УДК 343.147 : 336.7 : 004 (477)

ТАКТИЧНІ ОСОБЛИВОСТІ ПРОВЕДЕННЯ ОГЛЯДУ МІСЦЯ ПОДІЇ ПРИ РОЗСЛІДУВАННІ ЗЛОЧИНІВ, ВЧИНЕНИХ У БАНКІВСЬКІЙ СИСТЕМІ УКРАЇНИ З ВИКОРИСТАННЯМ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Поливанюк В.Д., к.ю.н., ст. викладач

Запорізький юридичний інститут
Дніпропетровського державного університету внутрішніх справ

У статті автор висвітлює питання щодо особливостей проведення огляду місця події при вчиненні злочинів у банківській системі України з використанням сучасних інформаційних технологій та складу слідчо-оперативної групи для проведення даної слідчої дії.

Ключові слова: огляд місця події, слідчо-оперативна група, інформаційні технології, банківська система.

Поливанюк В.Д. ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ПРОВЕДЕНИЯ ОСМОТРА МЕСТА ПРОИСШЕСТВИЯ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ В БАНКОВСКОЙ СИСТЕМЕ УКРАИНЫ С ИСПОЛЬЗОВАНИЕМ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ / Запорожский юридический институт Днепропетровского государственного университета внутренних дел Украины, Украина

В статье автор раскрывает вопросы, связанные с особенностями проведения осмотра места происшествия при совершении преступлений в банковской системе Украины с использованием современных информационных технологий и состава следственно-оперативной группы для проведения данного следственного действия.

Ключевые слова: осмотр места происшествия, следственно-оперативная группа, информационные технологии, банковская система.

Polyvanyuk V.D. TACTICAL FEATURES OF THE REVIEW OF CRIME SCENE WHILE INVESTIGATING CRIMES COMMITTED IN THE BANKING SYSTEM OF UKRAINE WITH USING MODERN INFORMATION TECHNOLOGIES / Zaporizhzhya law institute of the Dnepropetrovsk state university of internal affairs of Ukraine, Ukraine

The author reveals the issues related to the specifics of the examination of the scene of crimes in the banking system of Ukraine, using modern information technologies and staff of special operation and investigation group to conduct the investigative action.

Key words: the examination of the scene of crime, special operation and investigation group, information technologies, banking system.

Першочерговим, основоположним і найбільш розповсюдженим заходом при виявленні злочину є слідчий огляд (п.1 ст.190 КПК України). Це невідкладна слідча дія, що полягає в безпосередньому сприйнятті, дослідженні, оцінці і фіксації дізнавачем (слідчим) обстановки місця події, слідів та об'єктів, які мають відношення до справи, їх ознак, властивостей, станів та взаємозв'язків з метою з'ясування суті події, що сталася, механізму злочину і його обставин, які мають значення для встановлення істини по справі [1, 18]. Слідчий огляд являє собою цілеспрямовану діяльність, що має бути належним чином організована і спланована. Планування і організація слідчої діяльності виступають як тактичні прийоми [2, 151].

Огляд місця уособлює єдиний процес, тому він обов'язково повинен бути завчасно продуманий, виважений та підготовлений. Огляд – сама «продуктивна» дія, що дозволяє установити великий обсяг доказів, які відносяться до всіх сторін складу злочину – об'єкта, об'єктивної сторони, суб'єкта та суб'єктивної сторони; найскладнішого, яке потребує застосування певних тактичних прийомів і засобів криміналістичної техніки [3]. Таким чином, слідчий може проводити: огляд місця події, місцевості, приміщень, предметів та документів з метою виявлення та фіксації різних матеріальних об'єктів, а на них слідів, що імовірно мають відношення до справи, а, також, їхніх ознак, станів тощо. При розслідуванні комп'ютерних злочинів слідчий огляд має проводитися на місці:

- збереження й обробки комп'ютерної інформації, підданої злочинному впливу (наприклад, у разі незаконного втручання в роботу ЕОМ (комп'ютерів), їх систем чи комп'ютерних мереж);

- знаходження комп'ютерного обладнання, яке використовувалося при вчиненні злочину (наприклад, у разі розповсюдження комп'ютерного вірусу після незаконного проникнення в комп'ютерну мережу);

- збереження інформації, отриманої злочинним шляхом (наприклад, у разі заволодіння комп'ютерною інформацією шляхом викрадення, привласнення, вимагання, шахрайства чи зловживання службовим становищем);

- порушення правил експлуатації ЕОМ, комп'ютерної системи або мережі;

- настання шкідливих наслідків (знищення, блокування, модифікації, копіювання комп'ютерної інформації, порушення роботи комп'ютера, комп'ютерної системи або мережі [4, 77-78].

Як і при традиційних видах злочинів, так і в злочинах з інформаційними технологіями, слідчі дії здійснюються в три етапи: підготовчий, робочий (дослідний) та заключний. Кожний з них вимагає продуманості, злагодженості та логічної послідовності.

Підготовчий етап:

На нашу думку, підготовчий етап має складатися з двох стадій: до виїзду на огляд та дії на місці події до початку робочого етапу.

Перша стадія – до виїзду на місце події. Враховуючи специфіку розслідування злочинів з інформаційними технологіями, слідчому необхідно до виїзду на місцевість ознайомитися з матеріалами справи, які були йому надані як вихідна інформація. Але йому одному досить важко та навіть і неможливо справитися з таким обсягом робіт щодо опанування масиву криміналістично-значущої інформації за короткий проміжок часу. Тому з метою оперативності та ефективності підготовчої стадії до виїзду на слідчу дію до справи долучається оперативний працівник, одним із завдань якого буде проведення таких заходів:

- установити місцезнаходження засобів електронно-обчислювальної техніки (у подальшому – ЗЕОТ), комп'ютерної інформації та документів, що використовувалися під час підготовки, здійснення і приховування злочину, а також інших можливих предметів, які мали відношення до протиправної дії;

- при визначенні місця, де знаходяться ЗЕОТ і комп'ютерна інформація, за допомогою яких було здійснено правопорушення, провести оперативну установку з метою: а) виявити їх власника чи користувача або осіб, що допущені до програмного забезпечення; б) можливості процесуального вилучення комп'ютерної інформації;

- з'ясувати схематичний план місця (приміщення, ділянки місцевості, де буде проводитися слідча дія), також місцерозташування технічних засобів та їх кількість;

- встановити режим роботи об'єкта, де проводитиметься слідча дія, кількісний та персональний склад працюючих та допущених до операційної системи тощо.

Як уже зазначалося вище, на підставі отриманих даних слідчий спільно з оперативним працівником складає відповідний план проведення заходів щодо організації та ефективного проведення зазначених дій. Зосередити увагу на оптимальному варіанті формування слідчо-оперативної групи основного складу, а також тих, хто має сприяти в організації слідчої дії (консультанти, технічні оператори та ін.).

Вивчення криміналістичної літератури свідчить про те, що в цей час відсутні чіткі рекомендації щодо факультативного складу слідчо-оперативної групи (СОГ) у справах про злочини, вчинені в банківській системі з використанням сучасних інформаційних технологій. Акцентуючи увагу на цій обставині й беручи за основу методологічний підхід, запропонований В.Б. Вєховим [5, 30-31], слід запропонувати наступні методичні рекомендації щодо удосконалення діяльності СОГ.

Для проведення огляду місця події у справах про злочини в банківській сфері, які вчинені з використанням комп'ютерної інформації, залежно від конкретної слідчої ситуації до складу СОГ повинні входити наступні особи:

обов'язкові учасники – слідчий, що спеціалізується на розслідуванні кримінальних справ виділеної категорії (керівник СОГ); оперативні співробітники (КР, БЕЗ, податкової міліції, СБУ), працівники дізнання, що спеціалізуються на виявленні й розкритті злочинів розглянутої категорії; поняті (не менш двох осіб);

факультативні учасники – спеціаліст-криміналіст, що знає особливості роботи зі слідами по злочинах даної категорії; спеціаліст із ЗЕОТ конкретного виду; спеціаліст із мережевих технологій (у випадку наявності на місці події периферійного обладнання віддаленого доступу або локальної комп'ютерної мережі); спеціаліст із систем зв'язку (при використанні для дистанційної передачі даних каналів електрозв'язку); бухгалтер-ревізор конкретного профілю, що знає особливості електронного документообігу, або, як мінімум, користувач ЕОМ; спеціаліст ДНДЕКЦ або науково-дослідного інституту судових експертиз, співробітник оперативно-технічного підрозділу або приватної охоронної структури по профілю встановленого спеціального технічного пристрою; інспектор служби охорони або служби безпеки об'єкта, що оглядається, (у випадку, коли місце події або ЗЕОТ, що перебуває на ньому, одночасно є охоронюваним об'єктом).

При необхідності для участі в огляді місця події можуть бути запрошені й інші незацікавлені в справі спеціалісти, які знають специфіку роботи об'єкта, що оглядається, (предмета), а саме: інженери-електрики, спеціалісти супутникових систем зв'язку, оператори комп'ютерних систем і мереж (стільникових, пейджингових, Інтернет тощо).

Підбір понятих, що беруть участь у проведенні слідчого огляду місця події, ЗЕОТ, комп'ютерної інформації й «електронного» документа, а також при проведенні обшуку або виїмки з метою їхнього вилучення, доцільно здійснювати на підготовчому етапі до початку проведення слідчої дії із числа осіб, по-перше, не зацікавлених у справі, по-друге, що мають хоча б загальне уявлення про предмет, що вилучається або оглядається [6, 38].

Завершуючи першу стадію підготовчого етапу огляду місця події, слідчий повинен визначити, які техніко-криміналістичні засоби будуть використовуватися при огляді, і впевнитися в їхній комплектності й справності. Аналіз практики показує, що найчастіше при огляді місця події у справах про комп'ютерні злочини в банківській сфері використовується фотографування, звукозапис і відеозапис. Викликає подив той факт, що як техніко-криміналістичні засоби в таких справах практично не використовуються паспортизовані: комп'ютерна техніка й спеціальне програмне забезпечення; пошукова апаратура для виявлення пристроїв негласного одержання інформації й впливи на неї; спеціальні свинцеві або алюмінієві контейнери, ZIP-Диски й інші технічні пристрої, призначені для вилучення (копіювання), безпечного зберігання й переміщення великих масивів комп'ютерної інформації і їхніх носіїв. На думку багатьох фахівців, у справах розглянутої категорії слідча валіза (портфель) повинна бути додатково доукомплектована в такий спосіб. Крім стандартного набору приналежностей, у ньому повинні перебувати: хімічні засоби виявлення й фіксації слідів пальців рук, що не мають у своєму складі магнітовмістких матеріалів (наприклад, сажа, прожарений порошок оксиду цинку тощо) – для роботи зі слідами, залишеними на магнітних носіях інформації й ЗЕОТ; спеціальні алюмінієві або свинцеві контейнери або побутова алюмінієва фольга (можливо, алюмінієва каструля з кришкою з того ж матеріалу) для грамотного вилучення магнітних носіїв машинної інформації, що виключають сторонній вплив електромагнітних і магнітних полів, здатних модифікувати й знищити вилучену комп'ютерну інформацію; паспортизовані машинні носії інформації, призначені для копіювання комп'ютерної інформації у випадку неможливості фізичного її вилучення разом із «рідним» носієм, упаковані в алюмінієву фольгу або контейнер; паспортизовані машинні носії інформації з відповідним ліцензованим програмним забезпеченням, необхідним для проведення огляду пам'яті ЗЕОТ і комп'ютерної інформації, що цікавлять слідство (системні завантажувальні програми, тестові, антивірусні детектори, здатні відновлювати стерті файли, визначати конфігурацію або внутрішню специфікацію ЗЕОТ, що оглядається, індивідуальні характеристики комп'ютерної інформації – розмір, дату створення, назву тощо).

Після прибуття СОГ на місце події починається друга стадія підготовчого етапу огляду. Особливу увагу необхідно приділити певним заходам безпеки, спрямованим на запобігання знищення речових доказів або їхньої втрати. У цих цілях керівник СОГ повинен виходити з наявних методичних рекомендацій.

Після виконання цього слідчий повинен провести опитування осіб, які можуть дати яку-небудь нову інформацію про подію, що сталася. Особливу увагу необхідно звернути на категорію об'єкта огляду, на наявність ЗЕОТ і комп'ютерної інформації обмеженого доступу. У цьому випадку для проведення їхнього огляду й вилучення необхідний дозвіл судді, якою заздалегідь повинен заручитися слідчий. Зазначена обставина найбільш типова для юридичних осіб, що функціонують у наступних сферах: відомствах і установах виконавчої влади, кредитно-банківської, послуг електрозв'язку, приватної охоронної діяльності.

Склавши для себе повне й чітке уявлення про подію, що сталася, слідчий повинен остаточно вирішити питання про коло учасників огляду (можливо, йому буде потрібно додатково викликати якихось додаткових фахівців, оперативних працівників або охорону), а також провести інструктаж учасників огляду, у якому визначити наступне: роз'яснити кожному його функції і завдання, що конкретно він повинен робити, його права й обов'язки, запобіжні заходи при огляді ЗЕОТ, комп'ютерної інформації, роботі зі специфічними слідами тощо.

Після цього й повинен починатися безпосередній огляд місця події – його дослідницький етап, що, з урахуванням вимог наукової організації праці, у криміналістиці умовно поділяють на три стадії: загальний огляд (статична стадія), детальний (динамічна) і заключний (фіксація ходу й результатів огляду).

На стадії загального огляду вирішальне значення має складання плану розташування місця огляду щодо сусідніх з ним об'єктів і сторін світу; прив'язка місця події й основних предметів, що перебувають на ньому, до декількох постійних орієнтирів; попереднє визначення меж території, що підлягає огляду.

При розслідуванні справ про комп'ютерні злочини в банківській сфері дуже важливо правильно вирішити питання про вихідну точку огляду. У тактичному відношенні найбільш доцільною відправною точкою, на нашу думку, буде конкретний (встановлений оперативним або іншим шляхом) ЗЕОТ із комп'ютерною інформацією, що виступає як предмет або знаряддя вчинення злочину, що має максимально інформативні й численні сліди злочинної діяльності.

Аналіз емпіричних джерел слідчої практики показує, що в цьому випадку оптимально буде використовуватися об'єктивний метод огляду, при якому відбувається суцільний огляд усього місця події. Найбільш доцільним є ексцентричний спосіб, коли огляд провадиться від центра до периферії, де центр – вихідна точка.

У процесі проведення огляду місця події бажано використовувати відео- або фотозйомку.

Після того, як характер і розташування об'єктів будуть досліджені й зафіксовані, наприклад, складені схеми провідних з'єднань ЗЕОТ між собою, з засобами й каналами електрозв'язку, іншим периферійним обладнанням, починається друга стадія дослідницького етапу – детальний огляд кожного з виявлених предметів. При цьому допускається переміщення предмета, що оглядається, його розбирання й інші маніпуляції з ним, які продиктовані слідчою необхідністю. Таким чином, може бути розкритий корпус ЗЕОТ; відкритий захисний кожух друкуючого механізму принтера; знята передня панель банкомату, досліджена пам'ять ЗЕОТ і машинного носія інформації тощо. На цій же стадії потрібно провести необхідні пошукові дії з метою виявлення на місці події й на окремих об'єктах, які оглядаються (документах, машинних носіях інформації, ЗЕОТ тощо), слідів злочину.

За наявності даних, що свідчать про вчинення злочину в банківській сфері з використанням комп'ютерної інформації, не зайвим буде проведення пошукових заходів з метою встановлення можливого технічного каналу витоку такої інформації й конкретного технічного пристрою. Для цього необхідно за участю спеціаліста з оперативно-технічного підрозділу з використанням спеціальної апаратури провести контроль радіоефіру, перевірити наявні на місці огляду засоби охоронно-пожежної сигналізації, телекомунікаційне обладнання тощо. Можливе проведення й інших пошукових заходів.

При огляді місця події центральне місце посідають сліди злочинної діяльності. У криміналістиці під цим розуміють матеріальні та ідеальні сліди відображення. У злочинах з інформаційними технологіями особливу роль відіграють саме матеріальні сліди, адже вони мають неординарні індивідуальні особливості. Останні можуть бути притаманні традиційним видам злочинів, а також характерними лише новітнім системам. Тому вчиняючи огляд місця події, перш ніж занурюватися у внутрішній зміст комп'ютерних устаткувань, слід ретельно оглянути зовнішній вигляд предмета дослідження. У процесі роботи операційної системи на її поверхні осідає природний та побутовий пил (від роздруковуючих пристроїв), який не підлягає щоденному прибиранню, а також накопичується він в інших малодоступних місцях (під монітором, системним блоком, клавіатурою, факсом, принтером, у місцях з'єднання кабелів тощо [4, 84]. Отже, не виключено, що під час ймовірних несанкціонованих дій з комп'ютерними системами, особа-злочинець залишила по собі сліди відшарування, можливо, нашарування чи інші (невидимі-безбарвні, одорологічні, трасологічні тощо). До слідів внутрішніх відносимо:

- різнотипні зміни в будові комп'ютерного устаткування (наявність позаштатного обладнання, пристроїв розширення оперативної пам'яті, програми для зчитування оптичних дисків, заміна або відсутність мікросхем чи інших комплектуючих);

- будь-який вплив на саму інформацію, що знаходиться всередині машинних носіїв (зміни у файловій системі; шкідливі та небезпечні файлові програми;

- програми-файли зі зверненням до сайтів Інтернет; програми, що спричиняють копіювання, блокування, модифікацію чи знищення інформації; файлове програмне забезпечення підбору паролів до несанкціонованого доступу в Інтернет та ін.).

У цьому сенсі цікавою є точка зору Т.Е. Кукарнікової, яка зазначає, що слід комп'ютерного злочину – це будь-яка зміна середовища (файлової системи), пов'язана з подією злочину. Оскільки файлова система є сукупністю особливих інформаційних одиниць-файлів, спеціальних службових таблиць (каталогів, таблиці розділів, завантажувальних записів, таблиць розміщення файлів) і кластерів, ці зміни можуть виражатися в зміні місцеположення і вмісту файлів; зміні формату або характеристик файлів; створенні чи вилученні файлів; зміні вмісту спеціальних службових таблиць та зміні стану кластерів. Дія одного інформаційного об'єкта на інший може бути виявлена між двома відомими станами інформаційного об'єкта – за ознаками зміни змісту формату файлових характеристик та за зміною алгоритму роботи програми [7, 12].

Як правило, на даному етапі проведення слідчої дії виникає нагальна потреба детального огляду й наступного вилучення ЗЕОТ, машинного носія інформації, комп'ютерної інформації (у тому числі машинного документа). Як показує аналіз проведеної нами методичної літератури, стосовно предмета нашого дослідження оптимальними є рекомендації, які запропоновані В.Б. Вєховим [5, 34-37], тому доцільно використовувати їх у повному обсязі.

На заключному етапі огляду місця події провадиться фіксація його ходу й отриманих результатів: повністю оформлюється протокол проведення слідчої дії; упаковуються виявлені й вилучені предмети й сліди; остаточно допрацьовуються плани, схеми й креслення; розглядаються зауваження, що надійшли від учасників огляду даної слідчої дії.

Правила, що регламентують діяльність слідчого на цій стадії огляду, докладно регламентовані чинним кримінально-процесуальним законодавством, досить широко висвітлені в криміналістичній літературі й не вимагають додаткових пояснень.

Відзначимо, що в протоколі слідчої дії необхідно вказати всі дії щодо виявлення й вилучення слідів і предметів огляду в тій послідовності, у якій він проводився, і в тому вигляді, у якому виявлене спостерігалося (наприклад, маніпуляції спеціаліста із ЗЕОТ, програмним забезпеченням і комп'ютерною інформацією; натискання клавіші керування ЗЕОТ і їхній результат).

У протоколі обов'язково варто вказати всі застосовані для виявлення, фіксації, вилучення слідів і їхніх носіїв технічні засоби, включаючи програмне забезпечення: їхні паспортні дані – тип, вид, марка або назва, заводський або реєстраційний (інвентарний) номер виробу, серію

(модель), виробника тощо, умови й порядок їхнього використання (наприклад, при використанні ПЕОМ і програмного забезпечення зробити оцінку про те, що перед цим вони були протестовані спеціалістом на предмет відсутності в них шкідливих програмно-апаратних засобів – указати паспортні дані засобу тестування), а також докладно описати сліди й об'єкти, на яких знаходяться ці сліди, у статиці щодо місць їхнього виявлення; умови й порядок їхнього вилучення й упакування.

ЛІТЕРАТУРА

1. Колмаков В.П. Следственный осмотр / В.П. Колмаков . – М.: Юрид. лит., 1969. – 196 с.
2. Салтевський М.В. Криміналістика. Методика і тактика / М.В. Салтевський . – Харків: Консум, 2001— .—

   Ч. 2. – 2001. – 527 с.
3. Васильев А.Н. Тактика отдельных следственных действий / А.Н. Васильев. – М.: Юридическая литература, 1981. – 112 с.
4. Старушкевич А. Організація огляду місця події. Аналіз криміналістично-значимої інформації при розслідуванні злочинів у сфері комп'ютерної інформації / А. Старушкевич // Вісник прокуратури. – 2003. – № 12. – С. 77–86.
5. Вехов В.Б. Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники: [учеб.-метод, пособие] / В.Б. Вехов. – Волгоград: Перемена, 1998. – 72 с.
6. Селиванов Н.А. Проблемы борьбы с компьютерной преступностью / Н.А.Селиванов // Законность. – 1993. – №8. – С.36–40.
7. Кукарникова Т.Э. Проблема криминалистического исследования электронных документов / Т.Э. Кукарникова // Вести Тул. ГУ. Серия: «Современные проблемы законодательства России, юридических наук и правоохранительной деятельности». – Тула: Изд-во Тул. гос. ун-та, 2000. – Вып. 3. – С. 11–16.

УДК 340.66 : 343.98 (477)

ОРГАНІЗАЦІЙНІ І ТАКТИЧНІ ОСОБЛИВОСТІ СУДОВО-МЕДИЧНОГО ОСВІДУВАННЯ

Чаплинський К.О., к.ю.н., доцент

Дніпропетровський державний університет внутрішніх справ

Наукова стаття присвячена висвітленню актуальних проблем проведення освідування. Автором проаналізовані наявні в юридичній літературі точки зору щодо організації і тактики проведення судово-медичного освідування підозрюваних, обвинувачених, свідків і потерпілих.

Ключові слова: освідування, тактичне забезпечення, тактика, тактичні прийоми.

Чаплинский К.А. ОРГАНИЗАЦИОННЫЕ И ТАКТИЧЕСКИЕ ОСОБЕННОСТИ СУДЕБНО-МЕДИЦИНСКОГО ОСВИДЕТЕЛЬСТВОВАНИЯ / Днепропетровский государственный университет внутренних дел Украины, Украина

Научная статья посвящена рассмотрению актуальных проблем проведения освидетельствования. Автором проанализированы имеющиеся в юридической литературе мнения, касающиеся организации и тактики проведения судебно-медицинского освидетельствования подозреваемых, обвиняемых, свидетелей и потерпевших.

Ключевые слова: освидетельствование, тактическое обеспечение, тактика, тактические приемы.

Chaplinskiy K.A. ORGANIZATIONAL AND TACTICAL ASPECTS OF JUDICIAL MEDICAL EXAMINATION / Dnepropetrovsk state university of internal affairs of Ukraine, Ukraine

This scientific article is devoted to consideration of actual problems of carrying out of an examination. The author have analysed the opinions available in the legal literature about organization and tactics of carrying out of judicial medical examination of suspects, defendants, witnesses and victims.

Key words: examination, tactical supply, tactis, tactical methods.