УДК 343: 004.056

Осика І.М.

к.ю.н., доцент кафедри кримінально-правових дисциплін та адміністративного права Харківського економіко-правового університету

Особливості тактики проведення слідчих дій, спрямованих на виявлення, вилучення та огляд документів, виготовлених за допомогою засобів комп'ютерної техніки

В сучасних умовах розвитку високих технологій все більше документів виготовляється за допомогою засобів сучасної комп'ютерної техніки. Широкого розповсюдження набуло використання різноманітних комп'ютерних програм для спрощення документообігу, ведення бухгалтерського, господарського та фінансового обліку, а також було запроваджено електронний документообіг, який стрімко розвивається у сфері господарювання та державного управління. Назване не могло залишитися поза увагою злочинців, тому найбільш розповсюдженими способами підроблення документів в сучасних умовах є ті, які пов'язані з використанням засобів сучасної комп'ютерної та розмножувальної техніки [1, с.93-94]. Крім цього, об'єктами підроблення стають документи, виготовлення і застосування яких неможливе без засобів комп'ютерної техніки – банківські платіжні картки і електронні документи. Відповідно, більшість доказової інформації щодо підроблення документів в сучасних умовах зберігається в пам'яті комп'ютерів та на змінних носіях комп'ютерної інформації. Така ситуація призвела до необхідності виявлення, вилучення, зберігання доказів на комп'ютерних носіях інформації. Властивість комп'ютерних даних та носіїв інформації, які полягають у можливості бути швидко і легко знищеними, зміненими або заміненими іншими, обумовлює особливості тактики проведення виїмок, обшуків та оглядів документів, що зберігаються на комп'ютерних носіях інформації.

Питанням особливостей виявлення, вилучення, зберігання і дослідження документів на комп'ютерних носіях інформації при-

діляється чимала увага в сучасних публікаціях як українських, так і закордонних авторів [2, с. 5-7; 3; 4; 5; 6; 7; 8; 9].

На ставлячи завдання розробки загальної тактики проведення слідчих дій з комп'ютерною технікою потрібно відзначити, що основними завданням слідчого під час виявлення і вилучення документів на комп'ютерних носіях інформації є: 1) належним чином вилучити носії комп'ютерної інформації та периферійні пристрої (за наявністю) і зафіксувати це в протоколі; 2) належним чином упакувати всі елементи апаратно-програмного комплексу і носії інформації; 3) відправити їх для експертного дослідження в лабораторних умовах; 4) забезпечити цілісність інформації і запобігти її знищенню чи пошкодженню на всіх етапах роботи з нею.

Виїмка документів, що зберігаються на комп'ютерних носіях інформації можлива за умови переведення їх до паперової форми. В залежності від характеру кримінальної справи, в рамках розслідування якої проводиться виїмка документів, і результатів, які слідчий очікує отримати за допомогою даної слідчої дії, виникає необхідність отримання паперових копій електронних документів, роздруківок документів, що виготовляються за допомогою спеціального програмного забезпечення або комп'ютерних носіїв інформації. Копії електронних документів виготовляються особою, що уповноважена на це правилами електронного документообігу і засвідчуються підписами і печаткою суб'єкта господарювання, на якому було виготовлено копію. У разі складання та зберігання бухгалтерських документів на машинних носіях інформації за допомогою спеціалізованого програмного забезпечення, підприємство зобов'язане за свій рахунок виготовити їх паперові копії[1] . При цьому такі копії мають завірятися підписом директора або головного бухгалтера і скріпляються печаткою суб'єкта господарювання. В решті випадків має проводитися виїмка носіїв комп'ютерної інформації, які направляються для подальшого експертного дослідження, під час якого виготовляються паперові копії електронних документів або роздруківки електронних зображень паперових документів чи їх окремих елементів (реквізитів). Рішення щодо вилучення таких носіїв інформації шляхом виїмки, або під час обшуку залежить від конкретної слідчої ситуації, що склалася на певному етапі розслідування злочину.

[1] п. 6 ст. 9 Закону України "Про бухгалтерський облік та фінансову звітність в Україні"

Обшук проводиться з метою виявлення і вилучення: а) носіїв комп'ютерної інформації; б) комп'ютерна (включаючи принтер та іншу периферію) і розмножувальна техніка; в) технічна документація до окремих елементів апаратно-програмного комплексу (договори про надання послуг з функціонування системи електронного документообігу, надання послуг зв'язку тощо).

До носіїв комп'ютерної інформації, що підлягають пошуку, відносяться: дискети, оптичні диски (CD, CD-R, CD-RW, DVD, DVD-RW), портативні накопичувачі пам'яті (флеш), процесори персональних комп'ютерів, плати пам'яті персонального комп'ютера, електронні записники, портативні комп'ютери, мобільні телефони, чіп-картки послуг мобільного зв'язку, аудіо- і відеокасети та ін. [10, с. 162-163]. Вони можуть містити в собі наступну доказову інформацію: а) файли з текстовими зображеннями підроблених документів або графічними зображеннями їх окремих фрагментів; б) відсканові зображення паперового документа і його окремих реквізитів; в) програмне забезпечення, за допомогою якого формувалося електронне зображення документа і його реквізитів; г) файли-сліди електронного монтажу; ґ) файли, що містять інформацію довідкового характеру щодо способів підробки документів; д) викрадені бази даних; є) незаконно скопійовані чи генеровані коди електронного цифрового підпису; е) програмне забезпечення системи електронного документообігу; ж) шкідливі програми, що використовуються для несанкціонованого доступу до баз даних чи інших інформаційних ресурсів; з) програмне забезпечення функціонування принтера, сканера чи іншого периферійного обладнання; і) протоколи роботи в Інтернет, адреси сайтів і електронної пошти, що найбільш часто застосовуються, повідомлення електронної пошти; ї) фінансово-господарські дані ("чорнова" бухгалтерія) та ін.

Конкретні об'єкти пошуку залежать від виду злочину, що розслідується, способу його вчинення, а також властивостей документа, що став об'єктом злочинного посягання і, відповідно, пошуку та вилучення. Наприклад, об'єктами пошуку при розслідуванні незаконних дій з банківськими платіжними картками будуть: а) заготовки, викрадені чи виготовлені картки; б) носії комп'ютерної інформації з даними реквізитів карток, програмним забезпеченням для генерації номерів карток, зламу баз даних, ко-

піювання і записування номерів карток; в) обладнання для виготовлення карток або внесення до них змін (ембосери, термопринтери, ламінувальні машини та ін.); г) сканери; ґ) цифрові камери; д) матеріал для виготовлення карток (пластик, фольга, магнітна плівка); є) мобільні телефони; ж) карти або схеми населених пунктів з поміченими на них місцями розташування банкоматів; з) шматки паперу з написами, що можуть виявитися паролями і кодами доступу до електронної пошти та інших інформаційних ресурсів тощо.

Під час проведення обшуку в приміщенні і при затриманні підозрюваного необхідно проводити його особистий обшук. В процесі такого обшуку особлива увага звертається на мобільний телефон та інші носії комп'ютерної інформації. Практиці відомі випадки, коли в результаті огляду мобільного телефону за участю представника оператора мобільного зв'язку було встановлено, що на мобільний термінал підозрюваного неодноразово передавалися повідомлення про реквізити банківських платіжних карток, які в подальшому використовувалися зі злочинним цілями [11].

Огляд документів на комп'ютерних носіях інформації викликає дискусії у літературі щодо порядку і моменту його проведення. Так, Кримінально-процесуальний кодекс України вимагає проведення огляду документа або предмета під час його виявлення при проведенні виїмки або обшуку, а також проведення огляду будь-якого предмета чи документа, що набуває статусу речового доказу. Однак, не всі автори враховують специфіку документів на комп'ютерних носіях інформації, яка впливає на порядок їх огляду з метою забезпечення їх допустимості в якості доказів у кримінальній справі.

Слід зауважити, що у більшості публікацій слідчому рекомендується проводити огляд вмісту комп'ютера або іншого носія на місці проведення обшуку або виїмки. З цим не можна погодитися, оскільки: а) дослідження вмісту комп'ютера може зайняти багато часу; б) слідчий, навіть якщо і володіє певними знаннями у сфері комп'ютерної інформації, фізично не в змозі простежити за достатньо динамічним технічним розвитком, в результаті чого може допуститися помилки і втратити дані; в) не завжди можливо мати з собою всі необхідні сертифіковані і ліцензійні програмні та апаратні засоби дослідження носіїв комп'ютерної інформації; г) застосування не сертифікованих апаратних пристроїв, неліцензій-

них програмних засобів, здійснення некваліфікованих маніпуляцій з носієм комп'ютерної інформації, можуть створити сумніви щодо цілісності даних, що може негативно вплинути на вирішення питання щодо їх допустимості в якості доказів; г) експертне дослідження гарантує більш ретельне та кваліфіковане дослідження і забезпечує доказову силу отриманих результатів.

Але можуть бути ситуації, коли вилучення комп'ютера є неможливим і потрібне негайне дослідження вмісту комп'ютерного носія. Такими ситуаціями є: а) вилучення комп'ютерної техніки призведе до зупинення діяльності легально діючого суб'єкта господарювання; б) вилучення комп'ютерної техніки може завдати значних матеріальних збитків суб'єктам господарювання; в) зволікання з отриманням даних може привести до знищення інших цінних доказів у справі або потягти за собою завдавання шкоди здоров'ю і життю людей; г) настання інших тяжких наслідків. В таких ситуаціях можливі такі дії: 1) опечатування апаратно-програмного комплексу або приміщення (якщо комп'ютер один) з призначенням комп'ютерно-технічної експертизи, яка проводиться на місці; 2) копіювання вмісту твердого диску комп'ютера за допомогою спеціального сертифікованого обладнання [2] 3) проведення огляду вмісту комп'ютера за участю спеціаліста, який виконує всі дії з комп'ютером виключно у присутності понятих, пояснюючи їм сутність усіх дій, а за умови застосування програмних чи апаратних засобів звертає увагу на їх призначення, сертифікацію і ліцензування.

У випадках, коли документи на комп'ютерних носіях інформації вилучаються при розслідуванні підроблення документів на паперових носіях інформації, важливим є вилучення принтера, за допомогою якого, можливо, виготовлялися підроблені документи або їх окремі елементи (реквізити), з метою проведення ідентифікаційного експертного дослідження. У такому разі разом з принтером необхідно вилучати: а) картриджі, що знайдені на місці про-

[2] Наприклад, поліція Великобританії укомплектована спеціальними портативними комп'ютерами, що дозволяють виготовляти дзеркальну копію твердого диска комп'ютера на оптичний диск (Image Mirror Machine компанії Vogon International, Safeback компанії Syndex, DIBS компанії Computer Forensics ltd.) Такий пристрій дозволяє одночасно виготовлювати дві копії твердого диска, одна з яких автоматично опечатується електронною печаткою і залучається в якості доказу до кримінальної справи, а друга копія направляється для експертного дослідження.

ведення обшуку; б) барвники (чорнила, тонери, в залежності від виду принтеру); в) диски з програмним забезпеченням, що забезпечує комунікацію між принтером і персональним комп'ютером (драйверами); г) документи, що були роздруковані за допомогою цього принтера (в присутності слідчого або знаходилися в ньому); ґ) бухгалтерські та інші документи, що свідчать про заміну картриджу, барвника, ремонт принтера тощо; д) технічна документація на друкуючий пристрій. Під час збереження і транспортування струминних принтерів слід враховувати, що рідкі чорнила мають властивість висихати. Певної особливості має огляд банківських пластикових карток і електронних документів. Дані особливості обумовлені тим, що банківська платіжна картка має нетрадиційні носії інформації: пластик і магнітну смугу або електронний мікропроцесор, що містять важливу доказову інформацію, а електронний документ існує лише на комп'ютерних носіях інформації, тоді як до справи необхідно залучати документи на папері. Огляд банківських платіжних карток проводиться за тими ж правилами, що і огляд паперових документів, за виключенням дослідження вмісту магнітної смуги (електронного мікропроцесора), яке проводиться за допомогою відповідної експертизи чи іншими засобами. При візуальному огляді картки обов'язково звертається увага на її стан, наявність пошкоджень, розмір, колір та товщину пластика. В протоколі описується як лицева, так і зворотна сторона картки. При описуванні лицевої сторони вказуються наступні дані: а) назва платіжної системи, торговий знак якої зображений на картці; б) назва банку-емітенту; в) номер картки; г) ім'я держателя картки; ґ) дата, до якої вона чинна; д) додаткові реквізити (фотокартка). При огляді зворотної сторони описується стан паперової стрічки для підпису, наявність підпису та стан магнітної смуги.

Найбільш проблемним на сьогоднішній день є огляд електронних документів. В спеціальній літературі можна зустріти рекомендації щодо проведення огляду електронних документів, які описують порядок роботи з комп'ютером та відповідними програмами і файлами [12, с.31-63; 13, с. 194-202; 14, с.79-87; 15]. На нашу думку, такі рекомендації стосуються в першу чергу експерта, який проводить дослідження носія комп'ютерної інформації, а не слідчого. Як говорилося вище, основним завданням слідчого є належне вилучення і описання носія інформації з наступним направленням його на експертизу. У невідкладних випадках, коли існує

потреба у негайному огляді вмісту носія інформації, він має проводитися за участю кваліфікованого і спеціально підготовленого спеціаліста з дотриманням умов, описаних вище. Огляд паперових копій електронного документа, роздруківок інших комп'ютерних даних проводиться за загальними правилами огляду паперових документів. При цьому в протоколі обов'язково відображаються номери, що були присвоєні документу системою електронного документообігу та його користувачами.

Для забезпечення ефективності провадження розглянутих слідчих дій важливо залучати фахівця у сфері комп'ютерної техніки та програмного забезпечення. Допомога такого спеціаліста спрямована на належне виявлення, вилучення документа з метою забезпечення його допустимості в якості доказу в кримінальній справі та на кваліфіковану підготовку відповідних експертиз.

Під час розроблення тактичних рекомендацій щодо проведення окремих слідчих дій, спрямованих на виявлення, вилучення і дослідження документів необхідно враховувати сучасний стан розвитку високих технологій і можливості криміналістичної техніки. Окремо слід звертати особливу увагу на умови забезпечення допустимості документів, що вилучаються, враховуючи властивості самого документа, носія його інформації, умов та підстав його виявлення, вилучення та подальшого дослідження. Запорукою ефективного виявлення, вилучення та дослідження документа на комп'ютерних носіях інформації є своєчасне залучення спеціаліста до участі у відповідній слідчій дії, або під час підготовки до її проведення.

Література

1. Осика І.М. Поняття способу підробки документів, що використовуються при вчиненні злочинів у сфері підприємництва // Право і безпека. – 2005. – Т.4. - № 6. – с. 92 – 95

2. Салтевский М.В., Щербаковский М.Г., Губанив В.А. Осмотр компьютерных средств на месте происшествия: Методические рекомендации. Х.: ООО «ЛТД Знание» 1999. – 12 с.

3. Мацишин В.С. Особливості огляду місця події у справах про фальшивомонетництво, вчинене з використанням комп'ютерної техніки // Криміналістичний вісник. Науково-практичний збірник ДНДЕКЦ МВС України і НАВСУ. Київ, 2000. – С. 173 – 178

4. Башкарьова А.В. Особливості огляду місця події по злочинах, пов'язаних з використанням комп'ютерної техніки // Теорія та практика криміналістичного забезпечення розкриття та розслідування злочинів у сучасних умовах: Тези доп. Між нар. Наук. – пркт. Кофереції Ч.І. – К.: Національна академія внутрішніх справ України, 2001. - С. 132 – 135

5. Нудельштейн А.М. Подготовка следственных действий, связанных с обнаружением и изъятием компьютерной информации // Российский следователь. – 2002. - №11. – С. 10 – 13

6. Стратонов В.М., Захарченко С.О. Слідчі огляди у злочинах, скоєних з використанням комп'ютерної техніки // Вісник Національного університету внутрішніх справ. – 2003. – Вип. 24. - С. 49 – 55

7. Нехорошева О. Изъятие компьютерной техники и информации // Законность. – 2004. - №8. – С. 15 – 18

8. Вехов В.Б. Особенности организации и тактики осмотра места происшествия при расследовании преступлений в сфере компьютерной информации // Российский следователь. – 2004. - №7. – С. 2 – 5

9. Щербаковский М.Г. Проблемы выявления, фиксации и изъятия следов преступлений, совершённых с применением компьютерных технологий // Збірник наукових праць Харківського центру по вивченню організованої злочинності спільно з Американським Університетом у Вашингтоні. Випуск девятий. – Х.: Східно-регіональний центр гуманітарно-освітніх інститутів. – 2004. – С. 278 – 309

10. Огляд місця події при розслідуванні окремих видів злочинів: Наук.-практ. Посібник / За ред. Н.І. Клименко. – К.: Юрінком Інтер, 2005. – 216 с.

11. Справа № 69039053 // Матеріали прокуратури м. Дніпропетровська за 2004 рік.

12. Подволоцкий И.Н. Осмотр и предварительное исследование документов / Под ред. Проф. А.М. Зинина. М.: Издательство «Юрлитинформ». 2004. – 200с.

13. Вехов В.Б., Голубев В.А. Расследование компьютерных преступлений в странах СНГ: Монография / Под ред. Заслуженного деятеля науки Российской Федерации, д-ра юрид. наук, проф. Б.П. Смагоринского. – Волгоград: ВА МВД России, 2004. – 304 с.

14. Вехов В.Б., Попова В.В., Илюшин Д.А. Тактические особенности расследования преступлений в сфере компьютерной информации: научно-практическое пособие. – Самара: ООО «Офорт», 2003. – 188 с.

15. Кукарникова Т.Э. Предварительное исследование электронного документа // Воронежские криминалистические чтения: Сб. науч. трудов. Вып. 5 / Под ред. О.Я. Баева. – Воронеж: Изд-во Воронеж гос. ун-та, 2004. – С. 137 – 146.