

кож на практиці трапляються непоодинокі випадки зловживання особами своєю службовим становищем.

Тому враховуючи вище сказане, доцільно було б частину першу ст.7–2 КПК викласти таким чином: «Прокурор, а також слідчий за згодою прокурора за наявності підстав, зазначених у ст.45 Кримінального кодексу України, направляють своєю мотивованою постановою кримінальну справу до суду для вирішення питання про звільнення обвинуваченого від кримінальної відповідальності». Таке визначення частини першої статті 45 КК буде слугувати ще однією законодавчою гарантією особам, які вперше скоїли злочин невеликої тяжкості, щиро розкаялися, активно сприяли розкриттю злочину. Обов'язкове закриття кримінальних справ за наявністю підстав, передбачених ст.45 КК, буде сприяти ефективності кримінального судочинства, заощадженню матеріально-часового ресурсу насамперед органів досудового слідства, та повному відшкодуванню завданих потерпілій стороні збитків або усуненню заподіяної шкоди.

Слід наголосити, що широке використання інституту дійового каяття не тільки реально захищає інтереси особи, яка скоїла злочин і щиро розкалася в ньому, а й відповідає інтересам держави. Тому розширення комплексу правових гарантій застосування цього інституту потребує законодавчого закріплення.

У випадку ж відсутності реальних правових гарантій для осіб на звільнення від відповідальності навряд чи можна прогнозувати реальну життєздатність та ефективність цього інституту.

Список літератури: 1.Житний О.О. Умови звільнення від кримінальної відповідальності у зв'язку з дійовим каяттям // Вісник Національного університету внутрішніх справ. 2002. Вип.18. 2. Аликперов Х. Новый УК: проблемы освобождения от уголовной ответственности // Законность. 1999. №4. 3. Курс советского уголовного права. Часть общая. Л., 1970. Т.2; Кригер Г.А. Наказание и его применение. М., 1962. 4. Горелик И.И. Наказание и его назначение., Минск, 1978. 5.Чечель Г.И. Смягчающие ответственность обстоятельства и их значение в индивидуализации наказания. Саратов, 1978.

Надійшла до редколегії 13.06.03

В.М. Стратонов, С.О. Захарченко

СЛІДЧІ ОГЛЯДИ У ЗЛОЧИНАХ, СКОЄНИХ З ВИКОРИСТАННЯМ КОМП'ЮТЕРНОЇ ТЕХНІКИ

Масова комп'ютеризація всіх сфер життя суспільства призвела до розвитку ринку комп'ютерів та програмного забезпечення, підвищення професійної підготовки користувачів, збільшення потреб в удосконаленні технології обробки даних, значно розширила сферу застосування ЕОМ, які все частіше підключаються до мереж широкого доступу.

Одним із наслідків цих процесів стала криміналізація сфери обігу комп'ютерної інформації. Злочини в сфері комп'ютерної інформації, незважаючи на їх незначну питому вагу у загальній структурі злочинності, складають реальну загрозу національній безпеці країни, оскільки вони все

більше набувають транснаціонального організованого характеру, а спричинена ними шкода іноді не піддається підрахунку.

Огляд об'єктів у справах вказаної категорії злочинів є одним з найважливішим інструментаріїв встановлення обставин розслідуваної події.

Огляд місця події – це невідкладна слідча дія, направлена на встановлення, фіксацію та дослідження обстановки місця події, слідів злочину та інших фактичних даних, які дозволяють в сукупності з іншими доказами зробити висновок про механізм злочину та інші обставини злочину. Звідси й випливає значення огляду місця події для подальшого розслідування та розкриття злочинів, пов'язаних з комп'ютерними технологіями.

Перш за все огляд місця події – це слідча дія, направлена на встановлення, фіксацію та дослідження обстановки місця події, слідів злочину та інших фактичних даних, які мають значення для справи.

М.С. Строгович зазначав зокрема, що в момент самого огляду зазвичай не можна знати цілком достовірно, що з виявлених обставин у процесі подальшого розслідування набуде суттєвості, а що втратить свою значимість. Тому слід фіксувати все, що може мати значення, пам'ятаючи, що краще зафіксувати несуттєві обставини, чим упустити обставини важливі, потрібні для встановлення істини.

Тому останнім часом почали з'являтися рекомендації для слідчого щодо порядку проведення слідчих дій, пов'язаних з оглядом, виїмкою і підготовкою персональних комп'ютерів, периферійних пристроїв та інших комп'ютерно-технічних засобів до відправлення на експертизу. Такі рекомендації мають різноплановий, більш того, протилежний характер.

Основним завданням огляду місця події при вчиненні злочинів даної категорії є пошук інформації, яка містяться на комп'ютерному носії. Для того, щоб вилучити таку інформацію в повному обсязі і не пошкодити її, пропонуються різні рекомендації. Так, М.О. Селіванов та І. Дворкін вказують на те, що слідчому при пошуку, фіксації і вилученні речових доказів корисно мати при собі дискети для копіювання на них інформації, яка міститься в комп'ютері, а також дискету з набором сервісних програм, підбір яких може провадитися в ході нагромадження досвіду розслідування кримінальних справ розглянутої категорії і в міру створення нових, більш досконалих програм [1].

Рекомендований мінімальний набір включає сервісні програми, що забезпечують визначення властивості і якостей комп'ютера, перевірку справності окремих пристроїв і зовнішньої пам'яті. Крім того, для роботи з комп'ютером слідчому корисна будь-яка програма, яка дозволяє працювати з інформацією на твердому диску комп'ютера.

На думку В.А. Коршенка та В.М. Стратонові, такий підхід є абсолютно невірним і неприйнятним, тому що властивості найбільш розповсюдженого програмного забезпечення комп'ютерів дозволяють зробити висновок про заборону в категоричній формі будь-яких маніпуляцій з комп'ютерною технікою на місці події [2].

Ми вважаємо, що обидві пропозиції заслуговують на увагу й використання у роботі слідчого. Але застосовувати ту чи іншу рекомендацію пот-

рібно у кожному конкретному випадку, враховуючи думку спеціаліста з комп'ютерної техніки, який обов'язково повинен залучатися до огляду місця події при розслідуванні злочинів даної категорії.

Огляд місця події варто почати з вживання заходів щодо запобігання приховування злочинцем своїх дій з машинною інформацією. Для цього необхідно виключити можливість доступу до такої техніки всіх осіб, які працюють на об'єкті, вимкнути всі комп'ютери. Якщо зробити це не вдається через особливості функціонування системи, то потрібно вжити заходів для запобігання поширення шкідливих програм.

Для забезпечення збереження інформації на комп'ютерах необхідно забезпечити контроль за енергопостачанням об'єкта, що оглядається. У випадку, якщо на момент початку огляду електропостачання об'єкта виключене, то до його відновлення варто відключити від електромережі всі комп'ютери та периферійні пристрої, що знаходяться на об'єкті.

На думку В.А. Коршенка, друга розповсюджена помилка – це рекомендація «коректного» вимикання комп'ютера, який був виявлений на місці проведення слідчої дії у ввімкненому стані. Так, А.Н. Яковлев стверджує, що фіксація «комп'ютерних» слідів злочину можлива тільки за допомогою коректного завершення функціонуючих програм, вимикання комп'ютера і кваліфікованого рішення завдання щодо визначення комплексу комп'ютерної техніки або окремих компонентів, які підлягають вилученню слідчим [3].

Під «коректним завершенням» слід розуміти завершення конкретної запусненої програми і вимикання комп'ютера шляхом натискання клавіші «Живлення» («Power»). Але необхідно врахувати, що вимикання комп'ютера шляхом натискання на кнопку «Живлення» є неправильним, тому що в корпусах форм-фактора АТХ вона програмована. Користувач може запрограмувати вказану кнопку на виконання будь-якої дії, що повністю або частково знищить інформацію.

Ми погоджуємося з думкою А.В. Коршенка, який зазначає, що при виявленні комп'ютера на місці проведення слідчих дій у включеному стані потрібно негайно вимкнути його і периферійні пристрої від мережі електроживлення шляхом розірвання з'єднань. Таку ж пораду дає і Р.С. Белкін, зазначаючи, що слід не відключати тумблер блоку живлення, а витягнути вилку з розетки. Але перед цим екран дисплею та з'єднання кабелів потрібно сфотографувати [4].

Щоб запобігти зазначеним та іншим помилкам у процесі проведення слідчих дій, ми рекомендуємо залучати фахівця в галузі комп'ютерних технологій на всіх етапах розслідування злочинів, пов'язаних з використанням комп'ютерної техніки. А щоб цей процес був найбільш ефективним, слід залучати постійний контингент фахівців, з якими доцільно укласти угоду про співпрацю та оплату даної роботи. На цьому наголошують і російські криміналісти, до того ж вони взагалі пропонують використовувати допомогу спеціалістів в процесі інших слідчих оглядів [5, с.7].

Також під час підготовки до огляду потрібно вирішити питання про його матеріально-технічне забезпечення. Слідчий і фахівець можуть засто-

сувати як традиційні техніко–криміналістичні засоби виявлення, попереднього дослідження, вилучення і фіксації слідів, так і спеціальну техніку, спеціальне програмне забезпечення для доступу, зчитування і збереження комп'ютерної інформації.

Коли встановлено підозрюваного, то затримання слід проводити негайно, унеможливити доступ до комп'ютерних засобів, здійснити огляд та обшук робочого місця, а також обшук за місцем проживання. Під час огляду слід звернути увагу на наявність комп'ютера, ліній та засобів зв'язку, які злочинець використав для проникнення в комп'ютерну мережу. При особистому обшуку треба вилучити пейджер, стільниковий телефон, пристрій для встановлення транспортного засобу під охорону, а також інші пристрої дистанційного електричного керування, які здатні подавати радіосигнали та за допомогою яких злочинець може знищити в своєму або чужому комп'ютері сліди, котрі він залишив при несанкціонованому проникненні. Дискети, диски, чорнові записи програм, журнали реєстрації роботи на комп'ютері та деякі інші документи підлягають вилученню. Не рекомендується дозволяти затриманому самостійно користуватися засобами зв'язку. Він може знищити необхідні докази.

Виявлення, огляд та вилучення комп'ютерних засобів можуть проводитися не тільки під час слідчого огляду (ст.190 КПК України), але й у ході інших слідчих дій, наприклад, обшуку (ст.178 КПК України), виїмки (ст.179 КПК України), при відтворенні обстановки та обставин події (ст.194 КПК України), організаційних заходах під час попередньої перевірки повідомлень та заяв про ознаки злочину.

Проведення слідчої дії потребує ретельної підготовки, зумовленої особливостями комп'ютерних засобів. Слід пам'ятати, що приміщення та комп'ютерні засоби, як правило, знаходяться під надійною електронною охороною і один хибний крок може призвести до непоправних наслідків. Наприклад, інформація на вінчестері може бути знищена автоматично при: а) розкритті кожуха комп'ютера, б) відчиненні кімнати, де знаходиться комп'ютер; в) за інших обставин, відомих лише керівникові підприємства (фірми). У практиці застосовуються такі способи знищення інформації, що зберігається в комп'ютері: дистанційний (по локальній мережі); контактний (натиснення на кнопку тривоги); мовний (передача усного повідомлення телефоном на пейджер, який знаходиться в комп'ютері); електронно–хвильовий (застосування пристрою «брелок»).

Тому запропоновані рекомендації призначені для слідчих, дізнавачів, щоб кваліфіковано проводити слідчий огляд, обшук та виїмку комп'ютерних засобів. Для того, щоб одержати оптимальні результати, до участі в слідчій дії відповідно до ст.1281 КПК України необхідно обов'язково залучити спеціаліста з знаннями комп'ютерної техніки.

Щодо тактики слідча дія має три етапи: підготовчий, робочий та заключний, ці етапи детально розроблені М.В.Салтєвським [6, с.32].

Підготовчий етап потребує виконання низки дій:

1. У керівника підрозділу, особи, яка відповідає за експлуатацію комп'ютерної техніки, або іншого співробітника організації, фірми необхідно

взяти пояснення, а якщо кримінальну справу порушено, то допитати їх та з'ясувати такі обставини:

а) чи заблоковано приміщення, в якому знаходиться комп'ютер, електронною системою допуску або охоронною сигналізацією та які технічні засоби забезпечення використовуються для цього. Оскільки систему блокування обирає користувач, необхідно витребувати на неї документацію та відповідний електронний або фізичний пароль (код), а в деяких випадках – і додатковий пристрій (електронний ключ) для доступу до об'єктів, що охороняються. При цьому слід пам'ятати, що електронне блокування приміщення з'єднано з системою блокування самознищення важливої інформації в комп'ютері, яка працює від вмонтованого в комп'ютер джерела живлення. У разі порушення встановленого порядку входу в приміщення спрацьовує захист і комп'ютер знищує інформацію на вінчестері, навіть якщо він відключений від мережі живлення. Фірми, які застосовують подібні системи знищення важливої інформації на комп'ютері, обов'язково мають надійно захвану щоденну копію цієї інформації або використовують «дзеркальний» вінчестер, який знаходиться на значному віддаленні від основного та під особливою охороною. Зміст «дзеркального» є точною копією основного вінчестера, будь-які зміни в якому простежуються щосекундно;

б) які є засоби зовнішньої охоронної сигналізації та внутрішньої безпеки інформації, що знаходиться в комп'ютері;

в) чи встановлено спеціальні засоби в комп'ютері для знищення інформації у разі спроби несанкціонованого доступу до неї (з'ясувати місце знаходження організації, яка встановила цю систему);

г) чи є необхідним пароль (додатковий пристрій – електронний ключ) для доступу до інформації (окремих задач, областей даних тощо), яка знаходиться в комп'ютері, чи й до окремих частин; які правила його застосування; чи спричиняє порушення цих правил пошкодження інформації;

д) чи з'єднані (включені) комп'ютери в локальну мережу підприємства (фірми), об'єднання; яка схема локальної мережі, основні правила її безпечного використання;

е) чи проводилося обов'язкове резервне копіювання даних з введенням повного протоколу роботи комп'ютера за день; чи є протоколи роботи комп'ютера протягом дня, у яких відповідальних осіб вони знаходяться.

2. Якщо комп'ютер підключено до мережі ІНТЕРНЕТ (ІНТРАНЕТ), то попередньо необхідно вилучити договори у керівника підприємства (фірми), де буде проводитися огляд, негайно зв'язатися з мережевим адміністратором–провайдером вузла, до якого підключено дане підприємство (фірма), та організувати за його допомогою вилучення і зберігання електронної інформації, яка належить підприємству (фірмі) або надійшла на його адресу.

3. Вилучити та вивчити документацію, пов'язану з забезпеченням безпеки комп'ютерної інформації на підприємстві (фірмі), що становить інтерес для слідства; вилучити протоколи та резервні копії на вінчестері. За наявності протоколів можна відновити вилучену (стерту) інформацію на вінчестері (магнітному носії).

4. Перед тим, як безпосередньо приступити до огляду, слідчий ознайомлює спеціаліста з поясненнями чи протоколами допитів, вилученою документацією та копіями. Складається та обговорюється план проведення огляду (як безпечно для збереження комп'ютерної інформації ввійти в приміщення, як відключити комп'ютери від мережі, як зупинити їх роботу тощо).

Робочий етап огляду починається з усунення блокування вхідних дверей. Слідчий пропонує спеціалісту, який входить до складу слідчо-оперативної групи, виконати дії, спрямовані на недопущення пошкодження інформації. Ззовні, наприклад, по модемному, пейджерному чи радіозв'язку. Для цього необхідно:

а) відсторонити співробітників підприємства (фірми) від комп'ютерних засобів та розмістити їх у приміщенні, в якому виключено використання будь-яких засобів зв'язку.

б) у процесі огляду не приймати допомоги від співробітників підприємства (фірми);

в) вилучити у персоналу пейджери, електронні записні книжки, «ноутбуки», індивідуальні пристрої вимкнення сигналізації автомобіля тощо;

г) зафіксувати інформацію на екранах працюючих комп'ютерів фотографуванням чи складанням креслення;

д) вимкнути живлення міні-АТС та опечатати її;

е) скласти схему підключення зовнішніх кабелів до комп'ютерних пристроїв та позначити кабелі для правильного відтворення з'єднання у подальшому;

є) ізолювати комп'ютери від будь-якого зв'язку ззовні: модемного, комп'ютерної мережі, радіозв'язку;

ж) відключити всі комп'ютерні засоби від джерел живлення (у тому числі й від безперебійних джерел);

з) екранувати системний блок комп'ютера в спеціальний футляр.

Водночас із діями спеціаліста слідчий візуально фіксує загальну картину місця події, фотографує загальний вигляд обстановки (оглядова зйомка), організує охорону приміщення та спостереження за переміщенням осіб – співробітників підприємства (фірми). Фіксує вузловою зйомкою місце розташування та зовнішній вигляд комп'ютерних засобів.

Спеціаліст тим часом оперативно виконує дії згідно з планом, розробленим слідчим. Зовнішнім оглядом установлюються такі специфічні обставини стосовно комп'ютерних засобів, які заносяться до протоколу:

а) склад комп'ютерного засобу: наявність системного блоку, монітора, клавіатури, принтера, модему, безперебійного джерела живлення, колонок та інших периферійних пристроїв;

б) розташування пристроїв на передній панелі системного блоку; наявність та види пристроїв зберігання інформації (дисків), а також пристроїв зчитування кредитних та парольних карт (особливо відмічається наявність невідомих йому пристроїв, наприклад, для знищення інформації);

в) розташування роз'єднань на задній панелі системного блоку, наявність та види вмонтованих пристроїв, мережевої плати, модему (відмічається, чи був він підключений до телефонної або іншої лінії зв'язку); наяв-

ність портів послідовного та паралельного каналів (зазначається, чи були вони підключені до зовнішніх ліній зв'язку).

Завершальний етап огляду включає складання протоколу, схем, плану. Кабелі, що вимикаються, підлягають маркіруванню з метою відтворення з'єднання при провадженні наступної комп'ютерно-технічної експертизи. Екранований системний блок комп'ютера, принтер, виявлені дискети, магнітні стрічки та інші носії комп'ютерної інформації (наприклад, роздруковки) вилучають та опечатують, що зазначається у протоколі.

У протоколі слідчої дії підлягають обов'язковому опису:

1) системний блок:

- розміри блоку;
- найменування фірми-виготівника, модель, марка; ідентифікаційний номер.

2) принтер:

- розміри;
- найменування фірми-виготівника, модель, марка;
- ідентифікаційний номер.

3) модем:

- розміри;
- найменування фірми-виготівника, модель, марка;
- ідентифікаційний номер;

4) гнучкі магнітні диски (дискети):

- розміри та тип;
- найменування фірми-виготівника;
- фірмові та рукописні написи на наклейках (у разі їх наявності).

Список літератури: Селиванов Н.А., Дворкин И. Пособие для следователей. М., 1998; Салтвевский М.В. Селиванов Н.А., Дворкин И. Пособие для следователей. М., 1998; Рябов О.А. Проблемы огляду місця події по злочинах, скоєних з використанням комп'ютерної техніки // Вісник Нац. ун-ту внутр.справ. Вип.18. 2002. 2. Корщенко В.А. Деякі особливості поводження з комп'ютерними засобами під час проведення слідчих дій // Вісник Нац. ун-ту внутр.справ. Вип. 18. 2002. 3. Яковлев А.Н. Использование специальных познаний при расследовании «компьютерных» преступлений // Конфидент. 2000. № 6. 4. Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р. Криминалистика: Учебник для вузов / Под ред. Р.С. Белкина. М., 2001. 5. Белозерова И.И. Следственный осмотр документов и помещений при расследовании преступлений, связанных с незаконной предпринимательской деятельностью // Российский следователь. 2001. №2. 6. Салтвевский М.В. Основы методики розслідування злочинів, скоєних з використанням ЕОМ // Навчальний посібник. Х., 2000.

Надійшла до редколегії 08.08.03

А.С. Корж

КРИМІНАЛІСТИЧНА ТАКТИКА: МОРАЛЬНО-ЕТИЧНИЙ АСПЕКТ

Протягом багатьох століть юристи зверталися до моральних основ діяльності органів правосуддя, намагаючись з цих позицій підійти до рішен-