DOI 10.26886/2414-634X.3(22)2018.7

UDC 343.985.7

THE MAIN SOURCES OF FORENSIC-MEANINGFUL CRIME INFORMATION ARE RELATED TO MALICIOUS SOFTWARE

O. Volkov

National Academy of Internal Affairs, Ukraine, Kiev

The essence and content of the concept of forensic-meaningful information and its significance in the process of investigation of crimes connected with harmful software are analyzed. The relation of concepts of evidence in criminal proceedings with information evidence is considered. The characteristics of electronic documents are considered, taking into account the specificity of the source of their origin and the mechanism of formation. The requirements to which electronic evidence must comply must be defined. The sources of origin of such information and their location are determined. Substantiation of the principles of handling electronic evidence is given.

Key words: electronic information, actual data, sources of evidence, forensic-meaningful information, circumstances of crime, electronic evidence.

Волков О. О. Основні джерела криміналістично-значимої інформації про злочини пов'язані з шкідливими програмними засобами / Національна академія внутрішніх справ, Україна, Київ

Проаналізовано сутність та зміст поняття криміналістично-значущої інформації та її значенні в процесі розслідування злочинів пов'язаних з шкідливими програмними засобами. Розглянуто співвідношення понять доказів у кримінальному провадженні з інформаційними доказами. Досліджено характеристики електронних документів з урахуванням специфічності джерела їх походження та

механізму утворення. Визначено вимоги якимb повинні відповідати електронні докази. Визначено джерела походження такої інформації та місця їх знаходження. Надано обґрунтування принципів поводження з електронними доказами.

Ключові слова: електронна інформація, фактичні дані, джерела доказів, криміналістично-значуща інформація, обставини вчинення злочину, електронні докази.

Постановка проблеми. Працівники правоохоронних органів під час виявлення та фіксації слідів створення, використання та розповсюдження шкідливих програмних засобів припускаються типових помилок пов’язаних з таким видом електронної інформації. Неправильні дії з такими доказами у подальшому можуть привести до визнання їх недопустимими.

Актуальність дослідження. Поняття електронних доказів у кримінальному процесуальному законодавстві не визначено, тому їх збір, фіксація та використання повинно проводитися з дотриманням загальних критеріїв та правил збору доказів у кримінальному провадженні з урахуванням особливостей таких інформаційних слідів.

Ціль статті. Визначення поняття електронних доказів у кримінальному провадженні, правил поведінки з такими видами доказів, що повинні забезпечити їх допустимість, та їх загальні характеристики.

Відповідно до теорії криміналістики під криміналістично значущою інформацією розуміється сукупність знань про скоєний злочин.[1, с. 945] Успішне розкриття та розслідування злочинів значною мірою залежить від якості та кількості криміналістично значимої інформації, її доступності для особи, яка проводить розслідування.

Під такою інформацією в першу чергу, розуміється фактичні дані або відомості, які знаходяться в обумовленому та безпосередньому зв'язку з подією злочину і обставинами його вчинення. Такими фактичними даними при встановленні істини в кримінальному провадженні, відповідно до положень кримінального процесуального закону, визнаються докази.

Дослідженням та використанням електронних джерел доказів займалися різні вчені, серед них В. О. Мещеряков, В. М. Бутузов, С. Й. Гонгало, В. Б. Вехов, Т. Е. Кукарнікова, М. А. Іванов, Л. Б. Краснова, М. Ю. Літвінов, А. В. Касаткін, Д. В. Пашнєв, В. В. Лисенко, М. М. Федотов, які свої напрацювання викладали у наукових статтях, дисертаційних дослідженнях та монографіях.

Фактичні данні, які встановлюють та окреслюють таке явище матеріального світу як злочин, називають доказами. Порядок визначення доказів, їх фіксації та використання регламентований Кримінальним процесуальним кодексом України (далі КПК). У відповідності до диспозиції статті 84 КПК України доказами у кримінальному провадженні є фактичні дані, отримані у передбаченому цим Кодексом порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню.

Процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів. [2, с. 61 - 62]

Згідно до ст. 98 КПК України речовими доказами є матеріальні об’єкти, які були знаряддям вчинення кримінального правопорушення, зберегли на собі його сліди або містять інші відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження, в тому числі предмети, що були об’єктом

кримінально протиправних дій, гроші, цінності та інші речі, набуті кримінально протиправним шляхом або отримані юридичною особою внаслідок вчинення кримінального правопорушення.[2, с. 69]

Розкриваючи більш докладно зміст одного з джерел доказів, законодавець у статті 99 КПК України надає роз'яснення, що речовими доказами можуть бути також і документи, якщо вони містять у собі зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження.

Розподіл доказів на види є однією з класифікаційних систем, відповідно до якої докази розподіляються, виходячи із специфічних та найбільш суттєвих особливостей їх форми та змісту [3, 228]. Окремі види доказів утворюються у разі, коли їх форма та зміст має особливі характеристики наприклад цифрові, що визначають спеціальний режим їх отримання чи використання у кримінальному процесі. Традиційно, вчені пропонують поділяти докази за механізмом формування на особисті та речові [4].

Отже електронні докази – це докази у кримінальних провадженнях, які можна отримати в електронній формі. Електронні докази отримують за допомогою електронних пристроїв, комп'ютерних носіїв інформації, а також комп'ютерних мереж, у тому числі через мережу Інтернет. Вони стають доступними для сприйняття людиною після обробки засобами комп'ютерної техніки.

У значенні «електронні докази» (electronic evidence) часто застосовується термін «цифрові докази» (digital evidence), часом трапляється так, що у повсякденності обидва поняття розглядаються як однозначні. Але, оскільки законодавством ці поняття не окреслені їх потрібно використовувати паралельно.

Цифрова інформація з урахуванням унікальних характеристик не може бути віднесена до жодної класифікаційної групи, тому на думку Цехана Д.М. існує необхідність уведення категорії «цифрового доказу»[5].

Електронні дані набагато легше змінити чи підробити, ніж традиційні форми доказів, тому правоохоронцям потрібно дотримуватися таких правил поводження з даними, які нададуть можливість забезпечити допустимість доказів.

На відміну від звичайних паперових документів, характеристики та просторові межі яких ми звикли бачити, електронні документи мають інші природу і вирізняються такими характеристиками:

- електронний документ не може існувати без носія інформації. При цьому набувають значення ідентифікаційні ознаки носія інформації (зокрема найменування типу, марки, моделі, індивідуального машинного носія інформації, на якому записано документ);

- електронні докази невидимі «неозброєним оком» (без спеціального інструментарію), існують в нематеріальному вигляді, а для їх сприйняття та дослідження використовують програмно-технічні засоби;

- вони можуть бути змінені, пошкоджені або знищені в процесі експлуатації пристрою чи під впливом фізичних чинників (високий рівень вологості, висока температура, ультрафіолет, електромагнітні випромінювання тощо);

- за стадіями виготовлення документи, в тому числі й електронні поділяють на оригінали, дублікати, копії й виписки[6].

У ч. 3 ст. 99 КПК України визначено, що оригіналом документа є сам документ, а оригіналом електронного документа – його відображення, якому надається таке саме значення, як і документу. Разом із тим, для електронного документу такі поняття, як «оригінал»,

дублікат», «копія» є умовними, оскільки у всіх цих випадках електронний документ залишається оригіналом. Як оригінал такий документ може бути в декількох місцях одночасно[7, 13].

У ст. 7 Закону України від 22.05.2003 № 851-IV «Про електронні документи та електронний документообіг»[8], передбачено, що електронна копія та копія електронного документа на папері засвідчуються в порядку, передбаченому законом, але відповідний нормативний акт до цього часу не ухвалено.

Докази у кримінальному процесі повинні відповідати двом вимогам, що випливають з їх змісту та форми – належності (ст. 85 КПК України) і допустимості (ст. 86 КПК України). Закономірно, що такі ознаки повинен мати й електронний доказ, що може забезпечуватися коректністю фіксації та подальшою незмінністю комп'ютерних даних.

Джерелами доказів в електронній формі можуть бути: різноманітні носії інформації; моноблоки, мобільні пристрої (мобільні телефони, планшетні комп'ютери), цифрові камери, роутери, маршрутизатори, комп'ютерні мережі, глобальна мережа Інтернет, звукозаписи та відеозаписи тощо, тобто джерелом доказів може бути будь-який електронний пристрій, який заходиться на місці проведення процесуальної дії. Варто також зазначити, що постійно з'являються нові види електронних пристроїв, які можуть містити електронні докази.

Докази вчинення злочину можуть знаходитися:

- у комп'ютері потерпілого;
- інтернет-провайдерів, послугами якого користувався потерпілий;
- у комп'ютері підозрюваного;
- інтернет-провайдера, послугами якого користувався підозрюваний;
- іншому місці кіберпростору.

Важливим джерелом доказу є комп'ютерна система, яка складається з корпусу, де розміщені мікропроцесор, плати, накопичувачі інформації та порти для зовнішніх пристроїв; монітора; периферійних пристроїв (принтер, сканер, модем, веб-камера тощо), програмного забезпечення, зокрема:

- системне програмне забезпечення;
- прикладне програмне забезпечення (текстові, графічні редактори, системи управління базами даних, електронні таблиці, системи презентацій і т.п.).

До інформаційних об'єктів (даних), за наявності в них відомостей та вище передбачених процесуальним законом умов, можуть належати, зокрема, текстові та графічні документи, фотографії, звукозапис, відеозапис, інформація у форматах баз даних та інші носії інформації (у тому числі електронні), а також носії інформації на яких за допомогою технічних засобів зафіксовано процесуальні дії. Така інформація подекуди є важливою та представляє певний інтерес при розслідуванні злочинів цієї категорії[9].

Важливу інформацію можуть містити й тимчасові файли. Більшість текстових редакторів і систем управління базами даних створюють тимчасові файли як побічний продукт нормальної роботи програмного забезпечення.

Користувачі комп'ютерів зазвичай не усвідомлюють важливості створення цих файлів тому, що вони, як правило, знищуються програмою наприкінці сеансу роботи. Проте дані, які містять ці знищені файли, можуть виявитися найціннішими. Особливо, якщо вихідний файл був зашифрований чи документ із текстом був надрукований без збереження на диску, такі файли можуть бути відновлені.

Існують зовнішні та внутрішні накопичувачі інформації, а також змінні носії (CD, DVD-диски), та різноманітні USB-накопичувачі. У

цифрових камерах та мобільних телефонах широко використовуються невеликі за розмірами карти пам'яті (SD, Micro SD, Compact Flash CF тощо), які можуть містити значний обсяг інформації. Наприклад, карта Western Digital SanDisk Ultra, Micro SDXDC має обсяг пам'яті 400 Гб.

Багато електронних пристроїв можуть здійснювати обмін інформацією через локальні комп'ютерні мережі або глобальну комп'ютерну мережу Інтернет. Тому для дослідження спеціалізованих пристроїв (концентраторів, маршрутизаторів, комутаторів тощо) необхідні знання фахівців. Варто також зважити на те, що значний обсяг інформації зберігається у «хмарних технологіях», тобто поза місцезнаходженням фізичної чи юридичної особи.

Нині для перевірки цілісності даних використовується механізм розрахунку контрольної суми або хеш-суми (контрольна сума – певне значення, обчислене на основі набору даних із застосуванням одного із математичних алгоритмів (наприклад, MD5, SHA-1, Cr32 або інших), які використовуються для перевірки цілісності даних при їх передачі або збереженні.

Означені контрольні суми можна отримати, послуговуючись, наприклад, такою програмою як HashTab (відкрито розповсюджена в мережі Інтернет), яку вважають найбільш ефективною для цього.

Експертами Scientific Working Group on Digital Evidence, які часто працювали з таким видом доказів запропоновано під терміном «цифрові докази» розуміти будь-яку інформацію доказового значення, яка зафіксована чи передана у цифровій формі[10].

Пі час роботи з електронними доказами працівникам правоохоронних органів слід дотримуватися таких принципів:

1. Законність. Працівники підрозділів правоохоронних органів, що проводять розслідування і досліджують докази в електронній формі,

зобов'язані дотримуватися чинного законодавства, загальних процесуальних та криміналістичних принципів.

2. Цілісність даних. Дії фахівця не повинні призводити до матеріальних змін даних, електронних пристроїв чи носіїв інформації, які можуть використовуватися як докази.

3. Документування процесу. Документують будь-які дії, виконувані стосовно електронних доказів, і зберігають ці документи на випадок перевірки, щоб незалежна третя сторона могла повторити ці дії та отримати аналогічний результат.

4. Експертна підтримка. Якщо передбачається, що при огляді (обшуку) можуть бути виявлені електронні докази, отримують підтримку фахівців (спеціалістів), забезпечивши, за можливості, їх присутність на місці події.

5. Відповідна фахова підготовка. Якщо при огляді (обшуку) відсутні фахівці з електронних доказів, першочергові дії на місці події здійснюють особи, які мають необхідні знання та навички для виявлення і збирання доказів.

6. Розумна обережність. Уникають будь-яких навмисних або ненавмисних дій, які можуть призвести до пошкодження потенційних доказів, представлених у цифровій формі.

До прикладу, правоохоронці не повинні мати доступ до цифрових пристроїв, якщо їм бракує компетентності і вони не обізнані з відповідними процесами. Зокрема, якщо фізичний обсяг цифрового пристрою занадто великий, приміром, сервер в інформаційному центрі, чи це критично для безпеки цифрового пристрою, зупинка якого загрожуватиме життю людей, або коли необхідно зафіксувати спосіб роботи підозрюваного під час зловживання системою. У цьому аспекті необхідно звернути увагу, що доказова інформація є вкрай нестійкою, особливо якщо вона зберігається в оперативній пам'яті ЕОТ, оскільки

може бути легко знищена (у тому числі й некваліфікованими діями слідчого) [11, 438].

Необхідно також звернути увагу на те, що джерелами криміналістично-значимої інформації може бути увімкнений комп'ютер, мобільний телефон або інші електронні пристрої. Специфікою здобуття інформації, що має значення у кримінальному провадженні є те, що така інформація зберігається у ввімкнених електронних пристроях, а їх огляд необхідно проводити у режимі реального часу.

На початковому етапі огляду необхідно перш за все запобігти можливості будь-кому з присутніх осіб заблокувати комп'ютер, вимкнути його з мережі або зашифрувати інформацію що в ньому зберігається.

Специфікою такої інформації у ввімкненій комп'ютерній техніці є нестійкість та енергозалежність, тобто її самознищення у разі від'єднання від джерела живлення. Тому від працівника правоохоронного органу вимагається правильно і швидко зберегти таку інформацію оскільки вона буде втрачена.

Сучасна комп'ютерна техніка містить у собі дуже значні масиви оперативної пам'яті та може вміщати в себе від 2 до 64 Гб., а в серверній комп'ютерній техніці і того більше.

В останній час значного поширення набуло використання для обробки та зберігання інформації так званих «хмарних» сховищ, специфікою якого є збереження та обробка інформації на значному віддалені від комп'ютера користувача. Доступ до інформації що зберігається в таких сховищах регулюється законодавством тієї країни, де знаходиться фізичний носій інформації.

В оперативній пам'яті може знаходитися:

- інформація про виконувані у комп'ютері процеси;
- інформація про виконувані сервіси;

- системна інформація;

- дані про користувачів, які перебувають в системі;

- про відкриті порти;

- кеш ARP (протоколу визначення адреси);

- кеш DNS (доменної системи імен);

- інформація про автоматично завантажені додатки;

- незбереженні документи;

- бінарні процеси і сервіси, в тому числі шкідливі програмні засоби, які зберігають тільки в оперативній пам'яті. [12, ст. 25-26]

З метою збереження такої «енергозалежної» інформації та недопущення її необережного чи умисного знищення чи пошкодження необхідно:

- обмежити присутніх осіб від доступу до комп'ютерного обладнання;

- виявити, описати та сфотографувати кожен такий пристрій в якому на момент його огляду міститься «енергозалежна» інформація;

- За участю спеціаліста вжити заходів щодо унеможливлення її зміні або знищенню, провести її фіксацію.

Підводячи висновок слід зазначити, що криміналістично значущою інформацією визнається сукупність знань про скоєний злочин.

Інформацією, про яку йдеться мова, вважаються фактичні дані або відомості, які знаходяться в обумовленому та безпосередньому зв'язку з подією злочину і обставинами його вчинення. Такими фактичними даними при встановленні істини в кримінальному провадженні, відповідно до положень кримінального процесуального закону, визнаються докази.

Одним з видів доказів КПК визнає документ. До документів можуть належати різні носії інформації у тому числі електронні. Отже

електронні докази – це докази у кримінальних провадженнях, які можна отримати в електронній формі за допомогою електронних пристроїв (комп'ютерів).

На відміну від звичайних паперових документів, електронні документи мають іншу природу і вирізняються такими характеристиками:

- електронний документ не може існувати без носія інформації. При цьому набувають значення ідентифікаційні ознаки носія інформації (зокрема найменування типу, марки, моделі, індивідуального машинного носія інформації, на якому записано документ);

- електронні докази невидимі «неозброєним оком» (без спеціального інструментарію) і для їх сприйняття та дослідження використовують програмно-технічні засоби;

- вони можуть бути змінені, пошкоджені або знищені в процесі експлуатації пристрою чи під впливом фізичних чинників (високий рівень вологості, висока температура, ультрафіолет, електромагнітні випромінювання тощо);

- за стадіями виготовлення документи, в тому числі й електронні, поділяють на оригінали, дублікати, копії й виписки.

- при тому, якщо за звичай, оригіналом документа є сам документ, а оригіналом електронного документа – його відображення, якому надається таке саме значення, як і документу. Разом із тим, для електронного документу такі поняття, як «оригінал», дублікат», «копія» є умовними, оскільки у всіх цих випадках електронний документ залишається оригіналом.

Працюючи з електронними доказами необхідно дотримуватися перш за все принципу законності, незмінності виявленої інформації, документування процесу їх виявлення та фіксації, експертної

підтримки, наявної фахової підготовки працівників правоохоронних органів та обережності з їх поводженням.

Література:

1. Криминалистика. Учебник для вузов. Под редакцией професора Р. С. Белкина. М. НОРМА – ИНФРА. 2001. с. 969.

2. Кримінальний процесуальний кодекс України. Київ. «ПАЛИВОДА». 2017. с. 402.

3. Теория доказательств в советском уголовном процессе / отв. ред. Н. В. Жогин. – Изд. 2-е, испр. и доп. – М.: Юрид. лит., 1973. – 736 с.

4. Алексеев С. С. Обсуждение спорных вопросов теории доказательств в советском уголовном процес-се / С. С. Алексеев, В. П. Божьев // Соц. закон-ность. – 1965. – С. 95 –98.

5. Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. // Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція. 2013. - № 5, - С. 259

6. Цехан Д. М. Правові аспекти використання цифрової інформації як доказу у кримінальному судочинстві / Д. М. Цехан // Процесуальні, тактичні та психологічні проблеми, тенденції та перспективи вдосконалення досудового слідства: матеріали між-нар. наук.-практ. конф. (Одеса, 30 травня 2008 р.). – Одеса, 2008. – С. 206 –209.

7. Гонгало С. Й. Судова техніко-криміналістична екс-пертиза документів: сучасні можливості дослідження та перспективи розвитку: автореф. дис. на здобуття наукового ступеня канд. юрид. наук.: спец. 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність / С. Й. Гонгало. – К., 2013. – 20 с.

8. Закон України «Про електронні документи та електронний документообіг» // Відомості Верховної Ради України (ВВР), 2003, N 36, ст.275.

9. Casey E. Digital evidence and computer crime: forensic scene, computer, and the Internet / Eoghan Casey. – 2 nd ed. – Amsterdam: Elsevier Academic Press, 2004. – 690 p.

10. Scientific Working Group on Digital Evidence [Electronic resource]. – Electronic data (1 file). – Mode of access: http // www. swgde. org /. – Title from the screen.

11. Пономарев И. П. Цифровое алиби и его проверка / И. П. Пономарев // Вестник ВГУ. Серия: Право, 2011. – № 2 – С. 437-444

12. Використання електронних (цифрових) доказів у кримінальних провадженнях [Текст]: В 43 метод. рек. / [М. В. Гребенюк, В. Д. Гавловський, М.В. Гуцалюк, В. Г. Хахановський та ін.]; за заг. ред. М. В. Гребенюка. – Київ: МНДЦ при РНБО України, 2017. – 76 с.

References:

1. Kriminalistika. Uchebnik dlya vuzov. Pod redaktsiey profesora R.S. Belkina. M. NORMA – INFRA. 2001. s. 969.

2. KrimInalniy protsesualniy kodeks UkraYini. KiYiv. «PALIVODA». 2017. s. 402.

3. Teorija dokazatel'stv v sovetskom ugolovnom processe / otv. red. N. V. Zhogin. – Izd. 2-e, ispr. i dop. – M.: JUrid. lit., 1973. – 736 s.

4. Alekseev S. S. Obsuzhdenie spornyh voprosov teorii dokazatel'stv v sovetskom ugolovnom proces-se / S. S. Alekseev, V. P. Bozh'ev // Soc. zakonnost'. – 1965. – S. 95 –98.

5. Cehan D.M. Cifrovi dokazi: ponjattja, osoblivosti ta misce u sistemi dokazuvannja. // Naukovij visnik Mizhnarodnogo gumanitarnogo universitetu. Ser.: JUrisprudencija. 2013. - № 5, - S. 259

6. Cehan D. M. Pravovi aspekti vikoristannja cifrovoï informaciï jak dokazu u kriminal'nomu sudochinstvi / D. M. Cehan // Procesual'ni, taktichni ta psihologichni problemi, tendenciï ta perspektivi vdoskonalennja dosudovogo slidstva: materiali mizhnar. nauk.-prakt. konf. (Odesa, 30 travnja 2008 r.). – Odesa, 2008. – S. 206 –209.

7. Gongalo S. J. Sudova tehniko-kriminalistichna ekspertiza dokumentiv: suchasni mozhlivosti doslidzhen-nja ta perspektivi rozvitku: avtoref. dis. na zdobuttja naukovogo stupenja kand. jurid. nauk.: spec. 12.00.09 – kriminal'nij proces ta kriminalistika; sudova ekspertiza; operativno-rozshukova dijal'-nist' / S. J. Gongalo. – K., 2013. – 20 s.

8. Zakon Ukraïni «Pro elektronni dokumenti ta elektronnij dokumentoobig» // Vidomosti Verhovnoï Radi Ukraïni (VVR), 2003, N 36, st.275.

9. Casey E. Digital evidence and computer crime: forensic scene, computer, and the Internet / Eoghan Casey. – 2 nd ed. – Amsterdam: Elsevier Academic Press, 2004. – 690 p.

10. Scientific Working Group on Digital Evidence [Electronic resource]. – Electronic data (1 file). – Mode of access: http // www. swgde. org /. – Title from the screen.

11. Ponomarev I. P. Cifrovoe alibi i ego proverka / I. P. Ponomarev // Vestnik VGU. Serija: Pravo, 2011. – № 2 – S. 437-444.

12. Vikoristannya elektronnih (tsifrovih) dokazlv u krimlnalnih provadzhennyah [Tekst]: V 43 metod. rek. / [M. V. Grebenyuk, V. D. Gavlovskiy, M. V. Gutsalyuk, V. G. Hahanovskiy ta In.]; za zag. red. M. V. Grebenyuka. – KiYiv: MNDTs pri RNBO UkraYini, 2017. – 76 s.