МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
КИЇВСЬКИЙ ІНСТИТУТ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

Л. В. ПОЛУНІНА

ОСОБЛИВОСТІ ДОСУДОВОГО РОЗСЛІДУВАННЯ НЕЗАКОННОГО ЗБИРАННЯ АБО ВИКОРИСТАННЯ ВІДОМОСТЕЙ, ЩО СТАНОВЛЯТЬ КОМЕРЦІЙНУ АБО БАНКІВСЬКУ ТАЄМНИЦЮ

Монографія

Київ • 2024

УДК 343.98 : 343.533
П 53

Рекомендовано до друку Вченою радою Київського інституту Національної гвардії України (протокол № 16 від 27 червня 2024 р.)

Рецензенти:

Лисенко В. В., доктор юридичних наук, професор, професор кафедри кримінального права та процесу Державного податкового університету;

Завидняк В. І., доктор юридичних наук, доцент, старший партнер Адвокатського об'єднання «Лекс Юстум», адвокат;

Комісаров О. Г., доктор юридичних наук, професор, заступник начальника факультету забезпечення державної безпеки Київського інституту Національної гвардії України.

Полуніна Л. В.

П 53 Особливості досудового розслідування незаконного збирання або використання відомостей, що становлять комерційну або банківську таємницю: монографія/ Лілія Полуніна. – Київ: КІ НГУ, 2024. – 180 с.

ISBN-978-617-8361-18-1

Монографію присвячено комплексному дослідженню проблем методики розслідування незаконного збирання або використання відомостей, що становлять комерційну або банківську таємницю. Визначено поняття й елементи криміналістичної характеристики, окреслено способи і слідову картину кримінальних правопорушень, досліджено обстановку злочинного посягання та особу злочинця. Розкрито особливості організації та планування розслідування кримінальних правопорушень у сфері комерційної або банківської таємниць. Запропоновано алгоритми дій слідчого у типових слідчих ситуаціях початкового та подальшого етапів розслідування. Удосконалено організацію та тактику проведення окремих слідчих (розшукових) дій. Досліджено особливості використання спеціальних знань під час розслідування злочинів вказаної категорії.

Для науковців, викладачів, курсантів, студентів та слухачів вищих юридичних навчальних закладів, працівників правоохоронних органів, усіх тих, хто виявляє інтерес до юридичної науки.

ISBN-978-617-8361-18-1

ЗМІСТ

ПЕРЕДМОВА

Хто володіє інформацією – той володіє світом.
Натан Ротшильд, англійський банкір

Особливу роль у переході до ринкових відносин відіграє добросовісна конкуренція суб'єктів господарювання, яка покликана слугувати стабілізатором економічних процесів. Статтею 42 Конституції України визначено, що держава забезпечує захист конкуренції у підприємницькій діяльності. Не допускаються зловживання монопольним становищем на ринку, неправомірне обмеження конкуренції та недобросовісна конкуренція. Відповідно до ст. 41 Основного Закону кожен має право володіти, користуватися і розпоряджатися своєю власністю, результатами своєї інтелектуальної, творчої діяльності. Однак корінні зміни у роботі суб'єктів економічної діяльності, банківської системи, послаблення державного контролю та інші причини соціального і правового характеру призвели до появи нових, раніше невідомих суспільно небезпечних форм економічної поведінки. Особливе місце серед них займають злочинні дії з відомостями, що становлять комерційну або банківську таємницю.

Розслідування незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, пов'язане із значним обсягом роботи, специфікою умов розслідування, необхідністю проведення криміналістичних комплексів у вигляді послідовного проведення слідчих (розшукових) дій та організаційних заходів. Однак, як свідчить практика, працівники органів досудового розслідування не завжди володіють необхідними знаннями для успішного виявлення та розслідування цього виду кримінальних правопорушень. Відсутність упорядкованих, систематизованих відомостей та рекомендацій про особливості розслідування злочинних дій з відомостями, що становлять комерційну або банківську таємницю, зменшує ефективність боротьби з вказаними кримінальними

правопорушеннями. Водночас суб'єкти, які вчиняють ці кримінальні правопорушення, зазвичай добре орієнтуються в особливостях господарської діяльності підприємств, банківському законодавстві, володіють знаннями у сфері бухгалтерського обліку, особливостях зовнішньоекономічної діяльності, крім того, підтримують корупційні зв'язки з працівниками великих підприємств, банківськими установами, державними службовцями різних рівнів – усе це дозволяє приховувати злочинну діяльність і чинити протидію розслідуванню.

Сьогодні питання методики розслідування незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, не знайшли достатнього відображення у криміналістичній теорії. Цим зумовлено потребу у проведенні наукового дослідження, пов'язаного з розробленням криміналістичної характеристики таких кримінальних правопорушень та побудовою методики розслідування незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

КК України – Кримінальний кодекс України;
КПК України – Кримінальний процесуальний кодекс України;
ЦК України – Цивільний кодекс України;
ГК України – Господарський кодекс України;
ЄДРДР – Єдиний державний реєстр досудових розслідувань;
НП – Національна поліція України;
МВС – Міністерство внутрішніх справ;
СБУ – Служба безпеки України;
ДНДКЦ – Державний науково-дослідний експертно-криміналістичний центр;
СТЗ – Спеціальні технічні засоби;
СОГ – Слідчо-оперативна група.

РОЗДІЛ 1.
Особливості криміналістичної характеристики незаконного збирання або використання відомостей, що становлять комерційну або банківську таємницю

1.1. Поняття криміналістичної характеристики незаконного збирання або використання відомостей, що становлять комерційну або банківську таємницю

Методика розслідування окремих видів і груп злочинів є частиною криміналістики, в якій розглядаються методи й засоби розкриття і розслідування конкретних видів і груп злочинів з урахуванням їх криміналістичної характеристики і типових слідчих ситуацій [72, с. 69].

Об'єктом дослідження криміналістичної методики є різні злочини. Криміналістична класифікація злочинів є необхідною умовою ефективності пізнання даного об'єкта, основою для розроблення відповідних рекомендацій (їх системи). Поняття криміналістичної класифікації злочинів є достатньо новим і дискусійним у криміналістиці [70, с. 9].

Необхідно зазначити, що проблематику щодо визначення поняття та криміналістичної класифікації незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, а також розголошення комерційної або банківської таємниці, у криміналістичній літературі не досліджували.

Лише окремі кримінально-правові, кримінальні процесуальні та криміналістичні аспекти комерційної таємниці в Україні знайшли своє відображення у працях О. Є. Радутного [68, 69], А. О. Шаповалової [78], С. О. Харламової [76], О. В. Курмана [35; 36], В. М. Іващенко [22; 23; 24] та інших.

Дослідженням різних видів таємниць займалися як вчені криміналісти, так і фахівці у галузі кримінального права. Однак, незважаючи на високий науковий рівень дослідження питання, однозначного визначення поняття «комерційна таємниця», як еле-

менту криміналістичної характеристики злочинного посягання, у науковій літературі не відображено повністю [54, с. 17].

Відповідно до чинного Кримінального кодексу України (далі – КК України) такі кримінальні правопорушення віднесено до кримінальних правопорушень у сфері господарської діяльності. Своєю чергою серед кримінальних правопорушень, що вчиняються у сфері господарської діяльності, вчені виокремлюють дві групи злочинів: 1) злочини, пов'язані з порушенням порядку зайняття господарською діяльністю; 2) злочини, пов'язані з кримінальним банкрутством. Загальними криміналістичними критеріями злочинів першої групи є ознаки способу вчинення злочину, обстановка вчинення злочину, предмет злочинного посягання, а також типові сліди, які зберегли на собі інформацію про подію злочину [70, с. 32].

Оскільки об'єктом кримінальних правопорушень, передбачених ст. ст. 231 та 232 КК України, є встановлений порядок здійснення господарської діяльності в частині забезпечення чесної конкуренції між її суб'єктами [46, с. 578], то кримінальні правопорушення у сфері порушення комерційної або банківської таємниці доцільно віднести до першої групи, а саме до кримінальних правопорушень, пов'язаних з порушенням порядку зайняття господарською діяльністю.

Видовим об'єктом кримінальних правопорушень, що розглядаються, є суспільні відносини, які забезпечують обмеження монополізму у сфері господарської діяльності та (або) охорону суб'єктів цих відносин від проявів недобросовісної конкуренції. До вказаної групи злочинів, що мають спільний видовий об'єкт, можна зарахувати: 1) умисне введення в обіг на ринку України (випуск на ринок України) небезпечної продукції (ст. 227 КК України); 2) незаконне використання знака для товарів і послуг, фірмового найменування, кваліфікованого зазначення походження товару (ст. 229 КК України); 3) незаконне використання інсайдерської інформації (ст. 232-1 КК України) [33].

Безпосереднім об'єктом кримінальних правопорушень, передбачених ст. ст. 231, 232 КК України, виступають суспільні відносини,

що забезпечують охорону суспільства від недобросовісної конкуренції у сфері господарської діяльності [68, с. 110–113].

На думку В. Ю. Шепітька, з огляду на загальні критерії класифікації методик розслідування і розроблення рекомендацій щодо розслідування окремих видів злочинів, необхідно виділяти три підгрупи злочинів, пов'язаних з порушенням порядку зайняття господарською діяльністю: 1) злочини, пов'язані з порушенням порядку здійснення підприємницької діяльності; 2) злочини, пов'язані зі здійсненням забороненої підприємницької діяльності; 3) злочини, які вчиняються у сфері підприємницької діяльності та мають низку спеціальних ознак, пов'язаних з особливостями галузі господарювання [70, с. 34].

Враховуючи зазначене, вбачається нагальна необхідність виділення четвертої підгрупи кримінальних правопорушень, пов'язаних з порушенням антимонопольно-конкурентного законодавства, передбачених ст. ст. 231, 232, 232-1, 232-2 КК України. Своєю чергою серед кримінальних правопорушень антимонопольно-конкурентного законодавства можна виділити такі підгрупи кримінальних правопорушень: 1) злочини у сфері недобросовісної конкуренції; 2) монополістичні зловживання; 3) порушення антимонопольного законодавства [4, с. 355]. З огляду на викладене, обґрунтованим є віднесення незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, а також розголошення комерційної або банківської таємниці, до першої підгрупи кримінальних правопорушень.

Необхідно зауважити, що у випадку привласнення, вимагання комерційної таємниці у вигляді комп'ютерної інформації або заволодіння нею шляхом зловживання службовим становищем вчинене діяння може бути кваліфіковане за сукупністю злочинів, передбачених ст. 231 та ст. 363 КК України. Також варто відмежовувати збирання відомостей, що становлять комерційну або банківську таємницю, від викрадення чужого майна як злочин проти власності. Необхідно також наголосити, що оскільки

розголошення комерційної або банківської таємниці є одним із способів використання відомостей, що становлять комерційну або банківську таємницю, і всі випадки незаконного умисного розголошення комерційної або банківської таємниці крім тих, що передбачені ст. 232 КК України, необхідно вважати її використанням [46, с. 617], то розслідування розголошення комерційної або банківської таємниці буде здійснюватися за схемою, подібної до схеми розслідування незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, за винятком певних особливостей (зокрема, зменшення кола підозрюваних осіб у слідчих ситуаціях, подібних до типових слідчих ситуацій розслідування злочину, передбаченого ст. 231 КК України). Оскільки у цьому випадку, принаймні коло осіб, яким ця таємниця відома у зв'язку з професійною або службовою діяльністю, встановити простіше.

Отже, криміналістична класифікація незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, а також розголошення комерційної або банківської таємниці створює передумови формування комплексної криміналістичної методики розслідування даних злочинів.

Щодо структури окремої методики розслідування злочинів немає єдиної думки, однак більшість вітчизняних криміналістів – В. П. Бахін [1], В. Г. Гончаренко [6; 15], Н. І. Клименко [28; 50], В. К. Лисиченко [50], В. Ю. Шепітько [31; 32; 81] – у її структурі називають такі елементи: криміналістичну характеристику відповідного виду злочинів; перелік обставин, що підлягають встановленню; особливості початку кримінального провадження; перелік початкових слідчих (розшукових) дій і оперативно-розшукових заходів; характер наступних слідчих (розшукових) дій; виявлення обставин, що призводять до вчинення т злочинів, і визначення заходів для їх усунення [71, с. 417].

Криміналістична характеристика злочинів є важливою науковою категорією криміналістики і посідає центральне місце

в методиці розслідування окремих видів злочинів. Як зазначає В. Ю. Шепітько у підручнику з криміналістики: «Криміналістична характеристика – результат наукового аналізу й узагальнення типових ознак певного виду або роду злочинів. Вона відображає злочин і його складові елементи. Крім криміналістичної характеристики злочинів, існують: кримінально-правова, оперативно-розшукова, кримінологічна характеристики» [81].

Автор зазначає, що «криміналістична характеристика є системою відомостей про криміналістично значущі ознаки злочинів даного виду, що відображають закономірні зв'язки між ними, і слугує для побудови та перевірки слідчих версій у розслідуванні конкретних злочинів. Її мета – оптимізація процесу розкриття і розслідування злочинів» [81].

Криміналістична характеристика необхідна для того, щоб допомагати виробляти певні методики щодо розкриття кримінальних правопорушень; розробляти модельні програми розкриття кримінальних правопорушень; сприяти правильному спрямуванню розслідування певного виду кримінального правопорушення. Вона виступає для органу розслідування певним підґрунтям інформаційного характеру, сукупністю даних щодо певної групи кримінальних правопорушень.

Також криміналістична характеристика кримінальних правопорушень являє собою сукупність конкретних складових. Ми погоджуємося з авторами, які зазначають, що «основними елементами криміналістичної характеристики є сукупність ознак, що визначають: спосіб вчинення злочину; місце та обстановку; час вчинення злочину; знаряддя і засоби; предмет посягання; особу потерпілого; особу злочинця; типові сліди злочину» [81].

Криміналістична характеристика злочинів має властивість динамічності, яка виявляється в тому, що її зміст може змінюватися щодо тих або інших видів (родів) злочинів, поповнюватися новими відомостями внаслідок узагальнень слідчої практики [70, с. 13–14].

Криміналістична характеристика є інформаційною моделлю, що описує на якісно-кількісному рівні типові ознаки і властивості пев-

ної групи (виду) злочинів. Структура криміналістичної характеристики розкриває її зміст, тобто елементи злочину, які підлягають опису. Порівняльний аналіз запропонованих науковцями-криміналістами структур криміналістичних характеристик дає змогу стверджувати, що, в основному, вони описують чотири сторони злочину: 1) предмет безпосереднього посягання; 2) спосіб вчинення злочину в його широкому розумінні; 3) типову обстановку – «слідову картину» в її широкій інтерпретації; 4) особу злочинця [72, с. 419].

Звертаючись до висвітлення питання криміналістичної характеристики злочинів у сфері комерційної або банківської таємниці, необхідно зауважити, що кількість її елементів може коливатися залежно від завдань її розробки, однак у будь-якому випадку така інформаційна модель повинна утримувати опис цілей, типових особливостей підготовки, способів вчинення і приховування даного виду злочинів, відомостей про особу злочинця, а також про предмет безпосереднього замаху.

Структура криміналістичної характеристики злочинів має свої особливості і в неї передусім повинні входити такі елементи: 1) предмет злочинного посягання; 2) спосіб злочину; 3) сліди злочину, їх класифікація, механізм утворення; 4) обстановка вчинення злочину (місце, час, обставини, що призвели до вчинення злочину); 5) відомості про особу злочинця та злочинні угруповання.

На нашу думку, центральне місце в криміналістичній характеристиці цього виду злочину займають: 1) предмет злочинного посягання; 2) спосіб вчинення злочину; 3) обстановка вчинення злочину; 4) сліди злочину та механізм їх утворення; 5) особа злочинця.

Незаконне отримання відомостей, що становлять комерційну або банківську таємницю, здебільшого передбачає подальше неправомірне використання інформації з метою: 1) вдосконалення виробничої і комерційної діяльності організації, що заволоділа конфіденційною інформацією (підвищення конкурентоздатності продукції і ефективності виробництва, вибір оптимальної стратегії збуту товарів і торгових переговорів тощо); 2) завдання збитків організації-конкуренту (протидія збуту продукції,

порушення виробничих і торговельних зв'язків організації: зриву торговельних переговорів і угод, зниження інвестиційних можливостей організації, підготовка і розповсюдження дезінформаційних матеріалів ганебного характеру тощо).

У першому випадку вчиняються дії, метою яких є підвищення конкурентоздатності власних товарів шляхом реального покращення їх виробничих якостей, зниження їх собівартості за рахунок застосування на підприємстві засекреченої конкурентом технології, даних про розробку нових виробів і зразків, реалізації матеріалів за перспективними дослідженнями. Нерідко конфіденційні дані про техніко-економічні характеристики продукції конкурента використовуються з метою створення товарів, що перевершують ці характеристики.

До протиправних дій може також належати використання викрадених у конкурента відомостей з метою вдосконалення управління власним підприємством (організацією), підвищення ефективності і якості власних наукових, технологічних розробок і організаційної діяльності, вдосконалення комерційної стратегії власного підприємства тощо.

Наприклад, дані про допустиму (або заплановану ціну), на яку має намір погодитися протилежна сторона, про наміри віддати перевагу пропозиціям конкурента, використовуються з метою розробки стратегії і тактики орієнтовних комерційних переговорів або для випередження конкурента в укладенні вигідних контрактів (договорів).

Дані про клієнтуру, комерційну стратегію конкурентів використовуються з метою створення сприятливих умов в просуванні своїх товарів і послуг; відомості про фінансове становище ділових партнерів враховуються для оцінки ступеня економічного ризику під час укладення контрактів (угод).

Іншим напрямом використання незаконно отриманих конфіденційних відомостей («підривний» за своєю сутністю) є дезорганізація роботи окремих суб'єктів господарювання – конкурентів і галузей економіки в цілому. З цією метою застосовуються:

а) компрометування шляхом поширення завідомо неправдивих (а іноді і правдивих) відомостей, які порочать продукцію конкурента, керівників фірм і їх оточення; б) сплановане цілеспрямоване дезінформування потенційних партнерів своїх конкурентів, у тому числі з використанням можливостей мережі Інтернет або агентів у засобах масової інформації, які публікують завідомо неправдиві відомості про факти, що начебто викликають сумніви щодо якості виробів і продукції; в) зрив крупних контрактів шляхом обнародування правдивих або завідомо неправдивих відомостей про злочинні діяння конкурентів; порушення виробничих і торговельних зв'язків шляхом компрометування контрагентів, їхньої економічної і ділової надійності [54, с. 23].

Наприкінці вісімдесятих років французька компанія Dassaut несподівано для себе втратила два крупних контракти на поставку Саудівській Аравії літаків «Міраж». Ер-Ріяд вирішив купити англійські літаки «Торнадо». Французька контррозвідка встановила, що в обох випадках англійська розвідувальна служба викрадала відомості про торговельні умови Dassaut шляхом перехоплення факсимільної лінії зв'язку і доводила до саудівської сторони через завербованих посередників про торговельні переговори неправдиві дані про технічні характеристики французького літака [54, с. 24].

Указані факти було використано як аргументи на користь створення в структурі DGSE Служби крупних контрактів. Цю Службу було організовано в 1990 році з офіційно заявленою метою – надання сприяння французьким підприємствам у чесній конкурентній боротьбі на міжнародних ринках. З указаного часу її представники добувають і узагальнюють відкриту і конфіденційну інформацію, розробляють рекомендації з використання отриманих даних про підприємства, посередників, вищих посадових осіб, які впливають на перебіг і результати торговельних переговорів. Спеціальна інформаційна база Служби утримує детальні біографічні відомості про об'єкти з багатьох країн світу, їхні ділові і особистісні якості, їхніх друзів, офіційні і неофіційні джерела доходів, інтимні зв'язки тощо.

Завданням зарубіжних резидентур DGSE є надання допомоги Службі у відслідковуванні дій фірм, що конкурують з вітчизняними підприємцями, у прогнозуванні можливості укладення крупних контрактів, у плануванні і здійсненні операцій з видобутку необхідної документації, у вербуванні джерел в оточенні осіб, які приймають рішення [54, с. 24].

Останнім часом поширення набули випадки, коли конкуренти збирають відомості про прорахунки своїх партнерів в правовому оформленні статутної та іншої документації для подальшого використання цих даних у судовому розгляді з метою з'єднання та поглинення компаній.

Показовим є факт, що до відомостей, що становлять комерційну таємницю, окремі підприємці відносять і власні прорахунки в комерційній діяльності, які можуть негативно вплинути на ділову репутацію. Цією обставиною широко користуються суб'єкти, які вимагають гроші у правослухняних підприємців під загрозою розголошення допущених ними прорахунків і судових спорів. Особливо це стосується вразливості у таких випадках українських суб'єктів господарювання, які не мають достатнього досвіду діяльності на зовнішньому ринку.

Отже, дослідження питання криміналістичної характеристики незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, а також розголошення комерційної або банківської таємниці, створює передумови формування комплексної криміналістичної методики розслідування вказаних злочинів.

1.2. Предмет безпосереднього замаху та відомості про осіб, які вчиняють незаконне збирання або використання відомостей, що становлять комерційну або банківську таємницю

Інформація у сучасному світі – це стратегічний ресурс, вона стала об'єктом посягання злочинних намірів, а її захист від несанкціонованого використання, зміни або знищення набуває сьогодні першорядного значення. Забезпечення захисту інформації

– це спосіб запобігання несанкціонованому використанню цінних відомостей та уникнення порушень прав та інтересів їхніх законних власників [20].

Незаконні дії щодо комерційної або банківської таємниці заподіюють руйнівного впливу на одну з важливих сфер суспільного життя – господарську. Такий вплив загрожує умовам нормального існування суспільства, його позитивному розвитку.

КК України передбачає відповідальність за незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю (ст. 231 КК України) та за розголошення комерційної або банківської таємниці (ст. 232 КК України) [33].

Злочини, пов'язані з посяганням на відомості, що становлять комерційну або банківську таємницю, передбачають необхідність вироблення нових практичних підходів до їх розслідування, бо внаслідок активної інформаційної глобалізації видозмінилась обстановка вчинення вказаних кримінальних правопорушень, способи готування, вчинення і приховування злочинних посягань, арсенал знарядь і засобів досягнення злочинної мети, а це спричинило появу нових слідів протиправних діянь.

Комерційна таємниця є одним із найдавніших способів охорони результатів інтелектуальної діяльності.

Комерційна таємниця – це науково-технічна, комерційна, організаційна та інша інформація, яка використовується в підприємницькій діяльності і має реальну або потенційну економічну цінність. Фундаментом комерційної таємниці є можлива шкода, спричинена інтересам юридичної або фізичної особи, що виражається в прямих майнових втратах, які настали, або упущеній вигоді в результаті злочинного поводження або використання інформації, що містить такі відомості.

Інститут комерційної таємниці є одним із важливих компонентів системи, що забезпечує стійкість ринкових відносин, обмеження монополізму у виробничо-економічних відносинах. Без детальної розробки правового інституту комерційної таємниці

майже неможливий розвиток здорових ринкових відносин, а також повноцінне забезпечення прав авторів винаходів. Більшість корпорацій і фірм зобов'язані своєму процвітанню або взагалі самому існуванню саме вмілому зберіганню своїх секретів. Наприклад, зберігання рецепта напою «кока-кола» в глибокій таємниці дає можливість досягати успіху великій корпорації на світовому ринку протягом кількох десятиліть [59, с. 123].

Неправомірне отримання і використання у своїй діяльності чужих наукових здобутків, технологій, управлінських рішень та схем, іншої інформації, яка є комерційною таємницею, має наслідком отримання безпідставних переваг підприємством, організацією, установою чи підприємцем, які отримали цю інформацію, веде до знищення стимулів для розвитку і вдосконалення форм і способів економічної діяльності, завдає прямої шкоди власникам комерційної таємниці [46, с. 616].

Безпосередніми об'єктами злочину, передбаченого ст. 231 КК України, є засади добросовісної конкуренції в частині встановленого порядку обігу та захисту інформації, яка є комерційною або банківською таємницею, а також права і законні інтереси суб'єктів господарської діяльності та клієнтів банків [45, с. 529].

Предметом злочину є відомості, що становлять комерційну таємницю або банківську таємницю суб'єкта господарської діяльності [45, с. 529].

У зв'язку з проблемою забезпечення захисту комерційної таємниці виникає необхідність детального аналізу кожного з елементів криміналістичної характеристики злочинів, пов'язаних із посяганням на відомості, що становлять комерційну або банківську таємницю, зокрема такого її елементу як предмет злочинного посягання.

Сьогодні поняття комерційної таємниці наведено в ст. 505 ЦК України, комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які зазвичай мають справу з видом інформації, до якого вона належить,

у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію. Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого чи іншого характеру, за винятком тих, які відповідно до закону не можуть належати до комерційної таємниці [77]. Статтею 420 ЦК України визначено, що комерційна таємниця є одним з об'єктів інтелектуальної власності. Відповідно майнові права інтелектуальної власності на комерційну таємницю належать особі, яка правомірно визнала інформацію комерційною таємницею, якщо інше не встановлено договором.

Також ЦК України (ст. 507) закріплює обов'язок органів державної влади щодо охорони комерційної таємниці, а саме: органи державної влади зобов'язані охороняти від недобросовісного комерційного використання інформацію, яка є комерційною таємницею та створення якої потребує значних зусиль і яку надано їм з метою отримання встановленого законом дозволу на діяльність, пов'язану з фармацевтичними, сільськогосподарськими, хімічними продуктами, що містять нові хімічні сполуки. Ця інформація охороняється органами державної влади також від розголошення, крім випадків, коли розголошення необхідне для забезпечення захисту населення або не вжито заходів щодо її охорони від недобросовісного комерційного використання [77].

Яка саме інформація може належати до комерційної таємниці? Відповідно до ст. 36 ГК України відомості, пов'язані з виробництвом, технологією, управлінням, фінансовою та іншою діяльністю суб'єкта господарювання, що не є державною таємницею, розголошення яких може завдати шкоди інтересам суб'єкта господарювання, можуть бути визнані його комерційною таємницею. Склад і обсяг відомостей, що становлять комерційну таємницю, спосіб їх захисту визначаються суб'єктом господарювання відповідно до закону [7].

Отже, ЦК України закріплює досить широке коло видів інформації, яка може бути об'єктом комерційної таємниці. Комерційна

таємниця – це інформація, яка є корисною і не є загальновідомою суспільству. Вона має дійсну або комерційну цінність, з якої можна мати прибуток і щодо якої володілець вживає заходів щодо її захисту в усіх сферах життя і діяльності.

Необхідно наголосити, що у чинному законодавстві України відсутній перелік конкретних відомостей, які можуть визнаватися комерційною таємницею суб'єкта господарської діяльності.

Зауважимо, що встановлювати режим комерційної таємниці щодо певної інформації може лише її власник (співвласники за згодою між собою) або уповноважена ним особа; умовою відповідальності за незаконні дії щодо комерційної таємниці є усвідомлення того, що відповідна інформація є саме комерційною таємницею [8, с. 126].

Отже, перелік відомостей, які становлять комерційну таємницю, визначається керівником підприємства (юридичної особи). Проте обсяг цих відомостей не може встановлюватися довільно. Згідно із законодавством не можуть бути визнані комерційною таємницею: установчі документи, документи, що дозволяють займатися підприємницькою чи господарською діяльністю та її окремими видами; інформація за всіма встановленими формами державної звітності; дані, необхідні для перевірки обчислення і сплати податків та інших обов'язкових платежів; відомості про чисельність і склад працюючих, їхню заробітну плату в цілому та за професіями і посадами, а також про наявність вільних робочих місць; документи про сплату податків і обов'язкових платежів; інформація про порушення законодавства України та розміри завданих при цьому збитків; документи про платоспроможність; відомості про участь посадових осіб підприємства в інших організаціях, які займаються підприємницькою діяльністю; інші відомості, які підлягають оголошенню відповідно до чинного законодавства.

Але, крім комерційної таємниці, існує також і банківська. Закон України «Про банки і банківську діяльність» (ст. 60) містить перелік інформації, що є банківською таємницею. Інформація щодо

діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку, є банківською таємницею.

Банківською таємницею, зокрема, є:

1) відомості про банківські рахунки клієнтів, у тому числі кореспондентські рахунки банків у Національному банку України;

2) операції, які були проведені на користь чи за дорученням клієнта, здійснені ним угоди;

3) фінансово-економічний стан клієнтів;

4) системи охорони банку та клієнтів;

5) інформація про організаційно-правову структуру юридичної особи – клієнта, її керівників, напрями діяльності;

6) відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проєкту, винаходів, зразків продукції та інша комерційна інформація;

7) інформація щодо звітності по окремому банку, за винятком тієї, що підлягає опублікуванню;

8) коди, що використовуються банками для захисту інформації;

9) інформація про фізичну особу, яка має намір укласти договір про споживчий кредит, отримана під час оцінки її кредитоспроможності [64].

Інформація про банки чи клієнтів, що збирається під час проведення банківського та валютного нагляду, інформація про банки чи клієнтів, отримана Національним банком України відповідно до міжнародного договору або за принципом взаємності від органу банківського нагляду іншої держави для використання з метою банківського нагляду або запобігання легалізації (відмиванню) доходів, одержаних злочинним шляхом, чи фінансуванню тероризму, також є банківською таємницею [64].

Хоча законом встановлено досить жорсткі вимоги щодо охорони відомостей, які є банківською таємницею, для банку відповідна інформація є не інформацією про свою власну діяльність, а інформацією про сторонніх осіб. Тому поняття банківської таємниці не можна ототожнювати з поняттям комерційної таємниці.

Як постає із законодавчого визначення, поняття комерційної таємниці значно ширше за поняття банківської, оскільки до комерційної таємниці може бути віднесено як конфіденційну інформацію окремого клієнта банку (суб'єкта господарських відносин), так і інша конфіденційна інформація щодо його діяльності та фінансового стану, яка стала відомою банку у процесі обслуговування цього клієнта та взаємовідносин з ним. Тому, на нашу думку, будь-який банк може мати свою власну комерційну таємницю, яка буде відповідати зазначеним вище ознакам [54, с. 31].

Відомостями, що становлять комерційну таємницю, не можуть визнаватися також дані, які згідно з чинним законодавством підлягають оприлюдненню.

Комерційна таємниця – це інформація, яка є корисною і не є загальновідомою суспільству. Вона має дійсну або комерційну цінність, з якої можна мати прибуток і щодо якої володілець вживає заходів щодо її захисту в усіх сферах життя і діяльності [48, с. 823].

Необхідно зауважити, що встановлювати режим комерційної таємниці щодо певної інформації може лише її власник (співвласники за згодою між собою) або уповноважена ним особа; умовою відповідальності за незаконні дії щодо комерційної таємниці є усвідомлення того, що відповідна інформація є саме комерційною таємницею [42, с. 126].

Отже, перелік відомостей, які становлять комерційну таємницю, визначається керівником підприємства (юридичної особи). Проте обсяг цих відомостей не може встановлюватися довільно. Відповідно до постанови КМУ від 9 серпня 1993 р. № 611 «Про перелік відомостей, які не становлять комерційної таємниці» не вважаються такою: установчі документи, документи, що дозволяють займатися підприємницькою чи господарською діяльністю та її окремими видами; інформація за всіма встановленими формами державної звітності; дані, необхідні для перевірки обчислення і сплати податків та інших обов'язкових платежів; відомості про чисельність і склад працюючих, їх заробітну плату загалом та за професіями й посадами, а також про наявність вільних робочих

місць; документи про сплату податків і обов'язкових платежів; інформація про забруднення навколишнього природного середовища, недотримання безпечних умов праці, реалізацію продукції, що завдає шкоди здоров'ю, а також інші порушення законодавства України та розміри заподіяних при цьому збитків; документи про платоспроможність, інші відомості, які підлягають оголошенню відповідно до чинного законодавства.

З об'єктивної сторони злочин, передбачений ст. 231 КК України, може мати такі дві форми: 1) вчинення дій, спрямованих на отримання відомостей, що становлять комерційну таємницю (так зване комерційне шпигунство); 2) незаконне використання відомостей, що становлять комерційну таємницю, якщо це спричинило істотну шкоду суб'єкту господарської діяльності.

Вчинення дій, спрямованих на отримання відомостей, що відповідно до законодавства становлять комерційну або банківську таємницю, розуміють як пошук і добування таких відомостей будь-яким, зокрема злочинним способом (наприклад, викрадення, купівля відповідних документів, виготовлення їх копій, прослуховування телефонних розмов, перлюстрація поштової кореспонденції, візуальне спостереження та підслуховування усних розмов (у тому числі за допомогою застосування спеціальних технічних засобів негласного отримання інформації), фотографування, кіно- або відеознімання, проникнення до комп'ютерних систем, підкуп працівників підприємств-конкурентів чи шляхом застосування погроз, насильства тощо), якщо це спричинило або могло спричинити шкоду господарюючому суб'єкту (підприємцю) [45, с. 530].

Закінченим злочин у формі комерційного шпигунства треба вважати з моменту вчинення дій, спрямованих на незаконне отримання відомостей, що становлять комерційну таємницю, незалежно від того, були такі відомості розголошено чи використано іншим чином. Фактичне використання незаконно отриманих відомостей для наявності закінченого складу даного злочину у цій формі не обов'язкове, як не є обов'язковим і заподіяння реальної істотної шкоди власнику відомостей [44, с. 477].

Під незаконним використанням відомостей, що становлять комерційну таємницю, треба розуміти впровадження у виробництво або врахування під час планування або здійснення підприємницької (господарської) діяльності без дозволу уповноваженої на те особи неправомірно здобутих відомостей, що становлять комерційну таємницю. Незаконним використанням відомостей, що становлять комерційну таємницю, має вважатися їх незаконне розголошення.

Обов'язковою ознакою об'єктивної сторони незаконного використання відомостей, що становлять комерційну таємницю, є наслідки у вигляді спричинення істотної шкоди суб'єкту господарської діяльності. Заподіяна шкода може бути як матеріальна (як правило), так і нематеріальна. Під час визначення розміру заподіяної шкоди, яка має матеріальний характер, треба враховувати прямі матеріальні збитки, витрати на відвернення шкідливих наслідків використання відомостей іншими суб'єктами господарської діяльності, збитки від зниження реалізації продукції і товарів чи зниження попиту на послуги, затрати на перепрофілювання напрямів діяльності, збитки від зниження цін на товари і послуги тощо. У ст. 231 КК України не визначається, яка за розміром матеріальна шкода може бути визнана істотною, а тому це питання має вирішуватися індивідуально. Визнання істотною заподіяної шкоди суб'єкту господарської діяльності внаслідок використання відомостей, що містять комерційну таємницю (наприклад, підрив ділової репутації), має вирішуватися у кожному конкретному випадку.

Суб'єктивна сторона злочину у випадках вчинення дій, спрямованих на незаконне отримання відомостей, що становлять комерційну або банківську таємницю, характеризується прямим умислом. Обов'язковою ознакою є мета – розголосити чи іншим чином використати незаконно отримані відомості, що становлять комерційну таємницю [45, с. 531].

Щодо наслідків незаконного використання зазначених відомостей у вигляді спричинення істотної шкоди суб'єкту господарської діяльності, умисел може бути як прямим, так і непрямим. Непрямий умисел має місце, наприклад, у випадку, коли винна

особа незаконно використовує відомості, що становлять комерційну таємницю, для модернізації власного виробництва, поліпшення власного фінансово-господарського стану, не бажаючи заподіяння шкоди іншому суб'єкту господарювання, але водночас усвідомлюючи, що таку шкоду може бути заподіяно, і свідомо допускає настання таких наслідків [43, с. 595].

Суб'єктом злочину є фізична осудна особа, яка досягла 16-річного віку. Водночас немає значення, ким зібрано і як одержано використовувані незаконно відомості, що становлять комерційну таємницю [45, с. 531].

Мотив таких дій переважно корисливий; однак суб'єкт злочинного посягання може керуватися й іншими мотивами: усунення конкуруючої фірми, небажання фінансувати науково-дослідні роботи, підрив ділової репутації суб'єкта господарської діяльності тощо [9, с. 289].

Об'єкт злочину, передбаченого ст. 232 КК України, аналогічний об'єкту злочину, передбаченого ст. 231 КК України [45, с. 531].

Розголошенням комерційної таємниці є ознайомлення іншої особи без згоди уповноваженої на те особи з відомостями, що відповідно до чинного законодавства України становлять комерційну таємницю, особою, якій ці відомості було довірено у встановленому порядку або стали відомі у зв'язку з виконанням службових обов'язків (ст. 17 Закону України від 7 червня 1996 р. № 236/96-ВР «Про захист від недобросовісної конкуренції», ст. 36 ГК). Так само потрібно вирішувати і питання щодо банківської таємниці.

Способи розголошення відомостей, що становлять комерційну таємницю, можуть бути різними: усно, письмово, із застосуванням засобів зв'язку, шляхом повідомлення у ЗМІ, наукових статтях, умисного створення умов для ознайомлення з відповідними документами або предметами (наприклад, залишення документів на робочому місці для того, щоб стороння особа, яка знаходиться у приміщенні, мала можливість ознайомитись з ними, коли винна особа, під якимось приводом, виходить з приміщення на певний час) тощо [45, с. 531].

Обов'язковою ознакою об'єктивної сторони злочину є наслідки у вигляді істотної шкоди, заподіяної суб'єкту господарської діяльності, комерційну таємницю якого розголошено.

Закінченим злочин вважається з моменту фактичного заподіяння суб'єкту господарської діяльності істотної шкоди. У разі, якщо заподіяна шкода не є істотною або взагалі не заподіяна, але матеріалами кримінального провадження встановлено, що в особи був прямий умисел на її заподіяння, то її дії треба кваліфікувати як замах на вчинення злочину, передбаченого ст. 232 КК України. З суб'єктивної сторони, розголошення комерційної таємниці характеризується прямим умислом і спеціальними мотивами – корисливим мотивом чи іншими особистими мотивами [45, с. 532].

Суб'єкт злочину, передбачений ст. 232 КК України, – спеціальний. Це особа, якій відомості, що становлять комерційну або банківську таємницю, стали відомі у зв'язку з її професійною чи службовою діяльністю і які вона повинна зберігати в таємниці. До таких осіб належать працівники податкових органів, банківських установ, правоохоронних органів, органів виконавчої влади, аудитори, адвокати та інші особи, які згідно з чинним законодавством мають право ознайомлюватися з відомостями, що становлять комерційну таємницю, чи мають доступ до таких відомостей за характером виконуваних ними професійних чи службових обов'язків.

Отже, для правильного визначення суб'єкта злочину, передбаченого ст. 232 КК України, передусім, необхідно встановити, що особа була ознайомлена з комерційною таємницею на законних підставах. У протилежному випадку вчинене може бути визнане незаконним збиранням відомостей, що становлять комерційну таємницю, та самостійно кваліфіковане за ст. 231 КК України.

Можливим є виділення таких трьох груп спеціальних суб'єктів розголошення комерційної таємниці: 1) особи, які перебувають у трудових відносинах з власником (уповноваженим органом) комерційної таємниці, професійна або службова діяльність яких безпосередньо пов'язана з функціонуванням певного

підприємства – це, так зване, посягання зсередини; 2) особи, професійна або службова діяльність яких чи інші законні підстави обумовлюють виникнення певних правовідносин цивільно-правового характеру з власником комерційної таємниці; 3) особи, які наділені власними повноваженнями з витребуванням та використанням відомостей, що становлять комерційну таємницю (наприклад, суд, співробітники органів, що здійснюють контроль за додержанням податкового законодавства, Служби безпеки України). Друга і третя групи – це посягання ззовні. До другої групи необхідно також віднести осіб, які ознайомлені з таємницею зі згоди її власника, але це ознайомлення не було обумовлене певними професійними чи службовими обов'язками такої особи (наприклад, громадянин-замовник дізнається зміст комерційної таємниці будівельної організації під час виконання нею умов цивільно-правового договору підряду).

Обов'язковість наказу щодо подання інформації, яка належить до категорії комерційної таємниці, не має використовуватися учасником 3-ї категорії з метою завдання шкоди фізичним та юридичним особам, що є суб'єктами господарювання, а саме їх правам і свободам, що охороняються законом. Суб'єкти, які втілили у життя свої імперативні приписи та яким було надано потрібні інформаційні ресурси, але в подальшому здійснили виток комерційної таємниці, повинні понести відповідальність згідно з кримінальним законодавством, якщо будуть підстави, прямо передбачені в законі.

Коли інформацію зосереджено в певній матеріальній оболонці (річ, документ як результат фіксації на папері, магнітній, кіно-, відео-, фотоплівці або іншому носії), то визнання її предметом злочину не суперечить найбільш поширеній в науці кримінального права думці про нього. Проте інформація та її матеріальні носії співвідносяться між собою як зміст і форма, тому будь-яку таємницю (державну, комерційну, лікарську, таємницю усиновлення або досудового слідства тощо) не може бути зведено до свого носія – певної речі матеріального світу [68, с. 110–113].

Необхідно зазначити, що відсутність законодавчої регламентації розміру істотної шкоди суб'єкту господарської діяльності, заподіяної, зокрема, незаконним використанням відомостей, що становлять його комерційну таємницю, а також розголошенням комерційної таємниці, робить ст. ст. 231 та 232 КК України фактично незастосовними на практиці і призводить до наявності певних перепон у можливості кримінального переслідування осіб, які вчинили зазначені протиправні дії.

Розгляд та дослідження такого елементу криміналістичної характеристики вказаного виду злочинів, як предмета злочинного посягання, відомостей, що становлять комерційну таємницю, має важливе значення для правильної кваліфікації злочинів, висунення версій щодо причетних осіб, визначення способу вчинення злочину.

Особа злочинця є поняттям, що виражає сутність особи, яка вчинила злочин [70, с. 18]. Особу злочинця, як елемент криміналістичної характеристики, визначають всі вчені-криміналісти. Однак питання про те, які ознаки і властивості треба описувати, залишається відкритим. Тому іноді особу злочинця характеризують у кримінально-правовому, а частіше – кримінологічному аспекті, які є найбільш розробленими в науці [71, с. 422].

Варто зауважити, що суб'єктом кримінального правопорушення у галузі розголошення таємниці комерційного характеру не завжди виступає суб'єкт підприємництва. Загалом такими особами є ті, які (або через яких) втілюють у життя існуючі ризики щодо безпеки інформаційного простору – це є конкуруючі сторони, або їх агентура, складові злочинного простору, співвласники тощо.

Особливу категорію суб'єктів комерційного шпигунства становлять співробітники фірми (різновид внутрішніх загроз) – вони можуть діяти як за завданням, так і без завдання конкурентів (останнє найбільш характерно для так званих «ображених співробітників»).

В Україні суб'єктом цього виду злочинів може бути лише фізична особа. Однак світовий досвід переконує в тому, що на

підприємницькому шпигунстві спеціалізуються та заробляють чималі гроші навіть окремі юридичні особи, які використовують професійні, та, здебільшого, протиправні засоби отримання інформації.

Загалом можна виділити дві групи незаконного збирання відомостей, що становлять комерційну таємницю, зокрема: 1) незаконне збирання відомостей, що становлять комерційну таємницю, з метою вдосконалення виробничої і комерційної діяльності організації, що заволоділа конфіденційною інформацією (підвищення конкурентоздатності продукції і ефективності виробництва, вибір оптимальної стратегії збуту товарів і торгових переговорів тощо), з метою завдання збитків організації-конкуренту (протидії збуту продукції, порушення виробничих і торговельних зав'язків організації: зриву торговельних переговорів і угод; зниження інвестиційних можливостей, підготовки і розповсюдження дезінформаційних матеріалів ганебного характеру тощо); 2) незаконне збирання відомостей, що становлять комерційну таємницю, з метою дезорганізації роботи окремих суб'єктів господарювання – конкурентів і галузей економіки в цілому [54, с. 40].

З урахуванням того, що злочини, які належать до першої групи, вчиняються, переважно, у національному масштабі, збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, в межах групи злочинів, що розглядаються, може здійснюватися такими суб'єктами: 1) представниками (агентами) вітчизняних фірм-конкурентів; 2) представниками вітчизняних підприємств, які спеціалізуються на оцінці економічного стану суб'єктів господарської діяльності (зокрема, аудиторських, консалтингових компаній); 3) представниками вітчизняних охоронних організацій; 4) представниками служб безпеки вітчизняних підприємств, організацій, банків; 5) злочинними елементами, які спеціалізуються на незаконному збиранні і збуті відомостей, що становлять комерційну таємницю тощо.

Суб'єктами даної групи злочинів можуть застосовуватися такі незаконні способи отримання конфіденційної інформації: 1) прослуховування телефонних переговорів; 2) викрадення документів, які містять відомості, що становлять комерційну таємницю, або їх копіювання; 3) дистанційне звукове прослуховування; 4) підкуп посадових осіб; 5) прямий доступ до комп'ютерних банків даних; 6) копіювання носіїв інформації; 7) розшифровування радіовипромінювання комп'ютерів, факсів, телетайпів; 8) візуальний контроль приміщень (через вікна); 9) слуховий контроль через резонуючі перегородки, шибки, стіни, батареї центрального опалення; 9) розміщення мікропередавачів у приміщеннях і автомобілях; 10) індуктивне знімання інформації з будь-яких неекранованих провідників у приміщенні (лінії зв'язку, електроживлення, сигналізація); 11) завоювання довіри родичів, друзів дітей об'єкта спостереження; 12) використання шпигунів-професіоналів з метою отримання інформації; 13) переманювання з роботи працівників конкурента з метою отримання інформації; 14) засилання агентів до службовців чи спеціалістів конкурента тощо [23, с. 48–65].

Характеризуючи другу групу незаконного збирання відомостей, що становлять комерційну таємницю, необхідно зазначити, що з метою досягнення поставлених цілей застосовуються: 1) компрометування шляхом поширення завідомо неправдивих (а іноді і правдивих) відомостей, що порочать продукцію конкурента, керівників фірм і їх оточення; 2) добре сплановане цілеспрямоване дезінформування потенційних партнерів своїх конкурентів, у тому числі, з використанням можливостей міжнародної мережі Інтернет або агентів у засобах масової інформації, які публікують завідомо неправдиві відомості про факти, що начебто викликають сумніви щодо якості виробів і продукції; 3) зрив крупних контрактів шляхом обнародування правдивих або завідомо неправдивих відомостей про злочинні діяння конкурентів; 4) порушення виробничих і торговельних зав'язків шляхом компрометування контрагентів, їхньої економічної і ділової надійності [54, с. 42].

Враховуючи, що злочини цієї групи вчиняються переважно у транснаціональному масштабі і у деяких випадках дії конкурентів з числа іноземних суб'єктів виходять за межі приватної ініціативи окремих фірм і здійснюються у межах спеціально розроблених державних програм «підвищення конкурентоздатності», «збільшення обсягу експорту продукції» тощо, суб'єктами їх вчинення є: 1) представники (агенти) іноземних розвідувальних організацій; 2) представники іноземних державних підприємств; 3) представники іноземних установ і банків; 4) представники приватних іноземних фірм: а) спеціально створених зарубіжними спецслужбами з метою збирання розвідувальної інформації; б) незалежних фірм, які виконують договори з розвідувальними й іншими державними відомствами на предмет виявлення і добування конфіденційної інформації економічного характеру; в) міжнародних фірм, створених з метою недобросовісної конкуренції.

Необхідно зауважити, що оскільки розголошення комерційної таємниці є одним із способів використання відомостей, що становлять комерційну таємницю, і всі випадки незаконного умисного розголошення комерційної таємниці, крім тих, що передбачені ст. 232 КК України, необхідно вважати її використанням [46, с. 617], коло суб'єктів незаконного розголошення такого роду відомостей обмежується особами, яким ця інформація відома у зв'язку з професійною або службовою діяльністю [22, с. 50–58].

Отже, ними можуть бути такі групи суб'єктів: 1) «ображені» співробітники; 2) агенти вітчизняних та іноземних суб'єктів господарської діяльності, які діють за завданням конкурентів; 3) агенти спецслужб, «підіслані» на фірму як рядові співробітники; 4) котрагенти, представники інших суб'єктів господарської діяльності, які ознайомлені з відомостями, що становлять комерційну таємницю даного підприємства, внаслідок існування договірних відносин між компаніями; 5) представники правоохоронних органів державних структур та інші.

Предметом безпосереднього посягання злочинного діяння є речі матеріального світу, здійснюючи вплив на які, особа посягає

на ті чи інші суспільні відносини. Точне встановлення предмета посягання дає можливість відмежувати один злочин від іншого, суміжного з ним. Ті або інші ознаки предмета посягання можуть виступати як пом'якшуючі або обтяжуючі обставини одного і того самого злочину [70, с. 18].

Об'єктом протиправних посягань у формі незаконного збирання з метою використання відомостей, що становлять комерційну таємницю суб'єкта господарської діяльності, є люди (персонал фірми, службові особи державних органів та інші особи, які прямо чи опосередковано мають доступ до конфіденційної інформації), документи, технічні засоби [25, с. 89].

Що стосується першого об'єкту посягання, то загальновідомим є факт, що саме персонал суб'єкта господарської діяльності генерує нові ідеї, нововведення, відкриття і винаходи, які прискорюють науково-технічний прогрес, підвищують добробут працівників фірми і є корисними не тільки для фірми в цілому, а й для кожного окремого співробітника. Незважаючи на це, персонал, на жаль, є одночасно й основним джерелом втрати конфіденційної інформації компанії, до того ж, найбільш важко контрольованим.

Джерелом поширення відомостей, що становлять комерційну або банківську таємницю, яке іменується «персоналом», зазвичай є: 1) усі співробітники відповідного підприємства; 2) співробітники інших фірм – посередники, виробники комплектуючих деталей, торгових фірм, рекламних агентств тощо; 3) співробітники державних установ, до яких фірма звертається відповідно до закону – податкових та інших інспекцій, муніципальних органів, правоохоронних органів тощо; 4) журналісти засобів масової інформації, які співпрацюють з фірмою; 5) відвідувачі компанії, працівники комунальних служб, поштові службовці, працівники служб екстремальної допомоги тощо; 6) сторонні особи, які працюють або проживають поряд з будинком або приміщеннями фірми; 7) родичі, знайомі або друзі всіх зазначених осіб та інших. Перераховані особи тією чи іншою мірою є або можуть за певних обставин стати джерелом витоку відомостей конфіденційного характеру.

Доречно зауважити, що найбільш повно обізнаними з відомостями, що становлять комерційну таємницю суб'єкта господарської діяльності, є такі групи осіб: 1) керівний склад працівників підприємства, зокрема, керівник, його перший заступник, їх референти і секретарі, головний бухгалтер; 2) особи з допоміжного персоналу, які мають доступ до комерційної таємниці, зокрема, працівники служби конфіденційної документації; 3) співробітники, з боку яких потенційно існує небезпека надання злочинним елементам подібного роду відомостей – особисті охоронці, водії персональних машин керівників та інші; 4) співробітники служби безпеки підприємства [54, с. 44].

Щодо документів та технічних засобів як різновидів об'єктів посягання, то у загальному плані предметом безпосереднього замаху в структурі криміналістичної характеристики незаконного збирання з метою використання відомостей, що становлять комерційну таємницю, можуть бути такі, що містять комерційну таємницю: 1) записи, звіти, протоколи, схеми, креслення, матеріали, зразки, моделі, прилади, речовини й інші джерела інформації, що належать суб'єкту господарювання у вигляді неоформлених або неповних патентів, формул, технічних проєктів «ноу-хау», результатів наукових досліджень, програмних продуктів, а також калькуляції витрат виробництва, структури ціни, контрактів, даних про постачальників і клієнтів, відомостей про конфіденційні ділові переговори, оглядів ринку, інвестицій і відомості, що становлять комерційний інтерес; 2) ідеї, винаходи, відкриття; окремі формули, нові технічні проєкти; 3) нові методи організації праці та виробництва; 4) програмне забезпечення; 5) результати наукових досліджень; 6) описи технологічних іспитів; 7) відомості про матеріали, з яких виготовлено окремі деталі, умови експериментів, обладнання та устаткування, на якому вони проводилися тощо; 8) окремі нові або унікальні вимірювальні комплекси, прилади, верстати і устаткування, що використовуються на підприємстві; 9) відомості ділового характеру, зокрема, про укладені або заплановані контракти, дані про постачальників та клієнтів,

огляди ринку, маркетингові дослідження, інформація про конфіденційні переговори, калькуляція витрат виробництва підприємства, структури цін, рівень прибутку, плани розвитку підприємства та його інвестиції тощо [54, с. 45–46].

Отже, предметом безпосереднього посягання у структурі криміналістичної характеристики незаконного збирання з метою використання відомостей, що становлять комерційну таємницю підприємства, можуть виступати такі види інформації: 1) у сфері виробництва, технології і науково-дослідних робіт: а) продуктивний капітал, його потужність, технічний стан (зношеність); б) ефективність виробництва; в) стан технології, напрями її розвитку, модифікація і модернізація; г) технічні параметри продукції і її окремих вузлів; ґ) матеріали, що використовуються для виробництва продуктів і надання послуг; д) програмне забезпечення виробництва; е) інформаційний прогрес [54, с. 46]; є) транспортні канали фірми, їх стан, перспективи і плани розвитку; ж) науково-дослідні і експериментальні роботи, відкриття і винаходи, патенти, ліцензії, «ноу-хау» тощо; з) матеріали виробничих нарад, зібрань, оперативних розпоряджень тощо; 2) ділова і комерційна інформація: а) програми розвитку, бізнес-плани; б) відомості про плани підприємства щодо розширення виробництва та інші комерційні задуми; в) план виробництва та перспективний план; г) плани запасів і готової продукції; ґ) відомості про проєкти річних і перспективних експортно-імпортних планів щодо зовнішньоекономічної організації тощо [54, с. 47]; д) організація управління фірмою – відомості про застосовувані оригінальні методи управління, відомості про підготовку, прийняття і виконання окремих рішень керівництва підприємства з комерційних, організаційних, виробничих, науково-дослідних та інших питань; е) відомості про торгових клієнтів, постачальників, посередників тощо; є) цінова політика фірми, методики розрахунків цін; ж) умови угод, контрактів з діловими партнерами; з) плани реклами і маркетингу як провідної галузі господарського управління, до

функцій якого входить організація і керівництво усією сукупністю видів діяльності, пов'язаних з перевтіленням купівельної спроможності споживачів в ефективний попит на специфічний виріб або послугу, а також з доведенням цього виробу до кінцевого або проміжного покупця, щоб забезпечити встановлену компанією норму прибутку або досягнення іншої мети; и) протоколи переговорів з діловими партнерами тощо; 3) інформація про фінансовий стан суб'єкта господарської діяльності: а) показники балансу для розрахунків (коефіцієнт автономії, ефективності підприємництва, покриття, питомої ваги чистих мобільних засобів, коефіцієнт абсолютної ліквідності, загальний коефіцієнт ліквідності); б) прибутковість компанії та її окремих виробництв; в) кошти виробництва в цілому, окремих товарів і послуг; г) експертно-імпортні і валютні операції; ґ) стан інвестицій і інвестиційну політику; д) відомості про баланси підприємства; е) дані, що містяться в бухгалтерських книгах управління; є) відомості про обіг засобів підприємства; ж) відомості про фінансові операції компанії; з) про стан банківських рахунків суб'єкта господарювання, виробничі операції; и) відомості про боргові зобов'язання тощо; 4) інформація про соціальний стан в колективі фірми: а) інтелектуальний потенціал головних і провідних фахівців фірми, їхні ділові якості і моральний стан, біографічні дані, компрометуючі зв'язки; плани кадрових змін в колективі (просунення по службі, звільнення, відставки тощо); б) про систему матеріальних і моральних стимулів в колективі; в) про конфлікти в колективі серед менеджерів і працівників, між окремими формальними і неформальними групами працівників; г) про відносини між менеджерами підприємства; ґ) про наявність у окремих менеджерів, фахівців і працівників фінансових проблем; д) про наявність намірів створити власний бізнес окремими менеджерами, фахівцями і працівниками фірми тощо; 5) інформація про відношення до ринку: а) відомості про застосовувані підприємством оригінальні методи вивчення ринку; б) відомості про результати вивчення ринку,

що містяться в оцінках стану і перспектив розвитку ринкової кон'юнктури; в) відомості про ринкову стратегію підприємства; г) відомості про застосовувані суб'єктом господарської діяльності оригінальні методи здійснення продажу товарів, технологій, надання послуг тощо; ґ) відомості про ефективність комерційної діяльності підприємства; 6) відомості про партнерів, тобто систематизовані дані про внутрішніх і зарубіжних замовників, підрядників, постачальників, споживачів, покупців, компаньйонів, спонсорів, посередників, клієнтів та інші ділові відносини суб'єкта господарювання, а також про його конкурентів, які не містяться у відкритих джерелах (довідниках, каталогах тощо); 7) відомості про переговори суб'єкта господарської діяльності, що містять інформацію про підготовку, проведення і результати переговорів з його діловими партнерами; 8) відомості, умови конфіденційності яких встановлено у договорах, контрактах, угодах та інших зобов'язаннях підприємства; 9) відомості про методи розрахунків, структуру і рівень цін на продукцію та послуги і розміри скидок; 10) інформація про підготовку до торгів або аукціону та їх результати; 11) дані у сфері науки і техніки: а) відомості про цілі, завдання, програми перспективних наукових досліджень; б) точні значення конструкційних характеристик створюваних виробів і оптимальних параметрів розроблюваних технологічних процесів (розміри, обсяги, конфігурація, процентний вміст компонентів, температура, тиск, час тощо); в) аналітичні і графічні залежності, що відображають відкриті закономірності і взаємозв'язки; г) дані про умови експериментів і обладнання, на якому вони проводилися; ґ) відомості про матеріали, з яких виготовлено окремі деталі; д) відомості про методи захисту від підробки товарних знаків; 12) відомості про використовувані і розроблювані технології, їхні особливості і специфіку їх застосування; 13) інформація щодо забезпечення економічної безпеки суб'єкта господарської діяльності: а) відомості про порядок і стан організації захисту комерційної таємниці; б) відомості про порядок і стан організації охорони, пропускний

режим, систему сигналізації; в) найважливіші елементи систем безпеки, кодів і процедур доступу до інформаційних мереж і центрів [32, с. 62]; г) відомості, що становлять комерційну таємницю підприємств-партнерів, а також дані, передані на основі довіри [49, с. 24–26] та інші відомості.

Необхідно зауважити, що перелік відомостей, що можуть становити комерційну таємницю суб'єктів господарської діяльності, і, відповідно, виступати предметом посягання правопорушників, не є вичерпним. Його розширення безпосередньо залежить від здобутків науково-технічного прогресу щодо можливостей виробництва нових видів продукції або надання послуг і визначається видом конкретного підприємства, завданнями його створення і метою діяльності.

1.3. Характеристика способів та слідова картина незаконного збирання або використання відомостей, що становлять комерційну або банківську таємницю

У системі структурних елементів, що розкривають зміст криміналістичної характеристики злочинів, пов'язаних з незаконним збиранням та розголошенням комерційної або банківської таємниці, особливе місце посідає спосіб злочину. Інформація про спосіб злочину дає змогу визначити шляхи встановлення злочинця і його співучасників, предмет злочинного посягання [70, с. 37].

Крім того, відповідно до вимог п. 1 ст. 91 КПК України, у кримінальному провадженні підлягають доказуванню час, місце, спосіб та інші обставини вчинення кримінального правопорушення.

Характеристика способу вчинення злочину, його поширеність, конкретні прийоми реалізації, використовувані технічні засоби, їх конструктивні особливості, джерела отримання та інше можуть надати істотну для розслідування інформацію.

Дані про спосіб злочину мають також важливе значення для розкриття раніше вчинених аналогічним способом злочинів [70, с. 37].

Отже, спосіб злочинів у сфері порушення комерційної або банківської таємниці є ключовим елементом криміналістичної

характеристики злочинних посягань даного виду, оскільки в умовах сьогодення перелік таких способів не залишається сталим: він невпинно зростає, використовуючи здобутки науково-технічного прогресу [24, с. 113–118].

Основний перелік способів отримання інформації про конкурентів був опублікований доктором Уортом Уайдом в журналі «Chemical Engineering» ще в 1965 році [54, с. 50].

Цей перелік не втратив свою актуальність і досі. Він містить як законні, так і незаконні способи отримання відомостей, що становлять комерційну таємницю.

До числа законних можна віднести: 1) збір і узагальнення інформації ЗМІ; 2) вивчення реклами конкурента; 3) відвідування і вивчення фірмових магазинів конкурентів [54, с. 50]; 4) ознайомлення з публікаціями конкурентів і звітами про процеси, отримані звичайними шляхами; 5) доступ до відомостей, наданих публічно колишніми службовцями конкурента; 6) огляди ринків і доповіді інженерів-консультантів; 7) вивчення фінансових звітів конкурентів (публічного характеру); відвідування ярмарок і виставок, які влаштовуються конкурентами, і ознайомлення з видаваними ними брошурами; 8) аналіз виробів конкурентів; 9) ознайомлення зі звітами комівояжерів і відділів закупівлі тощо [54, с. 51].

На нашу думку, легальні методи добування інформації про конкурентів, які належать до арсеналу так званої «конкурентної розвідки» і передбачають отримання інформації з різних легальних джерел для того, щоб оцінити переваги і недоліки своєї продукції, послуг і методів маркетингу, можна вважати такими, що відповідають етично допустимим нормам ведення конкурентної боротьби. Зокрема, у Посібнику щодо здійснення бізнесу корпорацією IBM така практика визнається допустимою і необхідною в умовах конкуренції. Водночас зазначається про неприпустимість використання з метою отримання інформації про комерційні секрети конкурентів або іншої конфіденційної інформації такі методи як: несанкціоноване вторгнення в приватні володіння; злом, підслуховування, підкуп і крадіжки; намагання отримати

інформацію за допомогою найму або переманювання працівників фірми-конкурента, а також незаконне вимагання даних від працівників фірм-конкурентів або фірм-клієнтів.

Проте рівень прибутків і переваги у конкурентній боротьбі, які можна отримати в результаті використання відомостей конфіденційного характеру, що належать фірмам-конкурентам, змушує суб'єктів господарської діяльності використовувати незаконні способи добування зазначених даних.

До числа таких способів належать: 1) фінансування контрактів на виконання науково-дослідних робіт за кордоном з метою проникнення в деякі лабораторії; 2) відправлення на навчання за кордон студентів і стажерів [40, с. 220]; 3) спроби запросити на роботу спеціалістів, які працюють у конкурента, і вивчення заповнених ними з цією метою анкет; 4) обережно задані запитання спеціалістам конкурента на спеціальних конгресах тощо; 5) безпосереднє таємне спостереження; 6) удаване пропонування роботи службовцям конкурента без наміру брати їх на роботу з метою отримання від них інформації; 7) удавані переговори з конкурентом начебто для придбання ліцензії на один з патентів; 8) використання шпигунів-професіоналів для отримання інформації; 9) переманювання з роботи працівників конкурента для отримання інформації; 10) посягання на власність конкурента; 11) підкуп співробітників закупівельного відділу конкурента чи його службовців; 12) засилання агентів до службовців чи спеціалістів конкурента; 13) підслуховування розмов у конкурента; 14) викрадення креслень, зразків, документів тощо; 15) шантаж і різні способи тиску [54, с. 52]; 16) негласний контроль за діловою кореспонденцією; 17) перехоплення носіїв інформації, що становить комерційну таємницю суб'єкта господарської діяльності, на каналах їх транспортування (пошта, кур'єри), зокрема, використання телемоніторів-голок, які дають можливість через непроклеєні кути конвертів, якщо вони додатково не проклеєні липкою стрічкою, прочитати зміст документа, який містить відомості, що становлять комерційну таємницю, ділового листа тощо,

не розкриваючи конверт [54, с. 52]; 18) отримання інформації, що становить комерційну таємницю підприємства, через «кошик зі сміттям» (викинуті чернетки, пошкоджені носії, відпрацьовані документи тощо) тощо.

Міжнародна практика знає також багато інших способів, які використовуються для отримання конфіденційної інформації суб'єктів господарської діяльності. Ними є, зокрема, такі способи: 1) незаконне отримання конфіденційної інформації шляхом викрадення персональних комп'ютерів і магнітних носіїв; 2) незаконне отримання конфіденційної інформації шляхом вивідування відомостей, що становлять комерційну таємницю; 3) незаконне отримання конфіденційної інформації шляхом запровадження спеціальних співробітників – «кротів»; 4) незаконне отримання відомостей, що становлять комерційну таємницю суб'єкта господарської діяльності, шляхом перехоплення інформації, що циркулює у технічних засобах, транспортних засобах і приміщеннях: а) приміщеннях підприємства; б) квартирах (дачах, підсобних, нежитлових приміщеннях тощо) його співробітників [54, с. 53–54]; 5) незаконне заволодіння конфіденційною інформацією, що утримується в засобах обчислювальної техніки і автоматизованих системах тощо [54, с. 56–57]; 6) злом систем сотового зв'язку, що дає можливість: а) отримати інформацію про точне розташування абонента з метою отримання конфіденційних відомостей; б) записувати і прослуховувати розмови, які стосуються комерційних секретів фірми; в) дистанційно вмикати мікрофон для прослуховування зазначених розмов тощо [54, с. 56].

Характеризуючи незаконне збирання з метою використання відомостей, що становлять комерційну або банківську таємницю суб'єкта господарської діяльності, шляхом несанкціонованого отримання інформації, що циркулює в ЕОМ, необхідно зауважити, що попри існування значної кількості таких способів, їх можна класифікувати за двома ознаками: 1) наявність чи відсутність необхідності проникнення в приміщення, де працює ЕОМ, в якій циркулює інформація, що становить комерційну таємницю суб'єкта господарської

діяльності; 2) залежність виникнення каналу поширення інформації від процесу її оброблення (наявність чи відсутність необхідності перебування комп'ютера у працюючому стані) [54, с. 53–54].

Потрібно також зауважити, що поділ способів отримання відомостей, що становлять комерційну таємницю суб'єкта господарської діяльності, на законні та незаконні є, певною мірою, умовним і залежить від позиції конкретного підприємства у визначенні їх як таких.

Можна з упевненістю стверджувати, що в умовах сьогодення характер способів незаконного отримання інформації, що становить комерційну таємницю, істотно не змінився, проте завдяки досягненням сучасної науки і техніки значно збільшилися технічні можливості забезпечення практичної реалізації багатьох способів незаконного збирання комерційної таємниці [23, с. 48–65]. Зокрема, для отримання відомостей можуть використовуватися мініатюрні приховані і спеціальні (камуфльовані під звичайні предмети) фото- і відеокамери: а) мініатюрні (приховані), які монтуються в побутову техніку і передають відеоінформацію по кабелю або за допомогою телевізійного передавача; б) спеціальні, що маскуються під побутові предмети, наприклад, пачку цигарок, кейс, книгу, наручний годинник тощо. Апаратуру для прихованої фото- і відеофіксації зазвичай обладнано спеціальними об'єктивами і насадками, зокрема: а) мініатюрними об'єктивами, призначеними для виконання зазначених дій через отвори невеликого діаметру (до 5 мм); б) телескопічними об'єктивами, які дають змогу вести відеофіксацію з великих відстаней; в) камуфляжними об'єктивами, які використовуються для прихованої відеофіксації з різного роду побутових предметів, наприклад, з кейсів; г) об'єктивами, поєднаними з приладами нічного бачення (з інфрачервоною підсвіткою), і призначеними для проведення відеофіксації в темний час доби [54, с. 55].

Останніми роками розвиток засобів звукозапису, їх надійність, мініатюрність, простота та повнота організації різного роду аудіоінформації привели до широкого використання останніх у побуті, у роботі правоохоронних органів, у розвідувальній і

контррозвідувальній діяльності комерційних структур щодо заволодіння інформацією економічного характеру [38, с. 57].

Сьогодні значно поширилося використання радіомікрофонів, що виконують функцію мікропередавання інформації. Вони діють на відстані 300-500 м. Структурне підґрунтя сьогодення дає можливість виготовляти такі знаряддя навіть дома. «Вести слуховий контроль можна гостроспрямованими мікрофонами, які мають голчасту діаграму спрямованості. За допомогою такого мікрофона можна прослуховувати розмову на відстані до 1 км. Розмову за незахищеними віконними шибками офісу можна прослуховувати шляхом детектування відбитого від скла лазерного променя. Звукові коливання в приміщенні приводять до синхронної вібрації шибок, а вони, своєю чергою, модулюють відбитий лазерний промінь [54, с. 55].

Узагальнюючи викладене, зазначимо, що найпоширенішими засобами здобуття інформаційних ресурсів із категорії тих, що належать до комерційної таємниці, є такі:

1) прослуховування телефонних переговорів;

2) викрадення документів, які містять відомості, що становлять комерційну таємницю, або їх копіювання;

3) дистанційне звукове прослуховування;

4) підкуп посадових осіб;

5) прямий доступ до комп'ютерних банків даних; копіювання носіїв інформації; розшифровування радіовипромінювання комп'ютерів, факсів, телетайпів;

6) візуальний контроль приміщень (через вікна);

7) слуховий контроль через резонуючі перегородки, шибки, стіни, батареї центрального опалення;

8) установка мікропередавачів у приміщеннях і автомобілях; індуктивне знімання інформації з будь-яких неекранованих провідників у приміщенні (лінії зв'язку, електроживлення, сигналізація);

9) завоювання довіри родичів, друзів і дітей об'єкта спостереження;

10) незаконне отримання інформації через корумповані елементи в ешелонах влади тощо [54, с. 56].

У криміналістиці потрібно розрізняти два основні способи незаконного отримання відомостей, що становлять комерційну таємницю: 1) отримання відомостей шляхом заволодіння документом (або носієм інформації на твердій основі, технічними засобами), в якому вони утримуються; 2) отримання відомостей без заволодіння документом [54, с. 56].

Перший спосіб містить в собі: а) викрадення документів, що знаходяться у володінні відповідальної за них особи (у тому числі, «замовні викрадення» з участю спеціально запроваджених «кротів» – агентів, або представників кримінальних структур); б) заволодіння документами, що вийшли із законного володіння у результаті його втрати і такими, що знаходяться без охорони.

Другий спосіб охоплює: а) отримання відомостей в усній формі від обізнаних з ними осіб; б) отримання неврахованих копій документів (виготовлених шляхом ксерокопіювання, сканування, копіювання магнітних носіїв); в) отримання відомостей у результаті перехоплення інформації, що циркулює в технічних засобах, приміщеннях, засобах транспорту.

Зазвичай з метою незаконного отримання інформації застосовуються: 1) підкуп (або погрози) працівників організації, які мають доступ до документів, що містять комерційну таємницю; 2) схиляння до розголошення комерційної таємниці співробітників організації, які мають доступ до конфіденційних відомостей, а також співробітників, які змінили місце роботи і пенсіонерів, які мали доступ до закритої інформації (шляхом підкупу, погроз, або використання етнічної, релігійної або расової близькості); 3) запровадження «кротів» – агентури на посади, що дозволяють отримати безпосередній доступ до документів, що утримують комерційну таємницю, або приховано збирати конфіденційну інформацію в процесі службової (виробничої) діяльності; 4) підкуп посередників у торгових переговорах; 5) перехоплення інформації, що циркулює в технічних засобах і приміщеннях (службових, житлових та інших); 6) несанкціонований доступ до відомостей, що містяться в засобах обчислювальної техніки і електронних банках даних.

Особливим прийомом незаконного отримання відомостей, що становлять комерційну таємницю, без заволодіння документом, є так зване розвідувальне опитування. Його сутність полягає в замаскованому вивідуванні інформації в обізнаних осіб, які розголошують комерційну таємницю, не усвідомлюючи цього. Внаслідок складнощів, що виникають під час доказування суб'єктивної сторони подібних діянь, особи, які збирають інформацію, зазвичай залишаються непокараними.

Вибір способу викрадення документа нерідко визначається наявністю тих чи інших відступів від правил конфіденційного діловодства, які, відповідно, знижують ступінь захищеності об'єкта посягання.

У більшості випадків документи викрадаються таємно. Відкрите посягання на заволодіння документами, що містять комерційну або банківську таємницю, не є характерним для даного виду злочинів. Таке викрадення складається з таких елементів: підготовки до скоєння злочину; заволодіння документом; маскувальних дій. Добування відомостей, що становлять комерційну таємницю, нерідко пов'язане з проведенням масштабних, багатоходових підготовчих операцій. Найбільш об'ємною за затратами часу і енергії переважно є підготовка до викрадення документів, пов'язана із проникненням в організацію, що володіє секретними відомостями ділового характеру, спеціальних агентів. Іноді такі «кроти» запроваджуються поетапно через проміжні фірми або державні структури. В таких випадках підготовчі дії агентів спрямовано на отримання офіційного доступу до конфіденційного діловодства, або призначення на посаду, що дає можливість підтримувати ділові контакти з особами, які працюють із закритими матеріалами. Агенти встановлюють неслужбові зв'язки з особами, допущеними до конфіденційного діловодства. Вони: а) виявляють стійкі порушення правил поводження з конфіденційними документами з метою вибору ситуації, зручної для таємного заволодіння ними; б) шукають можливість безконтрольного перебування в приміщенні, де зберігається або оброблюється конфіденційна

інформація; в) намагаються отримати у своє користування штатний ключ від вказаного приміщення чи сейфа; г) завчасно готують схованки для короткострокового або довгострокового зберігання викрадених конфіденційних матеріалів тощо. Зазначені дії можуть доповнюватися: підшуканням співучасників злочину; виготовленням, пристосуванням знаряддя вчинення злочину; усуненням обставин, що заважають викраденню. Частина вказаних елементів підготовки до викрадення документів характерна і для протиправних дій підкупленого співробітника організації, а також особи, яка викрадає документи з власної ініціативи з метою їх продажу [54, с. 59].

В окремих випадках підготовчий етап і маскувальні дії можуть бути відсутніми зовсім, або бути наявними в стислій формі. До підготовчих дій стосовно викрадення документів необхідно віднести різні види стеження, яке здійснюється з метою виявлення обставин, що сприяють скоєнню злочину.

За способами заволодіння документом викрадення поділяється на два основних види: а) заволодіння документом, що знаходиться у віданні відповідальної особи без достатньої охорони; б) заволодіння документом, що вийшов з відання відповідальної особи в результаті втрати.

Практика засвідчує, що найбільш поширеним є перший вид викрадення. Дії, здійснені таким способом, несуть найбільш ґрунтовну криміналістично значущу інформацію, а узагальнені дані про них відображають стійкі характеристики злочинних посягань на заволодіння документами.

Встановлено, зокрема, що більше половини викрадень документів здійснюється із закритих приміщень – службових кабінетів, охоронюваних будівель, із використанням штатного ключа. Викрадачі використовували основний і запасний ключі, що зберігалися в неналежних місцях, викрадали його у відповідальної особи, присвоювали під час передачі сховища у користування інших співробітників. Випадки використання під час викрадення нештатного ключа (шляхом підбору чи підгонки) мали епізодичний характер.

Досить поширеним є спосіб заволодіння документами, залишеними на певний час поза сейфом у службовому кабінеті (іноді в квартирі, у номері готелю), шляхом проникнення через парадні двері з використанням ключа або відмички та інших пристроїв, іноді через невідкрите вікно.

Відносно менше поширені випадки, коли для протиправного заволодіння документом злочинець використовує факт його неврахованої видачі (видачі без належного оформлення) або приховує отриманий у встановленому порядку документ після внесення відповідних незаконних записів в обліки відповідальної особи (підставний підпис, викрадення розписки, реєстру, картки).

Останнє місце за поширеністю займають випадки заволодіння документом, залишеним без належної охорони в процесі санкціонованого знищення. Тим не менше, саме цей спосіб є найбільш небезпечним, оскільки факт викрадення і незаконного використання документів маскується найбільш переконливо.

Специфічний різновид викрадень становлять випадки протиправного заволодіння документами, не забезпеченими належною охороною, у процесі їхнього несанкціонованого переміщення в транспортних засобах (літаках і поїздах, зберігання в номерах і сейфах готелів та інших місць проживання). Зазвичай вказані викрадення є замовними і виконуються спеціально підготовленими співробітниками державних спецслужб, приватних організацій чи кримінальними елементами. Маршрути переміщення документів завчасно відслідковуються, дії викрадачів ретельно плануються і маскуються під звичайну крадіжку. Водночас не виключено, що в окремих випадках умисел викрадача дійсно було спрямовано на викрадення майна (ПЕОМ, портфель тощо), а документи, що знаходилися в ньому, не бралися до уваги. За наявними даними, документи, що містили комерційну таємницю, викрадалися під час посягань на майно відповідальних осіб шляхом крадіжки, грабежу, розбійного нападу. Показово, що в багатьох випадках відповідальні особи знаходилися в стані сп'яніння [54, с. 61].

Умисні посягання на викрадення документів з криміналістичного погляду характеризуються наявністю специфічних матеріальних слідів у місці зберігання документа. Ними є: 1) сліди несанкціонованого відмикання сейфа – траси нештатного ключа або відмички, металеві ошурки на деталях і коробці замка; 2) порушення цілісності печатки або сліди її тимчасового видалення (з наступним відновленням) шляхом зрізання, відокремлення від корпусу сховища після заморожування, пошкодження закріплюючих пристроїв для опечатування; 3) сліди використання запасного ключа, що зберігається у встановленому місці; 4) сліди пошкодження корпусу сейфа – злом, віджим, розрізання; сліди рук і одягу на корпусі сейфа, а також на документах і предметах, що залишилися після викрадення у сховищі, у тому числі частинки шкіри і сліди крові на гострих кромках корпусу сейфа; 5) сліди виїмки документа через щілину пошкодженого сховища; 6) сліди проникнення сторонньої особи на охоронюваний об'єкт і перебування в приміщенні, де виявлено відсутність конфіденційних матеріалів; виведення з ладу чи вимкнення захисної сигналізації; ознаки проникнення в приміщення через вікно або яким-небудь іншим чином; 7) сліди рук, ніг сторонньої особи в приміщенні, викинуті або випущені нею предмети.

Характерні матеріальні сліди під час подолання захисних засобів, розрізання сейфа і контакту з викраденими конфіденційними матеріалами залишаються на самому викрадачі і його одязі. До них відносяться садна, подряпини, мікрочастинки документа чи предмета.

Крім того, протиправне заволодіння конфіденційними матеріалами передбачає їх використання (а в окремих випадках – знищення) зловмисниками. Це своєю чергою створює передумови виявлення слідів викрадення і викриття винних осіб. До слідів використання викрадених конфіденційних матеріалів належать: 1) матеріальні сліди на викраденому документі – відбитки пальців, нашарування мікрооб'єктів тощо; 2) сліди знищення викраденого документа – шматки паперу, обвуглені його частини,

незгорілі фрагменти, скріпки; 3) деталі виробу, залишки речовини виробу або продуктів його згоряння тощо [54, с. 63].

Слідами використання викрадених конфіденційних матеріалів можуть слугувати факти використання документа підприємствами-конкурентами, приватними особами з метою розголошення або незаконного використання з корисливих міркувань, з навчальною метою, а також факти, що засвідчують отримання особою, яка підозрюється у викраденні конфіденційних матеріалів, значних грошових сум чи цінностей.

Спосіб, що полягає у незаконному отриманні конфіденційної інформації шляхом викрадення малогабаритних персональних комп'ютерів і магнітних носіїв, у цілому, не має істотних відмінностей від описаних вище прикладів викрадення документів. До особливостей у даному випадку необхідно віднести такі обставини: 1) технічні засоби, в яких міститься інформація, на відміну від документів, частіше за все, викрадаються за межами охоронюваних службових приміщень (в авіаційному або залізничному транспорті, готелях, тимчасових службових приміщеннях виставочних комплексів, у квартирах за місцем постійного проживання тощо); 2) до вчинення вказаного злочину нерідко мають безпосереднє відношення особи з кримінального середовища, які спеціалізуються на незаконному проникненні в приміщення і відкритті сейфів та інших сховищ; 3) нерідко в злочинну діяльність втягуються представники обслуговуючого персоналу готелів, залізничних і авіакомпаній, які надають викрадачам допомогу в проникненні у приміщення і відкритті сейфів; 4) вчинення злочину з метою незаконного отримання конфіденційної інформації зазвичай маскується під звичайну крадіжку майна.

Типові способи незаконного отримання конфіденційної інформації шляхом вивідування відомостей, що становлять комерційну таємницю, або незаконних оперативно-розвідувальних заходів, характеризуються такими ознаками: у разі застосування відкритого розвідувального опитування, як способу заволодіння інформацією, що становить комерційну таємницю суб'єкта

господарювання, особа підбурюється до розголошення довірених їй відомостей шляхом підкупу, погроз, умовляння. У цьому разі може бути використано також обставини, пов'язані з етнічною близькістю, родинними відносинами, бажанням помститися за несправедливість керівників та звільнення. Відомості можуть бути розголошені шляхом усного переказу, надання можливості ознайомитися з текстом документа або з текстом, виведеним на екран монітора ПЕОМ, а також шляхом передачі інформації, скопійованої на неврахований твердий носій (папір, диск).

Замасковане отримання відомостей здійснюється за допомогою застосування спеціальних прийомів отримання інформації від осіб, які розголошують комерційну таємницю, не усвідомлюючи цього. Відомості збираються з розрізнених висловлювань і обмовок таких осіб, ініційованих правопорушником. Цей прийом зазвичай доповнюється збиранням відповідної інформації з випадково почутих або навмисно підслуханих (без використання технічних засобів) службових переговорів, виступів на нарадах, перегляду тексту на екрані монітора. Водночас особа, яка збирає інформацію, може використовувати для підслуховування недостатню звукоізоляцію стін і перегородок, особливості конструкцій вхідних вентиляційних каналів і кондиціонерів, відсутність візуального захисту екранів від неохоронюваної зони. Зазначені способи незаконного отримання інформації застосовуються під час спільної роботи або неслужбового спілкування, у процесі торгово-промислових виставок, презентацій, семінарів експертів і бізнесменів [54, с. 65].

Значного поширення набули випадки замаскованого збирання інформації з використанням спеціальних анкет і переліків питань. Питання розвідувального характеру подрібнюються, ретельно маскуються серед інших. Безпека цього способу і порівняно невеликі витрати на його застосування дають можливість проводити такі акції в широких масштабах [54, с. 65].

Особливості незаконного отримання конфіденційної інформації шляхом запровадження спеціальних співробітників

– «кротів» – полягають в отриманні відомостей, що становлять комерційну таємницю, шляхом запровадження таких осіб на посади, які дозволяють отримати безпосередній доступ до інформації і документів, або приховано збирати конфіденційну інформацію у процесі службової (виробничої) діяльності. Дії таких осіб, спрямовані на збирання відомостей, можуть полягати у: викраденні документів, бракованих або неврахованих копій, копіюванні документів з використанням фототехніки, ксероксу, сканеру, телефаксу; виготовленні додаткових примірників документів під час їх тиражування; копіюванні магнітних носіїв; записі інформації на диктофон чи паперовий носій, запам'ятовуванні інформації тощо. Для передачі (розголошення) зібраних відомостей можуть використовуватися особисті зустрічі з «замовником» незаконно отриманої інформації (або іншою особою за його дорученням), а також поштові, технічні та інші канали зв'язку.

Підготовка до запровадження «крота» передбачає дії щодо добування відомостей про володільця і види охоронюваної інформації, місця її зберігання, процедуру отримання, обробки, накопичення, правила ознайомлення, можливості виносу документів та інших носіїв за межі території. У цьому випадку підлягає з'ясуванню встановлений в організації порядок ознайомлення з конфіденційною інформацією; структура і ефективність діяльності служби безпеки; технічні засоби охорони. Також повинно бути ретельно вивчено вимоги до осіб, які можуть влаштуватися на роботу, джерела поповнення кадрів тощо. Зокрема, може бути вироблено легенду, що переконливо аргументує факт вступу особи до організації, позитивно характеризує її з ділової та особистісної сторони. Вживаються дії щодо маскування її зв'язків з конкурентами і кримінальними елементами, окремі біографічні дані, факти негативної поведінки або конфліктів із законом, кредиторами, податковими та іншими правоохоронними органами [54, с. 67].

Дії, спрямовані на незаконне отримання відомостей, що циркулюють у технічних засобах і приміщеннях, істотно відрізняються

залежно від того, з яких об'єктів і яким способом знімається інформація, чи використовував правопорушник технічні засоби і прилади перехоплення інформації (і які саме) або отримував відомості шляхом безпосереднього сприйняття без використання технічних засобів.

Об'єкти, з яких знімається інформація, поділяються на основні технічні засоби і системи (та їх комунікації), використовувані для обробки, зберігання і передачі конфіденційної інформації та допоміжні технічні засоби і системи, безпосередньо не призначені для передачі, обробки і зберігання конфіденційної інформації, встановлювані разом з основними технічними засобами або в захищених приміщеннях. До них належать різного роду телефонні засоби, засоби радіозв'язку, охоронної і пожежної сигналізації, кондиціювання; системи провідної радіотрансляційної мережі, засоби електронної оргтехніки.

Електронні прилади перехоплення інформації поділяються на вбудовані в основні технічні засоби обробки і передачі інформації (зазвичай для їх придбання організацією-власником відомостей, які підлягають захисту), на такі, що знімають інформацію за рахунок побічних електромагнітних випромінювань, та на ті, що знімають інформацію у вигляді акустичного (мовного) сигналу.

Запровадження приладів перехоплення інформації другого і третього типів в огороджувальні конструкції приміщення, системи опалення і вентиляції, меблі та інші предмети інтер'єру, а також лінії та апаратуру систем зв'язку, електроживлення, освітлення і сигналізації зазвичай потребує проникнення у приміщення, яке охороняється, або на охоронювану територію.

Перераховані відмінності технічних засобів безпосередньо пов'язані зі способом їхньої установки та використання і визначають особливості особи правопорушника. Особа, яка запроваджує «закладку» в захищеному приміщенні, мусить мати певні технічні навички, мати можливість тимчасового або безконтрольного постійного перебування в приміщенні. Вказані особи переважно є співробітниками організації або представниками технічних чи

інших служб організацій, які беруть участь в налагодженні і ремонті обладнання.

Засоби перехоплення інформації, що приховано встановлюються за межами захищеного приміщення (території), можуть являти собою прилади, які не потребують механічного контакту з контрольованим об'єктом, або під'єднуватися до ліній і комунікацій, що виходять за межі захищеної території. Установку вказаних пристроїв може здійснити особа, не пов'язана з роботою у конкретній організації.

Перехоплення інформації, що циркулює в захищеному приміщенні або засобах інформатизації без використання спеціальних технічних засобів, переважно здійснюється шляхом прослуховування (підслуховування) розмов.

До розряду розглядуваних способів перехоплення інформації належить прослуховування телефонних переговорів за допомогою контрольної апаратури під виглядом проведення профілактичних робіт на АТС, кабельних комунікаціях тощо.

Отримання інформації без використання технічних засобів переважно пов'язано з перебуванням особи, яка її збирає, безпосередньо в такому приміщенні. Такою особою зазвичай є співробітник організації.

Слідами вчинення правопорушення можуть бути: а) наявність радіовипромінювань, що свідчать про функціонування електронних закладок і апаратури віброакустичного перехоплення, які знаходяться в технічних засобах, конструкціях приміщень, меблях та інших предметах інтер'єру, у механічному або оптичному контакті з віконними рамами, шибками та іншими конструкціями приміщення, або під'єднаних до каналів зв'язку; б) механічні зміни в конструкціях приміщення, системі опалення і вентиляції, меблях та інших предметах інтер'єру, а також на лініях і арматурі систем зв'язку, електроживлення, освітлення і сигналізації, що відбулися в результаті установки вказаних закладок і апаратури; в) наявність ушкоджень на дверях захищеного приміщення тощо; г) ознаки відмикання замка нештатним ключем; ознаки

несанкціонованого проникнення особи в захищене приміщення; ґ) ушкодження ізоляції кабелю і проводки зв'язку; поява несанкціонованого розриву лінії (і налагодження) зв'язку; д) порушення цілісності печатки або пломби кабельних колодців і розподільних пристроїв (коробок); е) пошкодження ізоляції шнурів на пультах комутаторів тощо [54, с. 69].

Незаконне заволодіння конфіденційною інформацією, що зберігається або циркулює в засобах обчислювальної техніки й автоматизованих системах, обумовлено видом і особливостями носія інформації. В одних випадках посягання може бути вчинено на технічні або програмні засоби обчислювальної техніки, засоби або лінії зв'язку, призначені для переміщення і копіювання інформації, в інших – зловмисник посягає на накопичувачі пам'яті ЕОМ, в яких може знаходитися інформація, на магнітні або паперові носії інформації.

Слідами незаконного заволодіння інформацією, що міститься в засобах обчислювальної техніки і автоматизованих системах, слугують зареєстровані ЕОМ відомості про спроби несанкціонованого доступу (дата, час, використання конкретних технічних і програмних засобів). Про вчинені протиправні дії може свідчити також виявлення в об'єкті інформатизації нештатних програмних або технічних засобів.

Ознаками незаконного заволодіння інформацією можуть слугувати сліди викрадення машинних або інших оригіналів носіїв інформації, програмних або апаратних ключів і засобів криптографічного захисту інформації. Способи їх виявлення і фіксації принципово не відрізняються від слідів викрадення документів, що містять комерційну таємницю, вже описаних.

На окрему увагу заслуговує висвітлення питання незаконного збирання та розголошення комерційної або банківської таємниці шляхом використання зловмисниками можливостей мережі Інтернет, що є відповідно одним із різновидів викрадення інформації, яка циркулює або міститься в технічних засобах. У цьому випадку всі види небезпеки умовно можна поділити на такі категорії: а) порушення цілісності даних, що полягає у доповненні,

зміні або знищенні інформації; б) втрата конфіденційності даних, внаслідок якої інформація стає доступною користувачам, яким доступ до неї заборонений, або особам, які не повинні її знати; в) відмова в обслуговуванні і втрата контролю – сервіси використовуються авторизованими користувачами, але неналежним чином.

Існують різні способи нападів. Один з них – прослуховування – полягає у відслідковуванні інформації, якою партнери обмінюються між собою. Комунікації в інтернеті є абсолютно незахищеними: інформація передається відкритим текстом. Відслідковуючи передану в мережі Інтернет інформацію, можна дізнатися про відомості і паролі, що не підлягають розголошенню.

Перехоплюючи інформацію, зловмисник може її змінити або підмінити до прибуття в пункт призначення або взагалі знищити. Без спеціального програмного забезпечення адресат не дізнається про зміни, зроблені третьою стороною.

Іншим способом нападу, який загрожує компанії серйозними неприємностями, є викрадення програмного або апаратного забезпечення. Програми, наприклад, бази даних, можуть містити особисту інформацію і паролі. Обладнання дозволяє зловмиснику зрозуміти принцип функціонування пристрою внутрішньої мережі або отримати доступ до закодованої інформації, наприклад, у випадку крадіжки старт-карти (електронних карток із вбудованою мікросхемою), зловмисник може встановити, для чого ці картки використовуються (наприклад, для відмикання дверей).

Окрім прослуховування комунікаційних каналів, можливим є перехоплення електромагнітного випромінювання від приладів, зокрема, від моніторів. Існує обладнання, здатне копіювати зображення екрану ПК на комп'ютер, що знаходиться на відстані кількох сотень метрів.

Ще одним надійним способом збирання конфіденційної інформації про компанію є банальний огляд вмісту кошиків для сміття в приміщенні фірми і ймовірне виявлення там викинутих носіїв інформації (дискет, компакт-дисків тощо), на яких можуть опинитися дані, необхідні для входу в систему. За умови

застосування такого способу нападу зловмисник змушений знаходитися в безпосередній близькості від об'єкта нападу, що полегшує його відшукання після проведеної атаки.

Іншим способом отримання доступу до паролів і внутрішньої конфігурації системи безпеки є підкуп когось із служби безпеки потрібної фірми. У даному випадку необхідним є проведення зловмисниками оперативної роботи на предмет виявлення бажаючих за винагороду розкрити секретні відомості.

Іншим традиційним способом добування конфіденційної інформації є фізичне вторгнення. Нападник входить до приміщення, минає контроль доступу і отримує інформацію. Але для цього необхідно, щоб особа знаходилася у фізичній близькості від об'єкта нападу, що, відповідно, досить часто допомагає визначити особу-здлчинця. Тому такий спосіб незаконного отримання відомостей, що становлять комерційну таємницю, застосовується доволі рідко.

Під час нападів з використанням людського фактору зловмисник експлуатує звички і маленькі слабкості службовців, які навіть не помічають, що за їх допомогою здійснюється викрадення конфіденційної інформації. За умов застосування цього методу можна обійтися без використання спеціальних комп'ютерних знань. Злом системи готується заздалегідь. Будь-яка стороння особа, яка вільно спілкується з працівниками підприємства, які відповідають за інформаційну безпеку, вже є потенційною небезпекою. Звернувшись до приймальні, легко дізнатися імена співробітників різних підрозділів фірми, які своєю чергою можуть непомітно для себе розкрити додаткову інформацію. Після кількох телефонних дзвінків (які здійснюються так, щоб неможливо було встановити номер, з якого телефонують) або електронних повідомлень (що надходять зі звичайних адрес) зловмисник інколи отримує достатньо інформації про компанію і відносини у ній, щоб подзвонити кому-небудь з відділу безпеки від імені зовсім іншої людини. Отримана таким чином інформація є подібною до фрагментів мозаїки, кожний з яких окремо здається достатньо беззмістовним. Для нападу на компанію використовуються

тільки дані, які є єдиним цілим. Отриману інформацію необхідно належно зіставити з внутрішніми процесами компанії. Щоб видати себе працівником компанії, злочинець може скористатися відомостями про організаційну структуру і загальновідомі дані про суб'єкт господарської діяльності [54, с. 74].

Отже, спосіб вчинення злочинів у сфері порушення комерційної або банківської таємниці є ключовим елементом криміналістичної характеристики злочинних посягань даного виду, оскільки в умовах сьогодення перелік таких способів не залишається сталим: він невпинно зростає, використовуючи здобутки науково-технічного прогресу. Саме тому для створення і забезпечення стану захищеності різного роду інформації, що становить комерційну таємницю, необхідне знання більшості з можливих шляхів отримання відомостей, які містять комерційну таємницю. Це допоможе виробленню найбільш ефективної системи заходів запобігання поширенню відповідної інформації і визначенню чіткого плану дій у випадку наявності ознак несанкціонованого її поширення.

РОЗДІЛ 2.
Організація досудового розслідування незаконного збирання або використання відомостей, що становлять комерційну або банківську таємницю

2.1. Особливості початку кримінального провадження та планування розслідування незаконного збирання або використання відомостей, що становлять комерційну або банківську таємницю

Початок досудового розслідування є актом застосування права, який здійснюється у формі внесення відповідних відомостей до Єдиного реєстру досудових розслідувань, що відкриває загальну юридичну можливість проведення усіх без винятку слідчих (розшукових) дій та застосування, за наявності для того відповідних підстав, заходів забезпечення кримінального провадження.

Стаття 214 КПК України передбачає, що слідчий, прокурор невідкладно, але не пізніше 24 годин після подання заяви, повідомлення про вчинення кримінального правопорушення або після самостійного виявлення ним з будь-якого джерела обставин, що можуть свідчити про вчинення кримінального правопорушення, зобов'язаний внести відповідні відомості до Єдиного реєстру досудових розслідувань, розпочати розслідування.

Сутність цієї стадії полягає у тому, що слідчий, прокурор, виявивши в події, про яку їм стало відомо, ознаки кримінального правопорушення, приймають рішення розпочати кримінальне провадження.

Початок кримінального провадження є правовою підставою для проведення слідчих (розшукових) дій і застосування передбачених законом заходів забезпечення кримінального провадження. Ці дії та заходи закон пов'язує з конкретним кримінальним провадженням. На стадії початку кримінального провадження не тільки вживають заходів щодо встановлення підозрюваної у вчиненні злочину особи, а й запобігають, у зв'язку із застосуванням

заходів процесуального примусу, можливості продовження нею злочинної діяльності [40, с. 199–205].

Стадія початку кримінального провадження має особливе значення, бо від того, як правильно буде оцінено первинні матеріали, одержані в ході перевірочних дій, залежить успіх подальшого досудового розслідування кримінального правопорушення.

Кримінальні провадження за фактами незаконного збирання з метою використання або використання відомостей, що становлять комерційну таємницю або банківську таємницю, а також розголошення комерційної або банківської таємниці, здебільшого розпочинаються за заявами або повідомленнями представників суб'єктів господарювання – керівників підприємств, установ, організацій, представників служб або підрозділів безпеки юридичних осіб, фізичних осіб-підприємців, членів експертних комісій із захисту комерційної таємниці суб'єктів господарювання, зокрема, керівників і спеціалістів структурних підрозділів юридичної особи та інших осіб. Рідше підставами для початку кримінального провадження можуть слугувати повідомлення, опубліковані в пресі.

У кримінальних провадженнях, розпочатих за фактами незаконного збирання з метою використання або використання відомостей, що становлять комерційну таємницю або банківську таємницю, а також розголошення комерційної або банківської таємниці, відповідно до вимог, закріплених у ст. 216 КПК України, досудове розслідування здійснюється слідчими органами Національної поліції України [34].

Відповідно до ст. 92 КПК України обов'язок доказування обставин вчиненого кримінального правопорушення при розслідуванні фактів незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, а також розголошення комерційної або банківської таємниці, покладається на слідчого.

Згідно зі ст. 91 КПК України, до обставин, які підлягають доказуванню у кримінальному провадженні при розслідуванні зазначеної категорії злочинів, належать:

1) наявність факту вчинення незаконного збирання з метою використання або використання відомостей, що становлять комерційну таємницю або банківську таємницю, а також розголошення комерційної або банківської таємниці;

2) час, місце вчинення злочину; яким способом він вчинений;

3) встановлення особи-злочинця і предмета його безпосереднього замаху;

4) вид і розмір шкоди, заподіяної злочинними діями підозрюваної особи юридичній особі – підприємцеві або фізичній особі, яка є власником комерційної або банківської таємниці тощо.

Під час досудового розслідування фактів вчинення незаконного збирання з метою використання або використання відомостей, що становлять комерційну таємницю або банківську таємницю, а також розголошення комерційної або банківської таємниці, алгоритм дій слідчого у загальному вигляді передбачає вжиття таких заходів:

1) перевірка заяви юридичної чи фізичної особи, чиї інтереси порушено у зв'язку з незаконним отриманням і розголошенням відомостей, що становлять комерційну таємницю;

2) детальний допит фізичної або представника юридичної особи, потерпілої організації з вказуванням на сутність зібраних відомостей, що становлять комерційну таємницю, з метою встановити, яким чином вони зібрані, ким, коли і за яких обставин;

3) підтвердження, що отримані від власника суб'єкта господарської діяльності, зібрані відомості містять комерційну таємницю, адже, як відомо, склад та обсяг відомостей, що становлять комерційну таємницю, порядок їх захисту визначаються самостійно її власником або керівником підприємства з дотриманням вимог чинного законодавства;

4) визначення кола правових, організаційних, технічних й інших заходів, вжитих власником комерційної таємниці щодо забезпечення її збереженості;

5) встановлення обставин, можливих наслідків, що могли настати у результаті розголошення такого роду інформації;

6) допит осіб, у віданні або зберіганні яких знаходилися документи, які містять відомості, що становлять комерційну таємницю, у тому числі у випадку викрадення документів;

7) витребування списку документів, що складають комерційну таємницю підприємства;

8) витребування статуту підприємства, організації;

9) здійснення аналізу трудових договорів працівників суб'єктів господарювання, які розголосили комерційну таємницю, зі встановленням конкретних порушень ними розділів і пунктів, викладених в договорах, що стосуються службових обов'язків;

10) у випадку розголошення комерційної таємниці необхідним є доказування наявності корисливих або інших особистих мотивів діянь суб'єкта злочину, у чому вони конкретно виражаються, встановлення наслідків, що можуть виникнути при досягненні ними мети;

11) вилучення документів за результатами аудиторських перевірок, якщо мало місце розголошення відомостей, отриманих під час їх проведення;

12) оцінка збитків шляхом проведення документально-бухгалтерської ревізії, документальної або аудиторської перевірки з вирішенням питань бухгалтерського, економічного характеру, а за умов необхідності – й інших питань, пов'язаних із застосуванням знань спеціалістів різного профілю;

13) у необхідних випадках проведення вилучення і додання пакетів документів щодо технології виробництва, винаходів, планів розвитку виробництва, контрактів суб'єкта господарювання тощо;

14) проведення науково-технічної експертизи для визначення ефективності розвитку підприємства, доцільності запровадження винаходу, його економічної вигоди з обґрунтуванням суми реально спричиненого матеріального збитку або упущеної вигоди у результаті розголошення комерційної таємниці;

15) встановлення умов утримання приміщень, в яких проводиться робота та зберігаються в неробочий час документи, які

містять відомості, що становлять комерційну таємницю; перевірка благонадійності ділових партнерів суб'єкта господарювання;

16) встановлення наявності результатів перевірки осіб, що приймалися на роботу;

17) ознайомлення з матеріалами службових розслідувань;

18) витребування, вивчення, попереднє дослідження та порівняльний аналіз документів, що містять відомості, які становлять комерційну таємницю;

19) допити заявників, осіб, які здійснювали перевірку підприємства, посадових осіб підприємства, осіб, підозрюваних у вчиненні злочину, та інших осіб.

На початковому етапі розслідування фактів незаконного збирання з метою використання або використання відомостей, що становлять комерційну таємницю або банківську таємницю, схема діяльності слідчого, у загальному вигляді, передбачає вжиття таких заходів: 1) перевірка заяви юридичної чи фізичної особи, чиї інтереси порушено у зв'язку з незаконним отриманням і розголошенням відомостей, що становлять комерційну таємницю; 2) детальний допит фізичної або представника юридичної особи, потерпілої організації з вказуванням на сутність зібраних відомостей, що становлять комерційну таємницю, з метою встановити, яким чином вони зібрані, ким, коли і за яких обставин; 3) підтвердження, отримані від власника суб'єкта господарської діяльності, що зібрані відомості містять комерційну таємницю, адже, як відомо, склад та обсяг відомостей, що становлять комерційну таємницю, порядок їх захисту визначаються самостійно її власником або керівником підприємства з дотриманням вимог чинного законодавства; 4) визначення кола правових, організаційних, технічних й інших заходів, вжитих власником комерційної таємниці щодо забезпечення її збереженості; 5) встановлення обставин, можливих наслідків, що могли настати у результаті розголошення такого роду інформації; 6) допит осіб, у віданні або зберіганні яких знаходилися документи, які містять відомості, що становлять комерційну таємницю, у тому числі, у випадку

викрадення документів; 7) витребування списку документів, що становлять комерційну таємницю підприємства; 8) витребування статуту підприємства, організації; 9) здійснення аналізу трудових договорів працівників суб'єктів господарювання, які розголосили комерційну таємницю, з встановленням конкретних порушень ними розділів і пунктів, викладених в договорах, що стосуються службових обов'язків; 10) у випадку розголошення комерційної таємниці необхідним є доказування наявності корисливих або інших особистих мотивів діянь суб'єкта злочину, у чому вони конкретно виражаються, встановлення наслідків, що можуть виникнути при досягненні ними мети; 11) вилучення документації за результатами аудиторських перевірок, якщо мало місце розголошення відомостей, отриманих під час їх проведення; 12) оцінка збитків шляхом проведення документально-бухгалтерської ревізії, документальної або аудиторської перевірки з вирішенням питань бухгалтерського, економічного характеру, а за умов необхідності, інших питань, пов'язаних із застосуванням знань спеціалістів різного профілю; 13) у необхідних випадках проведення тимчасового доступу до речей і документів, з метою отримання повної інформації щодо технології виробництва, винаходів, планів розвитку виробництва, контрактів суб'єкта господарювання тощо; 14) проведення науково-технічної експертизи для визначення ефективності розвитку підприємства, доцільності запровадження винаходу, його економічної вигоди з обґрунтуванням суми реально спричиненого матеріального збитку або упущеної вигоди у результаті розголошення комерційної таємниці; 15) встановлення умов утримання приміщень, в яких проводиться робота та зберігаються в неробочий час документи, які містять відомості, що становлять комерційну таємницю; перевірка благонадійності ділових партнерів суб'єкта господарювання; 16) встановлення наявності результатів перевірки осіб, що приймалися на роботу; 17) ознайомлення з матеріалами службових розслідувань; 18) витребування, вивчення, попереднє дослідження та порівняльний аналіз документів, що

містять відомості, що становлять комерційну таємницю; 19) допити заявників, осіб, які здійснювали перевірку підприємства, посадових осіб підприємства, осіб, винних у вчиненні правопорушень, та інших осіб; 20) використання конфіденційних джерел інформації щодо встановлення ознак злочину [54, с. 85].

На початковій стадії досудового розслідування кримінального провадження, розпочатого за фактами незаконного збирання з метою використання або використання відомостей, що становлять комерційну таємницю, а також розголошення комерційної або банківської таємниці, необхідним є вивчення і здійснення аналізу такого переліку документів:

1) установчих документів юридичної особи:

а) статуту підприємства, в якому повинно бути зафіксовано положення про наявність у нього права на комерційну таємницю, на визначення складу і обсягу відомостей, що становлять комерційну таємницю, організацію захисту даних відомостей тощо (практика показує, що не всі підприємства відповідально підходять до ретельної проробки в статуті тих нормативних положень, які дійсно закріплюють його право на комерційну таємницю та організацію роботи щодо її захисту) [49, с. 38];

б) установчого договору;

в) реєстру акціонерів;

г) свідоцтва про реєстрацію;

ґ) протоколів загальних зборів засновників або акціонерів;

д) документів, що свідчать про реєстрацію громадянина як підприємця тощо;

2) локальних нормативно-правових актів, які стосуються організації захисту комерційної таємниці:

а) колективного договору підприємства, в якому може бути передбачено єдиний порядок роботи з конфіденційною комерційною інформацією, що міститься у відповідних документах щодо співробітників, які притягуються до роботи з ними, визначено відповідальність за забезпечення і порушення порядку роботи з ними тощо;

б) правил внутрішнього трудового розпорядку, в яких, відповідно, зафіксовано основні положення, зведені до обов'язків адміністрації та, з іншого боку, працівників підприємства щодо забезпечення захисту комерційної таємниці, зокрема, обов'язки адміністрації щодо створення на підприємстві необхідних умов для виконання працівниками встановлених порядку і правил забезпечення збереженості конфіденційної комерційної інформації, проведення інструктажу працівників, трудова функція яких пов'язана з комерційною таємницею, про правила її зберігання з оформленням письмових зобов'язань про її нерозголошення (під час прийому на іншу роботу, під час звільнення або переводу на іншу роботу тощо); проведення комплексу організаційних, економічних, інженерно-технічних, виховних та профілактичних заходів, спрямованих на запобігання поширенню конфіденційної комерційної інформації, нейтралізацію загрози економічній безпеці суб'єкта господарювання; включення в посадові інструкції працівників обов'язку зі збереження комерційних секретів підприємства, здійснення контролю за дотриманням працівниками суб'єкта господарської діяльності встановленого порядку вимог щодо захисту комерційної таємниці, притягнення до дисциплінарної відповідальності порушників вимог щодо захисту комерційної таємниці, відповідно до ст. 147 КзПП України – обов'язки працівників стосовно суворого виконання вимог із забезпечення збереженості комерційної таємниці, встановлені на підприємстві відповідними нормативними документами (положеннями, правилами, інструкціями); вжиття заходів щодо виявлення причин і обставин, які можуть завдати економічних збитків суб'єкту господарської діяльності; надійного збереження інформації – носіїв комерційної таємниці (документів, рукописів, креслень, дискет, перфокарт, магнітних стрічок, моделей, дослідних зразків виробів тощо);

в) наказу керівника підприємства про введення в дію Положення про комерційну таємницю на підприємстві;

г) Положення про комерційну таємницю і правила її зберігання;

ґ) наказів керівників суб'єктів господарської діяльності про виділення відомостей, що становлять комерційну таємницю;

д) методики виділення відомостей, що становлять комерційну таємницю;

е) наказів керівників підприємств про затвердження Переліку відомостей, що становлять комерційну таємницю;

є) Положення про дозвільну систему доступу виконавців до документів і відомостей, що становлять комерційну таємницю, яка містить примірний перелік прав і обов'язків посадових осіб стосовно доступу виконавців до документів, відомостей, спецвиробів, продукції, що становлять комерційну таємницю, інформацію, права і обов'язки підрозділу безпеки щодо доступу виконавців до комерційних секретів, повноваження посадових осіб щодо доступу виконавців до документів і відомостей, що становлять комерційну таємницю, загальні вимоги до оформлення доступу виконавців до документів і відомостей, що становлять комерційну таємницю, порядок видачі документів, що утримують комерційну таємницю, на робочі місця виконавців, порядок доступу до документів обмеженого використання, порядок доступу виконавців до документів оперативної переписки, порядок розмноження і адресування документів, що становлять комерційну таємницю, у зовнішні організації і підрозділи підприємства, порядок доступу до документів і відомостей, що становлять комерційну таємницю, порядок доступу осіб на наради і засідання для обговорення комерційних секретів;

ж) положень про підрозділи безпеки підприємств;

з) угод про конфіденційність з відвідувачами суб'єкта господарської діяльності;

и) карток допущених до комерційної таємниці підприємства;

і) пам'яток працівникам про збереження комерційної таємниці підприємства з метою використання під час укладення підприємством господарських договорів, які містять відомості, що становлять комерційну таємницю, у тому числі, договорів, що містять конфіденційну комерційну інформацію, з іноземними

компаніями, для використання під час укладення трудової угоди (договору підряду) на виконання роботи, яка містить комерційну таємницю підприємства тощо;

ї) примірних планів виховання і навчання співробітників підприємства з питань збереження комерційної таємниці;

й) документів щодо організації і ведення діловодства документів, що становлять комерційну таємницю, зокрема: Інструкції про порядок організації і ведення на підприємстві діловодства документів з грифом «комерційна таємниця», яка містить положення щодо складання, оформлення і обліку документів з грифом «комерційна таємниця», роздрукування і розмноження документів; оформлення, адресування і відправлення вихідних документів, оформлення, облік і зберігання робочих зошитів, складення номенклатури, зберігання справ, знищення документів, перевірки наявності документів; щодо обов'язків, прав і відповідальності співробітників підрозділу безпеки з ведення діловодства документів, що становлять комерційну таємницю тощо;

к) номенклатуру справ, що містять комерційну таємницю (на конкретний рік);

л) актів знищення документів і справ;

м) журналів обліку вхідних, вихідних і внутрішніх документів;

н) журналів обліку карток про допуск до конфіденційної інформації;

о) журналів обліку виробів і продукції, що становлять комерційну таємницю;

п) контрольних карток попереднього обліку відомостей (матеріалів, виробів, дослідних зразків), які можуть становити комерційну таємницю;

р) документального підтвердження факту спричинення злочинними діями зловмисників істотної шкоди суб'єкту господарювання;

с) копій трудових договорів з конкретними працівниками, щодо яких є обґрунтована підозра про розголошення ними комерційної таємниці, які, відповідно, містять положення про нерозголошення комерційної таємниці;

т) розписок конкретних працівників про повернення ними підприємству матеріалів, що становлять комерційну таємницю, при звільненні тощо [54, с. 88].

Планування розслідування злочинів – це розумова діяльність слідчого, спрямована на оцінювання інформації про злочин, висунення версій, визначення на їх підставі обставин, що підлягають установленню, та необхідних для цього слідчих (розшукових) дій і термінів їх проведення. Планування являє собою метод упорядкування діяльності з розслідування злочинів, що є необхідною умовою успішного вирішення завдань кримінального провадження. На відміну від інших галузей людської діяльності, де використовується цей метод, планування досудового слідства має ту особливість, що із самого його початку неможливо зразу скласти план виконання всього обсягу роботи. Це обумовлюється низкою специфічних умов діяльності з розслідування злочинів.

По-перше, специфічною умовою планування розслідування є фрагментарність первинної інформації про злочин, який є подією минулого. Зазвичай досудове розслідування починається на підставі інформації, яка містить окремі ознаки кримінального правопорушення й підлягає перевірці процесуальними засобами. Тобто ця інформація нерідко має численні прогалини, й досить часто вирішення завдань розслідування виглядає як вирішення завдань із багатьма невідомими. По-друге, виявлені наслідки, характерні для вчинення певного злочину (наприклад, викрадення комп'ютерної техніки), можуть бути схожими на незлочинну подію (розголошення інформації). Іноді це є результатом створення штучної обстановки з боку певних осіб (інсценування). По-третє, треба враховувати й ту обставину, що розслідування завжди здійснюється в умовах наявної або очікуваної протидії з боку зацікавлених осіб, що може викликати швидку зміну ситуації, й, відповідно, характеру тактичних завдань розслідування. Тому планування розслідування здійснюється з використанням гіпотетичного методу – версій і має дискретний характер, тобто

ведеться частинами у міру одержання інформації про злочин та її оцінювання на різних етапах розслідування [31, с. 115].

Із плануванням розслідування тісно пов'язано і поняття його організації. Організацію розслідування розуміють як створення необхідних умов для успішного проведення запланованих слідчо-розшукових дій і забезпечення їх необхідними силами та засобами, адже ідеально складений план розслідування може так і залишитися на папері нереалізованим, якщо необхідні для його реалізації заходи не буде здійснено практично. Організація розслідування злочинів охоплює такі заходи: 1) технічне забезпечення запланованих слідчо-розшукових дій; 2) налагодження взаємодії слідчого із співробітниками оперативних підрозділів; 3) використання допомоги спеціалістів; 4) використання допомоги громадськості та засобів масової інформації [31, с. 115].

Успіх досудового розслідування кримінальних проваджень, розпочатих за фактами незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, а також розголошення комерційної або банківської таємниці, визначається його правильним плануванням та організацією. У теорії криміналістики планування розслідування розглядається як визначення шляхів розслідування злочинів, окреслення обставин, що підлягають з'ясуванню, а також встановлення найбільш доцільної системи слідчих (розшукових) дій і строків їх проведення.

Значення планування розслідування визначається важливістю завдань, які може бути вирішено з його допомогою. До завдань планування належать: 1) визначення правильних шляхів розслідування злочинів; 2) забезпечення об'єктивності, повноти та всебічності розслідування; 3) своєчасне застосування науково-технічних і тактичних прийомів криміналістики з урахуванням особливостей кожного кримінального провадження; 4) забезпечення найбільш ефективного поєднання оперативно-розшукових заходів і слідчих дій під час розслідування злочину; 5) сприяння економії сил і засобів слідчого апарату, швидкість розслідування тощо.

Під час розслідування злочинів у сфері господарської діяльності, як і інших злочинів, прийнято розрізняти такі види планування: а) просте планування; б) планування за епізодами; в) планування при розслідуванні групою слідчих (бригадою). Кожен із зазначених видів планування відрізняється метою, обсягом, внутрішньою структурою, методами реалізації дій, що входять до системи плану.

Наукове та практичне уявлення про планування розслідування передбачає з'ясування поняття і ролі версії як елементу, що визначає не тільки планування, а й, певною мірою, організацію розслідування злочину в цілому. Поняття версії, незважаючи на різні підходи до з'ясування її сутності, зводиться до визначення її як обґрунтованого припущення про подію злочину й осіб, які його вчинили.

Необхідно зауважити, що в процесі розслідування версія тісно пов'язана з плануванням. Роль версії стосовно плану розслідування можна назвати визначальною, оскільки версія є тим напрямом розслідування, що зумовлює побудову в плані комплексу слідчих, розшукових, організаційних заходів, здійснюваних з метою її перевірки. Проте визначальна роль версії не означає її відокремленості від планування. Побудова версій і планування так тісно взаємопов'язані, що самостійне їх існування неможливе [70, с. 24].

Під час розслідування незаконного збирання з метою використання або використання відомостей, що становлять комерційну таємницю, а також розголошення комерційної таємниці, постановку криміналістичних завдань на початковому етапі розслідування кримінального правопорушення спрямовано на досягнення головної мети вказаного етапу – встановлення основних обставин події злочину та особи підозрюваного. Зазначені завдання може бути розділено на дві основні групи:

1) завдання організаційно-управлінського характеру, що забезпечують відповідні умови для постановки й вирішення другої групи завдань, зокрема: а) з'ясування й оцінка слідчої ситуації,

що склалася на початку кримінального провадження; б) визначення джерел доказової інформації про обставини розслідуваної події; в) вибір форми і прийомів взаємодії з органами і службами, які здійснюють оперативно-розшукову роботу; г) визначення напряму розслідування злочину і складання плану дій тощо;

2) завдання розшукового й тактичного характеру, безпосередньо спрямовані на встановлення обставин розслідуваної події: а) одержання відомостей про спосіб, обстановку й інші обставини події, що дозволяє орієнтуватися у її змісті й характері; б) одержання й аналіз інформації про злочинця та його спільників, що дозволяє висунути обґрунтовані версії щодо особи злочинця тощо; в) встановлення даних про предмет посягання злочинця тощо.

На нашу думку, алгоритм слідчої діяльності під час розслідування злочинів, зокрема, незаконного збирання та розголошення комерційної таємниці, доцільно будувати за такою схемою: 1) оцінка вихідної слідчої ситуації; 2) постановка одного або кількох тактичних завдань; 3) розроблення версій за обставинами, які входять до змісту відповідного завдання; 4) прийняття рішення про способи перевірки висунутих версій і засоби виконання поставлених завдань.

Висунення версій завжди зумовлено видом злочину, способами його вчинення і здебільшого тією криміналістично значущою інформацією, яка надходить на початковому етапі розслідування кримінального правопорушення.

Процес планування розслідування незаконного збирання та розголошення комерційної таємниці передбачає вміле поєднання слідчих дій з оперативно-розшуковими заходами, координацію слідчої та оперативно-розшукової діяльності, розроблення і проведення тактичних операцій відповідно до сформованої у певний момент слідчої ситуації з урахуванням відомостей про елементи криміналістичної характеристики даного виду злочину.

Для планування розслідування незаконного збирання та розголошення комерційної таємниці характерним є те, що зазвичай на початковому етапі такого розслідування вихідна інформація

визначається обмеженістю, фрагментарністю щодо події злочину, особи злочинця, способу вчинення правопорушення та інших істотних обставин.

Необхідно зазначити, що в основі планування розслідування злочинного порушення комерційної таємниці становить формування версій.

Загальними версіями про характер події, що відбулася, під час розслідування незаконного збирання та розголошенням комерційної таємниці, є такі:

1) мають місце ознаки злочинного збирання з метою використання або використання відомостей, що становлять комерційну таємницю, або розголошення комерційної таємниці;

2) наявне свідомо неправдиве повідомлення або неправдиві показання про вчинення незаконного збирання або розголошення комерційної таємниці, зокрема, з метою компрометації конкретного конкурента тощо;

3) ознаки незаконного збирання та розголошення комерційної таємниці відсутні і має місце інший злочин або правопорушення.

Типовими версіями щодо способу незаконного отримання відомостей, що становлять комерційну таємницю суб'єкта господарювання, є такі:

1) відомості отримано шляхом викрадення документів, що містять комерційну таємницю;

2) відомості отримано шляхом перехоплення інформації, яка циркулює в технічних засобах і приміщеннях;

3) відомості придбано у кримінальних елементів, які спеціалізуються на їх незаконному отриманні;

4) відомості викрадено помилково (умисел був спрямований на викрадення безпосередньо їх носія, зокрема, ноутбука, портфеля тощо, і зловмисник не знав про наявність у них відомостей, що становлять комерційну таємницю суб'єкта господарської діяльності);

5) відомості отримано шляхом проведення незаконних оперативно-розшукових та розвідувальних заходів тощо.

Типовими версіями щодо мети незаконного отримання відомостей, що становлять комерційну таємницю, є такі:

1) відомості, що становлять комерційну таємницю, викрадено для вдосконалення виробничої і комерційної діяльності організації (підвищення конкурентоспроможності продукції і ефективності виробництва, вибору оптимальної стратегії збуту товарів і торговельних переговорів);

2) відомості викрадено з метою завдання шкоди організації-конкуренту (протидії збуту продукції, порушення виробничих і торгових зав'язків організації; зриву торгових переговорів і укладення угод; зниження інвестиційних можливостей організації, підготовки і поширення дезінформаційних матеріалів тощо);

3) відомості викрадено з метою отримання матеріальної винагороди за їх повернення;

4) відомості викрадено з мотивів помсти за неналежне ставлення (до конкретного працівника або групи працівників) без мети отримання матеріальної винагороди або передання їх організації-конкуренту тощо.

Типовими версіями щодо суб'єкта незаконного збирання або розголошення комерційної таємниці можуть бути такі:

1) незаконне збирання з метою використання або використання відомостей, що становлять комерційну таємницю суб'єкта господарської діяльності вчинено: а) представниками (агентами) вітчизняних фірм-конкурентів; б) представниками вітчизняних підприємств, які спеціалізуються на оцінці економічного стану суб'єктів господарської діяльності (зокрема, аудиторських, консалтингових компаній); в) представниками вітчизняних охоронних організацій; г) представниками служб безпеки вітчизняних підприємств, організацій, банків; ґ) злочинними елементами, які спеціалізуються на незаконному збиранні і використанні відомостей, що становлять комерційну таємницю тощо;

2) незаконне збирання з метою використання або використання відомостей, що становлять комерційну таємницю суб'єкта господарської діяльності, вчинено представниками (агентами) за

завданням: а) іноземної розвідувальної організації; б) іноземного державного підприємства; в) іноземної установи або банку;

3) незаконне збирання з метою використання або використання відомостей, що становлять комерційну таємницю підприємства, вчинено представниками приватної іноземної фірми: а) спеціально створеної зарубіжними спецслужбами з метою збирання розвідувальної інформації; б) незалежної фірми, яка виконує договори з розвідувальними й іншими державними відомствами на предмет виявлення і добування конфіденційної інформації економічного характеру; в) міжнародної фірми, створеної з метою недобросовісної конкуренції тощо;

4) розголошення комерційної таємниці суб'єкта господарювання вчинено: а) «ображеним» працівником (або працівниками); б) агентом (агентами) вітчизняних та іноземних суб'єктів господарської діяльності, які діють за завданням конкурентів; в) агентом (агентами) спецслужб, «підіслані» на фірму у якості співробітника; г) контрагентом (контрагентами), представником (представниками) інших суб'єктів господарської діяльності, які ознайомлені з відомостями, що становлять комерційну таємницю даного підприємства, внаслідок існування договірних відносин між компаніями; ґ) представником (представниками) правоохоронних органів державних структур та іншими суб'єктами тощо [54, с. 96].

Необхідно зауважити, що на початковому етапі розслідування кримінальних правопорушень у сфері порушення комерційної або банківської таємниці слідчі і оперативні працівники нерідко у своїй роботі допускають недоліки та помилки, зокрема: а) недостатньо повне та об'єктивне проведення першорядних заходів з метою перевірки заяв та повідомлень про вчинення злочинів подібного роду; б) неповний аналіз та перевірка первинної криміналістично значущої інформації з досліджуваної категорії кримінальних проваджень; в) не визначення та не з'ясування всього кола необхідних для встановлення обставин щодо незаконного збирання або розголошення комерційної таємниці, зокрема,

наявності факту вчинення незаконного збирання з метою використання або використання відомостей, що становлять комерційну таємницю, або факту розголошення комерційної таємниці, часу, місця вчинення злочину, способу його вчинення, особи-злочинця і предмета його безпосереднього замаху, характеру і розміру шкоди, спричиненої злочинними діями винної особи юридичній особі або підприємцеві, який є власником комерційної таємниці тощо; г) недостатнє вивчення і аналіз установчих документів юридичної особи-заявника, локальних нормативно-правових актів суб'єкта господарської діяльності, які містять положення щодо захисту комерційної таємниці; ґ) неврахування результатів відомчого розслідування служби або підрозділу економічної безпеки підприємства за фактом незаконного збирання або розголошення комерційної таємниці, а також недостатня співпраця з його працівниками; е) неправильна організація та планування розслідування, що знаходить прояв у обмеженій кількості висунених версій за фактом незаконного збирання або розголошення комерційної таємниці підприємства, у невстановленні найбільш доцільної системи слідчих (розшукових) дій та строків їх проведення тощо [54, с. 97].

2.2. Типові слідчі ситуації і програми дій слідчого щодо їх вирішення під час розслідування незаконного збирання або використання відомостей, що становлять комерційну або банківську таємницю

У криміналістичній тактиці слідча ситуація є спеціальним поняттям. Серйозне дослідження вказаного поняття було здійснено лише у 1967 р. правознавцем О. Н. Колесниченком, де він уперше дав визначення слідчої ситуації, розуміючи її як певний стан у розслідуванні злочинів, який характеризується наявністю тих чи інших доказів, що виникають у зв'язку з конкретними завданнями їх збирання і перевірки [71, с. 302].

Сьогодні поняття «слідча ситуація» дедалі частіше стали визначати в інформаційному плані, зокрема, як сукупність даних,

суму інформації, як картину, що відображає процес розслідування, як сукупність інформаційних та інших чинників, або як динамічну інформаційну систему, суму значущої для розслідування інформації, сукупність даних про подію злочину і обставини на конкретному етапі розслідування тощо [54, с. 98].

Необхідно зауважити, що характеристика слідчої ситуації завжди є статичною і, певною мірою, ретроспективною, оскільки відображає результати вже проведеної роботи у кримінальному провадженні. Водночас слідча ситуація є вихідним пунктом для створення слідчим програми подальшого розслідування. У цьому плані можна стверджувати, що слідча ситуація є об'єктивною, а її аналіз (характеристика) і розробка програми подальшого розслідування суб'єктивні. Кожна слідча ситуація може бути підставою для створення, принаймні, однієї програми розслідування. Водночас у деяких випадках аналіз однієї слідчої ситуації створює необхідність вироблення декількох програм розслідування. Кількість їх визначається у кожному конкретному випадку з урахуванням обставин, які підлягають доказуванню, а також висунутих версій і версій, які у даний момент перевіряються. Типові слідчі ситуації дають змогу будувати типові програми розслідування злочинів, і тому поняття слідчої ситуації є необхідною і важливою частиною теорії криміналістичної методики розслідування злочинів і криміналістичних методичних рекомендацій [54, с. 99].

Характер слідчої ситуації визначається передусім тим, в якому обсязі на цей момент вирішено завдання розслідування; які обставини, що підлягають доказуванню у кримінальному провадженні, вже встановлено, а які ще необхідно встановити; чи встановлено осіб, підозрюваних у скоєнні злочину; які є відомості про джерела доказів і орієнтуючої інформації тощо. Водночас характер слідчої ситуації залежить від тих умов, в яких проводиться розслідування, а також від наявних у слідчого сил і засобів для успішної роботи по кримінальному провадженню. Умови ж розслідування своєю чергою пов'язано, з одного боку з особливостями події, яка розслідується, кількістю злочинців, способом скоєння

і приховування злочину, матеріальних наслідків від злочинної діяльності і, з другого – зі ступенем забезпеченості слідчого техніко-криміналістичними й іншими засобами, можливостями залучення інших спеціалістів для вирішення задач розслідування, налагодженістю взаємодії із оперативними працівниками та ін.

За своєю природою і змістом слідча ситуація динамічна, рухлива. Будучи на певний момент розслідування відносно постійною, вона під впливом об'єктивних факторів змінюється, набуває в порівнянні з попередньою ситуацією нових рис, і нарешті, перетворюється на нову ситуацію. Зміна ситуацій – закономірний процес розслідування. Вона може проходити у вигляді стрибка, наприклад при різкій зміні умов розслідування, при отриманні слідчим інформації, що суперечить наявній та ін.

Як складова процесу розслідування, слідча ситуація відображає результати виконаної роботи за конкретний проміжок часу. Вона існує до тих пір, поки не виникла необхідність у постановці нових завдань розслідування або поки умови розслідування залишаються стабільними.

Під час розслідування злочинів найбільш практичне і теоретичне значення має поділ слідчих ситуацій на *індивідуальні і типові*. Індивідуальна слідча ситуація – це реальна обстановка розслідування щодо конкретного кримінального провадження. Їй властиві специфічні риси, характерні для окремого випадку розслідування кримінального провадження. Типова слідча ситуація складається з часто повторюваних закономірностей скоєння злочину, притаманних для розслідування певної категорії злочинів. Вона є результатом узагальнення слідчої практики. Типова слідча ситуація відіграє велику роль у формуванні і систематизації методичних рекомендацій щодо розслідування окремих видів злочинів.

Криміналістична методика на основі вивчення слідчої практики систематизує типові слідчі ситуації з урахуванням криміналістичної характеристики злочинів, визначає для кожного виду злочину завдання розслідування, типові слідчі версії, формує

оптимальний комплекс слідчих (розшукових) дій, послідовність і тактичні особливості їх проведення.

Важлива роль належить типовій слідчій ситуації про розслідуванні конкретного кримінального провадження. Особливо велике значення має типова слідча ситуація для початкового етапу розслідування з метою орієнтації в обстановці і визначення напрямів розслідування.

На нашу думку, зважаючи на практику діяльності правоохоронних органів і приватних охоронних структур, можна виділити найбільш актуальні (типові) слідчі ситуації, характерні для початкового етапу розслідування незаконного збирання та розголошення комерційної або банківської таємниці, які мають велике методичне значення для найбільш продуманого висунення слідчих версій, визначення напрямів розслідування і кола обставин, суттєвих для встановлення обставин вчиненого злочину, вибору комплексу і черговості слідчих (розшукових) дій, виявлення задач і характеру необхідної взаємодії слідчого з оперативно-розшуковими органами, а також прийняття обґрунтованих процесуальних і тактичних рішень:

1. Факт незаконного збирання та розголошення комерційної або банківської таємниці встановлено, наявна інформація про спосіб вчинення злочину, шкідливі наслідки, що настали, але немає інформації про особу злочинця (групу осіб).

2. Факт настання шкідливих наслідків встановлено, але причини таких наслідків відсутні (наприклад, пожежа у суб'єкта господарювання, який володіє комерційною або банківською таємницею, яка може замаскувати вчинення незаконного збирання комерційної або банківської таємниці та ін.).

3. Є відомості про подію злочину і особу злочинця, але немає твердої впевненості, що ця подія мала місце (наприклад, заява потерпілої сторони про збирання та розголошення комерційної або банківської таємниці конкретною особою та ін.).

4. Відома інформація про незаконне збирання та розголошення комерційної або банківської таємниці, спосіб вчинення злочину,

шкідливі наслідки злочину, є інформація про суб'єкта злочину, але більшість цих даних носять непроцесуальних характер.

Що стосується першої слідчої ситуації, то практика засвідчує, що в більшості випадків документи, що містять комерційну таємницю суб'єкта господарської діяльності, викрадаються таємно. Така подія на початковому етапі розслідування, зазвичай, характеризується відсутністю відповідного документа на місці його постійного зберігання, тобто є підстави говорити про його «вихід» із законного володіння за невідомих обставин. У зв'язку з цим перевірочні заходи проводяться за фактом втрати документа, що містить комерційну таємницю.

Під час першої слідчої ситуації розслідування на початковому етапі проводиться в напрямі отримання відомостей про особу злочинця і звуження кола осіб, серед яких варто його шукати. Крім того, необхідно відшукати якомога більше доказів незаконного збирання комерційної або банківської таємниці з метою її розголошення; виявити важливі сліди способів незаконного збирання інформації; забезпечити повернення викраденої інформації; забезпечити в майбутньому призначення і проведення відповідних експертиз. За цієї слідчої ситуації відшукання доказів незаконного збирання комерційної або банківської таємниці здійснюється з використанням чинника раптовості при проведенні таких слідчих (розшукових) дій як: затримання на місці злочину з викраденою інформацією (або без такої); обшуки (в тому числі і особисті); слідчі огляди; аудіоконтроль особи; допити підозрюваних і свідків.

Також під час виникнення другої слідчої ситуації – головний напрям розслідування спрямовано на перевірку версій про причини настання шкідливих наслідків для суб'єкта господарювання. Діючи в умовах цієї ситуації, слідчий повинен відштовхуватися від типових версій: 1) незаконне збирання та розголошення комерційної або банківської таємниці мало місце; 2) незаконне збирання та розголошення комерційної або банківської таємниці не мало місця, але існують порушення, які мають ознаки іншого

злочину. Черговість і характер слідчих (розшукових) дій в умовах даної ситуації обумовлено конкретною обстановкою злочину.

Під час третьої слідчої ситуації – розслідування спрямовано на встановлення події злочину і виявлення його характеру.

У ситуації, коли документ відсутній у місці його зберігання і обставини його виходу із законного володіння невідомі, загальний перелік слідчих (розшукових) дій на початковому етапі розслідування виглядає так: 1) огляд приміщення (місця) зберігання документа; 2) огляд сейфа (іншого сховища), в якому знаходився документ; 3) огляд місця, відведеного для знищення документів; 4) огляд звітної документації.

З метою встановлення обставин втрати документа доцільно проводити: 1) допит особи, відповідальної за документ, під час якого ставляться запитання, коли і у зв'язку з чим був нею отриманий документ; чи було дотримано встановленого порядку його отримання; коли і у зв'язку з чим була виявлена нестача документа; чи відомі обставини і причини виходу документа з володіння; чи допускалися порушення правил поводження з отриманим документом; 2) допит осіб, які виявили нестачу документа, з метою встановити, коли і за яких обставин була виявлена нестача; чи проявляв хто-небудь ознаки усвідомлення про неї до її виявлення; чи відомо свідку про обставини виходу документа з володіння відповідальної особи; які зміни вносилися в обстановку місця зберігання документа до початку досудового слідства.

Необхідно зауважити, що проведення зазначених слідчих (розшукових) дій допоможе слідчому отримати необхідний обсяг доказової інформації вже на початковому етапі розслідування незаконного збирання та розголошення комерційної або банківської таємниці.

Під час четвертої слідчої ситуації значне місце в діяльності слідчого займає робота зі збору доказів, які мають процесуальну форму (документування злочинної діяльності), повне встановлення обставин злочину.

Розслідування за фактом виходу документа із законного володіння за невідомих обставин здебільшого починається за наявності однієї з таких типових ситуацій: а) документ відсутній за місцем його зберігання; б) документ відсутній при закінченні маршруту слідування (під поняттям маршруту слідування об'єднуються дії спеціальних кур'єрів й інших осіб, пов'язані з переміщенням документа поза охоронюваним приміщенням); в) документ виявлений поза встановленим місцем зберігання; г) документ надійшов у розпорядження слідчого від сторонніх осіб.

У цьому разі слідчому необхідно отримати відповіді на такі питання: 1) що являє собою документ, що вийшов із законного володіння (його характеристики, зовнішні ознаки, наявність відомостей, що становлять комерційну таємницю тощо); 2) хто є відповідальною особою за збереженість документа; 3) яка причина виходу документа із законного володіння; 4) що відбулося: втрата документа чи його викрадення; 5) місце, час, спосіб втрати документа тощо.

У ситуації, коли документ відсутній у місці його зберігання і обставини його виходу із законного володіння невідомі, загальний перелік слідчих (розшукових) дій на початковому етапі розслідування виглядає так: 1) огляд приміщення (місця) зберігання документа; 2) огляд сейфа (іншого сховища), в якому знаходився документ; 3) огляд місця, відведеного для знищення документів; 4) огляд звітної документації.

Коли документ відсутній по закінченні маршруту слідування і обставини виходу його із законного володіння невідомі, проводяться: 1) огляд засобів доставки документа; 2) огляд документації, що доставлялася; 3) огляд документа, що є аналогічним втраченому; 4) призначається експертиза речових доказів; 5) допит особи, відповідальної за документ; 6) допити осіб, які помітили втрату документа; 7) розробка версій про встановлення сутності події; 8) розробка версій про встановлення осіб, винуватих у втраті або викраденні документа тощо.

У ситуаціях, коли документ виявлено поза місцем його зберігання або надійшов у розпорядження слідчого (володільця,

відомчої комісії тощо) після виходу із законного володіння за невідомих обставин, на початковому етапі розслідування проводяться: 1) огляд місця виявлення документа; 2) огляд документа або його частини; 3) огляд пакувального матеріалу; 4) огляд місця зберігання документа; 5) допити осіб, відповідальних за документ, тих, хто виявив документ та осіб, у яких виявили документ. Необхідним є також виконання дій, спрямованих на встановлення винуватої особи; підготовка доручення про проведення оперативно-розшукових дій та розробка версій про типові шляхи надходження документа в розпорядження слідчого.

Огляд місця зберігання документів проводиться з метою виявити і зафіксувати такі обставини: 1) сутність (характерні риси, особливості) порушень правил конфіденційного діловодства: а) відсутність передбачених правилами засобів технічного захисту приміщення, території (огорож, охоронної сигналізації тощо); б) неналежний технічний стан захисних засобів внаслідок їх несправності або інших причин; в) порушення правил зберігання основного і запасного ключів від сховища (сейфа); г) порушення правил здачі приміщення для охорони (у тому числі – включення охоронної сигналізації); ґ) наявність доказів (фактів) використання службового приміщення не за призначенням (для зустрічей зі сторонніми особами, вживання алкогольних напоїв, наркотичних засобів тощо), фактів неналежного зберігання документів (поза сейфом, сховищем); 2) перебування у службовому приміщенні сторонніх осіб: а) сліди ніг, рук, пальців, крові, слини, одягу; б) сліди вживання їжі, спиртних напоїв, куріння; в) сліди відправлення природних потреб; г) зникнення окремих предметів, зміна положення і місцезнаходження предметів, меблів, технічних засобів, засобів зв'язку; ґ) сліди використання предметів, приладів, обладнання; 3) сліди проникнення правопорушника на територію (у приміщення): а) сліди рук, ніг (взуття) на огорожі, зовнішніх стінах будівлі, підвіконні; б) сліди застосування знарядь злому та інших засобів (при цьому мається на увазі також їх виявлення, фіксація і вилучення); в) сліди пошкодження огорожі, вікон,

дверей, підлоги, стелі; г) сліди пошкодження цілісності печатки; ґ) сліди відключення, пошкодження охоронної сигналізації, приладів освітлення.

Огляд сховища (сейфа) здійснюється з метою виявити і зафіксувати такі обставини: 1) сліди порушення правил користування сховищем (сейфом): а) несправність замка, корпусу, що надає можливість доступу в сховище без ключа; б) відмикання замка сейфа дублікатом ключа; порушення правил опечатування сейфа; в) наявність у сейфі сторонніх предметів, цінностей, документів, літератури; 2) сліди правопорушника: а) сліди рук, ніг, взуття, одягу на корпусі сейфа; б) сліди пошкодження корпусу або замка (злом, розпил, свердління, віджимання); в) сліди вилучення документів через ушкоджену частину корпусу (волокна паперу, наявність сторонніх нашарувань на закраїнах щілини, отвори); г) порушення цілісності печатки (у тому числі повне знищення без відновлення); ґ) сліди тимчасового (з наступним відновленням) видалення печатки шляхом зрізання, заморожування тощо; д) опечатування сейфа іншою печаткою; е) сліди викрадача усередині сейфа (відбитки пальців на внутрішній поверхні сейфа); є) сліди біологічного походження (частинки шкірних покривів від саден, кров; мікросліди – відшарування від одягу тощо); ж) сліди відмикання замка нештатним ключем або відмичкою (наявність мастила, пасти, мастики, металічних ошурків у коробці замка, траси на кришці коробки замка).

Огляд ключів від сейфа проводиться з метою виявити і зафіксувати: 1) ознаки підміни одного з ключів: розходження заводських номерів на ключах і замку сейфа; ознаки кустарного виготовлення ключа; 2) ознаки використання ключа для виготовлення його дубліката: сліди затискного приладу; нашарування слідокопіюючої речовини; 3) ознаки несанкціонованого використання запасного ключа: порушення цілісності корпусу контейнера (конверта) з запасним ключем; видалення печатки, що скріплює контейнер (конверт), без наступного відновлення; видалення печатки з наступним маскуванням (зрізанням мастичної печатки

з наступним наклеюванням), видалення печатки з послідовним заморожуванням газовими сумішами або в морозильній камері і наступним наклеюванням тощо.

Огляд засобів доставки документа (поштовий залізничний вагон, купе, автомобіль, багажна тачка, портфель, папка тощо) проводиться з метою виявити і зафіксувати: 1) сліди порушення правил конфіденційного діловодства: відсутність передбачених правилами засобів технічного захисту вагона, автомобіля; порушення правил перевезення конфіденційних документів (відмова від використання спеціального сейфа, встановленого у вагоні, неправильне розміщення вантажу, наявність у поштовому сховищі (купе) сторонніх вантажів); технічна несправність запору дверей, корпусу вагона, автомашини, дефекти портфеля, папки; 2) сліди викрадення документа: ушкодження цілісності запору дверей, корпусу вагона, автомашини; ушкодження цілісності печатки, якою оперативно опечатано сховище, сейф; несанкціоноване відмикання запорів дверей, вікна транспортного засобу, сховища, сейфа; сліди приладів і пристосувань, використовуваних для проникнення у вагон (сховище).

Огляд і опис документа (предмета), що є аналогічним втраченому, проводиться з метою встановлення таких, що мають криміналістичне значення, властивостей, зокрема: способу виготовлення; виду документа, кількості сторінок, його призначення і змісту; реквізитів; наявності обкладинки, матеріалу, з якого вона виготовлена, її кольору, наявності підписів й інших позначень; розміру, форми (у необхідних випадках – і ваги документа); певних особливостей документа (нетипового забарвлення, перфорації по краях сторінок, наявності заміток тощо); важливих у криміналістичному плані властивостей предмета: способу виготовлення (заводський, серійний, дослідного виробництва тощо); виду предмета і його призначення; форми предмета, його розмірів і ваги; кольору і характеру поверхні (пофарбована, матова, пориста).

Проведення огляду облікової документації за місцем зберігання документа викликане необхідністю: з'ясування обставин

(підстав) надходження документа в організацію і постановлення його на облік; руху документа (доставка, розгляд, видання в тимчасове користування, передання під відповідальне зберігання, відсилання, знищення); наявності контролю керівників організації, співробітників підрозділів захисту інформації за збереженістю документів; встановлення наявності слідів порушень правил конфіденційного діловодства (без облікового зберігання документа, що надійшов або виготовлений; без облікової передачі його в тимчасове користування; відсутності контролю за збереженістю документа, його фактичною наявністю під час зникнення; відсутності періодичного контролю за збереженістю документа тощо).

Огляд документації, що надійшла, і аналіз фактичних обставин, пов'язаних з переміщенням документа, дає можливість встановити факт отримання документа для доставки, а також інші обставини, а саме: час, місце, кількість і вид пакування, вагу; обставини переміщення, доставки документів: документації слідування автотранспорту; стрічки виміру швидкості залізничного транспорту; здачі конфіденційних матеріалів: опис, реєстр, витратна відомість; список осіб, відповідальних за доставку; супровідний лист, постову відомість (час зміни постів у дорозі); ознаки порушення правил доставки: затримку доставки конфіденційних матеріалів для використання часу в особистих цілях (суперечності між даними поставки і особистими звітними документами відповідальної особи); відхилення від маршруту з метою відвідування непередбачених ним пунктів тощо.

Завданнями призначення ревізії конфіденційного діловодства є: пошук документів, яких не вистачає; виявлення відомостей, що можуть мати відношення до виходу документа з володіння; виявлення причин і умов, що сприяють виходу документа з володіння; нестача інших документальних матеріалів – конфіденційних або облікових; обставин, що свідчать про порушення правил знищення документів; наявність документів, що вважаються знищеними, записи про неодноразове знищення одного і того ж документа;

виявлення матеріалів, що подібні до документів, яких не вистачає за тематикою, внутрішнім виглядом, які вважаються знищеними.

Огляд місця, відведеного для знищення документів, проводиться з метою виявити і зафіксувати неналежне обладнання місця знищення: а) відсутність захисних сіток на димоході печі; б) ознаки виходу печі (пристрою для знищення паперу) з ладу, що завадили знищенню документа, дефекти окремих деталей, порушення вузлів тощо; в) відсутність належного освітлення, неналежні розміри приміщення, що не дає змогу проводити перевірку знищуваних матеріалів, бути присутнім у приміщенні всім членам комісії одночасно; г) сліди знищення документів: незгорілі залишки обкладинки, фрагменти аркушів, попіл, металічні скріпки.

З метою встановлення обставин втрати документа доцільно проводити: 1) допит особи, відповідальної за документ, під час якого ставляться запитання, коли і у зв'язку з чим був нею отриманий документ; чи було дотримано встановленого порядку його отримання; коли і у зв'язку з чим було виявлено нестачу документа; чи відомі обставини і причини виходу документа з володіння; чи допускалися порушення правил поводження з отриманим документом; 2) допит осіб, які виявили нестачу документа, з метою встановити, коли і за яких обставин було виявлено нестачу; чи проявляв хто-небудь ознаки усвідомлення про неї до її виявлення; чи відомо свідку про обставини виходу документа з володіння відповідальної особи; які зміни вносилися в обстановку місця зберігання документа до початку досудового розслідування.

З метою встановлення осіб, винуватих у втраті документа, необхідно здійснити: 1) виявлення осіб, яким відомі обставини втрати і винуваті у цьому особи, зокрема, осіб, які офіційно отримували документ, співробітників, яким документ був переданий по роботі без відповідного оформлення; свідків з оточення відповідальної за документ особи; 2) допит (опитування) осіб з метою отримання відомостей про особу, з володіння якої документ вийшов фактично, про місце, час й інші обставини виходу документа з володіння, про обставини, що передували виходу

документа з володіння і подальші обставини; встановлення фактів порушення правил конфіденційного діловодства, що потягли за собою вихід документа з володіння; 3) огляд: а) документів про допуск особи до роботи з конфіденційними матеріалами (наказ, підписка про нерозголошення конфіденційних відомостей тощо); б) документів про отримання відповідальною особою конфіденційних матеріалів (журнал, картки, реєстр, розписка тощо); в) місця зберігання документа; сейфа; засобів доставки документів; г) місця знищення документів – метою такого огляду є отримання відомостей про особу, відповідальну за документ; про обставини виходу документа з володіння; встановлення фактів порушення конфіденційного діловодства, що потягли за собою вихід документа з володіння.

З метою встановлення особи, винуватої у викраденні документа, проводяться: 1) виявлення і допит осіб з оточення працівника, відповідального за документ, серед яких може знаходитися викрадач або яким відомо про обставини виходу документа з законного володіння: а) за місцем роботи відповідальної за документ особи: співробітники, керівник, підлеглі; представники вищої, суміжної, проєктної, контрольної організації, з якими підтримувалися контакти по роботі; особи, які в минулому працювали на підприємстві; співробітники охорони, технічний персонал; б) за місцем навчання особи, відповідальної за документ (колеги по навчанню, викладачі, технічний персонал); в) за місцем проживання особи, відповідальної за документ (постійним, тимчасовим): сусіди за квартирою, готелем; обслуговуючий персонал тощо; г) з числа родинних зав'язків (члени сім'ї, родичі); ґ) з числа знайомих за захопленнями, інтимними зв'язками; 2) проведення огляду: місця зберігання документа; сейфа, в якому зберігався втрачений документ; ключів від сейфа; засобів доставки документа – метою якого є отримання відомостей про обставини викрадення і особу, яка його здійснила, про використання викрадачем порушень правил конфіденційного діловодства, допущених відповідальною особою; 3) виявлення і допит осіб, серед яких може знаходитися

викрадач чи яким відомо про обставини виходу документа із законного володіння; перевірці підлягають особи, які спілкувалися зі співробітником у процесі користування побутовими й іншими послугами (разом відвідували підприємства загального харчування, басейни, сауни, тенісні корти тощо); спільного проживання в готелях (у тому числі – обслуговуючий персонал вказаних підприємств, спортивних споруд і готелів: офіціант, касир, контролер, гардеробник); користування транспортом (попутники у поїзді, літаку, автобусі; провідники, стюардеса, водій, співробітник камери зберігання, касир, контролер); спільної участі в наукових, творчих заходах, презентаціях (учасники, забезпечувальний і обслуговуючий персонал); користування медичними послугами (одночасне знаходження на лікуванні або користування медичними процедурами; медичний і обслуговуючий персонал закладів: лікар, медсестра; масажист; реєстратор, санітарка); проведення відпустки (спільно відпочивали в санаторії, пансіонаті; особи з адміністрації і обслуговуючого персоналу); 4) допит осіб, у яких було знайдено документ, під час якого з'ясовуються такі питання: коли і за яких обставин документ опинився у допитуваної особи; кому належить знайдений документ; якими є обставини виходу документа з володіння відповідальної особи; з якою метою допитувана особа заволоділа документом; які дії для цього нею було вчинено; яким змінам піддався документ після його надходження допитуваній особі; чи було використано інформацію, що міститься в документі, і з якою метою [54, с. 134–137].

З метою встановлення часу втрати (викрадення) документа, що містить відомості, які становлять комерційну таємницю, проводяться: допит свідків (особи, яка заявила про відсутність документа); огляд місця події; обшуки у справах, не пов'язаних з втратою документа; огляд поштового відправлення, реквізитів конверта тощо; допит відповідальної за документ особи; допит свідків; огляд наказів щодо особового складу (про заохочення, призначення, переміщення, про відпустку тощо); огляд документів про відрядження, огляд медичних документів тощо.

З метою встановлення місця втрати документа доцільно проводити: допити відповідальних за документи, що містять комерційну таємницю, осіб; допити свідків; відтворення обстановки і обставин події; огляд місця події, огляд документа; призначати криміналістичні експертизи.

З метою встановлення способу скоєння втрати документа, зокрема, залишення документа без достатньої охорони або власне втрати, проводяться: огляд місця події, огляд ключа від сейфа, допит відповідальної за документ особи, допит інших свідків; слідчий експеримент, обшук, вилучення тощо.

Стосовно розкриття і розслідування незаконного збирання з метою використання відомостей, що становлять комерційну таємницю, шляхом перехоплення інформації, що циркулює у технічних засобах (автоматичних мережах телефонного зв'язку, системах телеграфного і факсимільного зв'язку, засобах гучномовного (селекторного) зв'язку, засобах звуко- і відеозапису, системах звукопідсилення мовлення, електронно-обчислювальній техніці, електронних засобах оргтехніки, мережах електроживлення і лініях заземлення і приміщеннях, необхідно зазначити, що у цьому випадку може мати місце безпосереднє перехоплення інформації (вся інформація шляхом підключення до лінії принтера записується з кабельних, провідних а також наземних мікрохвильових систем, систем супутникового і спеціального урядового зв'язку) або електронне перехоплення конфіденційної інформації (дозволяє без прямого контакту «зловити» випромінювання, яке дає центральний процесор, дисплей, принтер, лінії мікрохвильового зв'язку) [54, с. 112].

Вихідними ситуаціями, за умов наявності яких розпочинається розслідування за фактом незаконного отримання таких відомостей, є такі: 1) відомості, що становлять комерційну таємницю, незаконно отримані сторонньою особою (організацією); обставини виходу інформації із законного володіння невідомі; є в наявності підстави вважати, що вони зібрані шляхом перехоплення інформації, що циркулює в технічних засобах і приміщеннях; 2) у технічних засобах і приміщеннях виявлено

електронний прилад перехоплення інформації, впроваджений за невідомих обставин.

Завдання, які необхідно вирішити уповноваженим особам у першій ситуації, полягають у тому, щоб встановити і зафіксувати факт незаконного отримання відомостей, що становлять комерційну таємницю, виявити спосіб перехоплення інформації і винуватих осіб, встановити розмір збитків, що спричинені власнику відомостей.

У другому випадку необхідно встановити спосіб і обставини впровадження приладу перехоплення інформації, причетних до цього осіб, обсяг і зміст перехоплених відомостей, незаконного одержувача інформації, спосіб її використання і розмір збитків, спричинених власнику відомостей. В обох ситуаціях для організації і здійснення розслідування в цілому є допустимим і необхідним застосування тактичних прийомів і слідчих дій, зазначених вище, які здійснюються у випадку викрадення документів, у яких містяться відомості, що становлять комерційну таємницю. Однак необхідно зауважити, що виконання окремих слідчих дій у справах про перехоплення інформації, що циркулює у технічних засобах і приміщеннях, має певну специфіку, яка характеризується змістом предмета протиправного посягання і способу здійснення злочину, про що, відповідно, буде зазначено нижче.

З метою встановлення способу перехоплення інформації, що становить комерційну таємницю, та виявлення відповідних спеціальних пристроїв доцільно проводити: 1) огляд телефонних апаратів, розподільних коробок, магістральних кабелів, боксів розподільних шаф і розподільних коробок, кабельних ящиків телефонних ліній, побудованих за шафною системою, кабельних ящиків телефонних мереж, побудованих за принципом безшафної системи, токоведучих ліній, огляд комутаційних панелей і комунікаційних каналів, мереж пожежної і охоронної сигналізації тощо; 2) огляд комп'ютерного обладнання: а) автономного (за наявності комп'ютера, прямо не приєднаного до іншого чи інших комп'ютерів з власною операційною системою); б) у складі мережі: локальної (зосередження в одному приміщенні кількох

(багатьох) комп'ютерів, з'єднаних між собою) чи розподіленої (поєднання комп'ютерів, розміщених у різних кінцях міста, містах за допомогою телекомунікаційних систем) [73, с. 73–82] тощо; 3) огляд транспортних засобів (у деяких випадках) тощо; 4) допит працівників служби економічної безпеки підприємства, які виявили пристрої перехоплення інформації під час планових заходів щодо забезпечення збереження конфіденційної інформації, випадково або мають обґрунтовані підозри про їх наявність у відповідному приміщенні; 5) допит працівників, допущених до роботи з інформацією, що становить комерційну таємницю суб'єкта господарської діяльності, які під час виконання своїх службових обов'язків використовують відповідні пристрої, в яких циркулюють подібні відомості, з метою встановлення наявності фактів недоліків у роботі відповідних технічних пристроїв, зокрема, телефонних апаратів, збоїв у роботі ЕОМ тощо; 6) допит свідків, які бачили, як працівники підприємства, які допущені до роботи з комерційною таємницею або не допущені до роботи з подібного роду відомостями, сторонні особи несанкціоновано перебували у відповідних приміщеннях, де циркулює конфіденційна інформація, робили спроби проникнути у такі приміщення, впроваджували пристрій перехоплення інформації тощо.

З метою встановлення обставин розголошення комерційної таємниці і винуватої у цьому особи необхідно здійснити: 1) аналіз джерел конфіденційної інформації суб'єкта господарювання; 2) аналіз каналів об'єктивного поширення і передачі інформації, зокрема: а) речево-матеріальних (папір, фото, магнітні носії, відходи тощо); б) візуально-оптичних (спостереження, фотографування); в) акустичних; г) електромагнітних; 3) виявлення і класифікацію існуючих і можливих конкурентів компанії, кримінальних структур і окремих злочинних елементів, які цікавляться підприємством; 4) виявлення, класифікацію реального складу конфіденційної інформації, що циркулює на підприємстві (у контексті джерел, забезпечуваних функцій і видів робіт, з вказуванням на носії документів, дискет, файлів тощо);

5) вивчення даних обліку обізнаності співробітників з комерційною таємницею суб'єкта господарської діяльності, тобто вивчення ступеня і динаміки реального володіння нею співробітниками; 6) вивчення складу конфіденційної інформації в розрізі документів, тобто вивчення правильності розгалуження інформації, що становить комерційну таємницю, між документами; 7) облік і вивчення внутрішніх і зовнішніх, потенційних і реальних (пасивних і активних) загроз кожному джерелу конфіденційної інформації; 8) виявлення санкціонованих і несанкціонованих звернень співробітників суб'єкта господарської діяльності до інформації, що становить комерційну таємницю, документів, які містять подібного роду відомості, баз даних тощо [54, с. 116].

У цьому разі доцільною є співпраця слідчого і оперативних працівників з представниками служб або підрозділів економічної безпеки підприємств (або керівником суб'єкта господарської діяльності, якщо вказаний підрозділ або служба відсутні), оскільки до функціональних обов'язків вказаних органів, зазвичай, належить: 1) здійснення контролю і аналізу об'єкта захисту, рівня безпеки інформаційних ресурсів у джерелі і каналі поширення інформації; 2) виявлення і класифікація реального максимального складу каналів об'єктивного поширення конфіденційної інформації на фірмі; 3) вивчення складових елементів кожного каналу з метою виявлення небезпечних ділянок, які сприяють виникненню каналу несанкціонованого доступу до інформації; 4) дослідження і узагальнення способів і сфери розповсюдження інформації в кожному каналі; 5) дослідження (облік) складу конфіденційної інформації, яка циркулює між джерелами; 6) вивчення сфери розповсюдження інформації під час реалізації комунікативних зв'язків фірми (конкуренти, засоби масової інформації, виставки і ярмарки, рекламні видання тощо); 7) контроль і перекриття каналів несанкціонованого доступу для третіх осіб, випадкових, сторонніх людей; 8) дослідження складу ефективності методів захисту, які вживалися по кожному каналу, і додаткових заходів протидії зловмиснику під час активних загроз, екстремальних ситуацій тощо.

Кожна типова слідча ситуація має свою логіку розвитку. В практичній діяльності слідчий постійно зіштовхується з необхідністю аналізу і оцінки слідчих ситуацій.

Вивчаючи наявну інформацію, слідчий насамперед виявляє відомі ознаки тієї чи іншої типової слідчої ситуації, що дозволяє йому прийняти рішення про застосування в процесі розслідування кримінального провадження методичних рекомендацій, які відносяться до конкретної ситуації.

Подальший аналіз слідчої ситуації іде в напрямі виявлення специфічних особливостей обстановки розслідування з метою визначення характеру індивідуальної слідчої ситуації і застосування в подальшому відповідних їй специфічних прийомів і засобів розслідування.

Аналіз слідчої ситуації завершується її оцінкою. Слідчу ситуація може бути оцінено з різних точок зору. Якщо, наприклад слідча ситуація розглядається з точки зору характеру її впливу на хід розслідування, то в одному випадку вона може бути визнана як сприятлива, а в іншому (наприклад, при активній протидії розслідуванню з боку особи злочинця) – як несприятлива. Залежно від ступеню інформованості слідчого про обставини злочину, характер і об'єм здійснюваних дій, слідчі ситуації можуть бути простими і складними.

Загальна оцінка слідчої ситуації, а також визначення перспектив розслідування кримінального провадження виконуються на основі перевіреної і систематизованої інформації.

Характеризуючи умисне незаконне збирання та розголошення комерційної або банківської таємниці суб'єкта господарської діяльності, необхідно зазначити, що аналіз криміналістичної літератури не дає змоги виділити найбільш поширені типові слідчі ситуації, які є характерними для початкового етапу розслідування даного кримінального правопорушення. Враховуючи зазначене, на наш погляд, доцільним є виділення всіх можливих ситуацій, супутніх розкриттю і розслідуванню незаконного збирання та розголошення комерційної або банківської таємниці.

2.3. Тактика проведення слідчих (розшукових) дій початкового етапу розслідування незаконного збирання або використання відомостей, що становлять комерційну або банківську таємницю

Розслідування кримінальних правопорушень у сфері комерційної або банківської таємниці характеризується певними труднощами, обумовленими специфікою вчинення вказаного кримінального правопорушення. Злочинні дії зазвичай неочікувані для оточуючих, швидкоплинні за часом, складні за своїм механізмом. Ці особливості утруднюють сприйняття свідками і потерпілими особами процесу розвитку злочинної події.

Зміни, що відбулися в політичній і соціально-економічних сферах, внесли істотні корективи в шкалу цінностей інформації, що використовується в процесі розслідування кримінальних правопорушень. Якщо раніше основна роль в процесі доказування відводилась ідеальній інформації, то сьогодні на перше місце виходять матеріальні сліди. Зростання організованої злочинності, зниження рівня правової свідомості населення вплинули на об'єктивність показань потерпілих, свідків та ін. В таких умовах особливу роль в доказуванні відіграють слідчі (розшукові) дії, спрямовані на виявлення матеріальної інформації. Серед таких слідчих (розшукових) дій основне значення відводиться *слідчому огляду*, який спрямовано на виявлення, збирання і дослідження матеріальних слідів.

Від якісного проведення слідчого огляду місця події залежить успіх подальшого розслідування незаконного збирання з метою використання відомостей, що становлять комерційну або банківську таємницю. Дані, отримані під час огляду, мають істотне значення для вирішення питання про кваліфікацію діяння, виявлення осіб, причетних до вчинення кримінального правопорушення.

Наприклад, якщо при розслідуванні незаконного збирання з метою використання відомостей, що становлять комерційну або банківську таємницю, встановлено кримінальне правопорушення, вчинене шляхом перехоплення інформації, що міститься в

технічних засобах і приміщеннях, необхідно зазначити, що всю процедуру виявлення, під час слідчого огляду, технічних засобів і приміщень, в яких циркулює конфіденційна інформація підприємства, приладів негласного отримання інформації, можна умовно поділити на декілька етапів: 1) підготовчий етап; 2) фізичний пошук і візуальний огляд з метою виявлення: а) радіозакладних пристроїв; б) технічних засобів з функціями передачі інформації по лініях зі струмом; в) закладних пристроїв з функціями передачі інформації по інфрачервоному каналу; 3) перевірка наявності акустичних каналів розповсюдження інформації.

Підготовчий етап слідчого огляду призначено для визначення масштабів пошуку, а також формування переліку і порядку заходів, що проводяться. Він містить в собі такі елементи: а) оцінку можливого рівня використовуваних технічних засобів; б) аналіз ступеня небезпеки, що виходить від співробітників суб'єкта господарської діяльності і представників підприємств-конкурентів; в) оцінку можливості доступу сторонніх осіб у приміщення; г) вивчення історії будівлі, в якій планується проведення пошукових заходів, під час якого оцінюється можливість установки закладних пристроїв як під час будівництва, так і залишення їх у спадок від попередніх власників; ґ) визначення рівня підтримуваної інформаційної безпеки відповідно до економічних можливостей і ступеня бажання замовника, а також фактичної необхідності; д) вироблення плану дій, який повинен відповідати таким умовам: час огляду приміщень або технічних засобів повинен припадати на робочі години, коли закладні прилади є активними; необхідно буде створити умови, які провокують активізацію дії закладних приладів, наприклад, проведення фіктивних ділових переговорів; необхідно буде забезпечити таємність проведення заходів щодо виявлення закладних пристроїв тощо.

Фізичний пошук і візуальний огляд приміщень і технічних засобів є важливим елементом виявлення засобів негласного отримання інформації, що становить комерційну таємницю або банківську таємницю, особливо таких, як провідні і волоконно-оптичні

мікрофони, пасивні і напівактивні радіозакладні пристрої, дистанційно керовані пристрої та інші технічні засоби, які неможливо відшукати за допомогою звичайної апаратури.

Необхідно зазначити, що проведення пошукових заходів під час слідчого огляду технічних засобів і приміщень, в яких циркулює інформація, що становить комерційну або банківську таємницю суб'єкта господарської діяльності, необхідно починати з підготовки приміщення, яке підлягає огляду, яка характеризується такими особливостями: 1) необхідністю закриття вікон та занавісок з метою виключення візуального контакту; 2) необхідністю вимкнення світла і всіх звичайних офісних приладів, характерних для даного приміщення; 3) необхідністю увімкнення джерела «відомого шуму» (тестового акустичного сигналу) у центрі зони контролю, який у процесі огляду буде виконувати важливі функції, зокрема, маскувати більшість шумів, які виникнуть у процесі огляду, працювати як джерело для звукового зворотного зв'язку, необхідного для виявлення радіомікрофонів тощо.

Усі предмети в зоні проведення слідчого огляду, розміри яких дають змогу розмістити в них технічні засоби негласного отримання інформації, оглядаються візуально, а також обстежуються за допомогою засобів відеоспостереження і металодетекторів. Ретельному огляду також підлягають усі настільні прилади, рами картин, телефони, квіткові горщики, книги, прилади, які живляться від електромережі (комп'ютери, ксерокси, радіоприймачі тощо), а також такі предмети, як кулькові ручки, пачки цигарок, запальнички, електричні подовжувачі тощо, оскільки в них можуть бути вмонтовані акустичні радіомікрофони, які мають здатність ретранслювати всі звуки з приміщення на приймач оператора [54, с. 121].

У разі виявлення зазначених пристроїв перехоплення інформації, що становить комерційну таємницю, вони підлягають детальному опису у протоколі огляду місця події із зазначенням всіх можливих характеристик, зокрема: розмірів, ваги, призначення тощо. До того ж, до протоколу огляду приміщення, де циркулює

конфіденційна інформація підприємства, додається схема, на якій повинно бути вказано місце розташування зазначеного пристрою (пристроїв).

Огляду, у кримінальних провадженнях, розпочатих за фактами про незаконне отримання відомостей, що становлять комерційну або банківську таємницю, які циркулюють у засобах обчислювальної техніки, підлягають: а) технічні елементи системи обробки даних (термінали, електронно-обчислювальна техніка, вузли мережі електронно-обчислювальної техніки, канали зв'язку, зовнішні прилади електронно-обчислювальної техніки тощо); б) технічні елементи системи захисту інформації; в) програмні елементи системи захисту інформації (підсистеми управління доступом, механізми ідентифікації, автентифікації, контролю доступу, управління потоками інформації, підсистеми реєстрації і обліку, криптографічного захисту, підсистеми забезпечення цілісності тощо); г) ресурси захисту, що знаходяться в засобах обчислювальної техніки (програми, томи, каталоги, файли, записи, поля записів, усі види пам'яті електронно-обчислювальної техніки, в яких може знаходитися інформація); ґ) організаційно-розпорядча і поточна документація підрозділу захисту інформації з відображенням даних про зміну паролів, ключів, про зміну складу осіб, допущених до конфіденційної інформації, про реєстрацію і аналіз дій користувачів за системним журналом тощо.

Метою огляду технічних елементів системи обробки даних та технічних елементів системи захисту інформації є: 1) виявлення впроваджених електронних технічних засобів (або слідів їхнього застосування), які дозволили здійснити несанкціонований доступ до інформації; 2) виявлення слідів пошкоджень технічних елементів системи захисту інформації, які дозволяють здійснити несанкціонований доступ до відомостей, які становлять комерційну таємницю і підлягають захисту.

Метою огляду програмних елементів системи захисту інформації є: 1) виявлення слідів пошкоджень програмних елементів системи захисту інформації, які дозволяють здійснити

несанкціонований доступ до інформації, яка підлягає захисту; 2) виявлення незареєстрованих системними і програмними засобами відомостей про наявність заборонених зв'язків між суб'єктами і об'єктами доступу, незаконний доступ до інформаційних ресурсів ЕОМ (дата і час, суб'єкт запиту на доступ, об'єкт і тип доступу, виконання запиту на доступ; виявлення способу (виду) несанкціонованого доступу (доступ отриманий до файлів, програм, томів (інформаційних ресурсів), до яких суб'єкт не допущений; суб'єкт вийшов за межі типів дозволеного йому доступу (читати, редагувати, писати, копіювати) до конкретного документа або програми; суб'єкт отримав доступ до інформаційних ресурсів з використанням системних засобів (паролів, ключів, які належать іншому користувачу); суб'єкт отримав доступ до інформаційних ресурсів за допомогою використання власних програм роботи з пристроями; суб'єкт переніс конфіденційну інформацію на інформаційний носій з відкритим доступом тощо).

Огляд ресурсів, які належать до засобів обчислювальної техніки і підлягають захисту, проводиться з метою виявлення слідів копіювання, пошкодження або вилучення документів (інформації).

Огляд організаційно-розпорядчої і поточної документації підрозділу захисту інформації з відображенням даних про зміну паролів, ключів, про зміни в складі осіб, допущених до конфіденційної інформації, про реєстрацію і аналіз дій користувачів за системним журналом проводиться з метою виявлення обставин, які сприяли незаконному збиранню відомостей шляхом перехоплення інформації, яка знаходиться в технічних засобах і приміщенні, у тому числі, порушень правил організації технічного захисту охоронюваної зони приміщення, ліній і систем, які забезпечують функціонування технічних засобів, які в ньому знаходяться, порядку експлуатації систем обробки і передачі конфіденційної інформації, порядку генерації і зміни паролів, ключів, супроводження правил розмежування доступу, порядку оперативного контролю за функціонуванням системи захисту

інформації, порядку реєстрації і аналізу дій користувачів, порядку обліку, зберігання і видачі користувачам носіїв конфіденційної інформації, врахованого паперу для роздрукування, паролів і ключів, порядку допуску в приміщення, в яких проводиться автоматизована обробка конфіденційної інформації [54, с. 123] тощо.

Необхідно зауважити, що у випадку встановлення факту незаконного збирання з метою використання відомостей, що становлять комерційну або банківську таємницю, суб'єкта господарської діяльності шляхом перехоплення інформації, що циркулює у технічних засобах, зокрема, ЕОМ, організація і тактика огляду місця події відрізняється від аналогічної слідчої (розшукової) дії при розслідуванні традиційних злочинів. Це зумовлено не тільки небезпекою навмисного знищення інформації злочинцями, яка має доказове значення, а й необережним поводженням слідчого та інших членів слідчо-оперативної групи внаслідок неправильного, некваліфікованого поводження з програмно-апаратними засобами.

Проведення огляду місця події у цьому разі можна умовно розділити на чотири етапи: підготовчий, початок проведення, безпосереднє його проведення і заключний.

На стадії підготовки до огляду місця події ще до виїзду на місце події необхідно вирішити деякі організаційні питання, які надалі забезпечать якість проведення огляду місця події, зокрема: 1) вжити заходів із забезпечення охорони місця проведення огляду (досить часто огляд потрібно проводити одразу в кількох приміщеннях з комп'ютерним обладнанням; під час проведення огляду в комерційних структурах, які мають свої служби безпеки, не виключено спроби перешкодити проходу слідчо-оперативної групи до місця огляду – такі факти мають розглядатися як перешкоджання проведенню досудового розслідування); 2) одержати інформацію про комп'ютерну систему, яка підлягає огляду (один комп'ютер, робоча станція, сервер; яке програмне забезпечення використовується) тощо; 3) запросити спеціалістів, якими можуть бути системні програмісти, програмісти (фахівці зі

створення програм для ЕОМ), інженери з техніки експлуатації і ремонту ЕОМ (їх необхідно залучати з числа працівників сторонніх організацій науково-дослідних і навчальних закладів, компаній, які займаються розробкою й експлуатацією програмного і технічного забезпечення); 4) запросити понятих (як понятих необхідно запрошувати людей, які розуміються на комп'ютерній техніці); 5) підготувати відповідну комп'ютерну техніку для зчитування та збереження вилученої інформації; 6) провести інструктаж членів слідчо-оперативної групи, приділяючи особливу увагу їх поведінці під час огляду; 7) проконсультуватися зі спеціалістами (йдеться про випадки, коли до огляду місця події відомо, яка ком'ютерна техніка буде оглядатись) тощо.

Під час підготовки до огляду місця події після прибуття на місце необхідно додатково проінструктувати учасників огляду, а саме: а) усі вмикання (вимикання) комп'ютерів та інших технічних засобів з метою уникнення поломок мають здійснюватися тільки фахівцем або під його керівництвом; детальний огляд обчислювальної техніки, пов'язаний з проведенням різних фізичних маніпуляцій, здійснюється за умов вимкненого електроживлення. Якщо вимикання неможливе через особливості функціонування комплексу технічних засобів, потрібно вдатися до допомоги спеціаліста; б) забороняється проводити роз'єднання (з'єднання) кабельних ліній, не з'ясувавши попередньо їхнього призначення та переконавшись, що така дія не завдає шкоди; розкривання та монтаж засобів обчислювальної техніки має здійснювати тільки спеціаліст; в) застосування засобів криміналістичної техніки – магнітних шукачів, ультрафіолетового освітлювача, інфрачервоного перетворювача – має бути погоджено зі спеціалістом, щоб уникнути руйнування носіїв інформації і мікросхем пам'яті ЕОМ; необхідно також уникати потрапляння дрібних часток та порошку на робочі частини пристроїв вводу-виводу комп'ютерів; г) під час роботи з магнітними носіями інформації забороняється торкатися руками робочої поверхні дисків, піддавати їх електромагнітному впливу, згинати, зберігати без спеціальних конвертів

(пакет, коробка, діапазон припустимих температур при збереженні і транспортуванні – від 0 до + 50°С).

На робочій стадії етапу безпосереднього проведення огляду місця події кожен об'єкт підлягає ретельному обстеженню. У цей період часу важливо встановити, чи не міститься в комп'ютері інформація, яка може сприяти більш плідному та цілеспрямованому огляду (різні плани приміщень, ділянок місцевості, паролі, коди доступу, шифри тощо). Для цього спеціаліст проводить експрес-аналіз комп'ютерної інформації шляхом перегляду вмісту дисків. Інтерес можуть представляти також файли з текстовою чи графічною інформацією.

Далі під час робочої стадії етапу безпосереднього проведення огляду спеціаліст проводить такі дії. У разі, якщо комп'ютер працює: а) визначається, яка програма виконується на момент початку проведення огляду; при виявленні працюючої програми зі знищення інформації її зупиняють, і огляд комп'ютерної техніки починається саме з цього комп'ютера; б) після зупинки виконання програми здійснюється вихід в операційну систему для з'ясування, за можливості, яка програма викликалася останньою; в) встановлюється наявність у комп'ютері зовнішніх пристроїв віддаленого доступу до системи (під'єднання до локальної мережі, наявність модему); г) комп'ютер вимикається від мережі і вмикається модем; ґ) за потреби копіюється на машинний носій програма й інформація; д) якщо неможливо проаналізувати інформацію на місці (у більшості випадків проведення такого аналізу взагалі недоцільне через труднощі процесуального закріплення, вона вилучається разом з носієм, і це спеціально фіксується в протоколі огляду); е) після того, як з комп'ютера буде знято потрібну інформацію, він вимикається з електромережі. Усі зазначені дії бажано зафіксувати на фото- та відеоплівку.

При непрацюючому комп'ютері: а) фіксується (відображається) у протоколі огляду місцезнаходження комп'ютера, який цікавить слідчого і його периферійні пристрої, вказується пристрій (назва, серійний номер, комплектація: наявність і тип дисководів,

мережних карт, гнізд тощо), наявність з'єднання з локальною мережею і (чи) мережами, телекомунікації пристроїв (зі слідами чи без слідів розкриття тощо); б) описується порядок з'єднання між собою зазначених пристроїв, кількість сполучних гнізд, проводи, кабелі, а також порти, з якими кабель з'єднується; в) перевіряється барвна стрічка матричного принтера, на якій може бути виявлено сліди тексту; г) провадиться пошук і фіксація на комп'ютері та його пристроях, біля комп'ютерного обладнання та в інших місцях службового приміщення: слідів пальців рук, мікрочастинок та інших предметів на поверхні комп'ютера і його пристроях (зважаючи на характер і спосіб вчиненого злочину); змінних машинних носіїв інформації (дискет, оптичних компакт-дисків, магнітних стрічок тощо); паперових носіїв інформації – роздруківок, записів, записних книжок і тощо.

Під час огляду та попередньому дослідженні носіїв машинної інформації необхідно дотримуватися таких рекомендацій. Усі виявлені носії машинної інформації (особливо змінні), крім власне самої інформації, можуть містити на собі сліди рук і тому мають бути ретельно обстежені. Рекомендуються ці носії вилучити, упакувати відповідно до рекомендацій з упакування і транспортування, потім направити в спеціальну установу на експертизу. Перед упакуванням спеціаліст має перевірити носії на наявність механічних пошкоджень, характер яких відображається в протоколі. В окремих випадках за наявності спеціальної техніки, програмного забезпечення і відповідних знань у спеціаліста можна провести попереднє дослідження носіїв інформації, наприклад, на присутність вірусу в комп'ютерній системі тощо.

На заключній стадії під час складання протоколу огляду місця події фіксуються: а) програма, яка виконується (або виконана) комп'ютером на момент проведення (або до проведення) огляду місця події, для чого потрібно детально вивчити й описати зображення на екрані монітора комп'ютера, усі функціонуючі при цьому периферійні пристрої та результат їх діяльності; б) результат дії виявленої програми; в) усі маніпуляції із засобами

комп'ютерної техніки (включаючи натискання на клавіші клавіатури), зроблені під час проведення слідчої (розшукової) дії, та їхній результат (наприклад, при копіюванні програм і файлів, визначенні їх атрибутів, дати, часу створення і запису, а також при вмиканні і вимиканні апаратури, від'єднанні її частин) тощо [73, с. 73–82].

Під час огляду приміщення, в якому здійснюється обробка конфіденційної інформації, детально оглядаються конструкції приміщення і будівлі (стіни, підлога, стеля, вікна, двері); меблі і предмети інтер'єру. Метою огляду є: 1) виявлення порушень вимог інструкцій щодо захисту мовної інформації: а) приміщення (сховище інформації) розташоване за межами охоронюваної території або на мінімальній відстані від кордону контрольованої зони; б) приміщення має суміжні конструкції (стіни, стелі, підлоги) з приміщеннями, розташованими на не охоронюваній території; в) вікна приміщення виходять на відкриту для несанкціонованого доступу територію і не мають штор (жалюзі); г) конструкції огорожі приміщення не забезпечують надійну звукоізоляцію і дають змогу прослуховувати сховище (наявні тріщини і щілини); ґ) приміщення прослуховується через вентиляційні отвори; д) датчики охоронної сигналізації, двері, замки на дверях і силових щитах знаходяться в неналежному технічному стані (у процесі огляду необхідно також зафіксувати наявність (або відсутність) тамбура з подвійними дверима, прокладок у дверних та віконних притворах, застосування надійних шумопоглиначів для вентиляційних отворів тощо, що, відповідно, фіксується у протоколі огляду; 2) виявлення слідів перебування в приміщенні сторонніх осіб; 3) виявлення слідів особи, яка впровадила або вилучила раніше встановлену «закладку», особи, яка вкрала носій інформації тощо; 4) виявлення впровадженого радіозакладного пристрою; 5) виявлення можливості несанкціонованого візуального перегляду оброблюваних конфіденційних матеріалів тощо.

Огляду також підлягають: 1) засоби обчислювальної техніки; 2) засоби зв'язку і передачі даних обчислювальної техніки;

3) засоби телефонного зв'язку, звукозапису, звукопідсилення, переговорні і телевізійні прилади; 4) засоби виготовлення, тиражування документів та інші технічні засоби обробки інформації; 5) засоби охоронної і пожежної сигналізації; 6) засоби оповіщення і сигналізації; 7) контрольно-вимірювальна апаратура; 8) засоби і системи кондиціювання; 9) засоби провідної радіотрансляційної мережі; 10) засоби електронної оргтехніки; 11) електронні годинники тощо.

Метою огляду є: 1) виявлення впровадженої «закладки», слідів її встановлення або слідів вилучення раніше встановленого радіозакладного пристрою; 2) виявлення інших спеціальних пристроїв, призначених для перехоплення інформації або слідів їх підключення; 3) виявлення обставин, які сприяли незаконному збиранню відомостей, що становлять комерційну таємницю підприємства шляхом перехоплення інформації.

Здійснюються також: а) огляд технічних засобів, розміщених у приміщеннях, де оброблюється конфіденційна інформація; б) огляд документів, що регламентують організацію захисту інформації; в) огляд спеціальних електронних пристроїв перехоплення інформації; г) огляд виявленого технічного засобу з інформацією, що зберігається в ньому, або окремого носія інформації; ґ) огляд сейфа, в якому зберігався викрадений носій інформації; д) допити осіб, які виявили факт перехоплення інформації, тощо.

Під час огляду документів, які регламентують організацію захисту інформації, огляду підлягають: 1) паспорт приміщення, яке підлягає захисту і в якому, відповідно, відображаються склад технічних і програмних засобів обчислювальної техніки, плани розміщення основних і допоміжних технічних засобів; 2) склад і схеми розміщення засобів захисту інформації; 3) перелік і план розміщення обладнання і меблів (з вказуванням типу, заліково-го або інвентарного номеру й дати установки і заміни); 4) план охоронюваної зони організації; 5) схеми прокладки ліній передачі даних; 6) схеми і характеристики систем електроживлення і заземлення об'єкта інформатизації.

Метою огляду є: а) перевірка стану робіт і виконання організаційно-технічних вимог щодо захисту інформації; б) виявлення в охоронюваному приміщенні технічних засобів і систем, які не пройшли сертифікацію і спеціальну перевірку на наявність можливо запроваджених електронних пристроїв перехоплення інформації; в) виявлення не зафіксованого в паспорті приміщення факту заміни або перестановки технічних засобів і меблів (ознак ймовірного запровадження радіозакладного пристрою або застосування іншого способу перехоплення інформації); г) виявлення обставин, які сприяли незаконному збиранню з метою використання відомостей, що становлять комерційну таємницю, шляхом перехоплення інформації, що знаходилась у технічних засобах і приміщенні, у тому числі, порушень правил організації технічного захисту охоронюваної зони приміщення, ліній і систем, порядку експлуатації систем обробки і передачі конфіденційної інформації; порядку оперативного контролю за функціонуванням системи захисту інформації; порядку реєстрації і аналізу дій користувача; порядку обліку, зберігання і видання користувачем носіїв конфіденційної інформації, матеріалів для роздрукування, паролів і ключів; порядку допуску в приміщення, в яких проводиться автоматизована обробка конфіденційної інформації тощо.

Метою проведення огляду спеціальних електронних пристроїв перехоплення інформації є: 1) встановлення призначення і стану приладу, його придатності для перехоплення інформації, способу перехоплення інформації і її передачі, спосіб управління приладом, технічні параметри приладу, встановлення індивідуальних ознак приладу, які свідчать про призначення даного пристрою, про зв'язок пристрою з розслідуваним злочинним діянням; 2) встановлення індивідуальних ознак пристрою, які засвідчують приналежність пристрою конкретній організації або конкретній особі (спосіб виготовлення, застосування характерних деталей тощо); 3) виявлення слідів, які вказують на зв'язок пристрою з підозрюваним (сліди пальців рук, потожирові виділення, фарба

та інші речовини, які мають схожість з виявленими на тілі і одязі підозрюваного або в його житлі тощо) [54, с. 130].

У процесі проведення огляду технічних засобів і приміщень, в яких циркулює інформація, що становить комерційну таємницю суб'єкта господарської діяльності, слідчому необхідно пам'ятати, що загальним недоліком контактного під'єднання пристроїв прослуховування до телефонних ліній є наявність необхідності порушення цілісності проводки, а також впливу підключеного пристрою на характеристики ліній зв'язку.

Під час проведення візуального огляду з метою виявлення закладних пристроїв перехоплення інформації особливу увагу необхідно приділяти важкодоступним місцям як таким, що являють найбільший інтерес для зловмисників, які їх встановлюють. З метою полегшення процедури пошуку використовуються ліхтарі та дзеркала. Однак такі прості пристосування не завжди є зручними і ефективними, тому на практиці часто застосовують технічні засоби відеоспостереження, спеціально пристосовані для огляду важкодоступних місць, зокрема, оптико-електронні системи, які умовно можна поділити на дві групи: 1) ендоскопічне обладнання: а) волоконно-оптичні фіброскопи; б) жорсткі бароскопи; в) відеоскопи, які дають змогу здійснювати огляд важкодоступних місць тощо; 2) доглядові портативні телевізійні або відеоустановки: а) телескопічні штанги; б) підсвітки; в) мініатюрні рідкокристалічні відеомонітори; г) спеціальні жилети [54, с. 131].

Необхідно зазначити, що недоліком візуального огляду є необхідність довготривалої концентрації уваги слідчого (спеціаліста), що не завжди дає надійний результат. Тому раціональним кроком є поєднання візуального і детекторного досліджень з метою виявлення закладних пристроїв перехоплення інформації, що становить комерційну або банківську таємницю.

Детекторне дослідження – це застосування апаратури, яка контактним або безконтактним способом сприймає певні фізичні властивості, які засвідчують наявність у місці, яке оглядається, певних аномалій у вигляді неоднорідностей, характерних

випромінювань або деяких речовин. На нашу думку, ефективність дослідження шляхом застосування детекторів полягає в тому, що вони виробляють звуковий або світловий сигнали у випадку перевищення завданої межі параметром, по якому здійснюється детектування. Так відбувається не тільки виявлення, а й локалізація пристрою або предмета перехоплення інформації [54, с. 132].

З метою виявлення закладних пристроїв перехоплення інформації під час слідчого огляду технічних засобів і приміщень доцільним є також: 1) застосування індикаторів електромагнітного поля, спеціальних приймачів, комплексів радіоконтролю тощо; 2) застосування програмно-апаратних комплексів радіоконтролю і виявлення каналів розповсюдження інформації з метою виявлення випромінювань радіозакладок, фіксації дії радіозакладних пристроїв у реальному масштабі часу; визначення відстані до джерел випромінювання, аналогово-цифрової обробки сигналів з метою визначення їх приналежності до випромінення радіозакладок, контролю силових, телефонних, радіотрансляційних та інших мереж, робота в багатоканальному режимі, який дає можливість контролювати декілька об'єктів одночасно, постановки прицільних поміх на частотах випромінювання радіозакладок тощо [54, с. 132].

У процесі слідчого огляду приміщень з метою виявлення закладних пристроїв негласного отримання конфіденційної інформації особливо ретельному огляду підлягають місця, де, зазвичай, проводяться ділові переговори та наради: практика розслідування подібних кримінальних проваджень засвідчує, що більшість пристроїв негласного отримання інформації розташовано у межах відстані 7-ми метрів від цього місця.

Особливої уваги потребує проведення огляду телефонних ліній, мереж пожежної і охоронної сигналізації. Необхідно розбирати телефонні апарати, розетки і датчики й шукати деталі, несхожі на звичайні з різнокольоровими проводами і ознаками поспішної, неохайної установки.

Під час проведення огляду автомобіля з метою пошуку закладних пристроїв ретельному огляду підлягає не тільки салон, а й

рама автомобіля, багажник тощо, мережі, які мають вихід на автомобільну антену, тощо [54, с. 133].

Говорячи про незаконне збирання з метою використання інформації, що становить комерційну або банківську таємницю суб'єкта господарської діяльності, без застосування спеціально виготовлених технічних засобів, необхідно зауважити, що важливим тактичним завданням під час слідчого огляду приміщень, в яких циркулює інформація, що становить комерційну таємницю, є перевірка наявності акустичних каналів розповсюдження конфіденційної інформації, оскільки звук може поширюватися через вікна, стіни, водопровідні труби, пустоти в будівлі тощо і фіксуватися мікрофонами за межами охоронюваного приміщення. Тому під час огляду необхідною є перевірка вентиляційних і кабельних каналів на можливість прослуховування, а також на наявність у них винесених мікрофонів, поєднаних проводами з апаратурою звукозапису. За потреби проводиться повна акустична перевірка контрольованого приміщення [54, с. 133].

З метою встановлення факту втрати документа, що містить комерційну таємницю підприємства, зокрема, інсценування його санкціонованого знищення або удаваного відправлення в іншу організацію і перевірки версій про можливе складення фіктивного акту про знищення документа, внесення недійсного запису про знищення в дійсний акт, складення фіктивного реєстру на відправку документа, внесення запису про відправлення в справжній реєстр тощо доцільно проводити: огляд акта про знищення документа, огляд реєстру на відправлення документа, допит особи, відповідальної за документ, допит свідків тощо. Водночас обставинами, які спростовують інсценування, можуть бути такі: документ, який вважається знищеним, виявлено поза місцем його зберігання з ознаками виходу із законного володіння; документ видавався виконавцям після його удаваного знищення або відправлення в іншу організацію; інформація про втрату документа була в наявності до того, як він був включений в акт на знищення

або реєстр на відправлення; інформація про надходження документа в іншу організацію відсутня.

Для встановлення факту втрати документа, зокрема, шляхом інсценування його необережного знищення і перевірки висунутих версій про часткове або повне знищення подібного документа в спеціальному пристрої, про те, що залишки знищеного документа є частиною втрачених відкритих матеріалів, про те, що документ знищений у спеціальному пристрої раніше, доцільно проводити огляд місця знищення документа, призначити криміналістичну експертизу виявлених (наданих) об'єктів. Водночас негативними обставинами виявляються: неможливість знищення документа за обставин, вказаних підозрюваним, зокрема, внаслідок тимчасової несправності спеціального пристрою тощо; неможливість знищення документа в даному пристрої у зв'язку з великим форматом, особливостями паперу тощо; інформація про втрату документа зафіксована до того, як відбулося його удаване знищення; фрагменти паперу, скріпки та інші компоненти вмісту, виявленого у пристрої знищення конфіденційних матеріалів, не відповідають за хімічним, фізичним складом та за іншими параметрами залишкам втраченого документа тощо.

Щоб встановити факт втрати документа, зокрема, шляхом його підміни і перевірки версій про здійснення підозрюваним підміни втраченого документа аналогічним документом, запозиченим (або викраденим) тимчасово у іншої відповідальної особи, підміни втраченого документа спеціально виготовленим з даною метою екземпляром, доцільно проводити допит відповідальної за документ особи, допит свідків, призначати криміналістичну (технічну) експертизу документа тощо. У цьому разі можливими доказами, які заперечують інсценування, можуть бути: невідповідність реквізитів наданого документа реквізитам документа, закріпленим за відповідальною особою; відмінність наданого документа від втраченого за способом виготовлення тощо.

З метою встановлення обставин маскування причетності до втрати документа, зокрема, шляхом приховування факту його

отримання або твердження про його повернення або передачу та перевірки версій про можливе приховування факту отримання конфіденційних матеріалів шляхом викрадення (знищення) облікових документів (журналу обліку, картки, розписки), про те, що втрачений документ повернений в режимний орган, секретаріат, бібліотеку, з посиланням на те, що розписка про повернення відсутня з вини працівника вказаного органу, про те, що втрачений документ переданий без оформлення іншим особам у зв'язку з їх роботою, проводяться: огляд записів (робочих і особистих) підозрюваної особи, які підтверджують факт використання документа; огляд таких, що залишилися в наявності, облікових документів підрозділу (журналів, реєстрів, карток), які свідчать про факти передачі відповідальною особою іншим співробітникам в користування документа, якого, начебто, вона не отримувала; обшук за місцем роботи і проживання відповідальної за документ особи; допит свідків тощо. Водночас можливими доказами, які заперечують інсценування, можуть виявлятися: наявність у записах відповідальної за документ особи виписок з втраченого документа, який він начебто не отримував; виконання роботи відповідальною за документ особою, яка потребувала використання втраченого документа; передача відповідальною за втрачений документ особою іншим виконавцям; неможливість повернення підозрюваним втраченого документа іншій особі у зв'язку з її відсутністю на роботі у вказаний час або внаслідок інших об'єктивних причин; наявність зафіксованої інформації про втрату документа до його удаваної передачі (повернення) тощо.

Також для встановлення факту інсценування викрадення документа за умов відсутності порушень правил поводження з ним і перевірки версій про наявність імітації слідів проникнення сторонньої особи в закрите службове приміщення, імітації слідів злому сховища з конфіденційними матеріалами, імітації виводу з ладу захисної сигналізації, виклику на місце події працівників режимного або правоохоронного органу тощо доцільно проводити огляд місця події, обшук у відповідальної за документ особи з

метою виявлення і вилучення знарядь, використовуваних для інсценування, призначати криміналістичну (трасологічну) експертизу тощо. Негативними обставинами у цьому разі, зазвичай, виявляються: наявність слідів, які свідчать про злом зсередини; розташування пролому в місці, недоступному з зовнішньої сторони приміщення; відсутність слідів, які повинні були залишитися за умов застосування даного способу злому, виводу з ладу сигналізації; неможливість отримання втраченого документа через ушкодження на сейфі внаслідок їхнього розміру; відсутність слідів волокон паперу, які повинні були залишитися на краях пролому сейфу тощо.

З метою встановлення фактів приховування порушень правил конфіденційного діловодства і доказування обставин здійснення відповідальною особою з цією метою маскувальних дій щодо неналежного стану технічних засобів захисту, зокрема, встановлення захисних решіток на вікна, ремонту сигналізації, виготовлення втраченого екземпляра ключа від сейфа, приховування фактів перебування в службовому приміщенні сторонніх осіб, використання приміщення не за призначенням, зокрема, прибирання приміщення, ліквідації слідів розпивання алкогольних напоїв, підбурювання співробітників та інших осіб до давання свідомо неправдивих показань тощо, приховування факту відхилення від встановленого маршруту доставки документа, стоянок службового транспорту в непередбачених місцях, неправдивих (недійсних) записів про час виїзду з пункту відправлення, про маршрут пересування в супровідних документах, приховування справжнього місця і обставин викрадення документа під час відхилення від встановленого маршруту, звернення до правоохоронних органів із заявою про викрадення документа в місці і за обставин, які не відповідають дійсності, підбурювання співробітників та інших осіб до давання неправдивих показань про маршрут слідування відповідальної особи, місце та інші обставини, за яких був викрадений документ, доцільно проводити огляд місця події, огляд ключів від сейфа, огляд сейфа, огляд

супровідних і документів про відрядження, допит відповідальної за документ особи, допит свідків, призначати криміналістичну (технічну) експертизу документів. Обставинами, які спростовують інсценування, у цій ситуації є: невідповідність часу (дати) виготовлення і установки технічних захисних засобів (решітки, сигналізації) часу початку використання приміщення, сейфа в якості сховища конфіденційних документів; відмінності між ключами від сейфа за способом виготовлення, номерами тощо; незбігання номера на ключі (ключах) від сейфа і замка; наявність в приміщенні предметів, які належать стороннім особам, слідів розпивання алкогольних напоїв; невідповідність записів про час отримання документа (предмета) для доставки, що є в накладній, пропуску тощо даті виписки з готелю; виявлення слідів викрадення документа (предмета) в місці, яке не відповідає заяві відповідальної особи [54, с. 138].

Варто зазначити, що під час проведення огляду можуть використовуватися як традиційні технічні засоби (фото- і відеокамери, вимірювальні пристрої, освітлюючи засоби та ін.), що застосовуються під час проведення огляду будь-якого місця події, так і спеціальні (магнітний шукач (підіймач); викрутка-індикатор напруги «ІО-500», пінцет, алмазний склоріз; силіконові пасти у тубах одноразового використання та ін.). Основним засобом фіксації результатів огляду місця події є протокол.

Проведення слідчих (розшукових) дій у кримінальних провадженнях про незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю суб'єкта господарської діяльності, а також розголошення комерційної або банківської таємниці з дотриманням наукових рекомендацій, а також з врахуванням зазначених тактичних особливостей, сприятиме систематизованому та всебічному пошуку слідів злочинної діяльності, їх вилученню, успішному попередньому дослідженню та отриманню важливої криміналістично значущи ої інформації ще на початковому етапі розслідування.

РОЗДІЛ 3.
Тактичні особливості проведення окремих слідчих (розшукових) дій під час досудового розслідування незаконного збирання або використання відомостей, що становлять комерційну або банківську таємницю

3.1. Тактика проведення окремих слідчих (розшукових) дій наступного етапу розслідування незаконного збирання або використання відомостей, що становлять комерційну або банківську таємницю

Під час наступного етапу в слідчого буває зібрано досить доказів, щоб обґрунтувати одну з можливих версій, організувати всебічну її перевірку, викрити злочинця і розкрити злочин [71, с. 462].

Наступний етап розслідування характеризується аналітичною діяльністю, оцінкою і перевіркою зібраної інформації, а також збиранням інформації шляхом використання складних (системних) джерел доказової інформації [71, с. 484].

У ході наступного етапу розслідування незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, збирання доказів може здійснюватися шляхом проведення: 1) допитів свідків, потерпілих, підозрюваних; 2) одночасних допитів двох чи більше раніше допитаних осіб; 3) обшуків у підозрюваних (виконавців, організаторів, підбурювачів та замовників), зокрема, за місцем постійного або тимчасового проживання, роботи, проживання близьких осіб та родичів; 4) огляду місця події та вилучення документів; 5) призначення судових експертиз, зокрема, 1) криміналістичних експертиз речових доказів (судово-почеркознавчої, судово-технічної експертизи документів, судово-авторознавчої, судово-хімічної, фізико-хімічної, фізико-технічної) судово-технічної експертизи речових доказів: а) технічної експертизи транспортних й інших засобів доставки документів; б) технічної експертизи сховищ конфіденційних документів і ключів від них; в)

технічної експертизи охоронної сигналізації приміщення, в якому зберігався документ; б) судово-медичної (біологічної) експертизи речових доказів: а) експертного дослідження потожирових виділень, плям слини, сечі, поту та інших виділень людського організму; б) експертного дослідження волосся; в) експертного дослідження крові, частин шкіри людини (що залишилися на гострих кромках сейфа тощо); 7) судово-фонографічної експертизи речових доказів тощо; 8) слідчого експерименту тощо.

Способами збирання доказів є: 1) огляд місця події; 2) огляд знаряддя викрадення; 3) призначення криміналістичних експертиз; 4) допит підозрюваного; 5) допит свідків; 6) обшук; 7) слідчий експеримент.

Можливими доказами факту викрадення документа підозрюваним є: а) залишення відбитків пальців підозрюваним на місці події; б) виявлення на місці події слідів взуття підозрюваного; в) виявлення на одязі підозрюваного (на його речах) мікроволокон, мікрочастинок викраденого документа; г) виявлення однорідних сторонніх частинок на одягу, взутті підозрюваного; ґ) виявлення частинок речовини (фарби тощо) на одязі, взутті підозрюваного, які є однорідними частинками речовини, які є на місці події.

Способами збирання доказів є: 1) огляд місця події; 2) отримання у підозрюваного відбитків пальців; 3) призначення криміналістичної (дактилоскопічної) експертизи; 4) призначення криміналістичної (трасологічної) експертизи; 5) допит підозрюваного; 6) допит свідків; 7) огляд одягу і взуття підозрюваного, його особистих речей; 8) відібрання з місця події зразків речовини, ґрунту, 9) призначення судово-хімічної експертизи.

Іншими доказами факту викрадення документа підозрюваним є: а) наявність саден, подряпин на руках підозрюваного, що залишені деталями сховища під час викрадення з нього документів; б) підтвердження очевидцями факту викрадення документа підозрюваним; в) визнання підозрюваним факту викрадення ним документа; г) наявність фактів, які підтверджують наявність у

підозрюваного умислу на викрадення документа, зокрема, виказування підозрюваним наміру викрасти документ; виявлено лист, записку, щоденник, в яких він планував або виказував цей намір; ґ) наявність фактів, які підтверджують обізнаність підозрюваного про відсутність документа до того, як була виявлена його нестача; д) наявність обізнаності підозрюваного про зміст конфіденційних матеріалів, які йому не було довірено тощо.

Можливими способами збирання доказів у цьому разі є: 1) призначення комплексної судово-медичної і криміналістичної експертиз; 2) допит підозрюваного; 3) допит свідків; 4) обшук; 5) вилучення записів; 6) призначення почеркознавчої експертизи; 7) огляд викраденого документа або його аналога; 8) проведення слідчого експерименту.

У разі встановлення факту приховування документа або його частин та інших аналогічних дій доказуванню може підлягати факт знищення документа або його частин, зокрема, шляхом спалювання документа або його частин; шляхом подрібнення (розрізання тощо) документа або його частин у спеціальній машині, можливими доказами чого є: а) виявлення в топках печі, котельної, бані незгорілих частин документа, обкладинки, скріпок, інших металевих деталей (незгорілі об'єкти є частиною розшукуваного документа); б) виявлення в перемолотій масі частинок паперу і металевих, пластмасових деталей, які є частиною розшукуваного документа.

З метою збирання доказів проводять: 1) огляд місця спалювання документа з метою вилучення зразків попелу і виявлених у ньому предметів для дослідження; 2) огляд місця подрібнення документа та вилучення виявлених предметів для дослідження; 3) криміналістична експертиза речових доказів з використанням допомоги спеціалістів у галузі фізики і хімії.

У разі потреби встановлення факту вчинення підозрюваним дій, з метою приховування викрадення, доказуванню підлягають факти наявності дій підозрюваного, спрямовані на маскування слідів викрадення документа: а) шляхом маскування слідів

проникнення в місце зберігання документа; б) шляхом маскування слідів застосування знаряддя викрадення; в) шляхом знищення підозрюваним своїх слідів відбитків пальців з викраденого документа, можливими доказами чого є: а) наявність слідів тимчасового видалення (з наступним відновленням) мастичної печатки шляхом зрізання, відділення шляхом попереднього заморожування, викручування болтів, які прикріплюють бирку з печаткою; б) виявлення знаряддя викрадення або його частин (ножа, відмички, ключа) за місцем проживання підозрюваного або на шляху його слідування з місця вчинення кримінального правопорушення.

Збирання доказів у цій ситуації здійснюється за допомогою проведення: 1) огляду місця події; 2) призначення криміналістичної (трасологічної) експертизи з метою встановлення цілого за частинами; 3) призначення криміналістичної експертизи речових доказів із залученням спеціалістів у галузі фізики і хімії; 4) обшук за місцем проживання підозрюваного; 5) огляд шляху слідування підозрюваного додому з місця вчинення кримінального правопорушення.

За потреби встановлення факту приховування документа або його частин (або інших дій щодо приховування факту викрадення) доведенню підлягає факт вжиття підозрюваним заходів, які перешкоджали встановленню приналежності документа. Можливими доказами у цьому разі є: знищення реквізитів документа, знищення обкладинки або частини тексту документа з метою зробити неможливою його ідентифікацію тощо. З метою збирання доказів необхідно проводити такі слідчі (розшукові) дії: 1) допит підозрюваного; 2) допит свідків; 3) пред'явлення документа (або його частини) для впізнання; 4) призначати криміналістичні експертизи.

Встановлення у разі потреби приховування підозрюваним своєї участі у викраданні, інсценування втрати документа або його викрадання іншою особою доказуванню підлягає факт вчинення підозрюваним дій щодо створення інсценування, зокрема:

а) знищення або спроба приховування слідів проникнення в службове приміщення і сліди відмикання сейфа; б) знищення або приховування знаряддя викрадання; в) поширення помилкових чуток про втрату документа відповідальною особою, його помилкову відсилку, видачу тощо; г) висловлювання співчуття щодо відсутності документа, своєї версії того, що відбулося; ґ) поширення помилкових чуток про викрадання документа іншими особами, підкидання цим особам викраденого документа або його частини (частин), підкидання знаряддя викрадання; д) розсилка анонімних листів з вказівкою на уявного викрадача; е) підкидання на місце події предметів, що належать особі, що не має відношення до викрадання; є) створення собі помилкового алібі: прохання до родичів, товаришів по службі, друзів підтвердити обставини, які нібито свідчать про непричетність підозрюваного до вчинення кримінального правопорушення.

Способами збирання доказів у цьому разі є: 1) огляд місця події; 2) огляд документів, що підтверджують відсутність відповідальної особи в період зникнення документа на службі, у населеному пункті тощо; 3) допит підозрюваного; 4) слідчий експеримент; 5) допит свідків; 6) обшук у підозрюваного; 7) призначення криміналістичних експертиз, зокрема, трасологічної, дактилоскопічної; 8) пред'явлення знаряддя злочину для впізнання; 9) призначення криміналістичної експертизи (почеркознавчої, авторознавчої), технічної експертизи документів.

У разі потреби встановлення причетності особи, відповідальної за документ, в якому містяться відомості, що становлять комерційну або банківську таємницю, до викрадення документа можливими доказами того, що відповідальну особу було допущено до конфіденційного діловодства, ознайомлено з правилами конфіденційного діловодства і було зобов'язано їх виконувати, фактів її добросовісного або недобросовісного відношення до праці, наявності у неї державних нагород, почесних звань, вживання нею алкогольних напоїв тощо є дані, зафіксовані у відповідних наказах керівника підприємства, особовій справі, контракті, договорі, зобов'язанні тощо.

З метою збирання доказової інформації проводяться: 1) огляд документів; 2) вилучення і приєднання до матеріалів кримінального провадження оригіналів або копій документів; 3) допит свідків; 4) допит відповідальної за документ особи; 5) витребування і огляд медичних документів тощо.

Під час наступного етапу розслідування незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, може виникнути необхідність доказування, зокрема: а) наявності або відсутності факту знайомства підозрюваного з особою, відповідальною за документ (вони раніше не зустрічалися; знайомі (разом проводять час, разом навчаються, проживають тощо), знаходилися в інтимних відносинах, є членами однієї сім'ї), можливими доказами чого виступають дані, повідомлені підозрюваним, особою, відповідальною за документ, свідками, документальні дані навчального закладу, документальні дані з місця постійної роботи тощо; б) характеру їхніх відносин (дружні, неприязні, ворожі, байдужі), можливими доказами чого є наявність дружніх стосунків підозрюваного і відповідальної за документ особи, а також отримані відомості про їх взаємні послуги, спільний відпочинок; дані, повідомлені керівництвом або громадськими організаціями про вирішення конфлікту між підозрюваним і відповідальною за документ особою тощо.

Для отримання зазначених даних доцільним є проведення: 1) допиту підозрюваного; 2) допиту відповідальної за документ особи; 3) допиту свідків; 4) проведення одночасного допиту раніше допитаних осіб, зокрема, між підозрюваним і відповідальною за документ особою, між підозрюваним і свідком, між відповідальною особою і свідком, між свідками.

Характеризуючи цілі і мотиви викрадення документів, в яких містяться відомості, що становлять комерційну або банківську таємницю, необхідно зауважити, що вони можуть мати: 1) виробничий; 2) особистий характер, доказами чого є: а) наявність факту порушення відповідальною за документ особою

правил поводження з ним, щоб прискорити виконання службового завдання, виконати одночасно з основними службовими обов'язками й інші додаткові службові обов'язки; б) порушення відповідальною за документ особою правил поводження з ним з метою використання документа під час підготовки до виконання інших видів робіт, не пов'язаних із посадовими обов'язками; в) відхилення від маршруту доставки документа з метою відвідання магазину, знайомих тощо, керуючись корисливими, мотивами кар'єризму тощо.

Способами збирання доказів у цій ситуації є: 1) проведення допиту особи, відповідальної за документ; 2) допиту свідків; 3) огляду документів, що можуть засвідчити факти одночасного виконання відповідальною за документ особою додаткових службових обов'язків; використання документа в неслужбових цілях; знаходження відповідальної особи поза маршрутом доставки документа тощо.

Викрадення документів, які містять відомості, що становлять комерційну або банківську таємницю суб'єкта господарської діяльності, може бути здійснено: 1) з метою передачі документа конкуруючій організації, спецслужбі або іншій організації іноземної держави, зацікавленій особі тощо: а) з корисливих мотивів (підозрюваний мав намір отримати матеріальну винагороду в обмін на викрадений документ); б) під впливом погроз (підозрюваний піддавався психічному або фізичному насильству); в) на підставі помилкової етнічної солідарності (підозрюваний піддався психологічній обробці з використанням чинника етнічної близькості); 2) а) з метою вдосконалення виробничої і комерційної діяльності організації, яка заволоділа конфіденційною інформацією; б) з метою завдання збитків організації-конкуренту; 3) а) з метою компрометації особи, відповідальної за документ (підозрюваний мав намір скомпрометувати відповідальну за документ особу з мотивів помсти на ґрунті особистих взаємин або заздрощів тощо; підозрюваний мав намір скомпрометувати відповідальну за документ особу з мотивів кар'єризму); б) з метою помсти (викрадення

здійснено з мотивів помсти відповідальній особі за справедливе зауваження по службі, критичне зауваження); підозрюваний виявляв бажання помститися відповідальній особі; викрадання здійснено у зв'язку з необґрунтованим (на думку підозрюваного) підвищенням відповідальної особи по службі, заохоченням; підозрюваний виражав незадоволення щодо підвищення по службі (заохочення) відповідальної особи і бажання скомпрометувати його); в) у зв'язку з наміром домогтися звільнення, пониження на посаді відповідальної особи з метою посісти його посаду (підозрюваний закінчив навчальний заклад, набув навичок, що дають змогу виконувати службові обов'язки відповідальної особи); 4) за умов наявності наміру скомпрометувати відповідальну за документ особу: а) з метою завадити розкриттю раніше вчиненого злочину; б) з мотивів помсти; 5) з метою отримати заохочення за виявлення удаваної втрати документа тощо.

З метою встановлення зазначених мотивів і цілей викрадення документів, які містять відомості, що становлять комерційну або банківську таємницю суб'єкта господарської діяльності, доцільно проводити такі слідчі (розшукові) дії: 1) а) допит підозрюваного (з метою встановлення наміру викрасти документ за винагороду від представника розвідки (особи, яку він прийняв за представника розвідки), осіб з числа близького оточення; отримання підозрюваним письмових, телефонних та інших (у формі аудіо- записів тощо) погроз і вимог щодо вчинення викрадення документа, про що він розповідав представникам близького оточення; несподіване налагодження підозрюваним контакту з раніше незнайомим «земляком», повідомлення ним своїм близьким про прохання «земляка» викрасти конфіденційні матеріали; б) допит свідків; в) обшук у підозрюваного (з метою відшукування листування особистого характеру, записів у щоденнику, що засвідчують наміри підозрюваного щодо викрадення документа); г) вилучення викраденого документа (з метою встановлення використання відомостей, що містяться в документі і становлять комерційну або банківську таємницю, з метою підвищення

конкурентоспроможності продукції і ефективності виробництва; вибору оптимальної стратегії збуту товарів і проведення торговельних переговорів; про наявність запозичення технічних рішень, описаних у викраденому документі під час створення іншого приладу або пристрою; про наявність окремих положень викраденого документа у науковій доповіді, монографії; використання відомостей, що містяться в документі, з метою протидії збуту продукції, руйнування виробничих і торгових зв'язків суб'єкта господарської діяльності, зриву торгових переговорів і операцій, зниження інвестиційних можливостей організації, підготовки і розповсюдження дезінформаційних матеріалів ганебного характеру тощо; ґ) огляд записів підозрюваного; д) призначення почеркознавчої експертизи [54, с. 151].

Необхідно зауважити, що особливої уваги потребує проведення допиту осіб, які виявили факт перехоплення інформації, що становить комерційну або банківську таємницю суб'єкта господарської діяльності і циркулює у технічних засобах і приміщеннях.

Наявністю окремих тактичних особливостей характеризується і проведення слідчого експерименту, оскільки метою проведення вказаної слідчої (розшукової) дії наступного етапу розслідування незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, є: а) перевірка слідчих версій про можливість (або неможливість) перехоплення відомостей, які циркулюють у конкретних технічних засобах і приміщенні, шляхом використання відомих спеціалістам способів і пристроїв; б) перевірка показань підозрюваного, свідка про те, що мало місце, перехоплення відомостей у конкретних умовах з використанням конкретного способу і пристрою; в) перевірка параметрів і можливостей закладного пристрою або іншого технічного пристрою, програми ЕОМ, використаних підозрюваним, з метою незаконного перехоплення конфіденційної інформації і виявлених у результаті проведення слідчих (розшукових) дій тощо [54, с. 152].

У ході наступного етапу розслідування незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, може виникнути необхідність у встановленні: а) відношення винної особи у розголошенні комерційної або банківської таємниці до суб'єкта господарської діяльності, якому належать вказані відомості; б) відношення винної особи до предмета розголошення (чи був носій інформації переданий особі у встановленому порядку або знаходився у її володінні внаслідок порушення діючих правил); в) наявності права доступу винної особи до незаконно розголошеної конфіденційної інформації (особа мала дозвіл використовувати інформацію для виконання службових обов'язків або тільки здійснювала функції її зберігання або доставки); г) особистісних якостей і властивостей особи – стану здоров'я (наявності захворювання, яке зважає здійсненню нею якісного контролю за збереженістю носія інформації), навичок, звичок, окремих якостей характеру; ґ) даних про такі, що мали місце, порушення правил поводження з відомостями, які становлять комерційну таємницю суб'єкта господарської діяльності [54, с. 153] тощо.

З цією метою доцільно проводити: 1) допит підозрюваного; 2) допит колег підозрюваного по роботі; 3) допит осіб, зайнятих у сфері конфіденційного діловодства підприємства (установи, організації), свідків; 4) одночасний допит підозрюваного і свідків, свідків; 5) огляд приміщень і технічних засобів, в яких циркулює інформація, що становить комерційну або банківську таємницю суб'єкта господарської діяльності; 6) огляд актів перевірки документації і приміщень, довідок, заяв, планів, анонімних записок тощо.

У разі вчинення незаконного збирання з метою використання відомостей, що становлять комерційну або банківську таємницю суб'єкта господарської діяльності, шляхом перехоплення інформації, що циркулює в технічних засобах, зокрема, ЕОМ, може виникнути необхідність у доказуванні: 1) факту несанкціонованого проникнення підозрюваного (підозрюваних) у комп'ютерну систему чи мережу; 2) факту несанкціонованого проникнення в

комп'ютерну систему або мережу підозрюваним (підозрюваними) конкретним способом; 3) факту вчинення кримінального правопорушення підозрюваним (підозрюваними) у конкретний проміжок часу; 4) факту вчинення кримінального правопорушення (проникнення у комп'ютерну систему або мережу з метою збирання конфіденційної інформації) підозрюваним (підозрюваними) у конкретному місці тощо.

З метою доказування факту вчинення незаконного збирання інформації, що становить комерційну або банківську таємницю і циркулює в ЕОМ, підозрюваним у конкретному місці необхідно зафіксувати загальний технічний стан комп'ютерів, наявність інформації, що зберігається, провести огляд, обшук і вилучення документації, зокрема, інструкцій, що регулюють правила експлуатації і допуску до роботи на комп'ютері. Треба допитати осіб, що мають доступ до працюючої комп'ютерної системи, і встановити, як часто спостерігалися перебої в роботі комп'ютера, хто в цей час працював на комп'ютерах локальної системи; якими користувався дискетами, із записами чи чистими; як давно і за чиєї участі обновлялися коди, паролі та інші захисні засоби; хто приносив на роботу дискети, диски під приводом комп'ютерної гри чи перезапису; хто з працівників часто здійснює різні перезаписи, цікавиться роздруківками операторів інших локальних систем тощо.

Необхідно зауважити, що місце несанкціонованого проникнення може бути безпосереднім і опосередкованим (віддаленим). Віддалене місце несанкціонованого проникнення в комп'ютер або мережу з метою збирання інформації, що становить комерційну або банківську таємницю суб'єкта господарської діяльності, складніше встановити і, відповідно, складніше довести факт проникнення підозрюваного з віддаленого місця, оскільки в такій системі, як Інтернет, мільйони комп'ютерів, і з кожного з них за наявності певних знань можна проникнути в будь-яку індивідуальну систему. Для вирішення такого завдання треба проводити попереднє спеціальне дослідження, запрошувати фахівців з

різних профілів інформатики – програмування, обчислювальної техніки і засобів захисту комп'ютерних систем, мереж і в результаті клопотати про призначення судової експертизи.

Для доказування вчинення підозрюваним (підозрюваними) незаконного збирання інформації, що становить комерційну або банківську таємницю, вказаним способом необхідно проводити допит свідків з числа користувачів локальної мережі, допущених, а також не допущених до обробки відомостей, що становлять комерційну або банківську таємницю, та клопотати про призначення експертизи. Перед експертом, зазвичай, ставиться питання: «Яким способом могло бути вчинено несанкціонований доступ у певну комп'ютерну систему?».

З метою доказування факту вчинення незаконного збирання комерційної або банківської таємниці шляхом проникнення в ЕОМ чи їхні системи, де вона зберігається, необхідно проводити такі слідчі (розшукові) дії: 1) слідчий огляд; 2) допит; 3) слідчий експеримент; 4) призначення судових експертиз.

Допитуючи підозрюваного, необхідно пам'ятати, що несанкціонований доступ до закритих комп'ютерних систем чи мереж з метою незаконного збирання інформації, що циркулює в них і становить комерційну або банківську таємницю, може бути вчинено лише фахівцем. У підозрюваного, за наявності достатніх підстав, проводиться обшук за місцем роботи і проживання. Під час обшуку звертають увагу на комп'ютери різних конфігурацій, принтери, засоби телекомунікації з комп'ютерними системами, записні книжки, у тому числі електронні, дискети, компакт-диски, флеш-накопичувачі, магнітні стрічки, що містять відомості про коди, паролі, ідентифікаційні номери користувачів конкретною комп'ютерною системою, а також дані про її користувачів.

Необхідно зауважити, що перед допитом свідків, підозрюваних з числа користувачів комп'ютерної системи, в якій циркулює комерційна або банківська таємниця, і сторонніх осіб, необхідно з'ясувати: вид перешкод, за яких обставин вони були виявлені, яка

інформація пошкоджена, а яка залишилася у незмінному вигляді. Необхідно також пам'ятати, що не завжди зміни комп'ютерної інформації є умисними. Нерідко їх причиною стає випадковий збій.

Під час проведення обшуку необхідно вилучати: 1) журнали обліку робочого часу і доступу до обчислювальної техніки, збоїв і ремонту, реєстрації користувачів комп'ютерною системою чи мережею; проведення регламентованих робіт; 2) книги паролів; 3) накази та інші документи, що регламентують роботу підприємства (установи, організації). Багато документів зберігаються в електронній формі і тому з метою їх пошуку та вилучення необхідно запрошувати фахівців.

У разі потреби доказування порушення підозрюваним (підозрюваними) правил експлуатації ЕОМ та їхніх систем, в яких циркулює інформація, що становить комерційну або банківську таємницю суб'єкта господарської діяльності, з метою виявлення криміналістично значущої доказової інформації необхідно проводити огляд робочих місць співробітників, допущених (а також, за умов необхідності, і не допущених) до роботи з комерційною або банківською таємницею; пошук та вилучення документів, що регулюють правила роботи користувачів комп'ютерної системи; допити свідків, насамперед усіх співробітників, що мають доступ до комп'ютерної системи. Огляд і вилучення документів треба проводити за участю фахівця; допит свідків бажано починати після вивчення документації, що регулює роботу комп'ютерної системи, в якій циркулює конфіденційна інформація. У кожного свідка з'ясовують такі обставини: а) які у нього обов'язки по роботі з комп'ютерною системою і взагалі на підприємстві (установі, організації); б) яку конкретну роботу на комп'ютері або іншому устаткуванні він виконує; в) яку роботу виконував свідок, коли відбувся збій, зміна, блокування комп'ютерної інформації; г) які правила роботи порушено; ґ) де і як повинні фіксуватися факти знищення, зміни, блокування інформації; д) чи пов'язані зміни, що відбулися у комп'ютерній мережі, з порушенням правил експлуатації.

Необхідно зазначити, що локальні комп'ютерні системи і комп'ютери окремих користувачів може бути об'єднано засобами електронного зв'язку і утворювати глобальні мережі типу Інтернет. На початковому етапі досудового розслідування незаконного збирання комерційної або банківської таємниці необхідно встановити, як влаштовано мережу, комп'ютерну систему, де відбулися перебої (зміни) та інші порушення, що потягли за собою матеріальні збитки; як вони об'єднані з найближчими робочими станціями. Порушення правил експлуатації може спричинити порушення, блокаду, перебої в конкретній комп'ютерній системі тощо.

У цьому разі, насамперед, необхідно визначити місця, де за схемою розгортання мережі розташовано робочі станції, які можуть бути дисковими і бездисковими. Можливими є порушення правил експлуатації обвинуваченим ЕОМ або їх мереж, копіювання файлового сервера на свою дискету, використання дискети з різними програмами, у тому числі з комп'ютерними вірусами тощо. Проте усі зазначені дії виключені на бездискових станціях. Тут як свідків можна допитати адміністратора мережі і фахівців, які обслуговують файловий сервер, в якому відбулися зміни, перебої, знищення конфіденційної інформації тощо.

Час порушення правил експлуатації обвинуваченим комп'ютерної системи чи мережі, в якій циркулює інформація, що становить комерційну таємницю підприємства, з метою збирання подібного роду відомостей встановлюють оглядом, допитом свідків, виїмкою і дослідженням документації, що регулює нормальну роботу мереж. Фіксують випадки відключення електромережі, коли можливе миттєве знищення введеної в комп'ютер інформації. Момент відключення збігається з моментом порушення правил експлуатації. Однак необхідно пам'ятати, що можливим є наявність розриву у часі між порушенням правил і моментом настання шкідливих наслідків [71, с. 559–562].

Підсумовуючи сказане, необхідно зауважити, що проведення вищезазначених слідчих (розшукових) дій з дотриманням

наукових рекомендацій і тактичних особливостей на наступному етапі розслідування незаконного збирання з метою використання відомостей, що становлять комерційну або банківську таємницю, сприятиме швидкому та повному розкриттю зазначених кримінальних правопорушень.

Аналізуючи обставини, що призводять до вчинення незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, а також розголошення комерційної або банківської таємниці як елемент у структурі окремої методики розслідування зазначеної категорії злочинів [71, с. 417], необхідно зазначити, що першорядною причиною вчинення подібного роду кримінальних правопорушень є суперечливість національного законодавства, яке регулює інститут комерційної та банківської таємниці, встановлює кримінальну відповідальність за незаконне збирання та розголошення такого роду відомостей. Стан законодавчої регламентації захисту від злочинних посягань у цій сфері, висока латентність такого виду злочинів, рідкі випадки звернення потерпілих до правоохоронних органів, складнощі збирання доказів та деякі інші причини, зокрема відсутність спеціалістів, які могли б успішно розслідувати подібні кримінальні правопорушення, кваліфікованих спеціалістів у галузі визначення певних відомостей як таких, що становлять комерційну таємницю, тощо, породжують існування мізерної кількості кримінальних проваджень, які розпочинаються за фактами вчинення таких злочинів і, тим більше, кримінальних проваджень цієї категорії, які доходять до суду [22, с. 304].

3.2. Використання спеціальних знань під час розслідування незаконного збирання або використання відомостей, що становлять комерційну або банківську таємницю

Сьогодні неможливо зустріти кримінальне правопорушення, під час розслідування якого в тій чи іншій формі не використовувалися б спеціальні знання. Аналіз слідчої практики засвідчує,

що під час розслідування незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, в більшості випадків численні питання також неможливо вирішити без застосування спеціальних знань, тобто залучення спеціалістів та експертів.

КПК України пов'язує використання спеціальних знань з розв'язанням питань, що виникають під час розслідування кримінальних проваджень і, передусім, під час проведення експертиз (ст. 242 КПК України). Водночас закон не визначає поняття спеціальних знань. В юридичній і науковій літературі зазвичай вважають, що це знання не загальновідомі, не загальнодоступні, не мають масового поширення, тобто знання, якими володіє обмежене коло спеціалістів.

Аналіз юридичної літератури засвідчує наявність значної кількості визначень поняття «спеціальні знання». Їх, зокрема, розуміють як: 1) знання, якими не володіє адресат доказування; 2) засновані на теорії й закріплені практикою глибокі й різнобічні знання прийомів і засобів криміналістичної техніки, що забезпечують виявлення, фіксацію й дослідження доказів; 3) сукупність відомостей, отриманих у результаті професійної підготовки, що створюють для їх власника можливість вирішення питань у певній галузі тощо.

Найбільш вдале, на нашу думку, визначення спеціальних знань було сформоване В. Г. Гончаренком, який під спеціальними знаннями у кримінально-процесуальному значенні пропонує розуміти знання в науці, техніці або мистецтві, застосовані для отримання доказової інформації спеціально підготовленими особами [6, с. 24].

Отже, спеціальні знання в кримінальному процесі варто розглядати як систему відомостей, отриманих в результаті наукової і практичної діяльності в певній галузі (медицині, бухгалтерії, мистецтві та ін.) і зафіксовані в науковій літературі, посібниках, інструкціях.

Проблема використання спеціальних знань в кримінальному процесі є досить гострою. Адже інтенсивне застосування для

вчинення кримінальних правопорушень сучасних технологій змушує практичних працівників все частіше звертатися до спеціалістів, використовувати нові форми їх залучення. Для кваліфікованого виконання своїх професійних функцій експертам і посадовим особам, що проводять експертизи, потрібно знати процесуальні основи судової експертизи, права і обов'язки експерта, повноваження органів, що призначають експертизу, та інші правові питання, що мають відношення до предмета експертизи. Своєю чергою особи, які призначають експертизу (слідчий, дізнавач, прокурор, суддя), повинні знати не лише процесуальний порядок її призначення, а й існуючі види судових експертиз, їх сучасні можливості, експертні установи, де проводяться експертизи, уміти грамотно формулювати питання експерту. Лише за таких умов можливо розраховувати на отримання від експертизи максимально повної інформації.

Тому, на нашу думку, під час досудового розслідування кримінальних проваджень використання спеціальних знань може відбуватися у таких формах: 1) застосування спеціальних знань безпосередньо слідчим, прокурором, слідчим суддею, судом, яким закон надає право збирати й оцінювати докази (ст. 93, ст. 94 КПК України);

2) використання спеціальних знань спеціаліста, який у кримінальному провадженні залучається під час проведення слідчих (розшукових) дій (ст. 71 КПК України);

3) використання спеціальних знань експерта, який залучається для проведення експертизи (дослідження) об'єктів, явищ і процесів, що містять відомості про обставини вчинення кримінального правопорушення, та надання висновку з питань, які виникають під час кримінального провадження і стосуються сфери його знань (ст. 69 КПК України).

Якщо говорити про залучення спеціалістів для викриття незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, а також розголошення комерційної або банківської таємниці, варто

зазначити, що при провадженні конкретних дій під час стадії досудового розслідування допомога таких суб'єктів є обов'язковою.

З криміналістичного погляду, спеціаліст – це незацікавлена особа, яка володіє спеціальними знаннями і навичками з метою надання допомоги слідчому (дізнавачу, прокурору, судді) у виявленні, дослідженні, фіксації і вилученні криміналістичної інформації. Узагальнення практики проведення слідчих (розшукових) дій дало можливість виокремити досить широкий перелік видів діяльності спеціалістів, що застосовується під час їх проведення. В узагальненому вигляді цей перелік може бути представлено так. Сприяючі слідчому під час проведення слідчих (розшукових) дій спеціалісти: 1) з дозволу і під наглядом слідчого особисто застосовують науково-технічні методи і засоби (ч. 2 ст. 71 КПК України); 2) допомагають застосуванню науково-технічних методів і засобів безпосередньо слідчим, консультуючи його, надаючи необхідні довідкові відомості, висловлюючи власну думку про можливі версії, ознаки предметів та осіб, перелік необхідних слідчих (розшукових) дій; 3) консультують та дають поради слідчому (дізнавачу) при підготовці до проведення слідчих (розшукових) дій (огляду, допиту, обшуку та ін.).

Особливістю використання допомоги спеціаліста при розслідуванні незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, є те, що такими фахівцями можуть виступати особи, які володіють різноманітними знаннями і навичками (криміналісти, фахівці з комп'ютерної техніки, фахівці зв'язку, хіміки та ін.).

Залучення спеціаліста під час розслідування незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, обумовлене вимогами кримінального процесуального законодавства, а також потребами слідчої практики.

У разі викрадення документів, у яких містяться такі відомості, до проведення слідчих (розшукових) дій, зокрема огляду

місця події, огляду конфіденційної документації, огляду сховища (сейфа), необхідним заходом є запрошення спеціалістів у галузі організації забезпечення захисту комерційної таємниці суб'єкта господарської діяльності, конфіденційного діловодства та інших спеціалістів підрозділів або відділів економічної безпеки суб'єктів господарської діяльності. Можливим є також використання спеціальних знань зазначених осіб без залучення їх до проведення слідчих (розшукових) дій, зокрема отримання консультацій у разі потреби.

У разі вчинення незаконного збирання з метою використання відомостей, що становлять комерційну або банківську таємницю суб'єкта господарської діяльності, шляхом перехоплення інформації, що циркулює у технічних засобах і приміщеннях, під час проведення огляду місця події, огляду відповідних технічних засобів, приміщень, необхідним є використання допомоги спеціалістів, зокрема електриків, фахівців у галузі кабельного господарства, зв'язківців, інженерів зв'язку, програмістів, фахівців із захисту інформації та інформаційних комп'ютерних систем, архітекторів, фахівців з організації функціонування димохідних каналів, інженерів з техніки безпеки на підприємстві, працівників охорони суб'єкта господарської діяльності та інших осіб. У деяких випадках, відповідно до зазначеного, доцільним є використання спеціальних знань даних осіб без залучення їх до проведення слідчих (розшукових) дій.

Участь спеціаліста під час проведення слідчих (розшукових) дій відображається у протоколі проведення слідчої (розшукової) дії, що додає авторитетності протоколу як джерелу доказів.

Говорячи про використання спеціальних знань обізнаних осіб, які залучаються в якості судових експертів під час розслідування незаконного збирання з метою використання та розголошення комерційної таємниці, необхідно зазначити, що судова експертиза є практичною діяльністю із застосування спеціальних наукових знань тієї чи іншої галузі в кримінальному процесі. Судова експертиза – це складна процесуальна дія, що полягає в

дослідженні об'єктів експертом з метою встановлення фактичних даних і обставин, які мають значення для правильного вирішення кримінального провадження. Наприклад, В. Г. Гончаренко дає таке визначення: «Проведення експертизи – це слідча дія, яка полягає у дослідженні експертом за дорученням слідчого (суду) речових доказів та інших матеріалів з метою встановлення фактичних даних і обставин, що мають значення для правильного вирішення справи» [15, с. 57].

Відповідно до Інструкції «Про призначення та проведення судових експертиз та експертних досліджень», затвердженої Наказом Міністерства юстиції України 08.10.1998 № 53/5, підставою для проведення експертизи є процесуальний документ про призначення експертизи, складений уповноваженою на те особою (органом), або договір з експертом чи експертною установою, укладений за письмовим зверненням особи у випадках, передбачених законом [66].

У разі вчинення незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, шляхом викрадення документів, в яких вона міститься, зазвичай, проводяться такі експертизи: 1) криміналістичні експертизи речових доказів: а) почеркознавча; б) лінгвістична; в) техніко-криміналістична експертиза документів; г) хімічна, фізико-хімічна, фізико-технічна; 2) технічні експертизи речових доказів: а) технічна експертиза транспортних та інших засобів доставки документів; б) технічна експертиза сховищ конфіденційних документів та ключів від них; в) технічна експертиза охоронної сигналізації приміщень, в яких зберігалися документи, що містять відомості, що становлять комерційну або банківську таємницю; 3) судово-медична (біологічна) експертиза речових доказів: а) експертне дослідження потожирових виділень, плям слини, сечі, поту, інших виділень; б) експертне дослідження волосся; в) експертне дослідження крові, частинок шкіри людини (які залишилися на гострих кромках сейфа тощо); 4) фоноскопічна експертиза речових доказів; 5) комплексна судово-медична і криміналістична експертизи тощо [54, с. 167].

Призначення експертизи передбачає знання слідчим (дізнавачем) її предмета, об'єктів і методики дослідження. Під час призначення експертизи слідчий (дізнавач) повинен чітко усвідомлювати, які саме спеціальні знання необхідні для проведення конкретного дослідження, спеціалісту в якій галузі (або якої установи) необхідно доручити виконання потрібної експертизи. Ці знання, а також правильно сформульовані питання, сприятимуть швидкому і ефективному отриманню доказів, що мають принципове значення для кримінального провадження.

Характеризуючи почеркознавчу експертизу, необхідно зазначити, що під час розслідування незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, основними завданням її є ідентифікація виконавця підпису (у деяких випадках – рукописного тексту або цифрового запису).

Залежно від класу вирішуваних завдань почеркознавчі дослідження можуть бути ідентифікаційними, класифікаційними та діагностичними [15, с. 71].

З метою вирішення завдань ідентифікаційного характеру перед експертом ставляться такі питання: 1) Ким із зазначених осіб виконано підпис, рукописний текст (його частину), цифровий запис? 2) Чи виконано підпис (текст, фрагмент тексту, цифровий запис) конкретною особою (підозрюваним, обвинуваченим)? 3) Чи виконано підпис від імені певної особи конкретною особою (підозрюваним, обвинуваченим) або іншою певною особою? 4) Чи виконано текст документа і підпис у ньому однією особою (підозрюваним, обвинуваченим, іншою особою)? 5) Інші питання.

Необхідно зазначити, що іноді під час розслідування злочинів у сфері комерційної або банківської таємниці може виникнути необхідність у проведенні почеркознавчої експертизи з метою вирішення завдань діагностичного характеру з постановкою перед експертом таких питань: 1) Чи придатний певний текст, підпис для дослідження з метою ідентифікації особи виконавця? 2) Чи виконано рукопис навмисно зміненим почерком (скоропис-ним,

друкованим, незвичною рукою)? 3) Чи виконано підпис із зміною його ознак? 4) Чи виконано підпис (текст) з наслідуванням почерку (підпису) певної особи? 5) Чи не виконано підпис (рукопис) у незвичних умовах (відсутність або обмеження зорового контролю, незвична поза, незвичне тримання приладу для писання, температура навантаження тощо)? 6) Чи не перебувала особа, яка виконала підпис (рукопис) (підозрюваний, обвинувачений, відповідальна за документ, в якому містяться відомості, що становлять комерційну таємницю підприємства, особа), у незвичайному стані (захворювання, травми, стомлення, хвилювання, алкогольного або наркотичного сп'яніння, під дією фармакологічних препаратів збуджуючої дії тощо)? 7) Інші питання [15, с. 74].

Лінгвістична експертиза (синонім – «авторознавча експертиза») визначає фактичні дані про особу автора (чи виконавця) тексту та про умови створення мовного повідомлення (мотивацію, цілі, настанову автора, збиваючий фактор, викривлення відбитої у свідомості інформації, адаптацію мовних засобів до можливостей адресата, маскування мовної ситуації шляхом диктування, навмисного викривлення писемного мовлення, створення тексту у співавторстві тощо) [15, с. 75].

Характеризуючи лінгвістичну експертизу під час розслідування незаконного збирання та розголошення комерційної або банківської таємниці, необхідно зауважити, що у межах ідентифікаційних задач може бути встановлено авторство тексту відносно конкретної людини, зокрема відповідальної за документ особи, викрадача документа, заступника керівника суб'єкта господарської діяльності з питань інформаційної безпеки та інших осіб. Водночас експерту ставляться такі питання: 1) Чи є автором тексту, що починається та закінчується відповідними словами (надається конкретний опис), певна особа? 2) Однією чи різними особами складено тексти? 3) Інші питання.

У межах класифікаційних задач лінгвістичної експертизи може бути встановлено: стать, соціальний стан (чи є автор керівником, виконавцем, керівником у минулому тощо), професійну

належність (у тому числі конкретні професійні навички), вік, рівень освіти, рідна чи основна мови спілкування, місця формування мовних навичок або визначення діалекту тощо. За потреби вирішення класифікаційних задач експерту ставиться завдання: 1) описати соціально-демографічний портрет автора тексту; 2) визначити, чи не є автором тексту працівник підрозділу конфіденційного діловодства суб'єкта господарської діяльності, працівник правоохоронних органів.

Типовими питаннями для експерта у разі наявності необхідності вирішення діагностичних задач під час розслідування незаконного збирання та розголошення комерційної таємниці є такі: 1) Чи спостерігаються в тексті ознаки створення його автором у незвичному психофізіологічному стані, що міг бути спричинений загрозою життю, здоров'ю зазначеному автору (відповідальній за документ особі, керівнику відділу конфіденційної документації суб'єкта господарської діяльності, іншим особам) або його близькому оточенню? 2) Чи не перебував автор (виконавець) у незвичному психофізіологічному стані під час створення (виконання) тексту? 3) Інші питання [15, с. 78].

У рамках відтворення мовленнєвої ситуації сучасна лінгвістична експертиза може вирішувати такі питання: 1) Чи не створено текст з навмисним викривленням писемного мовлення? 2) Чи не виконано текст під диктовку? 3) Чи не створено текст у співавторстві? 4) Інші питання [15, с. 78].

Технічна експертиза документів (ТЕД), при розслідуванні незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, вирішує питання, пов'язані з дослідженням матеріалів документів, технічних прийомів та способів їх виготовлення, а також внесення в них змін [15, с. 79].

Під час розслідування кримінальних правопорушень у сфері комерційної або банківської таємниці може виникнути необхідність визначення способів зміни рукописних реквізитів документів, в яких містяться відомості, що становлять комерційну

або банківську таємницю, облікових документів відділів конфіденційної документації суб'єктів господарської діяльності тощо. У цьому разі технічна експертиза розв'язує такі питання: 1) Чи не піддавався запис у документі змінам шляхом підчищення (дописки, домальовування) штрихів? 2) Чи не піддавався запис зміні шляхом витравлювання? 3) Чи не дописано літеру (цифру, слово, частину тексту) в конкретному місці досліджуваного документа? 4) Чи не додруковано фрагмент тексту до основного тексту документа? 5) Чи не нанесено підпис з попередньою технічною підготовкою (олівцем, копіюванням, перетискуванням тощо)? [15, с. 85].

У разі необхідності встановлення часу виготовлення документів перед експертом ставляться такі питання: 1) Що було виконано раніше: підпис чи текст, відтиск печатки (штампа) чи підпис, текст чи відтиск печатки (штампа)? 2) Чи не замінялися аркуші в наданому на дослідження документі? 3) Чи відповідає час виготовлення документа даті, яка вказана в ньому, або він виготовлений пізніше? 4) Інші питання [54, с. 170].

Під час дослідження ознак матеріалів і технічних засобів, за допомогою яких було виготовлено досліджувані документи, експерт вирішує такі питання: 1) Однаковим чи різним є папір, на якому виготовлено досліджувані документи (бланки, записи)? 2) У який спосіб та якою барвною речовиною виконано текст (запис) документа (фрагменти) (чорнилом, пастою, олівцем, через копіювальний папір, стрічку друкарської машини, тонером або чорнилом принтера персонального комп'ютера, за допомогою копіювально-множильного апарата)? 3) На однаковому за видом друкуючому пристрої (друкарській машині, принтері) чи на різних виконано текст документа (на всіх аркушах документа)? 4) Інші питання [15, с. 95].

Перед призначенням технічної експертизи документів слідчому необхідно підготувати матеріали (як матеріали кримінального провадження, так і речові докази), правильно зібрати порівняльний матеріал та визначити задачі, які вирішуватиме експерт.

У процесі здійснення слідчого огляду документів нерідко виявляються підроблені документи і документи, в які внесено зміни. При огляді документів необхідно дотримуватися визначених правил поводження з ними. Брати документи треба чистими руками або пінцетом. Це необхідно для того, щоб не забруднити документи і не пошкодити відбитки пальців, що можуть бути залишені на них виконавцями. Документи необхідно оберігати від впливу світла, вологи, високої температури. На них не можна робити будь-які позначки, обведення, підкреслення. Над документами не треба проводити експерименти (роз'єднувати, склеювати їх, виправляти та вирівнювати, піддавати впливу хімічних реактивів тощо). Документи, що підлягають експертному дослідженню, варто зберігати в окремих конвертах, а не підшивати в матеріали справи. Складати і перегинати документи треба тільки за наявними на них складками [15, с. 98].

Головною задачею експертного дослідження в галузі трасології є встановлення або констатація віднесення до певної групи конкретних слідів на основі їх відображення на матеріальному носії; визначення стану об'єкту; визначення способів утворення слідів тощо.

Трасологічною експертизою можна також установлювати факти, які належать до просторових, функціональних, структурних, динамічних і деяких інших характеристик процесу слідоутворення, а також особливостей слідоутворювальних об'єктів [66].

Для вирішення дактилоскопічної експертизи під час розслідування незаконного збирання з метою використання відомостей, що становлять комерційну або банківську таємницю суб'єкта господарської діяльності, вчиненого, зокрема, шляхом викрадення документів, в яких такі відомості містяться, шляхом перехоплення інформації, що становить комерційну таємницю і циркулює у технічних засобах і приміщеннях, шляхом перехоплення усної інформації, а також розголошення комерційної або банківської таємниці, може бути поставлено такі питання: 1) Чи є на предметах, вилучених на місці події, сліди рук? 2) Чи придатні ці сліди для

ідентифікації особи? 3) Якою рукою і якими пальцями залишено сліди? 4) Якими ділянками долонної поверхні залишено сліди? 5) У результаті якої дії (торкання, захоплення тощо) залишено сліди рук? 6) Чи відобразилися в слідах особливості рук особи, яка залишила сліди (відсутність пальців, наявність шрамів тощо), і які саме? 7) Який приблизний зріст особи, котра залишила сліди рук на місці події? 9) Протягом якого часу могли зберігатися сліди на даному об'єкті в конкретних умовах місця події? 10) У якій послідовності утворено сліди рук, виявлені на місці події? 11) Чи залишено сліди рук, вилучені в різних місцях, однією особою? 12) Чи залишено сліди рук, вилучені на місці події, даною особою (відповідальною за документ особою, керівником, конкретним працівником підрозділу економічної безпеки підприємства, відділу конфіденційної документації, іншими працівниками, підозрюваним, потерпілим)? [15, с. 105].

Під час розслідування незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, може виникнути необхідність у призначенні трасологічної експертизи слідів ніг людини та взуття. Для вирішення перед експертом може бути поставлено такі питання: 1) Чи є на цій поверхні (цьому предметі) сліди босих ніг (панчіх, шкарпеток, взуття) людини та чи придатні ці сліди для ідентифікації людини (панчіх, шкарпеток, взуття)? 2) Чи залишено сліди даною особою, чи це сліди від шкарпеток, панчіх чи взуття, вилучених у певної особи? 3) Чи залишено сліди ніг (шкарпеток, панчіх, взуття), виявлені в різних місцях, однією особою (сліди тих самих шкарпеток, панчіх, взуття)? 4) Взуттям якого виду залишено дані сліди і які його характеристики і особливі ознаки (розмір, ступінь зношування тощо)? 5) Який орієнтовно зріст людини, яка залишила сліди? 6) Який механізм утворення слідів взуття? 7) Інші питання [66].

Під час вчинення незаконного збирання та розголошення комерційної або банківської таємниці досить часто є характерним утворення слідів знарядь та інструментів, які виникають

внаслідок подолання різного роду перешкод з метою проникнення в приміщення, де зберігаються документи, в яких містяться відомості, що становлять комерційну або банківську таємницю або циркулює і обробляється подібного роду інформація, зокрема, на сейфах, металевих шафах, замках, дверях і вікнах, стінах, стелях, підлогах тощо.

У цьому разі для з'ясування трасологічною експертизою слідів злому, інструментів перед експертом можуть ставитися такі питання: 1) Чи є на предметах речової обстановки місця події (двері, вікна тощо) сліди знарядь злому? 2) У результаті яких дій (розріз, розруб, розпил, свердління) утворилися ці сліди? 3) З якого боку (із зовнішнього чи внутрішнього) зроблено злом (руйнування) перешкоди? 4) Яка послідовність утворення слідів? 5) Якими знаряддями й інструментами утворено сліди злому? 6) Чи відобразилися в слідах характерні ознаки цих знарядь та інструментів (дефекти, сліди обробки тощо)? 7) Які особливості способу злому? 8) Які сліди (частки речовин) могли утворитися на застосованих для злому знаряддях та інструментах при здійсненні злому? 9) Які сліди (частки речовин) могли утворитися на тілі й одязі особи при здійсненні злому? 10) Чи залишено сліди, виявлені на місці події, знаряддям (інструментом), вилученим у підозрюваного? 11) Інші питання [15, с. 112].

Під час розслідування незаконного збирання та розголошення комерційної таємниці досить часто виникає необхідність у призначенні і проведенні експертизи комп'ютерної техніки і програмних продуктів.

Сьогодні за допомогою таких експертиз можуть вирішуватися такі завдання: 1) установлення робочого стану комп'ютерно-технічних засобів; 2) установлення обставин, пов'язаних з використанням комп'ютерно-технічних засобів, інформації та програмного забезпечення; 3) виявлення інформації та програмного забезпечення, що містяться на комп'ютерних носіях; 4) установлення відповідності програмних продуктів певним версіям чи вимогам на його розробку.

Під час експертизи може бути поставлено такі питання: 1) Комп'ютер якої моделі надано на дослідження? Якими є технічні характеристики його системного блока і периферійних пристроїв? 2) Які технічні несправності має даний комп'ютер або його окремі блоки та пристрої, і як ці несправності впливають на роботу комп'ютера (блока, пристрою)? 3) Чи міститься на даному носії якась інформація, і якщо так, яке її цільове призначення? 4) Коли і ким були створено досліджувані файли? 5) У який період часу створено файли та яка дата останнього редагування? 6) Чи не вносились у програми даного системного продукту які-небудь корективи, що змінювали виконання певних операцій? 7) Чи містилася на носії інформація, яку було знищено, якщо так, то яка саме? 8) З якого з наданих комп'ютерів здійснювався вихід у мережу Інтернет, за якими адресами, в який період часу? 9) Яким є механізм утрати інформації з локальних обчислювальних мереж і розподілених баз даних? 10) Чи можна за допомогою даного програмного продукту реалізувати функції, передбачені технічним завданням на його розробку? 11) Чи містяться на досліджуваному комп'ютері програмні продукти, які можуть використовуватися для злому пароля та несанкціонованого доступу до комп'ютерних мереж? 12) Чи можливе вирішення певного завдання за допомогою даного програмного продукту? 13) Яким є рівень професійної підготовки в галузі програмування і роботи з комп'ютерною технікою особи, яка виконала дані дії з комп'ютером і програмним забезпеченням? 14) Інші питання [15, с. 164].

Крім перерахованих видів експертиз, у кримінальних провадженнях про незаконне збирання з метою використання або розголошення відомостей, що становлять комерційну або банківську таємницю, можуть призначатися та проводитися експертизи та дослідження, пов'язані з комерційною таємницею та ноу-хау, а також дослідження, пов'язані з раціоналізаторськими пропозиціями.

Якщо визначати об'єкт експертного дослідження щодо комерційної таємниці, то це є інформаційні ресурси, що вивчаються працівником експертної установи, який володіє спеціальними знаннями,

які становлять таємницю комерційного характеру, інформаційний ресурс у сфері технологій, комерції, виробництва тощо.

Перед експертом для дослідження може бути поставлено такі питання: 1) Чи можна інформацію (вказати, яка інформація) віднести до комерційної таємниці? 2) Чи має інформація (вказати яка) ознаки ноу-хау? 3) Чи набута інформація (вказати яка), що використовується (юридичною особою або особою-підприємцем), шляхом вивчення відкритих даних, які містяться у відомостях (указати джерела інформації)? 4) Чи набута інформація (вказати яка) реінжинірингом зразків продукції (указати або надати зразки продукції)? 5) Чи міститься у відомостях, наданих (указати ким) даних, що інформацію (вказати яка) було отримано в результаті власних розробок або досліджень (указати яких саме)? Цей перелік питань не є вичерпним, експертизою можуть вирішуватись і інші питання, необхідність у яких може виникнути під час досудового розслідування кримінальних правопорушень у сфері комерційної або банківської таємниці [26].

Основна кількість експертиз (досліджень) під час розслідування кримінальних проваджень про незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, проводиться експертами науково-дослідних установ судових експертиз Міністерства юстиції України: Дніпропетровського науково-дослідного інституту судових експертиз; Донецького науково-дослідного інституту судових експертиз; Київського науково-дослідного інституту судових експертиз; Львівського науково-дослідного інституту судових експертиз; Одеського науково-дослідного інституту судових експертиз; Харківського науково-дослідного інституту судових експертиз імені заслуженого професора М. С. Бокаріуса; Науково-дослідного центру судової експертизи з питань інтелектуальної власності. Крім того, експертизи та дослідження проводяться у відповідних лабораторіях ДНДКЦ МВС України. Існує 24 територіальні підрозділи НДЕКЦ. В структурі ДНДКЦ МВС України є Відділ мистецтвознавчих, психологічних досліджень та досліджень об'єктів інтелектуальної власності [16].

Якщо провести характеристику експертних досліджень технологій, за допомогою яких відбувається таємне вилучення інформаційних ресурсів, що здійснюється на стадії досудового розслідування у кримінальних провадженнях досліджуваної категорії, варто зазначити, що якщо ці технології не мають чіткого спрямованого спектру дії, вилучені у конкретній справі, їх необхідно дослідити щодо їх належності до технологій спеціального призначення вилучення інформаційних ресурсів, та встановити їх тактичні та технічні здатності. Такі експертизи та дослідження проводить Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України.

Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України (далі – Інститут) є державною спеціалізованою експертною, науково-дослідною установою, яка здійснює наукову, науково-технічну, науково-організаційну, судово-експертну діяльність, виконує функції експертної служби СБУ, забезпечує виготовлення спеціальних технічних засобів для негласного отримання інформації, іншої спеціальної техніки та бере участь у їх впровадженні [75].

Основними напрямами діяльності Інституту у зазначеній сфері є: 1) дослідження СТЗ негласного отримання інформації про місцезнаходження та/або переміщення особи, транспортних засобів чи іншого володіння особи, зокрема для негласного установлення місцезнаходження радіоелектронного засобу зв'язку; 2) дослідження СТЗ негласного проникнення на об'єкт (публічно недоступні місця, житло чи інше володіння особи) шляхом відмикання (вимкнення та вмикання) електронних засобів його охорони; 3) дослідження СТЗ негласного зняття інформації з телекомунікаційних мереж; 4) дослідження СТЗ негласного зняття інформації з електронних інформаційних систем; 5) дослідження програмних засобів негласного отримання інформації.

Порядок призначення та проведення судових експертиз та експертних досліджень Інститутом визначено Інструкцією про призначення та проведення судових експертиз та експертних

досліджень в системі Служби безпеки України, затвердженою наказом Центрального управління СБУ від 29.05.2015 № 371, зареєстрований в Міністерстві юстиції України 22.06.2015 за № 738/27183 [75].

Експертна практика дозволяє визначити коло питань, які слідчий (суд) ставить перед експертом, та виділити серед них такі групи: 1) питання щодо призначення технічного засобу: а) Що являє собою вилучений пристрій? б) Чи можна за його допомогою здійснювати негласне зняття інформації і якої саме (акустичної, візуально-оптичної, з радіоефіру, з каналів зв'язку тощо)? 2) питання щодо роботоспроможності технічного засобу: а) Чи перебуває вилучений пристрій в робочому стані? б) Чи підлягає неробочий пристрій відновленню? 3) питання щодо визначення тактико-технічних характеристик засобу: а) Яким є час безперервної роботи пристрою ? б) З якої відстані пристрій може знімати інформацію? в) На яку відстань пристрій може передавати отриману інформацію і яким каналом (провідником, радіохвильовим, інфрачервоним, ультразвуковим тощо)? г) Чи може пристрій фіксувати отриману інформацію і на який тип носія (аудіо-, відеокасету, оптичний або магнітооптичний диск, дискету, мікросхему тощо)? ґ) Чи можливе дистанційне керування роботою пристрою? 4) питання щодо використання технічного засобу: а) Чи здійснено аудіозапис (відеозапис) на носіях (аудіо-, відеокасетах тощо), вилучених по кримінальному провадженню, за допомогою вказаного пристрою? 5) Інші питання.

Підсумовуючи сказане, необхідно зазначити, що використання спеціальних знань та, зокрема призначення і проведення експертиз, під час розслідування незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, а також розголошення комерційної таємниці, є необхідним та обов'язковим, забезпечує отримання криміналістично значущої доказової інформації під час розслідування і сприяє швидкому і повному розкриттю та розслідуванню даної категорії кримінальних правопорушень.

3.3. Тактичні операції під час розслідування незаконного збирання або використання відомостей, що становлять комерційну або банківську таємницю

Пошук і постійне удосконалення криміналістичною наукою окремих методик розслідування кримінальних правопорушень привели науку і практику до ідеї комплексного вирішення конкретних завдань розслідування у формі тактичних операцій.

Термін «операція» увійшов у лексикон криміналістів із військової термінології і на початку використовувався в криміналістиці у зв'язку із розробкою і вирішенням розшукових завдань. Поступово сфера його застосування поширилась на систему дій, пов'язаних із затриманням злочинця, його викриттям, розшуком викрадених речей та документів та ін.

Процес розслідування кримінальних правопорушень, пов'язаних із посяганням на відомості, що становлять комерційну або банківську таємницю, характеризується підвищеною складністю, обумовленою механізмом злочинної діяльності, значним обсягом роботи, кваліфікованою протидією досудовому розслідуванню та іншими подібними чинниками. Тому вирішення тактичних завдань досудового розслідування таких кримінальних правопорушень зазвичай потребує узгодженого, комплексного проведення слідчих (розшукових) дій, організаційних та інших заходів. Така форма вирішення тактичних завдань досудового розслідування злочинів у криміналістиці отримала назву тактичної операції [55, с. 163].

Удосконалення процесу розкриття і розслідування злочинів залежить від рівня запровадження у слідчу діяльність новітніх криміналістичних розробок, що базуються на синтезі теоретичних знань і передової судово-слідчої практики. Йдеться, насамперед, про такі категорії, як криміналістична характеристика та класифікація злочинів, типові слідчі ситуації, криміналістичні комплекси процесуальних дій у вигляді тактичних комбінацій та операцій. Саме ці категорії істотно впливають на формування сучасних концепцій криміналістичних методик розслідування

злочинів, є їх невід'ємними складовими, й обумовлюють ефективність конкретного акту розслідування [17, с. 30–36].

Традиційним елементом структури окремої криміналістичної методики завжди вважалася система слідчих (розшукових) дій [30, с. 155–160].

Узгоджена сукупність (система) слідчих (розшукових) дій є найбільш дійовим засобом перевірки висунутих версій, впливу на слідчі ситуації, що виникають. Водночас разом із системами слідчих дій у криміналістиці має місце ще одна відносно нова категорія, яка одержала назву «тактична операція». Засновники концепції тактичної операції виходили з того, що вона є: 1) сукупністю тактичних засобів реалізації методів розслідування; 2) засобом реалізації взаємодії слідчого з органами дізнання, державними установами й організаціями, окремими громадянами, необхідність у чому виникає під час вирішення завдань розслідування; 3) організаційним і тактичним засобом ліквідації протидії з боку правопорушника; 4) засобом алгоритмізації процесу розслідування злочинів; 5) засобом реалізації тактичних прийомів, що вимагають сукупності дій слідчого та представників інших органів.

Поява в криміналістиці категорії «тактична операція» викликана, передусім, потребами практики щодо необхідності комплексного провадження слідчих, оперативно-розшукових, ревізійних та інших дій з метою вирішення таких завдань, розв'язання яких іншими, не сукупними засобами, просто неможливе. Саме ці чинники стимулювали науковців до розроблення концепції тактичних операцій і запровадження її положень у практику розслідування злочинів [17, с. 30–36].

Пошук та постійне вдосконалення криміналістичною наукою окремих методик розслідування кримінальних правопорушень, розробка більш ефективних форм організації взаємодії органів досудового розслідування останніми роками цілком закономірно привели науку і практику до ідеї комплексного розв'язання конкретних завдань розслідування у формі тактичних операцій.

Розроблення концепції тактичних операцій як важливого елемента в системі організаційно-тактичних засобів слідчого знаходиться на новому етапі свого розвитку і, безперечно, потребує проведення подальших досліджень [79, с. 110–116].

Для отримання повного уявлення про характеристику тактичної операції як системи необхідно визначити її структуру. Що стосується структури тактичної операції, то вона містить в собі такі елементи: а) мету; б) суб'єкти; в) об'єкт; г) умови; ґ) засоби та способи досягнення мети [54, с. 182].

До принципів проведення тактичної операції належать: а) принцип законності; б) плановість; в) принцип наступальності; г) принцип оптимальності; ґ) принцип конспірації; д) принцип документальної фіксації тощо.

Говорячи про класифікації тактичних операцій, можна стверджувати, що вони можуть бути проведені на підставі різних критеріїв. Зокрема, за змістом вони поділяються на: а) неоднорідні тактичні операції, які мають у своєму складі слідчі (розшукові) дії, оперативно-розшукові заходи та інші дії; б) однорідні тактичні операції, які складаються з однієї слідчої (розшукової) дії, але виконуваної за допомогою декількох взаємопов'язаних тактичних прийомів, або такі, що складаються лише із слідчих (розшукових) дій або лише оперативно-розшукових заходів.

Враховуючи позицію В. А. Журавля, відповідно до якої тактичні операції повинні розроблятись у контексті формування відповідної видової або підвидової методики (мікрометодики), тобто вони мають бути їх невід'ємною складовою, а також повинні бути максимально «прив'язані» до типових слідчих ситуацій і виходити із конкретних тактичних завдань, що стоять перед слідчим [17, с. 30–36], необхідно зазначити, що під час розслідування злочинів у сфері комерційної або банківської таємниці тактичні операції повинні здійснюватися з метою вирішення тактичних завдань, які виникають під час розкриття незаконного збирання з метою використання відомостей, що становлять комерційну або банківську таємницю суб'єкта господарської діяльності, вчиненого шляхом:

1) викрадення документів, у яких відповідні відомості містяться; 2) перехоплення інформації, що циркулює в технічних засобах і приміщеннях; 3) перехоплення усної інформації – та розголошення комерційної або банківської таємниці, здійсненого усно, письмово, за допомогою жестів, міміки, умовних сигналів, особисто, через посередників, по каналах зв'язку, через друковані чи інші засоби масової інформації, через комп'ютерні мережі шляхом повідомлення вказаних відомостей іншим особам, надання іншим особам для ознайомлення документів, що містять комерційну таємницю, залишення документів на робочому місці для того, щоб стороння особа, яка знаходиться у приміщенні, мала можливість ознайомитися, коли винна особа, під якимось приводом, виходить з приміщення на певний час тощо: 1) «ображеним» співробітником (або співробітниками); 2) співробітником (співробітниками) суб'єктів господарської діяльності; 3) відвідувачами, які не є співробітниками суб'єкта господарської діяльності, але внаслідок певних обставин ознайомлені з відомостями, що становлять комерційну таємницю; 4) агентом (агентами) вітчизняних та іноземних суб'єктів господарської діяльності, які діють за завданням конкурентів; 5) агентом (агентами) спецслужб, «підісланими» на фірму у якості співробітника; 6) контрагентом (контрагентами), представником (представниками) інших суб'єктів господарської діяльності, які ознайомлені з відомостями, що становлять комерційну або банківську таємницю суб'єкта господарської діяльності, внаслідок існування договірних відносин між компаніями; 7) представником (представниками) правоохоронних органів державних структур та іншими суб'єктами.

Необхідно зазначити, що під час розслідування незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, а також розголошення комерційної або банківської таємниці для вирішення тактичних (проміжних) завдань, проводяться такі тактичні операції: 1) збирання і фіксація вихідної інформації про факт злочину; 2) пошук особи, яка вчинила кримінальне

правопорушення; 3) виявлення осередків злочину і використання даних про них з метою пошуку особи, яка вчинила злочин; 4) затримання злочинця з речовими доказами; 5) викриття особи, яка вчинила злочин; 6) способи встановлення вчинення декількох нерозкритих злочинів одним і тим самим злочинцем; 7) нейтралізація протидії підозрюваного у вчиненні злочину; 8) доказування функціональних ролей учасників злочинної групи; 9) встановлення алібі; 10) інші тактичні операції, характер яких визначається конкретними слідчими ситуаціями та відповідними завданнями, які виникають у процесі розслідування кримінальних правопорушень даного виду.

На наш погляд, доцільно зупинитися на загальних положеннях проведення, процесуальних і тактичних особливостях деяких з них.

Характеризуючи особливості проведення тактичної операції «Збирання і фіксація вихідної інформації про факт злочину», необхідно зауважити, що початковий етап розслідування незаконного збирання та розголошення комерційної або банківської таємниці, зазвичай, позначений гострим дефіцитом інформації про деякі важливі елементи криміналістичної характеристики даних злочинів, і саме за допомогою даної тактичної операції виявляється інформаційна сутність, інформативність конкретної слідчої ситуації.

Призначення тактичної операції «Збирання і фіксація вихідної інформації про факт злочину» є забезпеченням спрямованої уваги та дій слідчого на збирання інформації про елементарні структури злочину та розробка для досягнення цієї мети оптимальних засобів та умов. Зазначена тактична операція є базисом для проведення інших тактичних операцій. Збирання відомостей забезпечує підготовку інших операцій, наприклад, «Пошук та викриття злочинця» та інших. При цьому варто зазначити, що в системі кримінального процесуального доказування кожна тактична операція виступає в якості свого роду модуля і являє собою однотипну задачу зі специфічним набором засобів, логічних прийомів тощо, незалежно від характеру справи [54, с. 185].

Під час проведення цієї тактичної операції різні відомості накопичуються за певною схемою, у якій має бути враховано джерела інформації, способи її виявлення та обробка з метою «перетворення» інформації у докази у кримінальному провадженні. Виявлена, відповідно оброблена інформація групується, узагальнюється та аналізується.

Основними етапами проведення тактичної операції «Збирання і фіксація вихідної інформації про факт кримінального правопорушення» є такі: 1) підготовчий, на якому виявляється та аналізується інформація, яка міститься у повідомленні про незаконне збирання або розголошення комерційної або банківської таємниці та приймається на її основі рішення щодо організації перевірки цього повідомлення; на цьому етапі створюється слідчо-оперативна група і повідомляється завдання її майбутньої діяльності, сутність функцій, а також передається інформація, яка є необхідною для її проведення. Крім того, на цьому етапі визначаються всі можливі варіанти операції, необхідні тактичні засоби та умови; 2) робочий або етап безпосереднього проведення системи заходів під час проведення названої тактичної операції; під час цього етапу учасники слідчо-оперативної групи відповідними методами та з використанням необхідних прийомів і засобів збирають інформацію про кожний елемент криміналістичної структури вчиненого злочину; 3) заключний, під час якого виявлена необхідним чином інформація закріплюється у процесуальних та інших документах; з цим же етапом пов'язано і початкову оцінку зібраної інформації.

Первинна інформація про незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю суб'єкта господарської діяльності, а також про розголошення комерційної або банківської таємниці суб'єкта господарювання надходить, як було зазначено, від представників суб'єктів господарювання – керівників підприємств, установ, організацій, представників служб або підрозділів безпеки юридичних осіб, фізичних осіб-підприємців, членів

експертних комісій із захисту комерційної таємниці суб'єктів господарювання, зокрема, керівників і спеціалістів структурних підрозділів юридичної особи та інших осіб. Вказані особи, зазвичай, повідомляють про ознаки вчинення кримінального правопорушення у сфері комерційної таємниці, якими, зокрема, є: 1) відсутність документа, який містить відомості, що становлять комерційну або банківську таємницю, за місцем зберігання після проведення відомчих заходів щодо його пошуку і виключення можливості або факту виходу його з володіння відповідальної особи внаслідок необережності та інших подібних обставин, у разі настання яких не буде застосовуватися кримінальна відповідальність; 2) відсутність документа по закінченні маршруту його доставки; 3) виявлення документа поза місцем його зберігання; 4) факт отримання відомостей, що становлять комерційну або банківську таємницю суб'єкта господарської діяльності, сторонньою особою (організацією); 5) виявлення в технічних засобах і приміщеннях електронного пристрою перехоплення інформації, запровадженого за невстановлених обставин; 6) наявність у публікаціях, рекламі, виставочних матеріалах фірм-конкурентів інформації, що становить комерційну або банківську таємницю суб'єкта господарської діяльності тощо.

Важливою умовою успіху у проведенні тактичної операції «Збирання і фіксація вихідної інформації про факт злочину» є своєчасне прибуття слідчо-оперативної групи, до складу якої мають входити слідчий (дізнавач) – керівник групи, працівник оперативного підрозділу, інспектор-криміналіст (технік-криміналіст), а також (за необхідності) кінолог зі службовим собакою, за необхідності – інженер зі спецтехніки, фахівець із зв'язку та інші особи, на місце події. «Своєчасним прибуттям» називаємо прибуття їх в умови, можливі для проведення пошуку злочинців по «гарячих слідах», з максимальним залишенням слідових відображень порушниками закону. Як наслідок, – велика оперативність групи швидкого реагування, наділення її новітніми досягненнями науки і техніки роботи зі слідовими відображеннями та

доказовою інформацією, відображеною на матеріальних носіях, можливості проведення експрес-аналізу на місці події.

З метою збору первинної інформації доцільним є проведення таких слідчих (розшукових) дій та інших заходів: 1) а) огляду приміщення (місця) зберігання документа; б) огляду сейфа (іншого сховища), в якому зберігався документ; в) огляду місця, відведеного для знищення документів; г) огляду облікової документації; ґ) огляду засобів доставки документа; д) огляду документа, який є аналогічним втраченому; е) огляду місця виявлення документа; є) огляду пакувального матеріалу; ж) огляду документа або його частини; з) огляду транспортного засобу; и) огляду приміщення, в якому оброблюється конфіденційна інформація, зокрема, конструкцій приміщення і будівель (стіни, стеля, підлога, вікна, двері), меблів і предметів інтер'єру; і) огляду технічних засобів і систем обробки і передачі інформації, зокрема, засобів обчислювальної техніки, засобів зв'язку і передачі даних обчислювальної техніки, засобів телефонного зв'язку, звукозапису, звукопідсилення, звуковідтворення, переговорних і телевізійних пристроїв, засобів виготовлення, тиражування документів та інших технічних засобів обробки інформації; ї) огляду інших технічних пристроїв, розміщених у приміщеннях, де оброблюється конфіденційна інформація, зокрема, телефонних засобів і систем, засобів радіозв'язку, засобів охоронної і пожежної сигналізації, засобів оповіщення і сигналізації, контрольно-вимірювальної апаратури, засобів і систем кондиціювання, засобів провідної радіотрансляційної мережі, засобів електронної оргтехніки, електронних годинників тощо; й) огляду документів, які регламентують організацію захисту інформації, зокрема, паспорта захищеного приміщення, плану охоронюваної зони організації, схеми прокладки ліній передачі даних, схеми і характеристики систем електроживлення і заземлення об'єкта інформатизації; к) огляду спеціальних електронних пристроїв перехоплення інформації («закладок»); л) огляду технічного засобу з інформацією, що в ньому зберігається, або окремого носія інформації; м) огляду сейфа, в якому

зберігався викрадений носій інформації; н) огляду карток обізнаності співробітників про комерційну або банківську таємницю суб'єкта господарської діяльності, з метою виявлення кола співробітників, які могли володіти розголошеною інформацією тощо; 2) а) допиту особи, відповідальної за документ; б) допиту осіб, які виявили відсутність документа; в) допиту осіб, у яких виявили документ; г) допиту осіб, які виявили документ; ґ) допиту свідків; д) допиту осіб, допущених до сфери конфіденційного діловодства, виконання посадових обов'язків якими передбачало ознайомлення ними з комерційною таємницею, трудова функція яких не передбачала ознайомлення з відомостями, що становлять комерційну таємницю підприємства, ознайомлення яких з даного роду інформацією було ситуаційним, та інших осіб; 3) вилучення документів, зокрема, актів перевірки конфіденційної документації і приміщень (можливо – технічних засобів), де циркулює інформація, що становить комерційну або банківську таємницю, і в яких, відповідно, можуть бути вказані прізвища осіб, які проводили перевірку, їхні посади, обсяги і види проведеного огляду, результати, підписи, дата проведення даного заходу та інша інформація; 4) ознайомлення з матеріалами службового розслідування, якщо його проведення представниками служби або підрозділу економічної безпеки суб'єкта господарської діяльності, мало місце за фактом незаконного збирання або розголошення комерційної або банківської таємниці; 5) проведення опитування: а) працівників підприємства; б) співробітників відділу економічної безпеки суб'єкта господарювання, конфіденційної документації тощо; в) працівників, які мають справу з комерційною або банківською таємницею у ситуаційному порядку та інших осіб; 6) призначення експертизи речових доказів тощо, про порядок проведення і тактичні особливості яких йшлося вище.

Обов'язковим моментом є фіксація отриманої в результаті проведення відповідних слідчих (розшукових) дій та інших заходів інформації в процесуальних джерелах, зокрема, складання протоколів огляду місця події, креслень, планів, схем приміщень,

де циркулює інформація, що становить комерційну або банківську таємницю у якості додатків до протоколів огляду місця події, протоколів допиту осіб (у разі внесення відомостей в ЄРДР) та інших процесуальних документів.

На заключному етапі тактичної операції «Збирання і фіксація вихідної інформації про факт злочину» під час розслідування кримінальних правопорушень у сфері комерційної або банківської таємниці здійснюється обговорення її результатів всіма учасниками операції та оцінка проведеної роботи. Дуже важливо, щоб слідчий мав дані попередніх досліджень. Обмін інформацією та обговорення отриманих даних є підставою для розробки плану подальшого розслідування. Крім того, судження, які висловлюють учасники операції, є основою слідчо-розшукових версій відносно особи злочинців та мотиву вчиненого кримінального правопорушення.

Характеризуючи тактичну операцію «Пошук особи, яка вчинила злочин», необхідно зауважити, що діяльність правоохоронних органів щодо встановлення особи (осіб), які вчинили незаконне збирання з метою використання чи використання відомостей, що становлять комерційну або банківську таємницю, або розголошення комерційної або банківської таємниці, є однією з найважливіших умов, що забезпечують реалізацію принципу невідворотності покарання за вчинений злочин. Розв'язання цього завдання багато в чому залежить від узгоджених дій слідчого (дізнавача) з іншими учасниками СОГ. Найбільшого рівня ефективності подібна взаємодія досягає, як показує практика, саме під час проведення тактичних операцій.

Під час проведення зазначеної тактичної операції з урахуванням даних, отриманих в результаті тактичної операції «Збирання і фіксація вихідної інформації про факт злочину», доцільним є проведення таких слідчих (розшукових) дій та інших заходів: 1) проведення розшукових заходів: а) переслідування і затримання правопорушників за слідами або указаними потерпілими і очевидцями напрямками переміщення правопорушника або за

результатами роботи службового собаки, організація загороджувальних заходів, у тому числі в місцях можливого перебування або появи правопорушників; б) проведення розшукових заходів у місцях перебування осіб, схильних до вчинення правопорушень (у тому числі збуту викраденого майна); в) виявлення свідків та очевидців події, опитування (у разі внесення відомостей в ЄРДР – допит) з цією метою осіб, які проживають або працюють поблизу місця вчиненого діяння, а також осіб, які могли перебувати на можливих шляхах руху правопорушника до та від місця події; г) установлення базових станцій операторів мобільного (рухомого) зв'язку, що обслуговують територію, на якій знаходиться місце вчинення кримінального правопорушення, та можливих напрямків руху особи, яка його вчинила, а також інших місць з урахуванням обставин кримінального правопорушення; ґ) проведення поквартирного чи подвірного обходу для збирання відомостей про подію, обстеження місцевості в районі вчинення кримінального правопорушення, виявлення загублених, викинутих правопорушником знарядь учиненого діяння, інших предметів, отримання додаткової інформації про подію та осіб, які вчинили кримінальне правопорушення; д) орієнтування особового складу органів та підрозділів поліції на території обслуговування, на якій учинено кримінальне правопорушення, та суміжних територіях, а також (за необхідності) представників громадськості про характер, час, місце і спосіб учинення кримінального правопорушення, кількість осіб, які його вчинили, їх зовнішність, прикмети викраденого та про інші відомості, що мають значення для встановлення правопорушників та їх розшуку; ж) використання можливостей баз (банків) даних єдиної інформаційної системи Міністерства внутрішніх справ України та інших інформаційних ресурсів, а також засобів масової інформації; перевірку осіб за базами (банками) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України, та іншими інформаційними ресурсами, передбаченими статтями 26, 27 Закону України «Про Національну поліцію»; з) інші передбачені

законодавством заходи та дії, необхідні для встановлення події кримінального правопорушення та особи, яка його вчинила [66];

2) використання під час огляду місця події, приміщення або сховища (сейфа), де зберігався документ, в якому містяться відомості, що становлять комерційну таємницю, технічних засобів, в яких циркулює конфіденційна інформація суб'єкта господарської діяльності, виявлених технічних засобів перехоплення інформації, допомоги фахівців; 3) допиту заявника або представника потерпілої юридичної особи або фізичної особи-підприємця про подію, злочинця та його місцезнаходження; 4) ознайомлення з матеріалами відомчих розслідувань, якщо вони мали місце; 5) розсилання слідчих доручень оперативним працівникам – орієнтувань з докладним описом словесного портрета злочинця, перевірки його за оперативно-пошуковими обліками, витребування особової справи та фотографій злочинця; 6) у випадку підтвердження присутності злочинця за певною адресою – затримання його з одночасним проведенням обшуку за місцем перебування, з подальшим допитом тощо.

Такою є приблизна схема проведення зазначеної тактичної операції. Проте варто пам'ятати, що переліки слідчих (розшукових) дій, розшукових та інших заходів у межах зазначеної тактичної операції можуть значно варіюватися залежно від слідчої ситуації, яка має місце під час розслідування злочинів у сфері комерційної або банківської таємниці, характеру інформації, отриманої в результаті проведення збирання і фіксації вихідної інформації про факт кримінального правопорушення.

Варто також зауважити, що пошук злочинця під час розслідування незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, а також розголошення комерційної або банківської таємниці може проводитися і від такого базисного елементу криміналістичної характеристики як спосіб вчинення та приховування злочину. Адже, як відомо, спосіб вчинення злочину має двояке значення у його розкритті. Він дає можливість,

по-перше, звузити коло осіб, серед яких знаходиться злочинець, і, по-друге, висунути версію про вчинення двох або більше подібних злочинів однією особою, якщо спосіб вчинення злочинів є своєрідним.

У загальному плані найбільші можливості у плані звуження кола осіб, які перевіряються, під час розслідування злочинів у сфері комерційної таємниці відкриваються у випадку вчинення розголошення комерційної таємниці, адже принаймні коло осіб, яким ця таємниця відома у зв'язку з професійною або службовою діяльністю, встановити простіше [23, с. 48–65].

Існують певні випадки, за яких актуально звузити коло осіб, які можуть підлягати перевірці у зв'язку із вчиненням кримінального правопорушення, у випадках незаконного збирання інформації з метою використання даних, що становлять комерційну або банківську таємницю суб'єкта господарювання. До таких випадків можна віднести ситуації, коли конфіденційні документи були викрадені з приміщення або сховища без застосування знарядь злому; коли особа, відповідальна за транспортування або доставку такого документа, зникла разом із ним; за визначених обставин, коли сторонні особи, які не мають доступу до роботи з конфіденційними матеріалами, фізично не могли проникнути у приміщення, але там були виявлені пристрої для перехоплення інформації. Також подібні ситуації мають місце, якщо дані, що становлять комерційну таємницю і зберігаються в електронній формі на комп'ютерних системах, попри наявність серйозного захисту програмного характеру, були викрадені, пошкоджені чи знищені.

Отже, підсумовуючи, необхідно зауважити, що наявність у розпорядженні слідчої групи чіткої програми можливих дій під час реалізації тактичної операції «Пошук особи, яка вчинила злочин» в умовах конкретної ситуації дає змогу правильно і ефективно проводити пошук злочинця.

Характеризуючи тактичну операцію «Викриття особи, яка вчинила злочин», необхідно зауважити, що якщо підозрюваний, який

ськів незаконне збирання з метою використання відомостей, що становлять комерційну або банківську таємницю, або розголошення комерційної або банківської таємниці, затриманий, то ця типова ситуація передбачає проведення таких дій щодо викриття злочинця: 1) особистий обшук та освідування підозрюваного (при цьому під час огляду одягу, взуття, головних уборів, передусім, необхідно звертати увагу на сліди, які вказують на причетність до злочину, зокрема, пошкодження); інші явища, які є додатковими обставинами, що вказують на причетність підозрюваного до злочину; у разі знаходження у затриманого валіз, портфелів, сумок тощо, в яких можуть знаходитися викрадені документи, в яких міститься інформація, що становить комерційну або банківську таємницю, пристроями перехоплення інформації, ЕОМ, знімними носіями інформації тощо, необхідно ще до перевірки їх вмісту з'ясувати у підозрюваної особи належність цих речей, предметів, попросити перелічити докладно, що знаходиться всередині; будь-які заяви затриманих щодо цього мають бути занесені до протоколу; всі вилучені у підозрюваного речі, ушкодження на тілі, особливі прикмети також підлягають фіксації у протоколі та мають бути сфотографовані; 2) дактилоскопіювання та фотографування підозрюваного з метою перевірки його особи та минулої злочинної діяльності за реєстраційно обліковими даними; 3) перевірка особистих документів затриманого, за необхідності направлення їх на техніко-криміналістичну експертизу; 4) обшуки за місцем проживання та роботи підозрюваного з метою виявлення викрадених документів з конфіденційною інформацією, знімних носіїв, зокрема, дискет, компакт-дисків, флеш-накопичувачів, ЕОМ, в яких міститься в електронному вигляді інформація, що становить комерційну або банківську таємницю, засобів негласного зняття інформації, мікрофонів, інших технічних засобів перехоплення інформації, програмних продуктів, які використовувалися з метою незаконного отримання інформації, що циркулює, зокрема, в ЕОМ, знарядь злому, відмичок, які використовувалися для відкриття сховища (сейфа), де зберігалися документи (носії) інформації, що становить комерційну або

банківську таємницю тощо (особливу увагу при цьому необхідно приділяти предметам та знаряддям, які б могли бути використані під час вчинення кримінального правопорушення, а також одягу, взуттю, в яких могла бути підозрювана особа під час вчинення незаконного збирання з метою використання чи використання відомостей, що становлять комерційну або банківську таємницю, або розголошення комерційної або банківської таємниці, записникам, іншим документам, що можуть свідчити про злочинні зв'язки); 5) пред'явлення підозрюваного для впізнання потерпілим, свідкам та іншим особам, які могли бачити підозрюваного напередодні, у момент або відразу після вчинення кримінального правопорушення; 6) допити свідків; 7) одночасні допити раніше допитаних осіб; 8) слідчих експериментів; 9) перевірка підозрюваного на причетність до вчинення інших кримінальних правопорушень тощо.

Затримання правопорушника із речовими доказами є одним із найбільш ефективних методів використання доказів з метою встановлення істини у кримінальному провадженні. У цьому разі, стосовно розслідування кримінальних правопорушень, передбачених ст. ст. 231 та 232 КК України, доказами можуть бути: а) документи, в яких міститься інформація, що становить комерційну або банківську таємницю; б) облікова документація; в) довідки, записки, листи, інші документи подібного роду, які внаслідок свого змістовного наповнення, виходячи з матеріалів кримінального провадження, стосуються вчинення незаконного збирання або розголошення комерційної або банківської таємниці; г) комп'ютерна техніка, зокрема, персональні комп'ютери, ноутбуки; ґ) носії інформації, зокрема, дискети, компакт-диски, флеш-накопичувачі; д) пристрої негласного зняття інформації тощо.

Щодо цього варто зауважити, що самі по собі ці предмети достовірно не вказують на особу злочинця, і слідчому необхідно доводити їх зв'язок із вчиненням незаконного збирання або розголошення комерційної або банківської таємниці.

Необхідно зауважити, що в процесі розслідування можуть виникати такі ситуації: а) сприятлива, якщо у розпорядженні слідчого

є не тільки вилучені у підозрюваного зазначені предмети, а також і достатня сукупність інших доказів вчинення ним незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, або розголошення комерційної або банківської таємниці чи участі у них; б) несприятлива, коли інші докази відсутні зовсім або їх недостатньо.

У першому випадку наявна сукупність доказів достатня для викриття підозрюваного незалежно від тієї позиції, яку він займає. В іншому разі ситуацію може бути ускладнено негативною позицією підозрюваного, який став на шлях заперечення вчинення ним кримінального правопорушення або причетності до нього.

За умов наявності негативної позиції підозрюваного тактична операція передбачає: 1) допит підозрюваного про походження вилучених у нього предметів з детальним з'ясуванням причин та обставин, за яких вони опинилися у нього (за версією допитуваного); 2) дії щодо з'ясування вірогідності відомостей, які повідомив допитуваний про обставини придбання ним відповідних предметів: а) допити осіб, названих як свідків правомірного знаходження у підозрюваного вказаних предметів (без зв'язку з незаконним збиранням або розголошенням комерційної або банківської таємниці); б) проведення одночасних допитів між підозрюваним та свідком, який заперечує його показання про правомірне знаходження предметів у підозрюваного; в) витребування, огляд та залучення документів, в яких є відомості про предмети, які підлягають перевірці; г) у необхідних випадках розшукові заходи, наприклад, з метою виявлення незнайомих підозрюваному осіб, у яких, за його твердженням, він придбав ці предмети, зокрема, персональний комп'ютер, ноутбук, дискету (дискети), компакт-диски, флеш-накопичувачі, мобільний телефон, засоби негласного збору інформації тощо (подвірний обхід житлового сектору в населеному пункті, кварталі, де начебто була придбана річ, яка підлягає перевірці тощо); 3) допит підозрюваного з використанням результатів перевірки його первинних показань про надходження вилучених у нього об'єктів тощо.

Сукупність фактів, встановлених за допомогою комплексу вказаних дій під час реалізації тактичної операції «Затримання злочинця з речовими доказами» у процесі розслідування злочинів у сфері комерційної або банківської таємниці, може бути підставою для висновку про істинність або хибність показань підозрюваного і використовуватись з метою викриття винної у вчиненні кримінального правопорушення особи.

Характеризуючи тактичну операцію «Нейтралізація протидії підозрюваного у вчиненні злочину» під час розслідування кримінальних правопорушень, передбачених ст. ст. 231 та 232 КК України, необхідно зауважити, що у межах зазначеної тактичної операції з метою встановлення факту приховання втрати документа, який містить відомості, що становлять комерційну або банківську таємницю, підозрюваний може провести такі дії і заходи: 1) огляд акта про знищення документа; 2) огляд реєстру на відправлення документа; 3) призначення криміналістичної (технічної) експертизи акта, реєстру; 4) допит відповідальної за документ особи; 5) допит свідків; 6) огляд місця виявлення документа; 7) огляд документа, який вважається знищеним; 8) огляд облікових документів (журналу видачі, реєстру, картки тощо) з метою виявлення даних про рух конфіденційних матеріалів після їх удаваної втрати або відправлення; 9) огляд доставлених документів; 10) огляд журналу надходження документа у підрозділ тощо.

З метою викриття приховання підозрюваним факту втрати документа шляхом інсценування його необережного знищення або шляхом підміни може бути проведено: 1) огляд місця знищення документа; 2) призначення криміналістичної (технічної) експертизи виявлених (наданих) об'єктів; 3) огляд пред'явленого документа; 4) призначення криміналістичної (технічної) експертизи документа; 5) ревізія конфіденційного діловодства у підрозділі; 6) допит відповідальної за документ особи; 7) допит свідків та інші дії.

З метою встановлення факту маскування своєї причетності у межах зазначеної тактичної операції підозрюваним до

втрати документа шляхом приховування факту його отримання або твердження про його повернення або передачу можуть проводитися: 1) огляд записів (робочих і особистих) підозрюваного, які підтверджують факт користування документом; 2) огляд таких, що залишилися, облікових документів підрозділу (журналів, реєстрів, карток), які свідчать про те, що відповідальна особа передавала іншим співробітникам у користування документ, якого начебто не отримувала; 3) обшук за місцем роботи і проживання відповідальної за документ особи і її зв'язків; 4) допит відповідальної за документ особи; 5) допит свідків.

З метою нейтралізації протидії підозрюваного у формі інсценування викрадення документа за умов відсутності порушення правил поводження з ним проводяться: 1) огляд місця події; 2) слідчий експеримент; 3) обшук у відповідальної за документ особи з метою виявлення і вилучення знарядь, які використовувалися з метою інсценування; 4) призначається і проводиться криміналістична (трасологічна) експертиза та інші дії і заходи.

З метою встановлення приховування підозрюваним фактів порушення правил конфіденційного діловодства, встановлених на підприємстві, здійснюються: 1) огляд місця події; 2) огляд ключів від сейфа (сховища), де зберігалися відповідні документи, в яких міститься комерційна або банківська таємниця; 3) огляд сейфа або сховища; 4) огляд супровідних документів і документів про відрядження; 5) призначення і проведення криміналістичної (технічної) експертизи документів; 6) допит відповідальної за документ особи; 7) допит свідків тощо.

У разі потреби викриття маскування причетності підозрюваного до викрадення документа з відомостями, що становлять комерційну або банківську таємницю, проводяться: 1) огляд місця виявлення документа; 2) призначається і проводиться криміналістична (дактилоскопічна) експертиза; 3) призначається і проводиться криміналістична (трасологічна) експертиза з метою встановлення цілого по частинах; 4) обшук; 5) допит підозрюваного; 6) допит свідків тощо.

У разі вчинення підозрюваною особою дій щодо приховування документа або його частин (інших дій щодо приховування факту викрадення) у рамках проведення тактичної операції «Нейтралізація протидії підозрюваного у вчиненні злочину» може бути здійснено: 1) допит підозрюваного; 2) допит свідків; 3) пред'явлення документа (або його частини) для впізнання; 4) криміналістична експертиза документів.

Якщо підозрюваний приховує свою участь у викраденні документа, який містить відомості, що становлять комерційну або банківську таємницю, шляхом інсценування його втрати або твердження про викрадення даного документу іншою особою, з метою нейтралізації його протидії можуть проводитися: 1) огляд місця події; 2) огляд документів, які підтверджують відсутність відповідальної особи у період зникнення документа на службі, у населеному пункті; 3) допит підозрюваного; 4) слідчий експеримент; 5) допит свідків; 6) обшук у підозрюваного; 7) криміналістичні (трасологічна, дактилоскопічна) експертизи; 8) пред'явлення знаряддя злочину для впізнання; 9) криміналістичні експертизи (почеркознавча, авторознавча), технічна експертиза документів тощо [54, с. 198].

Проведення зазначених слідчих (розшукових) дій та інших заходів у рамках тактичної операції «Нейтралізація протидії підозрюваного у вчиненні злочину» допоможе вирішити тактичні завдання, які виникають у типових слідчих ситуаціях розслідування кримінальних правопорушень, передбачених ст. ст. 231 та 232 КК України, зокрема, незаконного збирання відомостей, що становлять комерційну або банківську таємницю, вчиненого шляхом викрадення документів, в яких містяться відомості, що становлять комерційну або банківську таємницю суб'єкта господарської діяльності.

Розкриваючи загальні положення тактичної операції «Встановлення алібі», необхідно зауважити, що алібі можна визначити як доказову відсутність особи, яка цікавить органи досудового розслідування (здебільшого підозрюваного, а в окремих випадках – свідка або потерпілого), на місці події або в іншому місці,

яке відноситься до розслідуваної події, під час події або протягом деякого проміжку часу, що підлягає дослідженню [63, с. 70–79].

Необхідно зауважити, що конкретний криміналістичний зміст встановлення алібі, тобто потрібної сукупності слідчих, оперативно-розшукових та інших дій значною мірою зумовлюється обставинами конкретного кримінального провадження і слідчою ситуацією на момент виникнення необхідності проведення цієї тактичної операції.

Передумовами встановлення алібі є визначення кола осіб, алібі яких треба перевірити, проміжку часу, на який необхідно встановити алібі, і місць, стосовно яких варто встановити алібі.

Відповідно до загальних тактичних і методичних рекомендацій, які стосуються перевірки алібі, встановленню підлягають, зокрема: 1) місце перебування підозрюваної особи перед вчиненням кримінального правопорушення і після нього, особливо якщо можна припускати, що кримінальне правопорушення вчинене групою осіб і особа, яка підлягає перевірці, може бути співучасником, а не безпосереднім виконавцем злочину (маються на увазі ті випадки, коли учасники злочинної групи разом здійснюють підготовку до злочину, а після – разом здійснюють заходи щодо приховування своїх злочинних дій); 2) час, потрібний для виконання окремих дій (наприклад, для прибуття на місце події, подолання перешкод, вчинення злочину, його приховування, залишення місця події), що допомагає дослідити співвідношення простору й часу, зіставити ці дії з місцем злочину, місцем алібі і часом, потрібним на скоєння злочину, тощо [63, с. 70–79].

З метою встановлення алібі під час розслідування незаконного збирання та розголошення комерційної або банківської таємниці, залежно від обставин кримінального провадження використовуються такі дії та заходи: 1) дослідження місця події і оперативна оцінка слідів; 2) аналіз способу вчинення злочину та його механізму, включаючи підготовчі дії, шляхи приходу й відходу, дії на місці події тощо; 3) активне встановлення підозрюваних і свідків; 4) одержання і фіксація інформації про послідовність виконання

певними особами дій та їх аналіз; 5) перевірка підозрюваних осіб; 6) проведення експертиз; 7) допит підозрюваної особи, під час якого їй ставляться такі питання: а) Де перебувала особа у період часу, що цікавить органи досудового розслідування? б) У який час повинен був бути вчинений злочин, якщо певна особа брала безпосередню участь у його вчиненні, або була його свідком? в) Яких осіб можна виключити як виконавців злочину, якщо злочин було вчинено в час, точно або приблизно встановлений досудовим розслідуванням? г) Які особи перебували у визначений час у місці, яке цікавить органи досудового розслідування? д) Коли певна особа перебувала у цьому місці? е) Інші питання; 8) використання різного роду допоміжної технічної документації під час встановлення алібі, зокрема: а) хронологічного огляду окремих етапів вчинення кримінального правопорушення; б) хронологічного огляду місця перебування певних осіб; в) графічного методу зображення співвідношення місця і часу перебування визначених осіб, складених за свідченнями підозрюваних і свідків; г) графічних територіальних оглядів місць вчинення кримінальних правопорушень, що входять до осередку (сукупності) однорідних злочинів тощо.

Необхідно зазначити, що до числа підстав, які повинні викликати підозру в удаваності алібі, належать такі: а) підозрювана особа дає дуже точні й детальні свідчення про алібі, не дивлячись на порівняно значний проміжок минулого часу; б) спочатку підозрюваний не повідомляє про алібі, а потім вказує абсолютно конкретні дані про нього; в) підозрюваний повідомляє відомості, які не можуть бути перевірені, або обмежуються неконкретними загальними поясненнями; г) підозрюваний повідомляє про поведінку, яка не відповідає його звичайному способу життя (наприклад, твердить, що був у ресторані, водночас уже відомо, що він їх ніколи не відвідує); ґ) показання підозрюваного й свідків помітно збігаються у дрібних деталях; д) зміна показань підозрюваним під час досудового розслідування, відмова від раніше наданих показань, а потім повернення до них; е) занадто часта зміна місць перебування підозрюваного до і після вчинення злочину тощо [63, с. 70–79].

За результатами проведення тактичної операції «Встановлення алібі» може бути зроблено такі висновки: 1) алібі підтверджено, тобто особа, яка перевіряється, не перебувала на місці злочину у відповідний час, а була в іншому місці; отже, ця особа повинна бути виключена з числа осіб, які брали безпосередню участь у вчиненні злочину, або були його свідками; 2) алібі не підтверджено, і є докази того, що особа, яка перевіряється, у відповідний час перебувала на місці злочину, зокрема, місці вчинення незаконного збирання з метою використання відомостей, що становлять комерційну або банківську таємницю, скоєного шляхом викрадення документів, в яких міститься інформація, що становить комерційну або банківську таємницю, шляхом перехоплення зазначеної інформації, що циркулює в технічних засобах і приміщеннях тощо; 3) докази, які свідчать про перебування особи, яка перевіряється, у відповідний час на місці злочину або в місці алібі, відсутні; такий висновок не дозволяє виключити цю особу з кола гаданих злочинців і вимагає наступної активної роботи з метою одержання інших доказів причетності цієї особи до вчинення злочину [63, с. 70–79].

Необхідно зауважити, що оцінка результатів проведення тактичної операції «Встановлення алібі» під час розслідування незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, а також розголошення комерційної або банківської таємниці, повинна проводитись у сукупності з іншими матеріалами кримінального провадження. У разі виникнення суперечностей слідчий має визначити перелік обставин, які підлягають подальшій перевірці, з метою одержання від підозрюваної особи правдивих показань.

Підсумовуючи сказане, необхідно зауважити, що проведення описаних тактичних операцій під час розкриття незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, а також розголошення комерційної або банківської, сприятиме вирішенню тактичних завдань, які виникають у типових слідчих ситуаціях під час розслідування вказаного виду злочинів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бахін В. П., Гора І. В., Цимбал П. В. Криміналістика : курс лекцій. Ірпінь : Академія ДПС України, 2002. Ч. 1. 356 с.

2. Біленчук П. Д., Перкін В. І. Тактичні прийоми, тактичні комбінації та тактичні операції в розслідуванні злочинів. Київ : НАВСУ, 1996. 32 с.

3. Великий тлумачний словник сучасної української мови / уклад. і голов. ред. В. Т. Бусел. Київ, Ірпінь : Перун, 2001. С. 218.

4. Вінник О. М. Господарське право : курс лекцій. Київ : Атіка, 2004. 624 с.

5. Гетманцев Д. О. Банківська таємниця: особливості її нормативно-правового регулювання в Україні та в законодавстві зарубіжних країн: дис. ... канд. юрид. наук: 12.00.07 / Київ. нац. ун-т ім. Тараса Шевченка. Київ, 2003. 206 с.

6. Гончаренко В. Г., Курдюков В. В., Легких К. В. Спеціальні знання: генезис, предмет, рівні, форми використання в доказуванні. *Вісник академії адвокатури*. Вип. 9. 2007. С. 22–24.

7. Господарський Кодекс України : Закон від 16.01.2003 № 436-IV. *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/436-15.

8. Господарський кодекс України : наук-практ. коментар / за заг. ред. О. П. Коцюби. Київ : А. С. К, 2004. 720 с.

9. Гурджи Ю. А. Питання про криміналістичну характеристику незаконного збирання відомостей, що становлять комерційну таємницю. *Актуальні проблеми держави і права*: збір. наук. праць. Одеса : Одеський держунівер., 1996. Вип. 3. 319 с.

10. Дергачов В. С. Відповідальність за розголошення державної та комерційної таємниці за трудовим законодавством України.: дис. ... канд. юрид. наук : 12.00.05 / Харків. нац. пед. ун-т ім. Г. С. Сковороди. Харків, 2009. 171 с.

11. Деєв М. В. Кримінально-процесуальне доказування та його елементи. *Науковий вісник Херсонського державного університету. Серія: юридичні науки.* 2015. Випуск 3-2. Т. 2. С. 212–215.

12. Дудоров О. О. Злочини у сфері господарської діяльності: кримінально-правова характеристика : монографія. Київ : Юридична практика, 2003. 924 с.

13. Дудоров О. О. Злочини у сфері господарської діяльності: особливості кримінальної відповідальності. *Вісник Асоціації кримінального права України.* 2014. № 1(2). С. 169–175.

14. Дудоров О. О., Мовчан Р. О. Законодавство України про кримінальну відповідальність за злочини у сфері господарської діяльності – час визначитися зі стратегією розвитку. *Вісник Асоціації кримінального права України.* 2015. № 2 (5). С. 215–263.

15. Експертизи у судовій практиці: наук.-практ. посіб. за заг. ред. В. Г. Гончаренка. 2-ге вид., перероб. і допов. Київ : Юрінком Інтер, 2010. 400 с.

16. Експертна служба МВС України: вебсайт. URL: https://dndekc.mvs.gov.ua/%d0%b5%d0%ba%d1%81%d0%bf%d0%b5%d1%80%d1.

17. Журавель В. А. Тактичні операції в системі криміналістичних засобів протидії злочинності. *Теорія та практика судової експертизи і криміналістики*. 2006. Вип. 6. 447 с.

18. Зав'ялов С. М. Спосіб вчинення злочину і сучасні проблеми вивчення та використання у боротьбі зі злочинністю: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.09 «Кримінальний процес та криміналістика, судова експертиза». Київ, 2005. 21 с.

19. Зажицький В. Нові норми доказового права та практика їх застосування. *Юстиція.* 2003. № 7. С. 45.

20. Іванців Я. І. Правовий захист комерційної таємниці. URL: https://ukrainepravo.com/scientific-thought/pravova-pozytsiya/pravoviy-zakhist-komerts-yno-ta-mnits.

21. Івахов А. А. Проблемні питання у розслідуванні кримінальних справ про розголошення державної таємниці та шляхи їх вирішення в умовах реформування кримінальної юстиції України. *Питання удосконалення діяльності органів дізнання та досудового слідства в умовах реформування кримінальної юстиції України*: матеріали наук.- практ. конф. (Харків, 30 трав. 2008 р.) / Ін-т

підготовки юрид. кадрів для Служби безпеки України. Харків, 2008. С. 113–117.

22. Іващенко В. М. Окремі положення методики розслідування незаконного збирання та розголошення комерційної таємниці. *Право і суспільство*. 2006. № 2. С. 50–58.

23. Іващенко В. М. Основи методики розслідування незаконного збирання та розголошення комерційної таємниці. *Юридичний журнал*. 2006. № 8 (50). С. 48–65.

24. Іващенко В. М. Спосіб злочину як елемент криміналістичної характеристики злочинної діяльності у сфері порушення комерційної таємниці. *Право і суспільство*. 2006. № 1. С. 113–118.

25. Камлик М. І. Економічна безпека підприємницької діяльності. Економіко-правовий аспект: навчальний посібник. Київ : Атік, 2005. 432 с.

26. Київський науково-дослідний інститут судових експертиз. Дослідження, пов'язані з комерційною таємницею (ноу-хау) і раціоналізаторськими пропозиціями: веб-сайт. URL: https://kndise.gov.ua/news/news-view/c-doslidzenna-povazani-z-komercijnoutaemniceu-nou-hau-i-racionalizatorskimi.

27. Килимник І. І., Харитонов О. В. Правова характеристика забезпечення комерційної таємниці на підприємстві в умовах ринкової економіки : монографія. Харків : ХНУМГ, 2014. 82 с.

28. Клименко Н. І. Судова експертологія: курс лекцій : навч. посіб. для студ. юрид. спец. вищ. навч. закл. Київ : Ін Юре, 2007. 528 с.

29. Когутич І. І. Криміналістика: курс лекцій. Київ : Атіка, 2008. 888 с.

30. Коновалова В. О. Методика розслідування злочинів: оптимальні системи слідчих дій. *Вісник Академії правових наук України*. Харків, 2005. Вип. 4 (43). С. 155–160.

31. Криміналістика. Криміналістична тактика і методика розслідування злочинів: підруч. за ред. В. Ю. Шепітька. Харків, 1998. С. 29.

32. Криміналістика: підручник / Кол. авт.: В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін. / За ред. проф. В. Ю. Шепітька. 4-е вид., перероб. і доп. Харків : Право, 2008. 464 с.

33. Кримінальний кодекс України: Закон від 05.04.2001 № 2341-III. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

34. Кримінальний процесуальний кодекс України: Закон від 13.04.2012 № 4652-VI. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/4651-17.

35. Курман О. В. Відомості, що становлять комерційну таємницю, як предмет злочинного посягання. *Право і суспільство*. 2015. № 5.2 (2). С. 177–181.

36. Курман О. В. Тактичні операції при розслідуванні злочинних посягань на відомості, що становлять комерційну або банківську таємницю. *Порівняльно-аналітичне право*. 2014. № 4. С. 181–183.

37. Курман О. В. Про криміналістичну характеристику злочинів, пов'язаних із посяганням на відомості, що становлять комерційну або банківську таємницю. *Теорія і практика судової експертизи і криміналістики*. 2012. Випуск 12. С. 44–51.

38. Лічман Т. В. Захист комерційної таємниці в системі економічної безпеки підприємств України в процесі євроінтеграції. автореф. дис. ... канд. екон. наук: 21.04.02. ВНЗ «Ун-т економіки та права «КРОК». Київ, 2014. 20 с.

39. Мельников Н. И. Некоторые методы противодействия техническим средствам несанкционированной звукозаписи. *Теорія та практика криміналістичного забезпечення розкриття та розслідування злочинів у сучасних умовах*: Тези доповід. нак.-практ. конф. Київ : НАВСУ, 2001. Ч. 2. 287 с.

40. Молдован А. В., Мельник С. М. Кримінальний процес України: навч. посіб. Київ : Центр учбової літератури, 2017. 368 с.

41. Назаров В. В., Омельяненко Г. М. Кримінальний процес України: підручник. Київ : Юридична думка, 2005. 548 с.

42. Науково-дослідний центр судової експертизи з питань інтелектуальної власності. Дослідження, пов'язані з комерційною

таємницею (ноу-хау) і раціоналізаторськими пропозиціями: вебсайт. URL: http://intelect.org.ua/content/138-doslidzhennya-povyazani-z.

43. Науково-практичний коментар до Господарського кодексу України / За ред. проф. О. П. Коцюби. Київ : А. С. К., 2004. 720 с.

44. Науково-практичний коментар до Кримінального кодексу України / Відп. ред. В. Ф. Бойко. Київ : А. С. К., 2000. 1120 с.

45. Науково-практичний коментар до Кримінального кодексу України / Відп. ред. С. С. Яценко. Київ : А. С. К., 2005. 848 с.

46. Науково-практичний коментар Кримінального кодексу України / Д. С. Азаров, В. К. Грищук, А. В. Савченко [та ін.]; за заг. ред. О. М. Джужі, А. В. Савченка, В. В. Чернея. 2-ге вид., перероб. і допов. Київ : Юрінком Інтер, 2018. 1104 с.

47. Науково-практичний коментар Кримінального кодексу України / За ред. М. І. Мельника, М. І. Хавронюка. Київ : Атіка, 2003. 1056 с.

48. Науково-практичний коментар Кримінального кодексу України від 5 квітня 2001 року / За ред. М. І. Мельника, М. І. Хавронюка. Київ : Каннон, А. С. К., 2001. 1104 с.

49. Науково-практичний коментар Цивільного кодексу України: У 2 т. / За відповід. ред. О. В. Дзери (кер. авт. кол.), Н. С. Кузнєцової, В. В. Луця. Київ : Юрінком Інтер, 2005. Т. 1. 832 с.

50. Нікіфоров Г. К., Нікіфоров С. С. Підприємництво та правовий захист комерційної таємниці: навч.-практ. посіб. для вищих навчальних закладів. Київ : Олан, 2001. 208 с.

51. Біленчук П. Д., Лисиченко В. К., Клименко Н. І. та ін. Криміналістика: підручник. / За ред. Біленчука П. Д., 2-ге вид., випр. і доп. Київ : Атіка, 2001. 544 с.

52. Полуніна Л. В. Види слідчого огляду при розслідуванні незаконного збирання та розголошення комерційної або банківської таємниці. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика).* 2018. Випуск 1–2 (10–11). С. 263–268.

53. Полуніна Л. В. Використання спеціальних знань під час розслідування незаконного збирання та розголошення комерційної

або банківської таємниці. *Південноукраїнський правничий часопис*. 2019. № 1. С. 28–31.

54. Полуніна Л. В. Висунення версій та планування на початковому етапі розслідування незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю. *Актуальні проблеми правознавства*. 2019. Випуск 1 (17). С. 145–151.

55. Полуніна Л. В. Методика розслідування незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю: дис. …канд. юрид. наук: 12.00.09. Київ, 2021. 250 с.

56. Полуніна Л. В. Особливості проведення тактичних операцій при розслідуванні злочинів, пов'язаних із посяганням на відомості, що становлять комерційну або банківську таємницю. *National law journal: teory and practice*. 2019. № 3 (37). С. 161–165.

57. Полуніна Л. В. Особливості тактики проведення слідчих (розшукових) дій під час розслідування незаконного збирання та розголошення комерційної або банківської таємниці. *Прикарпатський юридичний вісник*. 2020. № 1 (30). С. 195–197.220

58. Полуніна Л. В. Питання методики розслідування злочинів у сфері незаконного використання комерційної або банківської таємниці. *The scientific heritage. (Budapest, Hungary)*. 2020. № 50. Ч. 4. С. 55–57.

59. Полуніна Л. В. Поняття і структура криміналістичної характеристики злочинів, пов'язаних із посяганням на відомості, що становлять комерційну або банківську таємницю. *Актуальні проблеми держави і права*. Випуск 82. С. 157–163.

60. Полуніна Л. В. Поняття комерційної таємниці як предмета злочинного посягання. *National law journal: teory and practice*. 2019. № 2 (36). С. 124–127.

61. Полуніна Л. В. Спосіб злочину як елемент криміналістичної характеристики злочинів, пов'язаних із посяганням на відомості, що становлять комерційну або банківську таємницю. *Держава та регіони*. 2019. № 4 (66). С. 158–162.

62. Полуніна Л. В. Типові слідчі ситуації та процесуальні дії щодо їх вирішення під час розслідування незаконного збирання та розголошення комерційної та банківської таємниці. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2018. Випуск 3–4 (12–13). С. 25–256.

63. Полуніна Л. В. Висунення версій та планування на початковому етапі розслідування незаконного збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю. *Актуальні проблеми правознавства*. 2019. Випуск 1 (17). С. 145–151.

64. Постіка І. В. Загальні положення тактичної операції «Встановлення алібі». *Теоретичні та практичні проблеми використання можливостей криміналістики і судової експертизи у розкритті і розслідуванні злочинів:* зб. наук. праць. Київ : УАВС, 1996. 209 с.

65. Про банки і банківську діяльність: Закон від 07.12.2000 № 2121-III. *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/2121-14.

66. Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні: Наказ, Інструкція від 07.07.2017 № 575. МВС України. URL: https://zakon.rada.gov.ua/laws/show/z0937-17#Text.

67. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень: Інструкція, Рекомендації від 08.10.1998 № 53/5. Міністерство юстиції України. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text.

68. Про судову експертизу : Закон України від 25.02.1994 № 4038-XII. *Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/4038-12#Text.

69. Радутний О. Е. Кримінальна відповідальність за незаконне збирання, використання та розголошення відомостей, що становлять комерційну або банківську таємницю: монографія. Національна юридична академія України ім. Ярослава Мудрого. Харків: Ксілон, 2008. 202 с.

70. Радутний О. Е. Кримінальна відповідальність за незаконне збирання, використання або розголошення комерційної таємниці. *Право України.* 2002. № 3. С. 110–113.

71. Розслідування злочинів у сфері господарської діяльності: окремі криміналістичні методики: монографія. В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін.; за ред. В. Ю. Шепітька. Харків : Право, 2006. 624 с.

72. Салтевський М. В. Криміналістика (у сучасному викладі): підручник. Київ : Кондор, 2005. 588 с.

73. Скригонюк М. І. Криміналістична термінологія: навчальний посібник. Київ : Видавничо-поліграфічний центр «Київський університет», 2003. 125 с.

74. Старушкевич А. В. Організація та тактичні особливості огляду місця події при розслідуванні злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж. *Право і суспільство.* 2006. № 2.

75. Трембіцький А. М. Правові основи захисту комерційної таємниці: курс лекцій. Хмельниц. ін-т міжрегіон. акад. упр. персоналом. Хмельницький, 2010. 179 с.

76. Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України: вебсайт. URL: https://www.sbu.gov.ua/ua/pages/282

77. Харламова С. О. Кримінальна відповідальність за незаконні дії з відомостями, що становлять комерційну або банківську таємницю: дис... канд. юрид. наук: 12.00.08. Київ. націон. ун-т внутрішніх справ. Київ, 2007.

78. Цивільний Кодекс України: Закон від 16.01.2003 № 435-IV. *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/435-15.

79. Шаповалова А. О. Забезпечення охорони банківської таємниці у кримінальному процесі України: автореф. дис. …на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.09 / Київ. націон. ун-т внутрішніх справ. Київ, 2009. 19 с.

80. Шевчук В. М. Криміналістична теорія тактичних операцій: проблеми та перспективи формування. *Актуальні проблеми криміналістики:* мат. міжнар. практ. конф. Харків, 2003. С. 47–50.

81. Шепітько В. Ю. Криміналістика: підруч. За ред. В. Ю. Шепітька. 5-те вид., переробл. та допов. Київ : Ін Юре, 2016. 640 с.

82. Щербаковський М. Г. Судові експертизи: призначення, проведення, використання: навч. посіб. Харків : Еспада, 2005. 544 с.

КРИМІНАЛЬНИЙ КОДЕКС УКРАЇНИ

(станом на 01.01.2025 зі змінами та доповненнями)

Стаття 231. Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю

Умисні дії, спрямовані на отримання відомостей, що становлять комерційну або банківську таємницю, з метою розголошення чи іншого використання цих відомостей, а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб'єкту господарської діяльності, -

караються штрафом від трьох тисяч до восьми тисяч неоподатковуваних мінімумів доходів громадян.

Примітка. Публічне, у тому числі через засоби масової інформації, журналістів, громадські об'єднання, професійні спілки, повідомлення особою інформації про вчинення кримінального або іншого правопорушення, здійснене з дотриманням вимог закону, не є діями, передбаченими цією статтею, і не тягне за собою кримінальну відповідальність.

Стаття 232. Розголошення комерційної, банківської таємниці або професійної таємниці на ринках капіталу та організованих товарних ринках

Умисне розголошення комерційної, банківської таємниці або професійної таємниці на ринках капіталу та організованих товарних ринках без згоди її власника особою, якій ця таємниця відома у зв'язку з професійною або службовою діяльністю, якщо воно вчинене з корисливих чи інших особистих мотивів і завдало істотної шкоди суб'єкту господарської діяльності, карається штрафом від однієї тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян або пробаційним наглядом на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

ГОСПОДАРСЬКИЙ КОДЕКС УКРАЇНИ

(станом на 01.01.2025 зі змінами та доповненнями)

Стаття 36. Неправомірне збирання, розголошення та використання відомостей, що є комерційною таємницею

1. Відомості, пов'язані з виробництвом, технологією, управлінням, фінансовою та іншою діяльністю суб'єкта господарювання, що не є державною таємницею, розголошення яких може завдати шкоди інтересам суб'єкта господарювання, можуть бути визнані його комерційною таємницею. Склад і обсяг відомостей, що становлять комерційну таємницю, спосіб їх захисту визначаються суб'єктом господарювання відповідно до закону.

2. Неправомірним збиранням відомостей, що становлять комерційну таємницю, вважається добування протиправним способом зазначених відомостей, якщо це завдало чи могло завдати шкоди суб'єкту господарювання.

3. Розголошенням комерційної таємниці є ознайомлення іншої особи без згоди особи, уповноваженої на те, з відомостями, що відповідно до закону становлять комерційну таємницю, особою, якій ці відомості були довірені у встановленому порядку або стали відомі у зв'язку з виконанням службових обов'язків, якщо це завдало чи могло завдати шкоди суб'єкту господарювання.

4. Схилянням до розголошення комерційної таємниці є спонукання особи, якій були довірені у встановленому порядку або стали відомі у зв'язку з виконанням службових обов'язків відомості, що відповідно до закону становлять комерційну таємницю, до розкриття цих відомостей, якщо це завдало чи могло завдати шкоди суб'єкту господарювання.

5. Неправомірним використанням комерційної таємниці є впровадження у виробництво або врахування під час планування чи здійснення підприємницької діяльності без дозволу уповноваженої на те особи неправомірно здобутих відомостей, що становлять відповідно до закону комерційну таємницю.

6. За неправомірне збирання, розголошення або використання відомостей, що є комерційною таємницею, винні особи несуть відповідальність, встановлену законом.

ЦИВІЛЬНИЙ КОДЕКС УКРАЇНИ

(станом на 01.01.2025 зі змінами та доповненнями)

Стаття 420. Об'єкти права інтелектуальної власності

1. До об'єктів права інтелектуальної власності, зокрема, належать:

літературні та художні твори;

комп'ютерні програми;

компіляції даних (бази даних);

виконання;

фонограми, відеограми, програми організацій мовлення;

наукові відкриття;

винаходи, корисні моделі, промислові зразки;

компонування напівпровідникових виробів;

раціоналізаторські пропозиції;

сорти рослин, породи тварин;

комерційні (фірмові) найменування, торговельні марки (знаки для товарів і послуг), географічні зазначення;

комерційні таємниці.

Стаття 507. Охорона комерційної таємниці органами державної влади

1. Органи державної влади зобов'язані охороняти від недобросовісного комерційного використання інформацію, яка є комерційною таємницею та створення якої потребує значних зусиль і яка надана їм з метою отримання встановленого законом дозволу на діяльність, пов'язану з фармацевтичними, сільськогосподарськими, хімічними продуктами, що містять нові хімічні сполуки. Ця інформація охороняється органами державної влади також від розголошення, крім випадків, коли розголошення необхідне для забезпечення захисту населення або не вжито заходів щодо її охорони від недобросовісного комерційного використання.

2. Органи державної влади зобов'язані охороняти комерційну таємницю також в інших випадках, передбачених законом.

ЗАКОН УКРАЇНИ

Про банки і банківську діяльність

(станом на 01.01.2025 зі змінами та доповненнями)

Стаття 60. Банківська таємниця

Інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним або стала відомою третім особам при наданні послуг банку або виконанні функцій, визначених законом, а також визначена у цій статті інформація про банк є банківською таємницею.

Банківською таємницею, зокрема, є:

1) відомості про банківські рахунки клієнтів, у тому числі кореспондентські рахунки банків у Національному банку України;

2) інформація про операції, проведені на користь чи за дорученням клієнта, вчинені ним правочини;

3) фінансово-економічний стан клієнтів;

4) інформація про організацію та здійснення охорони банку та осіб, які перебувають у приміщеннях банку;

5) інформація про організаційно-правову структуру юридичної особи - клієнта, її керівників, напрями діяльності;

6) відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація;

7) інформація щодо звітності по окремому банку, за винятком тієї, що підлягає опублікуванню;

8) коди, що використовуються банками для захисту інформації;

9) інформація про фізичну особу, яка має намір укласти договір про споживчий кредит, отримана під час оцінки її кредитоспроможності;

10) інформація про організацію та здійснення інкасації коштів та/або перевезення валютних цінностей;

11) інформація про банки чи клієнтів банків, що збирається від банків під час здійснення банківського нагляду, валютного нагляду, нагляду за діяльністю надавачів платіжних послуг, оверсайту платіжної інфраструктури, а також нагляду у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення;

12) інформація про банки чи клієнтів банків, отримана Національним банком України відповідно до міжнародного договору або за принципом взаємності від органу банківського нагляду іншої держави;

13) рішення Національного банку України про застосування заходів впливу, крім рішень про накладення штрафів, про віднесення банку до категорії неплатоспроможних, про відкликання банківської ліцензії та ліквідацію банку.

Положення частин першої і другої цієї статті не поширюються:

на інформацію, що підлягає обов'язковому опублікуванню. Перелік інформації, що підлягає обов'язковому опублікуванню, встановлюється Національним банком України;

на відомості про боржників, які є пов'язаними з банком особами, що прострочили виконання зобов'язань (за основною сумою та процентами) перед банком на строк понад 180 днів, а також про вимоги банків до таких боржників, а щодо банку, процедура ліквідації якого розпочата відповідно до Закону України «Про систему гарантування вкладів фізичних осіб», – на відомості про всіх боржників, які, за даними бухгалтерського обліку банку, прострочили виконання зобов'язань (за основною сумою та процентами) перед таким банком незалежно від строку прострочення.

Інформація з системи депозитарного обліку, що знаходиться у володінні Національного банку України та банків як учасників депозитарної системи України, не є банківською таємницею. Розкриття та захист інформації, що міститься в системі депозитарного обліку, здійснюється Національним банком України та банками на підставі та в порядку, встановлених законом про депозитарну систему України.

Національний банк України видає нормативно-правові акти з питань зберігання, захисту, використання та розкриття інформації, що становить банківську таємницю, та надає роз'яснення щодо застосування таких актів.

Положення інших законів України щодо обсягу та порядку розкриття інформації, що становить банківську таємницю, діють у частині, що не суперечить цьому Закону.

Наукове видання

Лілія Валентинівна Полуніна

ОСОБЛИВОСТІ ДОСУДОВОГО РОЗСЛІДУВАННЯ НЕЗАКОННОГО ЗБИРАННЯ АБО ВИКОРИСТАННЯ ВІДОМОСТЕЙ, ЩО СТАНОВЛЯТЬ КОМЕРЦІЙНУ АБО БАНКІВСЬКУ ТАЄМНИЦЮ

Монографія

Редактор
Л. А. Рапіна
Макет обладинки
Л. В. Полуніна

Підписано до друку 23.12.2024 р.
Формат 60×84/16. Папір офсетний.
Умовн. друк. арк. 10,46. Наклад 50 прим.
Зам. № 0106/25

Видавець: Київський інститут Національної гвардії України.
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготовлювачів і розповсюджувачів
видавничої продукції Серія ДК № 7696 від 8.11.2022 р.
Виготовлювач: ФОП Андрієвська А.П.
Київ, вул. Бориспільська, 9а.
Свідоцтво Серія ВОЗ № 548018 від 10.09.2003 р.