мати лише орієнтовне значення, оскільки часто мають місце випадки їх імітації.

Таким чином, спостереження за поведінковими антроподжерельними невербальними проявами обшукуваної особи є ефективним прийомом, який сприяє встановленню місць приховування шуканих предметів. Водночас, будучи пов'язаним із застосуванням інших прийомів впливу на психіку обшукуваного, воно стає ще більш ефективним.

Хижняк Є. С.
доцент кафедри криміналістики
Національного університету «Одеська юридична академія»,
кандидат юридичних наук

ОСОБЛИВОСТІ ОГЛЯДУ ЕЛЕКТРОННИХ ДОКУМЕНТІВ ПІД ЧАС РОЗСЛІДУВАННЯ ЗЛОЧИНІВ ПІДРОЗДІЛАМИ ДЕРЖАВНОГО БЮРО РОЗСЛІДУВАНЬ

З аналізу положень Кримінального процесуального кодексу України та Закону України «Про Державне бюро розслідувань» можна зробити висновок, що слідчі Державного бюро розслідувань (далі — ДБР) мають повноваження ті ж самі, що і слідчі інших органів досудового розслідування. При розслідування злочинів, віднесених до підслідності ДБР слідчому необхідно використовувати криміналістичні знання, що стануть в нагоді. Однією з найскладніших процесуальних дій під час здійснення досудового розслідування є слідчий огляд електронних документів, складність якого полягає у відсутності достатніх теоретичних досліджень у даному напрямку, а як наслідок — відсутність узагальнених тактичних прийомів огляду електронних документів.

Під час огляду електронних документів варто брати до увагу, що електронний документ є більш «вразливим» доказом у порівнянні з традиційними засобами доказування. Вразливість електронного доказу полягає втому, що він може бути або легко знищений, або зміст якого може бути змінений, модифікований тощо без будь- яких очевидних ознак. Як правило, такі ознаки не можливо встановити шляхом традиційного дослідження змісту електронного документа, що, в свою чергу, може спричинити втрату важливої криміналістично значимої інформації.

«Вразливість» електронного документа зумовлює необхідність створення спеціальних правил фіксації електронної інформації, способів збереження та приєднання їх до матеріалів справи. Зокрема, на

рівні з традиційними правилами поводження із документами, необхідно враховувати технічні особливості збирання, зберігання та використання інформації.

Процес огляду електронних документів в цілому відповідає загальноприйнятому алгоритму дій, які вчиняються слідчим під час огляду звичайних документів. Такий комплекс дій повинен складатися з наступного: 1 — пошук і виявлення документів; 2 — візуальний огляд зовнішнього стану без зміни умов сприйняття; 3 — фіксація за допомогою фотозйомки; 4 — фіксація в протоколі відповідної слідчої дії (фіксуються всі дії посадових осіб, стан документа і виявлені сліди); 5 — виявлення слідів рук (на фізичному носії електронного документа); 6 — виявлення слідів зміни первісного змісту; 7 — підготовка до упаковки; 8 — упаковка (Бірюков В. В. Криміналістичне документознавство. — Київ: Паливода А. В. — 2007. — 331 с. — С. 129).

Разом з тим, слідчий огляд електронних документів здійснюється з урахуванням певних особливостей об'єкту дослідження, що впливає як на сам процес дослідження, так і на спосіб процесуального закріплення отриманих результатів.

Так, під час пошуку електронних документів необхідно мати на увазі, що вони завжди розміщені на окремих фізичних носіях (USB-флеш-накопичувач, диски, тощо), або можуть бути розміщені в мережі Інтернет, зокрема, на спеціальних на спеціальних «хмарних» сервісах зберігання інформації. Будь-які дії з електронними документами необхідно здійснювати за допомогою сертифікованого обладнання із ліцензійним забезпеченням. Несертифіковане обладнання може привести до втрати електронних документів, випадкового знищення реквізитів або окремих складових електронних доказів. За можливості до збирання та вилучення електронних доказів необхідно залучати спеціалістів, які з технічної точки зору забезпечать збереження необхідних документів.

Фізичні носії електронної інформації, на яких може знаходитися криміналістично важлива інформація, вилучаються при огляді місця події, оглядах та обшуках житла чи робочих приміщень, при огляді речей та комп'ютерної техніки учасників кримінального провадження. Якщо електронні докази розміщені на серверах чи жорстких дисках підприємств, установ або організацій, слідчому рекомендується здійснити побайтову копію носія інформації, адже вилучення майна підприємства може призвести до негативних наслідків. За допомогою спеціального обладнання відтворюється ідентична копія електронної інформації, яка знаходиться на технічному носії, після чого самі фізичні носії повертаються власникам. Аналогічні дії необхідно здійснювати, коли виникає необхідність в проведенні комп'ютерно-технічної експертизи.

Перед дослідженням змісту електронного документа слідчий повинен встановити тип фізичного носія, на якому розміщений електронний документ, для підготовки необхідного обладнання для роботи з таким носієм. У разі, якщо технічний носій інформації захищений від будь-якого стороннього доступу до їх змісту, то фізичний носій має бути переданий експерту на предмет встановлення можливого доступу до електронної інформації, яка зберігається на таких носіях. Окрім того, за допомогою експертизи можливо встановити факт втручання до електронного документа, факт внесення яких-небудь змін та час їх здійснення.

Огляд електронних документів, розміщених на фізичному носії інформації, здійснюється шляхом безпосереднього сприйняття слідчим інформації, що міститься в електронному документі, за допомогою службового комп'ютера. В змісті самого протоколу огляду варто зазначати технічні характеристики та серійні номери обладнання, назви та версії програмного забезпечення, що використовуються в ході слідчого огляду.

Під час дослідження електронного документа особливу увагу необхідно звертати на його формат, розмір, хронологію створення, користувача, яким було створено документ. За допомогою фото- та відеоматеріалів ідентифікуються місце зйомки. В процесі огляду документа слідчий в обов'язковому порядку звертає увагу на найменування та місцезнаходження установи, автора документа, назву виду документа, дату та час його виготовлення, зміст електронного документа, наявність електронного цифрового підпису.

Електронний документ перевіряється на зараження його вірусом, на цілісність і справжність усіх накладених на нього електронних цифрових підписів, включаючи ті, що накладені (проставлені) згідно із законодавством як аналоги печатки чи підпису посадової особи. Також перевіряється наявність супровідної документації — заповненої реєстраційно-контрольної картки в електронній та/чи паперовій формі, повідомлення про прийняття та реєстрацію електронного документа (Пчеліна О. В. Особливості огляду електронного документа / О. В. Пчеліна // Актуальні питання розслідування кіберзлочинів. Матеріали міжнародної науково-практичної конференції. — Х., 2013р. — С. 159-162. — С. 161). У разі неможливості встановлення вище перелічених обставин, слідчий розглядає можливість призначення комп'ютерно-технічної експертизи.

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 (Коваленко А. М. Особливості тактики огляду електронних

документів під час досудового розслідування посягань на життя та здоров'я журналіста / А. М. Коваленко // Вісник Національної академії правових наук України. — № 1(88). — 2017 — С. 182-191. — С. 186).

У порівнянні із оглядом традиційних документів огляд електронних документів є більш об'ємною та складнішою процесуальної дією, яка вимагає використання спеціальних знань, технічних засобів та програмного забезпечення, необхідності залучати спеціалістів для пошуку електронних доказів та їх вилучення під час кримінального провадження. Особливість огляду електронних документів полягає в особливих правилах фіксації отриманих результатів, необхідності використання фізичних носіїв зберігання електронних документів, а також вчинення додаткових процесуальних дій, спрямованих на забезпечення достовірності електронного документа та з метою подальшого їх використання в якості доказу.

Панасюк А. О.
інспектор Управління патрульної поліції в Одеській області, ДПП

ПРИЙОМИ ФІКСАЦІЇ ДАНИХ У МЕРЕЖІ ІНТЕРНЕТ

Технологізація сучасного соціального життя стрімко зростає у всьому світі, при цьому технологізується не лише матеріальне виробництво, але і решта сторін суспільства та діяльність кожної окремої особи. Розглядаючи мережу Інтернет у контексті її використання під час виявлення і розслідування злочинів, доцільно застосувати інструментальний підхід, згідно з яким він застосовується як інструментарій вирішення завдань цієї державно-правової форми боротьби зі злочинністю.

Робота в мережі Інтернет (організаційні, управлінські, кадрові, технічні, технологічні та інші чинники) та Кримінальний процесуальний кодекс (далі — КПК України) обумовлюють особливості криміналістичного дослідження даних, розміщених в мережі Інтернет. Таке дослідження включає в себе:

1. Пошук;
2. Виявлення;
3. Аналіз (стадії: попередня, робоча та заключна);
4. Формування висновків.

Характер досліджень даних в мережі Інтернет має свої особливості, які обумовлюються змістом та структурою мережі Інтернет, її апаратних засобів та програмного забезпечення. Означений порядок дослідження виправданий тим, що дійсно під час виявлення та до-