Оксана Пчеліна,
кандидат юридичних наук,
доцент кафедри криміналістики,
судової медицини та психіатрії
Харківського національного університету
внутрішніх справ

УДК 343.98

Окремі аспекти використання спеціальних знань у галузі інформаційних і комп'ютерних технологій під час розслідування злочинів у сфері службової діяльності

Сьогодення характеризується суцільними процесами інформатизації та комп'ютеризації в усіх галузях суспільного життя. Причому такі процеси не тільки вдосконалюють діяльність окремих інститутів соціального буття, будучи прогресивними факторами. Ці досягнення науки використовуються й особами під час реалізації їх злочинних намірів. Відповідно злочинна діяльність також використовує досягнення науково-технічного прогресу. Не є винятком і комп'ютерні системи, котрі містять в собі нові, дуже досконалі можливості для невідомих раніше правопорушень, а також для скоєння традиційних злочинів, але нетрадиційними засобами [1, с. 377]. Останнє характерне й для злочинів у сфері службової діяльності.

Злочини у сфері службової діяльності посягають на нормальну роботу та належне функціонування державного апарату, органів місцевого самоврядування, юридичних осіб всіх форм власності, чим і спричиняють колосальні збитки як економічній сфері, так і авторитету держави в цілому. Саме тому особливо актуальним є питання про організацію ефективної діяльності з розслідування зазначеної категорії злочинів. Часто неможливо з'ясувати всі важливі для слідства питання, не звернувшись за допомогою до фахівців у окремих галузях знань – економічних, комп'ютерних технологій тощо.

Тож, у представленому дослідженні приділимо увагу саме використанню спеціальних знань у галузі інформаційних і комп'ютерних тех-

нологій під час розслідування злочинів у сфері службової діяльності.

Характеристика злочинів у сфері службової діяльності й особливості розслідування службових злочинів, у тому числі й питання щодо використання спеціальних знань, досліджувалися в працях таких вітчизняних і зарубіжних вчених як П. Д. Біленчука, Д. А. Бондаренка, А. Ф. Волобуєва, О. О. Дудорова, В. А. Журавля, Г. Б. Перепелиці, М. В. Салтевського, Г. Р. Смолицького, Р. Л. Степанюка, В. Ю. Шепітька, М. П. Яблокова тощо. Але незважаючи на низку сформульованих принципово важливих положень у працях названих учених, залишається ряд невирішених або дискусійних питань. Зокрема, існує потреба у виділенні тактичних особливостей проведення окремих гласних і негласних заходів, спрямованих на дослідження комп'ютерних засобів і комп'ютерної інформації, важливих для ефективного розслідування злочинів у сфері службової діяльності. Саме цим і обумовлюється завдання статті, яке полягає у виділенні особливостей використання спеціальних знань у галузі інформаційних і комп'ютерних технологій у ході розслідування злочинів у сфері службової діяльності.

Представлена на розгляд категорія кримінальних правопорушень характеризується складним механізмом учинення, що знаходить своє відображення в специфічній слідовій картині. Зокрема, переважна кількість доказової інформації знаходиться в різного роду документації – засновницькій, установчій, документах з кадрового забезпечення (наказах, спеціальних дорученнях, трудових контрактах чи договорах, посадових інструкціях, функціональних обов'язках, договорах про матеріальну відповідальність тощо), угодах, чорнових записах, діловій чи особистій переписці та ін. З урахуванням інформаційно-технологічного процесу, в більшості установах для підготовки цих документів, їх зберігання, пересилання тощо використовуються комп'ютерні засоби. Зокрема, багато державних органів, органів місцевого самоврядування, підприємств, установ й організацій всіх форм власності у своїй діяльності користуються електронним документообігом (обігом електронних документів). Під останнім прийнято розуміти сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів [2].

Беззаперечно електронний документ, створений за допомогою засобів автоматизації документообігу, підписаний електронним цифровим підписом і збережений в системі у вигляді файлу відповідного формату, значно спрощує роботу з великими об'ємами інформації. І, природно, що електронний вигляд документів накладає на документообіг певні вимоги. Зокрема, кожен виконавець, залучений у документообіг повинен мати електронний підпис [3]. Відповідно під час кримінального провадження необхідно переконатися у автентичності електронного цифрового підпису. Для цього потрібно отримати тимчасовий доступ до відомчої документації, що визначає порядок присвоєння таких підписів за особою, порядок видачі необхідних ключів. Також доцільно допитати операторів і адміністраторів у якості свідків, попередньо отримавши консультацію у фахівця, можливо навіть із залученням останнього до цих слідчих (розшукових) дій. І, отримавши попередньо весь пакет необхідних матеріалів, слідчий приймає рішення про доцільність призначення комп'ютерно-технічної експертизи.

При цьому, огляд електронного документа безумовно відрізняється своєю тактикою проведення. Остання продиктована формою документа. Електронний документ – це документ, інформація в якому зафіксована у вигляді електронних даних, вклю-

чаючи обов'язкові реквізити документа [2]. Тому слідчий під час огляду електронного документа повинен зафіксувати наявність, зміст і розміщення всіх реквізитів електронного документа. Особливу увагу слід звернути на кількість оригіналів електронного документа та його копій. Оригіналом електронного документа вважається електронний примірник документа з обов'язковими реквізитами, у тому числі з електронним цифровим підписом автора. У разі надсилання електронного документа кільком адресатам або його зберігання на кількох електронних носіях інформації кожний із електронних примірників вважається оригіналом електронного документа. Якщо автором створюються ідентичні за документарною інформацією та реквізитами електронний документ і документ на папері, кожен із документів є оригіналом і має однакову юридичну силу. При цьому варто звірити відповідність їх змісту та форми одне одному. Досліджуючи документ на папері, слідчий перевіряє наявність відмітки про наявність документа в електронній формі. Остання містить повне ім'я файла і його місце зберігання, код оператора та інші пошукові дані. Її ставлять у центрі нижнього краю лицьового боку першого аркуша документа.

Також слідчому потрібно зафіксувати наявність приєднаної до електронного документа (електронних даних) або логічно поєднаної з ним позначки часу. До того ж 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. Також перевіряється наявність супровідної документації – заповненої реєстраційно-контрольної картки в електронній і/чи паперовій формі, повідомлення про прийняття та реєстрацію електронного документа [4, с. 160-161].

Документ, отриманий з інформаційної системи, набирає юридичної сили після того, як його підпише посадова особа в порядку, встановленому законом. Юридична сила документа, який зберігається, оброблюється і передається за допомогою автоматизованих інформаційних і телекомунікаційних систем, може підтверджуватися електронним цифровим підписом. Юридична сила електронного цифрового підпису визнається за наявності в інформаційній системі програмно-технічних засобів, які забезпечують його ідентифікацію, і за умови дотримання встановленого режиму їх використання. Право засвідчити ідентичність електронного цифрового підпису здійснюється на підставі ліцензії [5, с. 6-7].

Електронний цифровий підпис (електронний еквівалент власноручного підпису)накладається за допомогою особистого (закритого) ключа та перевіряється за допомогою відкритого ключа. Останній передається зацікавленій стороні. Відправник повідомлення шифрує його своїм закритим ключем і передає одержувачу по каналах зв'язку. Одержувач дешифрує повідомлення відкритим ключем від правника [6]. У зв'язку із зазначеним слідчому потрібно паралельно перевірити наявність і правильність ведення журналів аудиту щодо подій, пов'язаних із генерацією, використанням і знищенням особистого ключа; порядок і умови розміщення, зберігання, доступу та використання особистого ключа; порядок і умови розміщення, зберігання та доступу до резервної копії особистого ключа; порядок реєстрації (формування сертифіката ключа) центру сертифікації ключів і його відповідність політиці сертифікації та регламенту роботи; порядок і умови зберігання сформованих сертифікатів ключів, а також сертифікатів та документованої інформації, яка підлягає обов'язковій передачі центрами сертифікації ключів у разі припинення їх діяльності; відповідність змісту сформованих сертифікатів установленим законодавством вимогам; факт

і порядок розміщення на електронному інформаційному ресурсі документів та інформації, установлених політикою сертифікації; наявність і правильність ведення журналів аудиту щодо подій, пов'язаних з формуванням, скасуванням, блокуванням і поновленням сертифікатів ключів; функціонування електронного інформаційного ресурсу щодо надання доступу до основних даних (реквізитів) акредитованих центрів, центрів сертифікації ключів, переліку сертифікатів центрів сертифікації ключів, а також інформації про статус сертифікатів [4, с. 161].

Вищезазначене вказує на необхідність залучення до огляду електронних документів відповідних спеціалістів (комп'ютерного техніка чи програміста). Доцільніше залучати в якості спеціалістів тих осіб, які в подальшому будуть проводити відповідні судові експертизи.

Великий масив доказової інформації під час розслідування злочинів у сфері службової діяльності отримується у ході проведення таких слідчих (розшукових) дій як слідчі огляди й обшуки. Плануючи названі заходи, потрібно проаналізувати вихідну інформацію, визначити тактичні завдання, з'ясувати коло об'єктів, що підлягають дослідженню, та методи їх дослідження. Слід усвідомлювати, що інформаційне система не є окремим комп'ютером, а є ланцюгом, який складається з цілої низки ланок. Тому потрібно попередньо з'ясувати зі скількох і яких саме компонентів складається інформаційна система, яка підлягає дослідженню. Зокрема, це можуть бути наступні компоненти: (а) робочі місця користувачів і персоналу інформаційної системи (користувача дисплейного типу з візуальним відображенням інформації; користувача (програмований персональний комп'ютер), який може функціонувати в режимі обміну інформацією зі спряженою ЕОМ і в автономному режимі; оператора, призначеного для налагодження програми; адміністратора, призначеного для управління та контролю за використанням якихнебудь ресурсів); (б) зв'язні компоненти (між мережні мости (шлюзи, центри комутації пакетів, комунікаційні ЕОМ); канали зв'язку з вузлами комутації; апаратура зв'язку типу модем; апаратура зв'язку типу мультиплексом передачі даних; канали зв'язку, виділені й комутовані); (в) допоміжні елементи (приміщення, в яких розміщено зовнішні запам'ятовуючі пристрої великих ЕОМ; приміщення, в яких розміщено пристрої попередньої підготовки даних; сховище машинних носіїв інформації; сховище документів на паперових носіях; службові приміщення користувачів і персоналу інформаційної системи); ЕОМ різного функціонального призначення (центральна ЕОМ (мейнфрейм), яка здійснює основні процедури обробки інформації; сервер чи Host машина; ЕОМ з функціями зв'язної машини, шлюзу, мосту між мережними структурами) [5, с. 13-14].

Розслідування злочинів у сфері службової діяльності неможливе без проведення негласних слідчих (розшукових) дій, серед яких вважаємо за необхідне зосередити увагу на знятті інформації з транспортних телекомунікаційних мереж і електронних інформаційних систем.

Зазначеним заходам, окрім процесуальних і тактичних, притаманні ще й технічні особливості їх проведення. Зокрема, С. В. Андрусенко вказував на складність з технічної точки зору зняття інформації з мережі Інтернет. Вчений зазначив, що важливим аспектом для дотримання принципів повноти й достатності даних та їх всебічного аналізу слідчим або оперативним працівником є розуміння того, за допомогою яких саме засобів або програм відбувається зняття інформації з каналів зв'язку та мережі Інтернет, механізму їх роботи й технічних можливостей [7, с. 182].

Зняти інформацію з каналів зв'яз-ку можна декількома способами

– звернутися з офіційною вимогою надати конкретну інформацію до адміністраторів компаній, провайдерів тощо або самостійно за допомогою фахівців перехопити потрібну інформацію. При цьому, отримуючи дозвіл на проведення вказаних негласних заходів, потрібно враховувати, що право власності і засоби обробки інформації не означає права власності на інформаційні ресурси, які належать іншим власникам [5, с. 7]. Тому у відповідній графі потрібно вказувати інформацію про всіх суб'єктів, права яких негласні заходи будуть обмежувати.

ЩО ж стосується перехоплення інформації, то воно можливе в разі отримання фізичного доступу до джерела її зберігання, за допомогою апаратних і/чи програмних засобів. Перехоплення здійснюється шляхом:

- з'ясування логінів і паролів користувача з інших джерел (за наводкою, дослідивши чорнові записи, прослуховуючи особисті розмови тощо);

- використання штатних засобів встановленої операційної системи;

- використання Trojan ("Троянський кінь") – програми, створеної для знищення, блокування, внесення змін або крадіжки інформації, а також для порушення роботи комп'ютерів чи комп'ютерних мереж. Зазначена програма, як приклад, може спочатку пересилати всю цінну інформацію з комп'ютера користувача, а потім відформатувати жорсткий диск для видалення слідів своєї діяльності.

- використання "сніфферів" на кшталт Mipko Personal Monitor, Lan Detective Internet Monitor, Wireshark, Smartsniff, SearchInform та інших.

На даний час існує широкий спектр уже створених програмних рішень перехоплення запитів до їх виконання системою управління базами даних: UIBSQL Monitor; FBHook; Sinatica Monitorfor Firebird; Jdb Monitor; SQL ServerProfiler [8, с. 65].

Також можливо перехоплювати інформацію з оптоволоконних кабелів.

Окрім того, спеціальні знання можуть і повинні використовуватися у формі отримання консультативної допомоги щодо правильного планування та проведення окремих слідчих (розшукових) заходів. Зокрема, спеціаліста можна допитати стосовно питань, які викликають інтерес і роз'яснення яких дозволить наочніше відобразити як способи вчинення злочинів у сфері службової діяльності, так і технології проведення експертних досліджень з використанням комп'ютерних систем і програм.

І чи не найважливішою і розповсюдженою формою використання спеціальних знань у галузі комп'ютерних та інформаційних технологій під час розслідування вказаних злочинів є проведення відповідних експертиз, а саме – комп'ютерно-технічних. Звичайно й тут існують певні труднощі, з якими може зіткнутися слідчий. Більш детально питання щодо реалізації спеціальних знань у форматі судової експертизи за умов дії нормативно-правових положень чинного Кримінального процесуального кодексу України досліджувала О. Д. Калаянова [9]. Ми ж вважаємо за необхідне вказати тільки на ті труднощі, які пов'язані з неправильним формулюванням експертові питань. Інколи експертові на вирішення ставляться некоректно побудовані питання або питання, що не входять до його компетенції. Також зустрічаються випадки, коли слідчий неправильно визначає вид експертизи, яку потрібно провести для вирішення конкретних питань. Адже нерідко існує потреба в проведенні комплексних експертних досліджень. У випадку розслідування злочинів у сфері службової діяльності мова йде про комплексну комп'ютерну та судово-бухгалтерську експертизу.

Окрім слідчих (розшукових) дій, під час розслідування злочинів у сфері службової діяльності активно застосовуються заходи забезпечення кримінального провадження. Адже компанії у галузі інформаційних тех-

нологій збирають і зберігають деякі дані про своїх користувачів. Як приклад, розглянемо детальніше які компанії й який обсяг даних збирають.

1. Деякі з сайтів компанії Microsoft збирають електронні адреси, імена, домашні чи робочі адреси або телефонні номери, інформацію від веб-браузерів про відвідані сайти, разом з IP-адресами, з зазначенням адреси сайту і часу, коли він був відвіданий. Компанія також користується cookie-файлами, які надають розширену інформацію про перегляд веб-сторінок.

2. Yahoo збирає особисту інформацію при реєстрації для користування продуктами й сервісами компанії та зберігає інформацію з комп'ютерів користувачів, в тому числі IP-адреси.

3. Щоб користуватися аккаунтами Google, необхідно зареєструватись, зазначивши особисті дані. Електронна пошта від компанії Google – Gmail – зберігає електронні контакти і ланцюжки повідомлень для кожного аккаунта (обсягом до 10 Гб). Також зберігаються пошукові запити, IP-адреси, журнал телефонних викликів і cookie-файли, що разом складають унікальний профіль користувача. Сеанси чату також записуються, якщо користувач не вибере опцію "не зберігати чат".

4. Facebook вимагає особисті дані під час реєстрації; сервіс також зберігає оновлення статусу, опубліковані фото і відео, записи на "стін", коментарі до записів інших, повідомлення і розмови у чаті. Записуються й імена друзів, а також електронні адреси тих друзів, якщо вони вказали їх у своєму профілі. Зберігаються теги, якими можна позначати себе або друзів, і дані GPS або інші географічні відомості.

5. Користувачі Paltalk повинні надати компанії свою контактну інформацію, включно з електронною адресою. Компанія застосовує cookie-файли, щоб відстежувати поведінку користувачів з метою цілеспрямованої реклами.

6. Сервіс You Tube належить компанії Google, а отже, застосовує ті ж методи збору даних.

7. Skype – це частина компанії Microsoft. Під час реєстрації користувачі надають особисті дані, включно зі справжнім іменем, іменем користувача, адресою. Зберігаються списки контактів і географічні координати з мобільних пристроїв. Миттєві повідомлення, голосова пошта і відеоповідомлення зберігаються зазвичай від 30 до 90 днів, хоча користувачі можуть подовжити термін зберігання миттєвих повідомлень.

8. Компанія Aol теж зберігає особисті дані, надані користувачами при реєстрації.

9. Користувачі, що хочуть отримати Apple ID – ідентифікаційний запис, необхідний для користування iTunes та реєстрації пристроїв – повинні надати особисті дані, в тому числі ім'я, адресу, електронну адресу, номер телефону. Компанія також збирає дані про людей, з якими користувачі Apple діляться контентом, зокрема їхні імена й електронні адреси [10].

Тож, до зазначених компаній (їх представництв) можна звернутися із офіційними запитами задля отримання тимчасового доступу до інформації, яка має значення для розслідування злочинів у сфері службової діяльності.

Також під час розслідування окресленої категорії злочинів потрібно з'ясувати чи з боку керівництва юридичної особи (від якої потрібно отримати доказову інформацію) не ведеться контроль за своїми підлеглими з метою забезпечення інсайдерської безпеки за допомогою DPL-систем (DataLeakPrevention). У разі використання останніх – слід отримати доступ до збереженої інформації задля її дослідження.

Отже, вищевикладене дозволяє дійти висновків, що під час проведення гласних і негласних слідчих (розшукових) дій, спрямованих на виявлення, фіксацію, вилучення та

подальше дослідження комп'ютерних систем, програмного забезпечення й іншої комп'ютерної інформації, обов'язково потрібно залучати спеціалістів у галузі знань комп'ютерних технологій та інформаційної безпеки. Це пояснюється тим, що для здійснення безпечних для комп'ютерної інформації маніпуляцій потрібні спеціальні знання. Адже тільки фахівець може правильно дослідити зазначені об'єкти, а за необхідності своєчасно й адекватно зреагувати на "підготовлені пастки-сюрпризи" задля недопущення пошкодження та/чи знищення доказової інформації, необхідної для своєчасного, якісного й ефективного розслідування злочинів, зокрема в сфері службової діяльності.

Список використаних джерел

1. *Біленчук П. Д.* Криміналістика. Кредитно-модульний курс : [підручник] / П. Д. Біленчук, Г. С. Семаков; за ред. П. Д. Біленчука. – 4-те вид., змін., допов. і доопр. – К. : ВД "Дакор", 2014. – 520 с.

2. *Про* електронні документи та електронний документообіг : закон України від 22.05.2003 № 851-IV // Відомості Верховної Ради України. – 2003. – № 36. – Ст. 275.

3. *Електронний* документ – єдиний механізм по роботі з документами [Електронний ресурс]. – Режим доступу : http://www.ca.upg.kiev.ua/info/ecp/workflow/index.php

4. *Пчеліна О. В.* Особливості огляду електронного документа / О. В. Пчеліна // Актуальні питання розслідування кіберзлочинів : [матеріали Всеукр. наук.-практ. конф., м. Харків, 10 груд. 2013 р.] / МВС України, Харк. нац. ун-т внутр. справ. – Х. : ХНУВС, 2013. – С. 159-161.

5. *Кузьменко Б. В.* Захист інформації. Організаційно-правові засоби забезпечення інформаційної безпеки : [навчальний посібник] / Кузьменко Б. В., Чайковська О. А. – К., 2009. – 83 с.

6. *Крівопалов Д. В.* Безпека електронної комерції // ALLS.IN.UA [Електронний ресурс]. – Режим доступу : http://alls.in.ua/22383-bezpeka-elektronno-komerci.html

7. *Андрусенко С. В.* Процесуальні й технічні аспекти зняття інформації з мережі Інтернет / С. В. Андрусенко, Г. С. Романюк // Південноукраїнський правничий часопис. – 2010. – № 3. – С. 181-183.

8. *Костенко П. П.* Програмне забезпечення автоматичного перехоплення SQL-запитів до їх виконання системою управління базами даних / П. П. Костенко, М. І. Гученко, В. В. Стовба, О. Г. Славко // Вісник КрНУ імені Михайла Остроградського. – 2012. – Випуск 2 (73). – С. 64-69.

9. *Калаянова О. Д.* Експертні інституції в сучасних умовах кримінальних проваджень / О. Д. Калаянова // Південноукраїнський правничий часопис. – 2014. – № 2. – С. 119-121.

10. *Як* американські спецслужби збирають відомості? // Українська правда [Електронний ресурс]. – Режим доступу : http://www.pravda.com.ua/inozmi/bbc/2013/11/5/7001427/view_print/?attempt=1

Пчеліна О. В. Окремі аспекти використання спеціальних знань у галузі інформаційних і комп'ютерних технологій під час розслідування злочинів у сфері службової діяльності

У статті вказується на обумовленість слідової картини злочинів у сфері службової діяльності складним механізмом їх учинення. Як джерело доказової інформації

виділяється комп'ютерна інформація. Автором виділені особливості використання спеціальних знань у галузі інформаційних і комп'ютерних технологій під час розслідування злочинів у сфері службової діяльності.

Ключові слова:спеціальні знання, інформаційні та комп'ютерні технології, злочини у сфері службової діяльності

Пчелина О. В. Отдельные аспекты использования специальных знаний в отрасли информационных и компьютерных технологий во время расследования преступлений в сфере служебной деятельности

В статье указывается на обусловленность следовой картины преступлений в сфере служебной деятельности сложным механизмом их делания. Как источник доказательной информации выделяется компьютерная информация. Автором выделены особенности использования специальных знаний в отрасли информационных и компьютерных технологий во время расследования преступлений в сфере служебной деятельности.

Ключевые слова: специальные знания, информационные и компьютерные технологии, преступления в сфере служебной деятельности

Pchelina O. Some aspects of the use of specialized knowledge in the field of information and computer technologies during investigation of crimes relatedservice activity

The conditionality of track picture of crimes related serviceactivity bycomplicated mechanism of difficult mechanism of their doing. As a source of evidence-based information allocated computer information. The author highlights the features of the use of specialized knowledge in the field of information and computer technologies during the investigation of crimes related serviceactivity.

Key words: thespecialknowledge, informationandcomputer technologies, crimes related serviceactivity