КУРМАН О. В.,
кандидат юридичних наук,
доцент кафедри криміналістики
(Національний юридичний університет імені Ярослава Мудрого)

УДК 343.98

ТАКТИЧНІ ОСОБЛИВОСТІ ПРОВЕДЕННЯ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ ПІД ЧАС РОЗСЛІДУВАННЯ ЗЛОЧИННИХ ПОСЯГАНЬ НА ВІДОМОСТІ, ЩО СТАНОВЛЯТЬ КОМЕРЦІЙНУ АБО БАНКІВСЬКУ ТАЄМНИЦЮ

У статті розглядаються тактичні особливості проведення слідчого огляду та допиту в рамках розслідування злочинних посягань на відомості, що становлять комерційну або банківську таємницю. Надаються рекомендації стосовно огляду приміщень різного функціонального призначення та обставин, які належить з'ясувати під час допитів різних категорій осіб.

Ключові слова: *тактика слідчих дій, допит, огляд місця події, комерційна таємниця, банківська таємниця.*

В статье рассматриваются тактические особенности проведения следственного осмотра и допроса в рамках расследования преступных посягательств на сведения, составляющие коммерческую или банковскую тайну. Даются рекомендации относительно осмотра помещений разного функционального назначения и обстоятельств, подлежащих выяснению во время допросов разных категорий лиц.

Ключевые слова: *тактика следственных действий, допрос, осмотр места происшествия, коммерческая тайна, банковская тайна.*

The article deals with tactical features of the investigatory examination and interrogation during the investigation of criminal encroachment on information containing trade secret or banking secrecy; gives some recommendations regarding the inspection of premises of different functional purpose and circumstances which have to be clarified during the interrogation of different categories of persons.

Key words: *investigative tactics, interrogation, crime scene inspection, trade secret, banking secrecy.*

Вступ. Методика розслідування злочинних посягань на відомості, що становлять комерційну або банківську таємницю в умовах сьогодення, є недостатньо розробленою в практичному і теоретичному аспектах. Рівень професіоналізму практичних працівників у цьому плані залишається низьким, повільно впроваджуються в практику адекватні форми й методи слідчої діяльності. Відсутність упорядкованих, систематизованих відомостей про особливості розслідування зазначених видів злочинної діяльності також не сприяє ефективній боротьбі з такими негативними проявами. Тому питання розробки окремої криміналістичної методики розслідування злочинних посягань на відомості, що становлять комерційну або банківську таємницю, є важливим і актуальним завданням.

Постановка завдання. Традиційно до структури криміналістичної методики розслідування конкретного виду злочинів включається тактика проведення окремих слідчих (розшукових) дій. Цій проблематиці в криміналістиці приділялася значна увага [2; 3; 4, с. 106–208; 5;

7, с. 312–398]. У той же час тактичні особливості проведення таких слідчих (розшукових) дій, як огляд та допит у рамках розслідувань злочинних посягань на відомості, що містять комерційну або банківську таємницю (ст.ст. 231, 232 КК України), не мали належного наукового опрацювання, що викликає потребу дослідження зазначеної проблеми та визначає новизну теми.

Результати дослідження. Після початку досудового розслідування шляхом проведення слідчих (розшукових) дій встановлюються обставини, що входять до предмету доказування. Відповідно до ч. 2 ст. 91 КПК України доказування полягає в збиранні, перевірці та оцінці доказів з метою встановлення обставин, що мають значення для кримінального провадження. До обставин, які належить встановити, відносяться: 1) чи є дані відомості комерційною таємницею, які заходи було вжито для збереження інформації власником. Чи містять відомості банківську таємницю; 2) на якому матеріальному носії була зафіксована інформація, що складає комерційну або банківську таємницю (його характеристики, зовнішні ознаки, що говорять про наявність комерційної таємниці, реквізити, відповідні грифи); 3) характеристики юридичної особи (власника), яким чином використовувалась зникла інформація; 4) хто відповідальний за збереження документа (коли був отриманий документ, як оформлено отримання); 5) що відбулося: втрата документу або його викрадення; 6) спосіб викрадення документу, незаконного отримання інформації (які технічні засоби використовували злочинці); 7) які предмети зникли разом з документом або з'явилися на місці події; 8) час та місце заволодіння інформацією; 9) чи є ознаки маскування порушення правил зберігання документу; 10) хто винен у втраті документу; 11) кількість осіб, що брали участь у злочині; 12) мотиви та цілі злочинців; 13) кого може зацікавити викрадена інформація; 14) кому була передана інформація, що становить комерційну або банківську таємницю, та на яких умовах; 15) які обставини сприяли виходу документа із законного обігу; 16) спосіб розголошення відомостей, що становлять комерційну або банківську таємницю; 17) час та місце розголошення інформації, що становить комерційну або банківську таємницю; 18) чи не були здійснені дії з отримання інформації внаслідок шантажу чи погрози насиллям; 19) розмір матеріальної шкоди, яка була завдана власнику комерційної чи банківської таємниці.

Дані обставини встановлюються цілим комплексом слідчих (розшукових) дій. Спрямованість слідчої дії, її мета та завдання залежать від версії, яку відпрацьовує слідчий. Важливе місце в цій системі криміналістичних заходів посідає огляд місця події та допит (як найбільш розповсюджені процесуальні дії).

Місцем події при злочинному посяганні на відомості, що становлять комерційну або банківську таємницю, можуть бути: офіс, де працюють рядові працівники; кабінети керівництва; приміщення, де встановлені електронні технічні засоби обробки інформації; кімнати, де зберігаються конфіденційні відомості; виробничі та складські приміщення. Огляд кожного місця повинен проводитися з урахуванням його призначення, графіку роботи, доступності стороннім особам, режиму охорони. Загальними завданнями огляду місця події є виявлення та фіксування: 1) можливих способів проникнення до службового приміщення; 2) характерних рис та особливостей порушень правил зберігання документів, що складають комерційну або банківську таємницю; 3) наявності чи відсутності передбачених правилами засобів технічної охорони приміщення (огорожі, грати, сигналізація тощо); 4) технічного стану охоронних засобів; 5) порушення правил зберігання ключів від сховища; 6) порушення правил передачі приміщення під охорону; 7) наявності доказів використання службового приміщення не за призначенням (для зустрічей зі сторонніми, вживання спиртних напоїв); 8) фактів неналежного зберігання документів (поза сейфом).

Під час огляду встановлюється: 1) відповідність приміщення роду діяльності організації, можливість розміщення в ньому працівників у кількості, зазначеній у документах; 2) наявність у приміщенні інших організацій; 3) цільове призначення приміщення; 4) наявність у приміщенні матеріалів, продукції, устаткування відповідно до зазначеної документації.

У процесі огляду службових приміщень необхідно звернути увагу на сліди, що залишені сторонніми особами (сліди рук, ніг, одежі, куріння, зникнення окремих предметів, сліди користування речами, приборами, засобами зв'язку), а також сліди проникнення.

Особливої уваги заслуговує огляд сейфа з метою виявлення та фіксування обставин, що підтверджують несправність замку, відмикання сейфу дублікатом ключа, порушення правил опечатування сейфу, наявність сторонніх предметів у сейфі. При огляді ключів від сейфу слід звернути увагу на ознаки заміни ключів, розходження заводських номерів на них, сліди кустарного виготовлення ключа, ознаки використання ключа для виготовлення дублікату тощо.

Під час огляду місця події повнота і всебічність реалізації аналітичної діяльності забезпечується завдяки можливості застосування різних спеціальних знань у формі участі спеціалістів, які дозволяють з'ясувати походження і природу окремих слідів, виявити їх приховані ознаки, що вказують на місце й роль у події, яка відбулась [1, с. 54]. Не останню роль у прийнятті рішення про залучення спеціаліста відіграє і той факт, що слідчий, отримавши гуманітарну освіту, часто без особливого бажання використовує науково-технічні засоби. Тому при огляді, як правило, особливо затребувана саме технічна допомога спеціаліста [6, с. 106].

Так, під час огляду електронних пристроїв спеціаліст допоможе слідчому: 1) визначити, які програми виконуються; 2) зупинити виконання програм; 3) визначити наявність підключених пристроїв-накопичувачів інформації; 4) встановити підключення зовнішніх пристроїв дистанційної передачі інформації; 5) скопіювати програми та файли; 6) правильно вимкнути електронні пристрої.

У процесі проведення огляду місця події увага приділяється дослідженню технічних засобів, що знаходяться в приміщенні (комп'ютери, засоби зв'язку, пристрої для виготовлення копій документів тощо). Такі об'єкти оглядаються з метою виявлення: 1) вбудованих електронних пристроїв дистанційного зняття інформації із каналів зв'язку або слідів їх перебування та недавнього демонтажу; 2) слідів несанкціонованого використання техніки для виготовлення копій документів, пошкодження технічних засобів; 3) обставин, що сприяли незаконному збиранню відомостей шляхом перехоплення інформації. Зокрема порушень: а) порядку експлуатації систем обробки та передачі інформації; б) правил зміни паролів та електронних ключів; в) порядку реєстрації дій користувачів; г) порядку обліку, зберігання та видачі співробітникам носіїв інформації; ґ) регламенту допуску до приміщень, де здійснюється автоматична обробка електронної інформації.

Огляд технічних засобів, що використовувалися для зберігання, обробки та передачі відомостей, охоплює вивчення: 1) комп'ютерної техніки (портативної та стаціонарної); 2) засобів телефонного зв'язку; 3) пристроїв передачі інформації через мережу Інтернет. Цей етап динамічної стадії огляду проводиться з метою виявлення вбудованих електронних технічних засобів, слідів пошкоджень технічних засобів захисту інформації, слідів несанкціонованого вмикання (вимикання), переміщення, заміни, підключення сторонніх пристроїв. Окремо з'ясовуються обставини несанкціонованого доступу та дій, що вчинила особа, яка: 1) мала офіційний повний доступ до файлів та програм; 2) мала обмежений офіційний доступ; 3) не мала права на роботу з конкретними файлами або програмами. Додатково встановлюється, що саме зробила особа – тільки ознайомилася з інформацією, скопіювала дані на інший електронний носій, роздрукувала інформацію або передала її через мережу Інтернет чи стільниковий зв'язок.

Однією з найпоширеніших слідчих дій, без проведення якої не обходиться розслідування жодного злочину, є допит. На початку розслідування злочинів цієї категорії проводиться допит осіб, що заявили про викрадення та використання відомостей, що складають комерційну або банківську таємницю. У результаті такого допиту слідчий може отримати інформацію про місце зберігання носія інформації, час його викрадення, спосіб вчинення злочину, спосіб незаконного використання інформації, можливі мотиви та цілі злочинних дій, особу злочинця. Зазначених осіб доцільно допитувати без гаяння часу, тому що це певною мірою запобігає можливості розпорядитися злочинцем отриманою інформацією.

Допит особи, відповідальної за зберігання документів, проводиться з метою встановити: 1) порядок отримання таких носіїв співробітниками підприємства для роботи; 2) коли та ким останній раз використовувалася інформація в службових цілях; 3) чи дотримувався встановлений порядок доступу; 4) чи були порушення правил обігу документів, які саме; 5) коли та у зв'язку з чим була виявлена відсутність документів; 6) чи відомі обставини та причини виходу документа (інформації) із законного володіння; 7) чи проявляв хто-небудь ознаки обізнаності про злочинну подію до її виявлення; 8) які відомі свідку обставини виходу носія інформації з володіння відповідальної особи; 9) які зміни відбулися в обстановці на місці події до початку розслідування; 10) кому може бути потрібна ця інформація та для яких цілей.

Під час допиту особи, яка відповідала за роботу електронних систем зберігання, обробки та передачі інформації, з'ясовується порядок: 1) експлуатації електронних систем обробки і передачі інформації; 2) ведення службових протоколів системи захисту інформації; 3) оперативного контролю за функціонуванням системи; 4) реєстрації та аналізу дій користувачів; 5) отримання доступу співробітниками до певних баз даних, реєстрів, програм, файлів; 6) розробки, реєстрації, видачі логінів, паролів, електронних ключів; 7) допуску в приміщення, де встановленні електронні системи.

Допиту в якості свідків також підлягають: 1) особи з оточення співробітника, відповідального за збереження носіїв інформації, що містять комерційну або банківську таємницю (серед них може знаходитися викрадач або особа, якій щось відомо про злочинця); 2) особи, які офіційно отримували документи для роботи; 3) співробітники, яким документ був переданий для роботи без відповідного дозволу; 4) представники проектної, суміжної, контрольної організації, з якими підтримувався контакт при роботі і які мали можливість ознайомлення із документами; 5) особи, що колись працювали на підприємстві; 6) охоронці; 7) технічний персонал.

При підготовці до допиту підозрюваного необхідно ретельно вивчити особу допитуваного, спланувати тактику слідчої дії. Слід враховувати, що підозрювані в цій категорії справ можуть мати високий рівень освіти, володіти знаннями в галузі економіки, інформаційних технологій і уявляти реальну вартість викраденої інформації. У процесі допиту необхідно з'ясувати: 1) у яких стосунках знаходиться з керівництвом підприємства (власником відомостей); 2) з якою метою отримана інформація та за яких обставин вона з'явилася у підозрюваного; 3) хто і коли приймав рішення про заволодіння інформацією; 4) яким змінам піддавався носій після надходження до підозрюваного; 5) на який носій було скопійовано інформацію; 6) у яких стосунках із працівниками підприємства; 7) кому були передані документи або повинні бути передані тощо. Особливу групу складають питання, що відображають боргові зобов'язання підозрюваного, його матеріальне становище, а також питання, спрямовані на з'ясування причин вчинення злочину.

Висновки. Викрадення комерційних секретів в Україні сьогодні представляє серйозну загрозу правовідносинам у сфері добросовісної конкуренції. У той же час відсутність теоретичних розробок та рекомендацій стосовно методики розслідування розглядуваних видів злочинів створює певні труднощі в протидії цим злочинним проявам.

Отже, недостатня розробленість питань тактики проведення окремих слідчих (розшукових) дій в рамках методики розслідування злочинних посягань на відомості, що становлять комерційну або банківську таємницю, потребує подальшого дослідження та опрацювання для забезпечення сучасних потреб практичної правоохоронної діяльності.

Список використаних джерел:

1. Алексєйчук В.І. Огляд місця події: тактика і психологія : [монографія] / [В.І. Алєксейчук] ; за ред. В.О. Коновалової. – Х. : Апостіль, 2011. – 232 с.

2. Дулов А.В. Тактика следственных действий / А.В Дулов, П.Д. Нестеренко. – Минск : Вышэйш. шк., 1971. – 272 с.

3. Коновалова В.Е. Допрос: тактика и психология / В.Е. Коновалова. – Х. : Консум, 1999. – 157 с.
4. Коновалова В.О. Вибрані твори / В.О. Коновалова. – Х. : Апостіль, 2012. – 528 с.
5. Следственные действия (процессуальная характеристика, тактические и психологические особенности) : [учеб. пособие] / А.К. Гаврилов, Ф.В. Глазырин, С.П. Ефимичев и др. – Волгоград : ВСШ МВД СССР, 1984. – 238 с.
6. Телегина Т.Д. Использование специальных знаний в современной практике расследования преступлений : [монография] / Т.Д. Телегина. – М. : Юрлитинформ, 2011. – 152 с.
7. Шепітько В.Ю. Вибрані твори / В.Ю. Шепітько. – Х. : «Апостіль», 2010. – 574 с.

МАКАРЕНКО Є. І.,
кандидат юридичних наук, професор
(Дніпропетровський гуманітарний університет)

УДК 343.985.2

ЧИ Є ДОКАЗОМ ФАКТ ЗАТРИМАННЯ ПІДОЗРЮВАНОГО У ВЧИНЕННІ ЗЛОЧИНУ

У татті висвітлюється реальна мета, яку має переслідувати кримінально-процесуальне затримання особи, підозрюваної у вчиненні злочину.
Ключові слова: *підозрюваний, затримання, захід забезпечення кримінального провадження, процесуальна (слідча) дія, доказування.*

В данной статье освещается реальная цель, которую преследует уголовно-процессуальное задержание подозреваемого в совершении преступления.
Ключевые слова: *подозреваемый, задержание, мера обеспечения уголовного производства, процессуальное (следственное) действие, доказывание.*

This article highlights the real goal pursued criminal procedure detention of the suspect to the crime.
Key words: *suspect, detention, measures to ensure criminal proceedings, procedure (investigation) action proof.*

Вступ. На жаль, статус кримінально-процесуального інституту затримання підозрюваного тривалий час залишається невизначеним, про що певною мірою свідчить троїста позиція вітчизняного законодавця. Нагадаємо, що згідно з п. 8 ч. 2 ст. 131 КПК України [2] затримання є заходом забезпечення кримінального провадження, використовуваним слідчим в якості більш жорсткої міри для досягнення дієвості кримінального провадження в разі, якщо підозрюваний не з'являється за викликом. Трохи інакше позиціонує затримання ч. 2 ст. 176 цього ж кодексу, вбачаючи в ньому тимчасовий запобіжний захід, що полягає в короткочасному (що не перебільшує 72-х годин) ув'язненні підозрюваного шляхом поміщення його до ізолятору тимчасового тримання (далі – ІТТ), який застосовується виключно слідчим суддею в ході досудового чи судового слідства. Оскільки в якості способу констатації й закріплення факту, змісту і результатів затримання особи, підозрюваної в учиненні злочину, законодавець (ч. 1 ст. 104, ч. 5 ст. 208 і ч. 6 ст. 223 КПК) вимагає складання протоколу, що є