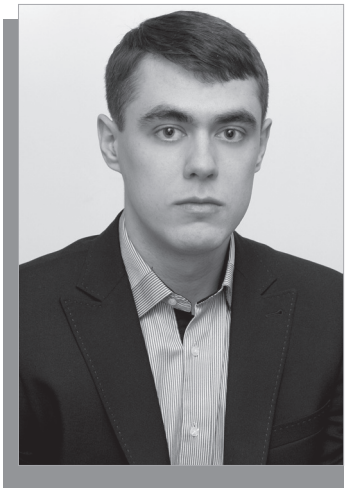
КОВАЛЕНКО АРТЕМ ВОЛОДИМИРОВИЧ,
аспірант кафедри криміналістики та судової експертології Харківського національного університету внутрішніх справ, Україна, м. Харків
e-mail: new4or@gmail.com
ORCID orcid.org/0000-0003-3665-0147



УДК 343.98

Особливості тактики огляду електронних документів під час досудового розслідування посягань на життя та здоров'я журналіста

Досліджено особливості тактики огляду електронних документів під час розслідування посягань на життя та здоров'я журналіста. Наведені загальні рекомендації щодо здійснення огляду електронних документів. Висвітлено особливості огляду електронних документів, що розміщені на фізичних носіях інформації, у мережі Інтернет (зокрема, інтернет-публікацій журналіста), а також у сервісах хмарного зберігання інформації. Запропоновано орієнтовний перелік атрибутів таких документів, описано специфіку фіксації результатів їх огляду.

Ключові слова: огляд, електронний документ, журналіст, фізичний носій інформації, мережа Інтернет, сервіс хмарного зберігання інформації.

Постановка проблеми. Відомості про характер, напрями та об'єкти здійснення професійної журналістської діяльності потерпілим від посягань на життя та здоров'я журналіста є одним із найважливіших джерел отримання доказової інформації під час розслідування даних злочинів. Вивчення публікацій, чернеток, робочих записів журналіста тощо дозволяє встановити осіб, які могли бути зацікавлені у посяганні з метою впливу на його професійну діяльність.

Із розвитком комп'ютерної техніки та інформаційних технологій представники журналістської професії все частіше вдаються до зберігання робочої інформації в електронному вигляді.

З метою найбільш ефективного провадження практичними працівниками огляду та попереднього дослідження електронних документів, що містять таку інформацію, зазначена слідча (розшукова) дія потребує додаткового наукового осмислення. За проміжними результатами проведеного нами анкетування слідчих Національної поліції України, 53,8% респондентів визнали огляд електронних документів найскладнішою слідчою (розшуковою) дією, що провадиться в рамках розслідування посягань на життя та здоров'я журналіста.

Аналіз останніх досліджень і публікацій. Тактиці огляду документів увагу в своїх працях присвячували В. І. Алєксєйчук, Р. С. Бєлкін, А. Г. Волеводз, А. Ф. Волобуєв, В. А. Журавель, Н. І. Клименко, В. О. Коновалова, О. В. Одерій, В. Ю. Шепітько та ін. Питання правового та процесуального статусу, а також криміналістичної значущості електронних документів досліджували А. П. Вершинін, Т. Е. Кукарнікова, К. А. Сергєєва, С. П. Сереброва та ін. Втім особливості тактики огляду електронних документів під час розслідування посягань на життя та здоров'я журналіста на сьогодні не були висвітлені в науковій літературі та лишаються недостатньо розробленими на практиці.

Метою даної статті є дослідження особливостей тактики огляду електронних документів під час розслідування посягань на життя та здоров'я журналіста та надання практичних рекомендації щодо здійснення даної слідчої (розшукової) дії.

Виклад основного матеріалу. Огляд як слідча (розшукова) дія є досить ретельно вивченою вітчизняними та зарубіжними вченими-криміналістами. Наведені в науковій літературі визначення огляду в більшості випадків виокремлюють такі його ознаки: це слідча (розшукова) дія, що полягає у безпосередньому сприйнятті слідчим, прокурором об'єктів з метою виявлення та фіксації відомостей щодо обставин вчинення кримінального правопорушення, а також слідів злочину та інших речових доказів [1, с. 275; 2, с. 272].

Щодо електронного документа, то на сьогодні науковцями ще не було вироблено єдиного визначення даного поняття. Наприклад, Т. Е. Кукарнікова електронний документ як джерело судових доказів визначає як об'єкт, що несе інформацію, яка має значення для встановлення обставин, що підлягають доказуванню у кримінальному провадженні, та існує тільки в електронному середовищі у вигляді, допустимому для використання у кримінальному провадженні [3, с. 17]. На думку К. А. Сергєєвої, електронний документ – це матеріальний носій, на якому за допомогою електронних апаратно-технічних і програмних засобів зафіксована інформація, яка має змістове значення, що засвідчує будь-який факт або подію, що підтверджує право на що-небудь; яка може бути перетворена у форму, придатну для однозначного сприйняття людиною, та має атрибути для ідентифікації [4, с. 1486].

Деякі автори [1, с. 159; 4, с. 1486; 5, с. 40] погоджуються з думкою про те, що електронний документ пов'язується

з матеріальним об'єктом – носієм електронної інформації, який містить інформацію, що має значення для кримінального провадження. Зазначена позиція кореспондує з положенням КПК України, за частинами 1, 2 ст. 99 якого документом є спеціально створений з метою збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження, а документами можуть бути носії інформації (у тому числі електронні).

Одночасно з цим ч. 3 ст. 99 КПК України визнає оригіналом електронного документа, що має бути надано суду, його відображення, якому надається таке ж значення, як документу. Зазначена норма дозволяє використовувати в кримінальному проваджені як докази електронні документи без безпосереднього задіяння фізичних носіїв інформації, якщо відображення такого документа було створене в порядку, передбаченому кримінальним процесуальним законодавством України. Відповідно, відкриваються можливості сторін кримінального провадження використовувати як докази електронні документи, матеріальними носіями яких є частини складних та важкодоступних електронних інформаційних систем (наприклад, жорсткий диск сервера, на якому розміщено веб-сторінку, може знаходитися у будь-якій точці світу).

Виходячи з особливостей огляду та попереднього дослідження електронних документів, з якими слідчий найчастіше має справу в процесі розслідування посягань на життя та здоров'я журналіста, пропонуємо їх групувати за такими категоріями: 1) електронні документи на фізичних носіях інформації; 2) електронні документи у вигляді публікацій у мережі Інтернет; 3) електронні документи, розміщені у хмарних сервісах зберігання інформації.

Вважаємо за доцільне навести деякі загальні рекомендації з провадження огляду електронних документів, перш ніж докладно розглянути особливості тактики огляду кожного з наведених різновидів зазначених об'єктів.

Так, С. П. Сереброва рекомендує провадження слідчих (розшукових) дій, що пов'язані з оглядом та вилученням комп'ютерної інформації, проводити за участю спеціаліста [6, с. 7]. Такої ж позиції дотримуються Т. Е. Кукарнікова [3, с. 19], О. В. Одерій та співавтори [7, с. 8] тощо.

Будь-які дії з електронними документами мають здійснюватися уповноваженими особами за допомогою сертифікованого службового обладнання, з використанням ліцензійного програмного забезпечення. Використання несертифікованого обладнання або неліцензійного програмного забезпечення може призвести до викривлення інформації, отриманої з електронного документа через апаратні та/або програмні збої та помилки.

У протоколі огляду електронного документа в обов'язковому порядку мають зазначатися технічні характеристики та серійні номери обладнання, назви та версії програмного забезпечення, що використовуються в ході даної слідчої (розшукової) дії. Також мають бути вивчені та відображені в протоколі усі

реквізити електронного документа, орієнтовний перелік яких буде наведений нами у даній статті для кожного різновиду електронних документів, що розглядаються.

Огляд електронних документів на фізичних носіях інформації. Такими носіями можуть виступати: 1) зовнішні фізичні носії пам'яті електронно-обчислювальної машини (жорсткий диск – HDD, SDD; дискові носії – CD, DVD, Blue-Ray-диски, дискети; USB-диски); 2) оперативний запам'ятовуючий пристрій ЕОМ (скорочено ОЗП); 3) ОЗП периферійних пристроїв (наприклад, принтер, у пам'яті якого знаходяться документи у «черзі друку»); 4) ОЗП пристроїв зв'язку тощо [8, с. 149–150]. На наш погляд, до даного переліку доцільно додати флеш-карти пам'яті (SD, micro SD тощо), які на сьогодні активно використовуються у портативній техніці.

Окремо слід звернути увагу на огляд електронних документів, розташованих у пам'яті мобільних пристроїв. Сучасні мобільні телефони й смартфони оснащені функцією запису звуку (диктофон) та запису розмови, за допомогою яких журналістами створюються аудіозаписи, які можуть містити відомості, що мають значення для кримінального провадження. Крім того, за допомогою мобільного пристрою журналістом можуть створюватися фото- та відеозаписи в ході здійснення професійної журналістської діяльності, які також потребують огляду та попереднього дослідження. Зазначена позиція підтверджується статистичними даними: за проміжними результатами проведеного нами анкетування журналістів, 94,4% респондентів використовують мобільні пристрої зв'язку (мобільні телефони, смартфони, планшети тощо) при здійсненні професійної журналістської діяльності.

Як і інші докази, електронні документи на фізичних носіях відповідно до ч. 2 ст. 93 КПК України можуть бути зібрані стороною обвинувачення в результаті проведення слідчих (розшукових) дій (огляд, обшук), негласних слідчих (розшукових) дій, шляхом витребування чи отримування їх від органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, службових та фізичних осіб, а також шляхом проведення інших процесуальних дій, передбачених кримінальним процесуальним законодавством. Так, фізичні носії електронної інформації, на яких може знаходитися інформація, що має значення для кримінального провадження, вилучаються при огляді місця події, оглядах та обшуках житла чи робочого приміщення журналіста, при огляді його речей та комп'ютерної техніки.

При тимчасовому доступі до речей та документів такі носії інформації можуть бути оглянуті, їх вміст може бути скопійовано, а у випадках, коли сторона кримінального провадження доведе наявність достатніх підстав, вони можуть бути вилучені. Такі підстави закріплені п. 7 ст. 163 КПК України, де, зокрема, йдеться про випадки, коли без вилучення об'єктів тимчасового доступу існує реальна загроза зміни або знищення таких речей чи документів, або таке вилучення необхідне для досягнення мети отримання доступу до речей і документів.

На наш погляд, огляд та попереднє дослідження електронних документів у більшості випадків потребують вилучення фізичних носіїв інформації, на яких такі документи розміщено. Втім не можна не погодитися з думкою науковців про те, що у випадках, коли вилучення носія інформації може унеможливити подальшу законну діяльність підприємства, організації, більш доцільним є створення побайтової копії такого носія інформації (створення його образу) за допомогою спеціального програмного забезпечення [7, с. 38]. Очевидно, таке копіювання, так само як і вилучення носіїв інформації, що є структурною частиною електронно-обчислювальних машин (наприклад, HDD-дисків), потребує допомоги спеціаліста.

На підготовчому етапі огляду електронних документів, розміщених на фізичному носії інформації, слідчому, прокурору рекомендується з'ясувати, якого типу фізичний носій інформації містить документи, що підлягають огляду та, відповідно, яке обладнання потрібне для роботи з таким носієм. Якщо носій захищено будь-яким типом захисту від зчитування чи копіювання, слід призначити судову експертизу комп'ютерної техніки і програмних продуктів та поставити перед експертом питання про можливість отримання доступу до вмісту такого носія, файлів, що розміщені на носії та їх атрибутів. За допомогою такої експертизи також можливо встановити технологію та хронологію створення конкретного електронного документа [9].

Основними атрибутами таких документів є їх формат, технологія та хронологія створення, користувач, яким документ було створено, каталог розміщення документа на носії, зміст документа тощо. У випадках фотознімків можливе з'ясування місця створення фотознімку (gps координати), якщо така опція була активована у камері. Зазвичай, уся зазначена інформація про електронний документ може бути отримана штатними засобами за участю спеціаліста. У менш сприятливих ситуаціях для з'ясування такої інформації доцільно призначати судову експертизу комп'ютерної техніки і програмних продуктів.

Огляд електронних документів, розміщених на фізичному носії інформації, здійснюється шляхом безпосереднього сприйняття слідчим інформації, що міститься в електронному документі, за допомогою службового комп'ютера. Аудіо- та відеофайли відтворюються з використанням відповідного комп'ютерного обладнання та програмного забезпечення.

На завершальному етапі огляду електронних документів, розміщених на фізичному носії інформації, такі документи роздруковуються або копіюються на диск та додаються до протоколу як його невід'ємний додаток, із зазначенням серійних номерів та технічних характеристик обладнання, за допомогою якого створено такий додаток.

Огляд публікацій у мережі Інтернет. Із метою встановлення напрямів та об'єктів здійснення журналістом його професійної журналістської діяльності доцільно вивчити його публікації за деякий період часу. Із розвитком Інтернету все більше ЗМІ починають діяти у всесвітній павутині, традиційні ЗМІ

дублюють свої матеріали у мережі та публікують на своїх інтернет-сайтах ексклюзивні матеріали. У зв'язку з цим виникає потреба в розробленні практичних рекомендацій з тактики здійснення слідчого огляду електронних документів, розміщених у мережі Інтернет у відкритому доступі, зокрема, інтернет-публікацій журналіста.

Слідчим рекомендується здійснювати зазначений тип огляду у службовому кабінеті з використанням службового комп'ютера, на якому встановлено ліцензійне програмне забезпечення та організовано доступ до мережі Інтернет. Якщо навички слідчого, пов'язані з роботою у мережі Інтернет, є недостатніми, рекомендується залучення спеціаліста.

У протоколі огляду слід зазначити серійний номер службового комп'ютера, назву та версію операційної системи, якою керується даний комп'ютер, назву та версію програми-браузера, за допомогою якої здійснюється доступ до мережі Інтернет.

Огляд здійснюється шляхом безпосереднього сприйняття слідчим інформації, розміщеної на веб-сторінці за допомогою службового комп'ютера з доступом до мережі Інтернет. Веб-сторінка має бути масштабована у браузері на повний розмір (100%). У браузері мають бути відключені усі додатки та надбудови, що можуть змінити вигляд вебсторінки, яка оглядається.

Основними реквізитами такого електронного документа можуть бути адреса у мережі Інтернет, на якій розміщено веб-сторінку; назва веб-сайту, категорія чи жанр публікації, якщо вони зазначені на веб-сторінці; назва публікації; основний текст публікації; прикріплені зображення та аудіо- чи відеофайли; відомості про автора публікації (якщо публікація не є анонімною). Як і у випадку огляду традиційних документів, усі зазначені реквізити мають бути зафіксовані у протоколі огляду.

Зокрема, у протоколі огляду обов'язково має бути зазначено адресу вебсторінки, яка оглядалася. Відображенню у протоколі підлягають заголовок журналістської публікації, локалізація публікації в межах сторінки; має бути наведено скорочений виклад основного тексту, перелічено фізичних та юридичних осіб, установи та організації, що згадуються у публікації, а також прізвище, ім'я та по батькові або псевдонім автора публікації.

Крім того, у протоколі має бути перелічено та коротко описано фото-, відео та аудіофайли, прикріплені до публікації, із зазначенням посилання на кожний із таких файлів у мережі Інтернет. Слідчому слід пам'ятати, що значна кількість мультимедійних файлів на сучасних веб-сторінках є рекламними оголошеннями, які не стосуються публікації, що вивчається. Такі елементи вебсторінки не потрібно описувати у протоколі огляду електронного документа.

Більшість інтернет-сайтів дозволяють користувачам коментувати опубліковані матеріали шляхом розміщення повідомлень на відповідній сторінці. Виходячи з цього, рекомендуємо практичним працівникам досліджувати зміст та час публікації таких коментарів, з метою виявлення погроз чи інших проявів агресії на адресу автора матеріалу, які можуть свідчити про намір коментатора заподіяти такому журналісту шкоду.

Веб-сторінку, що оглядається, необхідно роздрукувати за допомогою службового принтера та додати до протоколу огляду як невід'ємний додаток, із зазначенням серійного номера, назви та моделі принтера. Фото-, відео- та аудіофайли, що є частиною публікації, мають бути збережені та записані на диск, який стане другим додатком до протоколу огляду. Альтернативним засобом фіксації веб-сторінки є збереження її у форматі html засобами програми-браузера, з подальшим записом такого файла на диск.

Огляд електронних документів, розміщених у хмарних сервісах зберігання інформації. За визначенням Національного інституту стандартів і технологій США (National Institute of Standards and Technology (NIST)), хмарні обчислення – це модель забезпечення повсюдного, зручного мережевого доступу за вимогою до спільного пулу обчислювальних ресурсів, що підлягають налаштуванню (наприклад, до комунікаційних мереж, серверів, засобів зберігання даних, прикладних програм та сервісів), які можуть бути оперативно використані з мінімальними управлінськими витратами та зверненнями до провайдера послуг [10].

Хмарні сервіси зберігання інформації набувають усе більшої популярності серед представників різних професій, у тому числі серед журналістів. Так, В. Л. Рябічев підкреслює, що використання хмарних сервісів забезпечує миттєвий доступ до даних та додатків користувача з будь-якого місця земної кулі в будь-який час, однак лише за наявності Всесвітньої павутини. Такий підхід дозволяє оптимізувати і прискорити роботу, зменшити витрати та залучити широке коло виконавців і експертів, у тому числі й у сфері журналістики [11, с. 99]. За проміжними результатами проведеного нами анкетування журналістів, 51,4% респондентів використовують хмарні сервіси для зберігання робочої інформації, що підтверджує актуальність дослідження електронних документів у таких сховищах.

Серед популярних сервісів хмарного зберігання даних можна назвати український eDisk Ukr.net, американські GoogleDrive, DropBox, російські Яндекс Диск, Диск Mail.ru тощо.

У хмарних сервісах зберігання інформації можуть міститися робочі матеріали журналіста – чорнові варіанти публікацій, фото-, відео- та аудіоматеріали, створені журналістом у ході здійснення професійної журналістської діяльності; особисті записи, плани роботи та розклади тощо. Доступ до хмарних сервісів зберігання інформації зазвичай захищений паролем, який встановлюється власником облікового запису даного сервісу. Слідство може отримати доступ до документів, розміщених у таких хмарних сервісах, у такий спосіб:

1) отримання від потерпілого журналіста, його родичів, колег чи третіх осіб інформації про авторизаційні дані (логін та пароль) для доступу до аккаунта журналіста;

2) отримання тимчасового доступу до електронних інформаційних систем компанії, що надає послуги хмарного зберігання інформації (в порядку ст. 159 КПК України). Слід зауважити, що зазначена процесуальна дія може бути ускладненою через те, що не всі компанії, які надають послуги хмарного збе-

рігання інформації, мають представництва на території України, а звернення до їх іноземних представництв у порядку запиту про міжнародну правову допомогу (ст. 551 КПК України) призведе до затягування строків досудового розслідування. Оскільки, відповідно до п. 7 ч. 1 ст. 164 КПК України строк дії ухвали слідчого судді про тимчасовий доступ до речей і документів не може перевищувати одного місяця з дня постановлення ухвали, звернення до іноземних представництв компаній у порядку міжнародного співробітництва з такою постановою є практично неможливим. Із метою врегулювання описаної проблеми, видається доцільним встановлення у законі початку перебігу строку дії такої постанови з моменту прийняття уповноваженим органом іноземної держави рішення про задоволення запиту про міжнародну правову допомогу;

3) зняття інформації з електронних інформаційних систем у порядку ст. 264 КПК України.

У другому та третьому випадках слідчий, прокурор отримують електронні документи, що були скопійовані з сервера хмарного сервісу зберігання даних на традиційних носіях інформації (диск або роздрукований на папері варіант), що дозволяє їх оглянути та дослідити в порядку ст. 266 КПК України з використанням методів, що вже були описані нами у даній статті.

У випадках, коли слідчий, прокурор здійснюють доступ до хмарних сервісів зберігання інформації самостійно, з використанням авторизаційних даних журналіста, процедура огляду електронних документів у таких сервісах значно збігається з оглядом публікацій у мережі Інтернет та має важливі особливості.

Так, у протоколі мають бути зазначені адреса в мережі Інтернет та назва сервісу, до якого отримується доступ. На нашу думку, логін та пароль доступу до аккаунту не мають зазначатися у протоколі, з метою забезпечення захисту особистих даних журналіста. Крім того, таке обмеження допоможе запобігти несанкціонованому доступу до зазначених даних з боку сторонніх осіб, які на різних етапах кримінального провадження ознайомлюються зі змістом протоколу та відповідно можуть отримати доступ до аккаунту журналіста та змінити чи знищити інформацію, що зберігається у хмарному сервісі.

Більшість сервісів хмарного зберігання інформації дозволяють отримати інформацію про каталог розміщення у сховищі, час та авторство створення документа, що там зберігається, а також хронологію його редагування. Зазначену інформацію має бути відображено в протоколі огляду, так само, як і постійне посилання в мережі Інтернет на документ, що оглядається, якщо на момент доступу слідчого до хмарного сервісу таке посилання було створене володільцем аккаунту.

Текстові документи, а також зображення, що оглядаються, доцільно роздрукувати за допомогою службового принтера та додати до протоколу огляду як невід'ємний додаток, із зазначенням серійного номера, назви та моделі принтера. Фото-, відео- та аудіофайли, аналогічно з оглядом публікацій у мережі Інтернет, мають бути збережені та записані на диск, який стане другим додатком до протоколу огляду.

Висновки. Електронні документи є важливим джерелом доказової та орієнтуючої інформації у кримінальних провадженнях щодо посягань на життя та здоров'я журналіста. Залежно від того, розміщені такі документи на фізичних носіях інформації, у відкритому доступі в мережі Інтернет, чи у хмарних сервісах зберігання інформації, вони мають проходити специфічні процедури слідчого огляду та попереднього дослідження.

Список використаних джерел

1. Криміналістика : підручник / В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель [та ін.] ; за ред. В. Ю. Шепітька. – 5-те вид., переробл. та допов. – К. : Ін Юре, 2016. – 640 с.
2. Криміналістика : навч. посіб. / за ред. А. Ф. Волобуєва. – К. : КНТ : Самміт-Книга, 2011. – 504 с.
3. Кукарникова Т. Э. Электронный документ в уголовном процессе и криминалистике : автореф. дис. ... канд. юрид. наук : 12.00.09 / Т. Э. Кукарникова. – Воронеж, 2003. – 28 с.
4. Сергеева К. А. О современных подходах к понятию электронного документа / К. А. Сергеева // Актуальные проблемы российского права. – 2014. – № 7. – С. 1481–1487.
5. Вершинин А. П. Электронный документ: правовая форма и доказательство в суде : учеб.-практ. пособие / А. П. Вершинин. – М. : Городец, 2000. – 247 с.
6. Сереброва С. П. Использование компьютерной информации при расследовании преступлений в сфере экономики / С. П. Сереброва // Рос. следователь. – 2000. – № 4. – С. 5–7.
7. Одерій О. В. Тактика слідчого огляду комп'ютерних систем та їх елементів / О. В. Одерій, С. О. Корона, С. В. Самойлов. – Донецьк, 2010. – 88 с.
8. Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А. Г. Волеводз. – М. : ООО «Юрлитинформ», 2001. – 496 с.
9. Інструкція про призначення та проведення судових експертиз та експертних досліджень [Електронний ресурс] : затв. наказом М-ва юстиції від 08.10.1998 № 53/5 (у ред. наказу М-ва юстиції України від 26.12.2012 № 1950/5). – Режим доступу: http://zakon5.rada.gov.ua/laws/show/z0705-98/.
10. Mell P. The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology [Електронний ресурс] / P. Mell, T. Grance // National Institute of Standards and Technology Special Publication 800-145. – Режим доступу: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.
11. Рябічев В. Л. Мультиплатформна концепція в сучасній журналістиці / В. Л. Рябічев // Наукові записки Інституту журналістики : наук. зб. / за ред. В. В. Різуна ; КНУ ім. Тараса Шевченка. – 2013. – № 52. – С. 98–101.

References

1. Kryminalistyka : pidruch. (2016) / V. Yu. Shepitko, V. O. Konovalova, V. A. Zhuravel [tain.] : zared. V. Yu. Shepitka. – Kyiv : InYure[inukrainian].
2. Kryminalistyka : navch. posib. (2011) / Zared. A. F. Volobuieva. – Kyiv : KNT; Sammit-Knyha [inukrainian].
3. Kukarnykova, TatianaEduardovnaElektronnyi dokument v ugolovnomprotsesse ikriminalistike : avtoreferatdys. ... kandidatayuridicheskihnauk : 12.00.09 (2003)//– Voronezh. gos. un-t [inrussian].
4. Sergeeva K. A. O sovremennyh podhodah k poniatiiu elektronnogo dokumenta (2014) / Aktualnye problemyrossiiskogo prava. – №. 7. 1481-1487 [in russian].
5. Vershynin A. P. Elektronnyidokument: pravovaiaformaidokazatelstvo v sude: ucheb.-prakt. posobie. (2000) /Moskva :Horodets [inrussian].
6. Serebrova S. P. Ispolzovanie kompiuternoiinformatsiiprirassledovaniiprestuplenii v sfereekonomiki(2000) //Rossiiskiisledovatel. – №. 4. – 5-7 [inrussian].
7. Oderii O. V., Korona S. O., Samoilov C. V. Taktykaslidchohoohliadukompiuternykhsystemtayikhelementiv. (2010) / Donetsk: PROMIN [in ukrainian].

8. Volevodz A. G. Protivodeistvie kompiuternym prestupleniiam: pravovye osnovymezhdunarodnogo sotrudnichestva.(2001) / Moskva :Yzdatelstvo «Iurlytynform» [inrussian].
9. Instruktsiiapropryznachenniataprovedenniasudovykhekspertyztaekspertnykhdoslidzhen(2012) / [in ukrainian].
10. Mell, PeterThe NIST DefinitionofCloudComputing. RecommendationsoftheNationalInstituteofStandardsandTechnology / NationalInstituteofStandardsandTechnology[in english].
11. Riabichev V. L. Multyplatformnakontseptsiia v suchasniizhurnalistytsi (2003) / NaukovizapyskyInstytutuzhurnalistyky : naukovyizbirnyk KNU imeniTarasaShevchenka. 98-101 [inukrainian].

Коваленко А. В., аспирант кафедры криминалистики и судебной экспертологии Харьковского национального университета внутренних дел, Украина, г. Харьков
e-mail: new4or@gmail.com
ORCID orcid.org/0000-0003-3665-0147

Особенности тактики осмотра электронных документов в ходе расследования посягательств на жизнь и здоровье журналиста

В статье исследуются особенности тактики осмотра электронных документов при расследовании посягательств на жизнь и здоровье журналиста. Приведены общие рекомендации по осуществлению осмотра электронных документов. Освещены особенности учета электронных документов, расположенных на физических носителях информации, в сети Интернет (в частности, интернет-публикаций журналиста), а также в сервисах облачного хранения информации. Предложен ориентировочный перечень атрибутов таких документов, описана специфика фиксации результатов их осмотра.

Ключевые слова: обзор, электронный документ, журналист, физический носитель информации, сеть Интернет, сервис облачного хранения информации.

Kovalenko A. V., graduate student of Criminalistics and forensic expertology chair, Kharkiv National University of Internal Affairs, Ukraine, Kharkiv
e-mail: new4or@gmail.com
ORCID orcid.org/0000-0003-3665-0147

The Features of Tactics of Inspection of Electronic Documents During the Pretrial Investigation of Infringements on the Life and Health of a Journalist

The article focuses on the features of tactics of inspection of electronic documents during the investigation of infringements on the life and health of journalists. The views of scientists on the concept and nature of the electronic documents are reviewed. Author classifies electronic documents examined by investigators during the investigation of the studied crimes. General recommendations for inspection of electronic documents are suggested. The features of inspection of electronic documents placed on physical data storages, on the Internet (including Internet publications of journalist) as well as on cloud storage services are studied. The ways of obtaining access to these types of documents by the investigator are illustrated. The author considers the opportunities of involving specialists into this kind of inspections. An indicative list of attributes of such documents, as well as the specifics of recoding the results of their inspection are described. It is established, that electronic documents are an important source of evidential and orienting information in criminal proceedings regarding infringements on the life and health of journalists, which must undergo specific procedures of inspection.

Key words: inspection, an electronic document, journalist, physical data storage, the Internet, the cloud storage service.