский

экспертно-криминалистический центр

Министерства внутренних дел Украины

Pilipenko Oleksandr

Forensic Expert

Kharkiv Scientific Research Forensic Center of the

Ministry of Internal Affairs of Ukraine

МЕТОДИ ФІКСАЦІЇ ІНФОРМАЦІЇ ВЕБ-САЙТІВ, ЯКІ МОЖУТЬ БУТИ ВИКОРИСТАНІ В КОМП'ЮТЕРНО-ТЕХНІЧНІЙ ЕКСПЕРТИЗІ

МЕТОДЫ ФИКСАЦИИ ИНФОРМАЦИИ ВЕБ-САЙТОВ, КОТОРЫЕ МОГУТ БЫТЬ ИСПОЛЬЗОВАНЫ В КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЕ

METHODS OF RECORDING WEBSITE INFORMATION THAT MAY BE USED IN COMPUTER EXAMINATION

Анотація. *В статті розглянуто поняття веб-сайту, чому саме проблема фіксації інформації веб-сайтів тісно пов'язана з важливими завданнями комп'ютерно-технічної експертизи, а також візуальні та технологічні методи фіксації інформації веб-ресурсів.*

Ключові слова: *сайт, ресурс, методи, дослідження, візуальні, технологічні, скріншот, роздрукування, відеозапис, архів, веб-архів, лог-файл, журналювання, веб-сайт, веб-ресурс.*

Аннотация. *В статье рассмотрено понятие веб-сайта, почему именно проблема фиксации информации веб-сайтов тесно связана с важными заданиями компьютерно-технической экспертизы, а также визуальные и технологические методы фиксации информации веб-ресурсов.*

Ключевые слова: *сайт, ресурс, методы, исследование, визуальные, технологические, скриншот, распечатка, видеозапись, архив, веб-архив, лог-файл, журналирование, веб-сайт, веб-ресурс.*

Summary. *The article deals with the concept of the website, why the problem of fixing information of websites is very closely related to the important tasks of computer-aided technical examination, as well as the visual and technological methods of fixing information of web-resources.*

Key words: *site, resource, methods, research, visual, technological, screenshot, print, video, archive, web archive, log file, journaling, website, web resource.*

Особливістю сучасного періоду розвитку суспільства є інформатизація у всіх сферах людської діяльності. Стрімкий розвиток і вдосконалення інформаційних технологій постійно породжує нові способи вчинення і приховування злочинів. Одне із завдань правоохоронних органів є протидія тероризму, корупції та кіберзлочинності. Інформаційні системи все частіше стають не тільки об'єктом злочинного зазіхання, але і самі використовуються як знаряддя скоєння різноманітних злочинів, залишаючи при цьому своєрідні «інформаційні» сліди, які необхідно досліджувати. Подібні дослідження вимагають спеціальних інженерних

знань в області комп'ютерних систем та комп'ютерної інформації та проводяться в рамках судової комп'ютерно-технічної експертизи.

Судова комп'ютерно-технічна експертиза - самостійний рід експертиз, об'єктами дослідження якої є цифрові носії інформації, комп'ютерна техніка, мобільні телефони, смартфони, планшетні ПК та цифрові носії інформації в них, відеореєстратори, файли баз даних, текстові документи, таблиці, графічні та відеофайли, інформаційне наповнення веб-сайтів в мережі Інтернет. Проводиться по цивільних та кримінальних справах з метою виявлення і вивчення його ролі в розслідуваному злочині, а також отримання доступу до інформації з подальшим всебічним її дослідженням.

Здебільшого об'єктами експертизи є знаряддя вчинення злочинів, наприклад, виготовлення фальшивих грошей, фіктивних документів, розповсюдження конфіденціальної інформації, забороненого контенту тощо. Проте, будь-який носій цифрової інформації може бути місцем зберігання або приховування інформації, яка може бути цікава слідству.

Швидка інформатизація породила новий вид діянь, які несуть в собі суспільно-небезпечний характер, коли цифрова інформація використовується в якості об'єкта посягання або неправомірно використовується злочинцями. На жаль не всі талановиті люди займаються законною діяльністю, постійно з'являються люди, які свої знання та талант використовують для створення нових унікальних способів вчинення злочинів, це не обходить стороною і галузь інформаційних технологій. Глобальна мережа Інтернет надає великі можливості в якості розвитку як прогресу, так і злочинності.

В даній статті мова піде про різноманітні методи фіксації інформації веб-сайтів, візуальні та технологічні, які можуть бути використані в комп'ютерно-технічній експертизі. Будуть розглянуті методи за допомогою знімків екрану (скріншотів), збереження та/або роздрукування веб-

сторінок, відеозапис вмісту веб-сторінок, огляд судом за місцезнаходженням доказів, огляд веб-ресурсу адвокатом, фіксація веб-сторінок за допомогою онлайн ресурсів та отримання файлів журналювання дій користувача від інтернет провайдерів.

Веб-сайт представляє собою набір цифрової інформації (сукупність веб-сторінок), до якої здійснюється доступ через мережу Інтернет. Ця інформація зберігається на одному або декількох серверах. Тут з'являється проблема в вилученні серверів органом досудових розслідувань, тому що сервери взагалі можуть бути розташовані в інших країнах.

Слід звернути увагу, оскільки під об'єктом дослідження інформації на цифрових носіях розуміють матеріальні об'єкти (носії інформації) існує проблема зарахування до можливих об'єктів судової комп'ютерно-технічної експертизи віддалених об'єктів, що не знаходяться в повному розпорядженні експерта, наприклад, комп'ютерні мережі та веб-сайти.

Під загальною характеристикою злочинів, скоєних за допомогою мережі інтернет, слід розуміти протиправні соціально небезпечні діяння, які здійснюються в мережі інтернет, або за допомогою мережі інтернет. Злочинці в глобальній мережі можуть розповсюджувати шкідливе програмне забезпечення та влаштовувати DDoS атаки на сервера різноманітних компаній, тим самим гальмувати або навіть зупинити роботу компанії, що, звичайно, буде приносити останній великі збитки. Також злочинці можуть вимагати у компанії гроші, під приводом припинення таких атак.

Для інтернет злочинів характерною є ситуація, коли одна частина дій, які відносяться до об'єктивної сторони злочину, була здійснена на території однієї країни, а інша – на території іншої країни. Як приклад таких шахрайських дій можуть бути шахрайські дії, скоєні шляхом виставлення рахунків за ненадані послуги.

Злочинність в мережі інтернет та за допомогою мережі інтернет відносять до злочинності у сфері інформаційних технологій та включають в себе розповсюдження шкідливого програмного забезпечення, крадіжку персональних даних, наприклад, банківських карт та банківських реквізитів, а також розповсюдження через мережу інтернет протиправної інформації (матеріали порнографічного характеру, завідомо неправдиві вигадки, що ганьблять іншу особу, матеріали, що збуджують міжрелігійну та міжнаціональну ворожнечу).

Приводом для написання даної статті посприяв стрімкий розвиток злочинності в мережі інтернет, з кожним роком все більше осіб звертаються до правозахисних органів за допомогою в цьому питанні. Це свідчить про актуальність теми даної статті. Метою даної статті є розгляд існуючих методів фіксації веб-сайтів та методів, які можуть бути використані в комп'ютерно-технічній експертизі.

Виявлення інформації, що міститься на комп'ютерних носіях та установлення обставин, пов'язаних з використанням комп'ютерно-технічних засобів та інформації є одними з важливих завдань комп'ютерно-технічної експертизи. Оскільки будь-який веб-сайт створюється та зберігається на цифрових носіях інформації, проблема фіксації інформації веб-сайтів дуже тісно пов'язана з важливими завданнями комп'ютерно-технічної експертизи.

Отже методи фіксації веб-сайтів можна розглядати як візуальні та технологічні. У випадку візуальних методів – фіксується зображення, яке виводиться на екран монітора або пристрою, з якого проводиться візуальний огляд. До технологічних методів відноситься безпосередньо технічні аспекти функціонування веб-сайту.

Існує декілька візуальних методів фіксації:

1) За допомогою створення знімків екрану (скріншотів);
2) Збереження та/або роздрукування веб-сторінки;

3) Відеозапис вмісту веб-сторінки;

Під технологічними методами фіксації розуміють:

1) Фіксація веб-сторінок за допомогою онлайн-ресурсів;
2) Файли, отримані від провайдерів;

Візуальні методи фіксації веб-сайтів

1) Знімок екрану (скріншот) – зображення, отримане комп'ютером, телефоном, планшетним ПК, що зображує те, що бачить користувач на екрані.

На нормативному рівні електронні докази отримали правове закріплення нещодавно, проте застосовуються вже доволі часто. Так, наприклад, в рішенні Косівського районного суду Івано-Франківської області у справі № 347/1491/19 від 01 жовтня 2019 року вказується [1, рішення № 84638382], що відповідач подав декларацію особи уповноваженої на виконання функцій держави або місцевого самоврядування за 2017 рік 01 лютого 2019 року, хоча граничною датою подання ним вищевказаної декларації є 31 березня 2018 року. Витяг з Єдиного Державного реєстру декларацій щодо інформації відносно відповідача був наданий суду у вигляді скріншоту.

Також, наприклад, в ухвалі Кіровоградського окружного адміністративного суду у справі № 340/2141/19 від 20 вересня 2019 року вказується [1, рішення № 84562391] на надання до суду відповідачем (Петрівську сільську раду Знам`янського району Кіровоградської області) належним чином засвідчену інформацію про дату створення файлу розпорядження про звільнення позивача зі службового комп'ютера секретаря або голови Петрівської сільської ради Знам`янського району Кіровоградської області у вигляді скріншоту.

Як один з прикладів не прийняття скріншоту як належного доказу є постанова Ставищенського районного суду Київської області у провадженні № 3/378/302/19 від 16 вересня 2019 року, в якій вказується

[1, рішення № 84266753], що доданий до матеріалів справи скріншот з результатами пошуку Єдиного державного реєстру декларацій належним чином не завірений, у вказаному витязі не вказано, якою посадовою особою він завірений, та підпис вказаної особи не скріплено печаткою установи.

2) Збереження та/або роздрукування веб-сторінки. Відповідно до п. 46 Постанови Пленуму Вищого Господарського Суду України від 17.10.2018р. №12 [2], роздруківки веб-сторінок самі по собі не можуть бути доказом у справі, але якщо відповідні документи видані або засвідчені закладом або спеціально уповноваженою особою в межах їх компетенції за встановленою формою і скріплені офіційною печаткою на території однієї з держав-учасниць Співдружності Незалежних Держав, то згідно із статтею 6 Угоди про порядок вирішення спорів, пов'язаних із здійсненням господарської діяльності від 20.03.1992 вони мають на території України доказову силу офіційних документів.

Збереження веб-сторінки досить спірний метод. Сучасні веб-сторінки складаються з великої кількості елементів, таких як зображення, файлів конфігурації зовнішнього вигляду сторінок (Cascading Style Sheets, CSS), файлів сценаріїв (файлів JavaScript). У комплексі всі ці файли впливають на остаточну структуру та зовнішній вигляд веб-сторінки. Інколи деякі файли не зберігаються при використанні браузером повного збереження веб сторінки, через особливості "підключення" цих файлів. В результаті, при подальшому відкритті збереженого файлу сторінки, він буде виглядати зовсім по іншому.

3) Відеозапис вмісту веб-сторінки. Відповідно до п. 46 Постанови Пленуму Вищого Господарського Суду України від 17.10.2018р. №12 [2], як засіб доказування може бути використаний відеозапис процесу дослідження будь-якою заінтересованою особою веб-сайту, стосовно якого є відомості використання його з порушенням авторських чи суміжних

прав; такий запис, здійснений на цифровому носії інформації, подається до суду із зазначенням того, коли, ким і за яких умов цей запис здійснено і може бути речовим доказом у справі.

Технологічні методи фіксації веб-сайтів

1) Фіксація веб-сторінок за допомогою онлайн-ресурсів. Цей метод досить суперечливий, тому що фіксуються не сторінки вихідного сайту, а сторінки онлайн ресурсу, який зберігає кешовану копію сторінок вихідного сайту. Це створено для більш швидкого доступу до інформації, яка міститься на вихідному веб-сайті.

Один з прикладів таких онлайн ресурсів, які зберігають кешовані копії веб-сайтів, це пошукові системи. Пошукові системи використовують індексування сторінок веб-сайтів, тобто збирають, сортують та зберігають дані з метою швидкого та точного пошуку інформації. Для пошуку необхідної сторінки в пошуковій системі треба виконати пошук по URL адресі вихідного веб-сайту, далі відкрити контекстне меню та обрати «Кеш» (див. рис. 1).

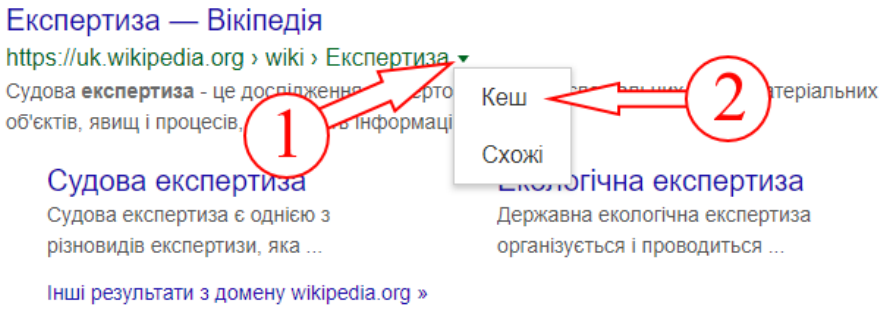

Рис. 1. Спосіб відкриття кешованої копії веб-сторінки

[3, запит «Експертиза»]

Пошукові системи зберігають вихідний код сторінки, адресу сторінки та час фіксації сторінки вихідного сайту (див. рис. 2). Проте зберігається лише остання копія веб-сайту, тобто копія, яка була зроблена пошуковим роботом під час останнього відвідування.

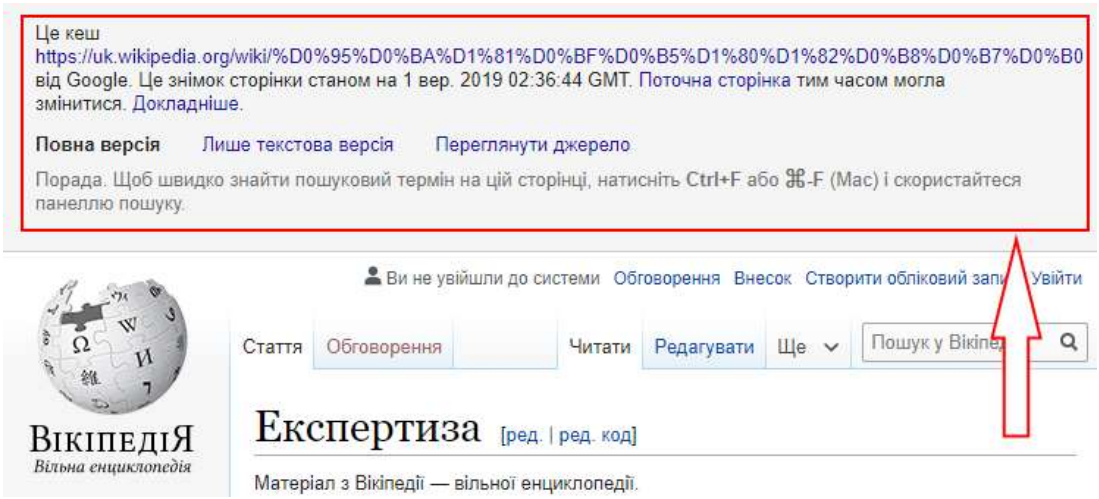

Рис. 2. Інформація про кешування веб-сторінки в пошуковій системі Google [4]

Також не завжди пошуковий робот відвідує всі сторінки веб сайту, на якісь він заходить частіше, на якісь рідше, а якісь зовсім не відвідує. Це обумовлено популярністю веб-сайту, його внутрішньою сіткою посилань та частотою оновлення інформації. Тому важливо враховувати, якщо інформація з веб-сайту була видалена, то вона ще може зберігатись у вигляді кешованої копії у пошукових системах.

Також одним з прикладів онлайн ресурсів, що зберігають копії сторінок веб-сайтів, можна відмітити ресурс Internet Archive WayBackMachine. WayBackMachine це унікальний безкоштовний не комерційний сервіс створений у 1996 році, який займається архівуванням веб-ресурсів. Містить в собі копії сторінок веб-сайтів у різні проміжки часу, наприклад, на Рис. 3 показано, як виглядав веб-сайт Міністерства Внутрішніх Справ України 14 лютого 2012 року. Також портал Internet Archive зберігає програмне забезпечення та мультимедійні дані, що містились на копійованому ресурсі.

Рис. 3. Вигляд веб-сайту МВС України 14 лютого 2012 р., відображений за допомогою сервісу WayBackMachine [5, запит «mvs.gov.ua», дата 14.02.2012]

Цей портал зберігає копії сторінок як в автоматичному режимі, так і на запит користувача. Веб архів з 2007 року входить до складу Американської бібліотечної асоціації, що підтримує розвиток бібліотек, та офіційно визнана бібліотекою в штаті Каліфорнія.

2) Журнали хостингу, тобто файли с записами про події в хронологічному порядку (log файли), отримані від провайдерів. В цих файлах може зберігатись інформація про розміщену користувачем інформацію на веб-ресурсі, в залежності від налаштувань хостингу. В цьому методі є суттєвий недолік, в журналах хостингу фіксується тільки назва завантаженого файлу, а не його зміст.

Подальше збільшення користувачів мережі інтернет збільшує кількість потенціальних злочинців в мережі, тому це зазвичай впливає на кількість ошуканих осіб та впливає на кількість досліджень веб-сайтів, або окремих сторінок сайтів, в комп'ютерно-технічній експертизі. В статті

розглянуто візуальні та технологічні методи фіксації веб-ресурсів, це дозволяє зробити висновок, що аналіз проблемних технічних та юридичних питань, які виникають в процесі дослідження веб-ресурсів, допоможуть в реалізації створення та вдосконалення методичних рекомендацій щодо дослідження веб-ресурсів в комп'ютерно-технічній криміналістиці.

Література

1. Єдиний державний реєстр судових рішень. URL: http://reyestr.court.gov.ua/ (дата звернення: 16.10.2019).
2. Постанова Пленуму Вищого Господарського Суду України від 17.10.2012р. №12. URL: https://zakon.rada.gov.ua/laws/show/v0012600-12 (дата звернення: 16.10.2019).
3. Пошукова система компанії Google Inc. URL: https://www.google.com.ua/ (дата звернення: 16.10.2019).
4. Збережена кешована копія інтернет сторінки https://uk.wikipedia.org/wiki/Експертиза в пошуковій системі Google. URL: https://webcache.googleusercontent.com/search?q=cache:bTlWXDFtYWcJ:https://uk.wikipedia.org/wiki/Експертиза+&cd=2&hl=ru&ct=clnk&gl=ua (дата звернення 16.10.2019).
5. Інтернет архів WayBackMachine. URL: http://web.archive.org/ (дата звернення 16.10.2019).