

ОРГАНІЗАЦІЯ РОБОТИ ОРГАНІВ ВНУТРІШНІХ СПРАВ

УДК 343.3

Рижков Е. В., к.ю.н., доцент Донецький юридичний інститут МВС України

Отримання підрозділами ОВС по боротьбі з економічною злочинністю інформації про злочини у сфері економіки за допомогою сучасних інфотелекомунікаційних технологій

У статті досліджуються питання отримання підрозділами ОВС по боротьбі з економічною злочинністю інформації про злочини у сфері економіки за допомогою сучасних інфотелекомунікаційних технологій. Висвітлено роль обліково-звітних даних про факт передачі та зміст переданої телекомунікаційними мережами інформації, а також перспективи використання підрозділами ОВС по боротьбі з економічною злочинністю інформаційно-телекомунікаційних технологій в отриманні криміналістично значущої інформації при оперативно-розшуковому документуванні та розслідуванні кримінальних правопорушень.

Ключові слова: економічні злочини, інформаційно-телекомунікаційні технології, обліково-звітні дані, отримання інформації.

В статье исследуются вопросы получения подразделениями ОВД по борьбе с экономической преступностью информации о преступлениях в сфере экономики с помощью современных инфотелекоммуникационных технологий. Освещена роль учетно-отчетных данных о факте передачи и содержании передаваемой телекоммуникационными сетями информации, а также перспективы использования подразделениями ОВД по борьбе с экономической преступностью информационно-телекоммуникационных технологий в получении криминалистически значимой информации при оперативно-розыском документировании и расследовании уголовных правонарушений.

Ключевые слова: экономические преступления, информационно-телекоммуникационные технологии, учетно-отчетные данные, получение информации.

The article deals with the question of obtaining police units to combat economic crime information on crimes in economy with sophisticated technology ICT. The role of accounting and reporting data on the assignment and the content of the transmitted data telecommunications networks, as well as prospects of police units to combat economic crime ICT in obtaining meaningful information in forensic detective and search for documentation and investigation of criminal offenses.

Keywords: economic crimes, information and telecommunication technologies, recording and reporting data, getting information.

Сьогодні Україна переживає процес реформування, в епіцентрі якого знаходяться правоохоронна та економічна сфери життя суспільства [1; 2]. Поширення тінювих форм соціальної та економічної взаємодії на фоні глобалізаційних процесів та структурної перебудови вітчизняної економіки в напрямку розширення її взаємодії зі світовим господарством призвело до збільшення масштабів економічної злочинності, виникнення нових форм і способів учинення протиправних діянь в економіці. При цьому неухильно

зростає кількість випадків використання при вчиненні економічних злочинів сучасних інформаційно-телекомунікаційних технологій (Інтернету, мобільного зв'язку) [3]. Особливу небезпеку в контексті появи нових видів злочинів у сфері економіки становить поява віртуальних форм розрахунків. Більшість фінансових операцій, учасниками яких виступають як фізичні, так і юридичні особи, сьогодні відбувається за допомогою Інтернету. Електронні системи кредитно-фінансових установ і банків, як потенційні об'єкти злочинного посягання, а також активне користування цими системами фізичними особами, стали природною причиною виникнення, існування та збільшення економічних злочинів з використанням сучасних інфокомунікаційних технологій.

У зв'язку з цим усе більш актуальним стає питання вдосконалення методики й тактики діяльності оперативних підрозділів ОВС щодо протидії економічним злочинам з використанням таких способів організації роботи, які дозволять оперативним підрозділам ОВС законно, максимально швидко та з мінімальними ресурсними витратами отримувати оперативну та доказову інформацію, швидко її передавати на відстані, з можливістю її подальшої реалізації в оперативно-розшуковому та кримінальному провадженні. Такого ефекту можна досягти шляхом використання в діяльності оперативних підрозділів ОВС України наукомістких інноваційних методик, сучасних інформаційно-телекомунікаційних технологій.

Як справедливо зазначає Є.Д. Лук'янчиков, практика завжди потребує розробки й законодавчого закріплення засобів інформаційного забезпечення, адекватних характеру сучасної злочинності [4, с. 230]. Мова йде не лише про полегшення співробітникам ОВС «спілкування» з сучасними технічними засобами та його сучасним інформаційно-методичним забезпеченням за допомогою спеціального програмно-математичного та організаційно-технічного забезпечення, яке можна було би для зручності користування компактно представити у вигляді нових інформаційних технологій, на що вказує О.Г. Фролова, досліджуючи проблеми сучасного інформаційно-методичного забезпечення управління в ОВС [5, с. 60, 100]. Сьогодні важливим завданням організації протидії злочинам, що вчиняються у сфері економіки, є розробка теоретичних, організаційно-правових основ використання сучасних інфокомунікаційних технологій у протидії економічним злочинам оперативними підрозділами ОВС України

Особливості провадження ОРД підрозділів ОВС по боротьбі з економічною злочинністю відобразились у дослідженнях К.В. Антонова, Л.І. Аркуши, О.М. Бандурки, Б.Є. Богданова, В.В. Бойцова, Д.В. Гребельського, О.Ф. Долженкова, Г.О. Душейка, В.П. Захарова, О.В. Кириченка, О.О. Кисельова, І.П. Козаченка, Д.Й. Никифорчука, С.І. Ніколаюка, С.В. Обшалова, В.М. Омеліна, О.О. Подобного, О.О. Савченка, В.О. Сілюкова, Д.М. Середи, О.П. Снігерьова, І.Р. Шинкаренка та ін. Важливим аспектам використання інформаційно-телекомунікаційних технологій у протидії злочинності присвячені роботи В.В. Бірюкова, В.М. Бутузова, О.Г. Волеводза, І.О. Воронова, В.Д. Гавловського, С.В. Єськова, А.В. Іщенко, А.Є. Користіна, М.В. Карчевського, М.Ю. Литвинова, Є.Д. Лук'янчикова, Т.В. Михальчук, О.В. Межового, М.П. Нестеренка, Ю.Ю. Орлова, С.М. Рогозіна, А.С. Сизоненка, Д.Б. Сергєєвої, Ю.В. Степанова, Д.В. Сулацького, І.Ф. Харабєрюша, В.П. Шеломенцева та інших учених, кожен із яких зробив свій внесок в науково-методичне забезпечення ОРД підрозділів ОВС по боротьбі з економічною злочинністю. Однак проблематика отримання цими підрозділами інформації про злочини у сфері економіки за допомогою сучасних інформаційно-телекомунікаційних технологій у роботах указаних авторів була досліджена фрагментарно. Також вважаємо не розкритою роль високих технологій в

інформаційно-аналітичному забезпеченні ОРД цих підрозділів. Саме тому метою цієї статті є дослідження питань отримання підрозділами ОВС по боротьбі з економічною злочинністю інформації про злочини у сфері економіки з визнанням ключовою ролі у цьому процесі сучасних інформаційно-телекомунікаційних технологій. Разом із цим потрібно враховувати сучасні тенденції росту економічної злочинності, а також процеси реформування правоохоронної системи, пов'язані з прийняттям у 2012 році нового Кримінального процесуального кодексу України (далі – КПК України), внесенням змін до оперативного-розшукового законодавства та переорієнтацією вітчизняного кримінального процесу з розшукового на змагальний.

Згідно Закону України «Про Національну програму інформатизації», для реалізації інформаційних технологій використовують такі засоби інформатизації: електронні обчислювальні машини, програмне, математичне, лінгвістичне та інше забезпечення, інформаційні системи або їх окремі елементи, інформаційні мережі та мережі зв'язку [6]. Більшість цих засобів використовується працівниками ДСБЕЗ у повсякденній діяльності. Коло завдань підрозділів ДСБЕЗ у протидії економічній злочинності, обумовлене їх компетенцією, є дещо специфічним порівняно з завданнями державного управління та економіки, що обґрунтовує необхідність застосування того чи іншого засобу ОРД.

Чітке уявлення про функції підрозділів ДСБЕЗ у боротьбі з економічними злочинами та їх компетенцію при проведенні оперативного-розшукових заходів з використанням сучасних інфокомунікаційних технологій, впливає з вимог наказу МВС України № 769 від 03.09.2012, згідно положень якого основними завданнями ДСБЕЗ є:

1. Участь у формуванні та забезпеченні реалізації державної політики у сфері боротьби зі злочинністю, захисту економіки та об'єктів права власності.

2. Своєчасне припинення злочинів у сфері економіки та запобігання їм.

3. Аналіз, прогнозування криміногенних процесів у сфері економічної діяльності та своєчасне інформування про них керівництва МВС України та інших органів виконавчої влади.

4. Виявлення та припинення фактів порушення прав інтелектуальної власності.

5. Виявлення причин і умов, які сприяють учиненню правопорушень у сфері економіки, та вжиття заходів щодо їх усунення [7].

Слід зазначити, що діяльність підрозділів ДСБЕЗ щодо протидії економічній злочинності складається переважно з негласних засобів і методів, завдяки чому реалізується принцип соціальної справедливості в специфічній галузі правовідносин, оскільки дає змогу максимально забезпечити вчасність, повноту та об'єктивність розслідування, невідворотність покарання, відшкодування завданої державі та громадянам шкоди, виявлення латентних злочинів і притягнення до відповідальності осіб, які їх учинили.

Метою цієї діяльності є отримання криміналістично значущої оперативної (орієнтуючого характеру) та доказової інформації, яка має значення для протидії економічним злочинам, а об'єктом, на який спрямована пізнавальна діяльність працівників підрозділів ДСБЕЗ, є всі процеси та явища, що містять ознаки злочину, і вкупі дають підстави щодо визнання певної економічної діяльності нелегальною (або тіньовою). При цьому роль сучасних інформаційно-телекомунікаційних технологій в оперативного-розшуковій діяльності підрозділів ДСБЕЗ визначається обсягом інформації про злочини у сфері економіки, яку можливо отримати в ході цієї діяльності. Зробити це, на нашу думку, дозволить висвітлення особливостей економічного злочину та тіньової економічної діяльності, спираючись на фундаментальні праці, присвячені проблематиці

боротьби з економічною злочинністю та економічній девіантології.

Так, досліджуючи наукові основи забезпечення економічної безпеки за допомогою ОРД з метою вироблення стратегії боротьби з злочинами економічної спрямованості, О.Є. Шаріхін розглядає тіньову економіку як продукт активної життєдіяльності організованої економічної злочинності, яка репродукує стратагемні відносини в суспільстві. Протидія цьому явищу вимагає активних дій суспільства й держави по розробці програми декриміналізації економіки, що, в кінцевому підсумку, дозволить виробити науково обґрунтований підхід до інфраструктури економічної безпеки, включаючи й розробку механізму її захисту [8, с. 118; 9, с. 21].

Щодо висвітлення ознак економічних злочинів, слід навести думку Б. Свенссона, який під ними розуміє протиправні діяння, що вчиняються систематично і в рамках легальної господарської діяльності. До економічних злочинів не належать майнові злочини традиційного характеру, вчинені окремими особами, якщо вони не мають жодного відношення до господарської діяльності [10, с. 24]. О.М. Яковлев слушно зазначає, що дані злочинні діяння, зазвичай, відбуваються у зв'язку або з приводу реалізації економічних відносин, і вчиняються особами, які виконують певні функції в конкретній економічній системі [11, с. 51]. Поділяючи думки цих учених, ми підтримуємо існуючу точку зору, згідно якої під економічними злочинами слід розуміти протиправні діяння, які здійснюються під виглядом законних господарських операцій, що детермінують неминучість їх відображення в системі економічної інформації [12, с. 6, 173].

Цікавим є висловлювання М.Н. Умарова, який, досліджуючи родову криміналістичну модель економічних злочинів, робить висновок, що всі економічні злочини споріднені за цілою низкою ознак, серед яких провідними та обов'язковими є дії обману. Сутність обману полягає в тому, що за допомогою певних операцій створена неправда (дезінформація) подається як правда. З інформаційних позицій обман завжди являє собою метадезінформування, тобто подання створеної брехні (дезінформування) як правди (трансінформування) [13, с. 28].

З цих позицій стає зрозуміло, що обманні дії складаються з двох частин: спочатку потрібно створити дезінформацію, а потім представити її як правду. У цих механізмах і з'являється та частина слідів економічних злочинів, яку М.К. Камінський визначив як «натуральні основи слідів» [14, с. 15.].

З цього приводу М.Н. Умаров зазначає, що оскільки об'єктами впливу при скоєнні економічних злочинів в основному є документи, документопотоки, документозбереження, документооблік як у формі рукописів, так і в електронному вигляді на комп'ютерних носіях, то основними слідами економічної злочинної діяльності є так звані «паперові сліди», що існують в різних формах. Крім них існують сліди у вигляді невідповідностей між наявністю та обліковою кількістю матеріальних об'єктів, цінностей та ін. [13, с. 28-29].

Розглядаючи проблеми нелегальної економічної діяльності слід зазначити, що особливістю економічної злочинності в Україні є постійно зростаючий рівень організованості та професійності. У свою чергу організована професійна злочинна діяльність, як стверджує В.І. Куліков, є особливим видом кримінального промислу, що здійснюється згуртованими в кримінальному середовищі мобільними з побудованою відповідно до злочинних цілей структурою, внутрішньою організацією, управлінням і зовнішніми зв'язками злочинними формуваннями (групами), у вигляді динамічно планованих, адаптованих для досягнення кримінальних цілей, колективно здійснюваних систем певних базових (корисливих, господарських, посадових), а також багатьох

інших, в основному, умисних злочинних діянь [15, с. 34].

Зважаючи на особливості економічної злочинності в країнах пострадянського простору, О.О. Матвеев зазначає, що під організованим злочиним у сфері економіки слід розуміти вид динамічно планованої, адаптованої до досягнення кримінальних цілей злочинної діяльності, здійснюваної навмисно злочинними групами, які мають певну структуру, внутрішню організацію та управління в процесі або під виглядом законних господарських операцій, що детермінує обов'язковість взаємодії даної діяльності з функціонуючою на об'єкті системою економічної інформації [12, с. 19-20].

Наведене визначення розкриває специфіку вчинення економічних злочинів з криміналістичної точки зору та узагальнює ряд схожих злочинних діянь, ґрунтуючись на оперативно-розшуковому критерії, що визначає компетенцію підрозділів ДСБЕЗ у протидії цим злочинам. Таким критерієм є характер відносин під час взаємодії події злочину з існуючою системою економічної інформації та результат цієї діяльності (закономірності механізмів виникнення слідів злочину, їх виявлення, а також використання в правоохоронних цілях).

Визначною рисою економічних злочинів є необхідність маскуванню злочинної діяльності під виглядом законних господарських операцій. Дійсно, злочинна (тіньова) економічна діяльність є прихованою і високолатентною [3]. Високий відсоток латентності, як зазначив І.І. Рожков, визначається безперервним удосконаленням організації, тактики й техніко-інформаційного забезпечення організованої злочинної діяльності у сфері економіки [16, с. 9].

При цьому латентність злочинної діяльності економічної спрямованості буває двох типів: перша — злочинна діяльність, про яку знає достатньо широке коло осіб, але, попри це, конкретні злочини не виявляються правоохоронними органами; друга — злочинна діяльність тіньової форми, що здійснюється окремими «сім'ями», наприклад тіньова банківська діяльність, про яку знає вельми обмежене коло осіб, як правило, пов'язаних «сімейними» чи корпоративними узами [17].

Тут слід звернути увагу на вказані М.К. Камінським стадії (фази) розвитку організованої злочинної діяльності у сфері економіки, в кожній з яких відбуваються дії з приховування економічної злочинної діяльності та її результатів. Це такі фази:

— збір та оцінка інформації про предмет посягання: здійснюється шляхом безпосереднього спостереження, вивчення необхідної документації, організації зустрічей з фахівцями в даній сфері, встановлення контактів з важливими людьми, які можуть володіти інформацією, що становлять інтерес;

— ретельне моделювання майбутнього злочину: при цьому визначаються предмет злочинного посягання, кількість і конкретні функції кожного учасника, способи створення резерву товарно-матеріальних цінностей чи грошових коштів, способи вилучення створеного резерву, канали збуту й реалізації матеріальних цінностей, розміщення грошових коштів, прийоми маскуванню злочинної діяльності та її результатів, способи зв'язку між спільниками, запасні варіанти;

— організація злочинної групи (завершує процес підготовки при вчиненні злочину): остаточно формується склад учасників для вчинення конкретного злочину, здійснюється розподіл завдань між членами злочинної групи, призначаються особи, які несуть відповідальність за проміжні результати;

— реалізація злочинного задуму (безпосереднє виконання злочину): вилучається та реалізується створений резерв, частина якого, зазвичай, іде на розширення злочинної діяльності [18, с. 6].

ОРД підрозділів ДСБЕЗ має забезпечувати реалізацію правоохоронної (юрисдикційної) функції українського права, захищати властивими їй специфічними засобами людину, суспільство й державу від злочинних зазіхань. Використання в боротьбі зі злочинністю даних, отриманих під час поєднання гласних і негласних (переважно) засобів і методів(заходів), є вимушеною захисною мірою суспільства та держави. Врахування цих фаз, на нашу думку, є вкрай важливим для вдосконалення процедури отримання за допомогою інформаційно-телекомунікаційних технологій інформації про злочини у сфері економічної діяльності та загалом оперативнорозшукової тактики підрозділів ДСБЕЗ. Також слід враховувати фактор уявної анонімності в інформаційно-телекомунікаційних мережах, користувачі яких приховують свої справжні імена, використовуючи псевдоніми (ніки).

Не торкаючись організаційно-тактичних особливостей оперативного обслуговування об'єктів і галузей економіки підрозділами ДСБЕЗ, за рахунок чого здійснюється ефективна протидія економічній злочинності, зазначимо, що оперативнорозшуковий аспект такого обслуговування розкривається в інформаційному забезпеченні ДСБЕЗ [19], що дозволяє отримати чітке або відносно чітке уявлення про злочинні наміри осіб, спрогнозувати розвиток майбутніх подій та планувати подальші заходи щодо протидії злочинності.

У свою чергу тактика отримання оперативної інформації про злочини у сфері економічної діяльності тісно переплітається з тактикою економічної розвідки, що посідає визначне місце в арсеналі засобів економічної безпеки. Адже з метою вивчення оперативної обстановки на об'єкті обслуговування та її оцінки на наявність інформації, що містить ознаки злочинів у сфері економіки, підрозділи ДСБЕЗ проводять комплекс гласних і негласних заходів, більшість із яких має розвідувальний характер. Необхідність вжиття таких заходів зумовлена посиленням загроз з боку злочинної діяльності, новими можливостями та вимогами до потенціалу сил і засобів правоохоронної діяльності щодо протидії економічній злочинності [20].

Сутність економічної розвідки можна представити як різновид спеціальних заходів забезпечення економічної безпеки, що застосовуються в ОРД. Так, згідно Закону України «Про оперативнорозшукову діяльність», завданням ОРД є пошук і фіксація фактичних даних про протиправні діяння окремих осіб та груп, відповідальність за які передбачена Кримінальним кодексом України, розвідувально-підкривну діяльність спецслужб іноземних держав та організацій з метою припинення правопорушень та в інтересах кримінального судочинства, а також отримання інформації в інтересах безпеки громадян, суспільства й держави. При цьому, беручи до увагу специфіку ОРД підрозділів ДСБЕЗ, їх завданням, є отримання в інтересах безпеки громадян, суспільства і держави інформації про злочини, які вчиняються саме у сфері економіки.

Беручи до уваги вищенаведене, цілком закономірно, що тактика отримання економічної інформації оперативного характеру обумовлена як специфікою завдань підрозділів ДСБЕЗ, так і особливостями економічної інформації, що представляє оперативний інтерес, що відрізняють її від оперативної інформації про злочини загальнокримінальної спрямованості. У свою чергу джерела даних про економічні злочини можна поділити на такі, що містять інформацію про будь-який злочин (універсальні), і такі, що містять інформацію, яка представляє інтерес лише в межах протидії економічним злочинам і не використовується при розкритті інших (загальнокримінальних) злочинів.

З цього приводу О.О. Матвеев зазначає, що загальною домінантою в діяльності щодо

протидії економічним злочинам є необхідність використання даних, отриманих з обліково-звітних документів, у єдиній системі з іншими джерелами інформації у справі [12, с. 18]. Обліково-звітні документи, на його думку, слугують матеріальним виразом джерел, які містять інформацію, що представляє інтерес лише в межах протидії економічним злочинам і не використовується при розкритті інших (загальнокримінальних) злочинів [12, с. 18-19]. Однак, враховуючи роль сучасних інформаційно-телекомунікаційних технологій в економічній інфраструктурі держави та в діяльності правоохоронних органів, дане твердження навряд чи слід вважати апріорним.

Як зазначає М.Ю. Литвинов, сьогодні високого рівня набула комп'ютеризація банківського сектору, обліково-фінансових послуг, інформаційно-телекомунікаційних послуг та зв'язку. Ці сфери стали залежними від безпечного та сталого функціонування інформаційно-телекомунікаційної техніки, що забезпечує їх роботу [21, с. 40]. Так, без використання сучасних інформаційно-телекомунікаційних технологій не обходиться організація обліково-звітної діяльності банківських і кредитно-фінансових установ.

Банківська система забезпечує весь банківський облік за прибутками та видатками, а також підготовку балансових звітів відповідно до вимог як Національного банку, так і міжнародного банківського та аудиторського секторів. Відповідно до п. 4.2 Положення про здійснення банками фінансового моніторингу реєстрація фінансових операцій, що підлягають фінансовому моніторингу, здійснюється у відповідному реєстрі, який формується і ведеться банком (філією) і є електронним документом визначеної структури [22]. Завдяки можливостям автоматизованих банківських систем нового покоління сьогодні широко розповсюджені технології «клієнт-сервер» на сучасній СУБД із можливістю роботи он-лайн та «Клієнт-банк», що дозволяють напряму переносити відпрацьовані технічні рішення в нове середовище [23, с. 4]. Водночас сучасне інформаційно-технічне забезпечення надає комерційним банкам можливість збирати інформацію щодо клієнтів та обліку, підтримуючи безпеку системи [23, с. 4].

Однією з перших автоматизованих банківських систем була система «Операційний день банку», яка обслуговує внутрішню поточну діяльність банку (бухгалтерський облік, обслуговування рахунків клієнтів тощо). Ця система включає внутрішню платіжну систему банку (програмно-технічний комплекс із власними засобами захисту інформації, який експлуатується банком і здійснює платіжний обіг між підрозділами банку та іншими банківськими установами). Головним завданням цієї системи є ведення всіх рахунків бухгалтерського обліку, включаючи розрахункові й кореспондентські рахунки клієнтів [23, с. 10].

При цьому банківські установи, як правило, на власний розсуд визначають деякі кількісні показники, що стосуються здійснення фінансових операцій (наприклад, «суттєве збільшення залишку на рахунку», «суттєве збільшення частки готівки», «регулярне здійснення зарахування на рахунок особи», «згодом», «значна кількість платежів від фізичних осіб», «великий пакет цінних паперів» та ін.). Тому контроль і втручання правоохоронних органів у цю діяльність, як зазначає О.О. Савченко, вкрай важливе і доцільне [24, с. 204].

Таким чином сучасні інформаційно-телекомунікаційні технології відіграють важливу роль в організації обліково-звітної діяльності банківських і кредитно-фінансових установ. Однак їх можливості не обмежуються завданнями організації документообігу в сфері банківської діяльності, а також бухгалтерського обліку та аудиту з використанням комп'ютерних технологій [25], в результаті проведення яких, дійсно, можна отримати відомості, які представлятимуть інтерес лише в рамках

протидії економічним злочинам.

Так, контроль за доступом до комп'ютерних систем шляхом чіткої обліково-звітної діяльності зменшує ймовірність втручання у роботу цих систем програм-«вірусів». У подальшому в процесі розслідування фактів використання шкідливої комп'ютерної програми чи технічного засобу досліджуються такі джерела інформації: журнали обліку (робочого часу, доступу до обчислювальної техніки, її збоїв і ремонту, реєстрації користувачів комп'ютерної системи чи мережі, проведення регламентних робіт); ліцензійні угоди та договори на користування комп'ютерними програмними продуктами, технічними засобами та їхню розробку, порівняння їх із діючими комп'ютерними програмами та технічними засобами; книги паролів, доступу до автоматизованої системи; накази та інші документи, що регламентують роботу установи і, зокрема, використання автоматизованої інформаційної системи, тощо [26].

Отримання інформації, що утворюється при використанні сучасних інформаційно-телекомунікаційних технологій, передбачає застосування спеціальних технічних засобів та дотримання певного процесуального порядку, що забезпечує її доказове значення. Процесуальною формою пізнавальної діяльності негласного характеру при розслідуванні кримінального правопорушення є негласні слідчі (розшукові) дії (далі – НСРД), які, згідно ч. 2 ст. 246 КПК, проводяться у випадках, якщо відомості про злочин та особу-злочинця, неможливо отримати в інший спосіб. НСРД «зняття інформації з транспортних телекомунікаційних мереж» (ст. 263 КПК) та «зняття інформації з електронних інформаційних систем» (ст. 264 КПК) в частині дій, що проводяться на підставі ухвали слідчого судді, проводяться виключно у кримінальному провадженні щодо тяжких або особливо тяжких злочинів [27].

Незалежно від тяжкості злочину проводиться установлення місцезнаходження радіоелектронного засобу без розкриття змісту повідомлень, що передаються, якщо в результаті його проведення можна встановити обставини, які мають значення для кримінального провадження (ст. 268 КПК), а також зняття інформації з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем чи не пов'язаний з подоланням системи логічного захисту (ч. 2 ст. 264 КПК України) [28].

Водночас слід звернути увагу на недосконалість процедури отримання (надання) дозволу на проведення НСРД. Як підставу для проведення НСРД, що тимчасово обмежують конституційні права громадян, КПК передбачає наявність ухвали слідчого судді про дозвіл на її проведення. Водночас слід мати на увазі, що механізм оцінки правомірності та наявності підстав для зняття інформації з транспортних телекомунікаційних мереж в частині судового контролю за дотриманням конституційних прав громадян, регламентований КПК, не є досконалим. Як зазначає професор Б.Г. Розовський, санкціонування прослуховування телефонних переговорів та інших НСРД за новим КПК – це формальність. Слідчий суддя не досліджує необхідну інформацію в першооснові, а обмежений закритою інформацією про інформацію – документами, складеними слідчим (прокурором) [29]. Отже, вирішальну роль процесуальної фігури «слідчого судді» в забезпеченні конституційних прав громадян під час НСРД у КПК вочевидь перебільшено. Іншими словами, дотримання законності залежить від компетентності слідчого (прокурора) та оперативних працівників. При цьому процедурні проблеми безпосереднього проведення НСРД та реалізації отриманої інформації залишаються, але відходять на другий план.

Шляхом проведення негласної слідчої (розшукової) дії «установлення місцезнаходження радіоелектронного засобу», можна встановити зв'язки осіб, що вчинили злочин, розшукати підозрюваного (обвинуваченого), вирішити широке коло інших завдань. У свою чергу пізнавальне значення негласної слідчої (розшукової) дії «зняття інформації з транспортних телекомунікаційних мереж» може мати не лише зміст інформації, що передається каналами зв'язку, але й її емоційне забарвлення, фонова та інша інформація, що супроводжує мову. Крім того інформація, виявлена в засобах (мережах, системах) зв'язку, підлягає реалізації при проведенні слідчих (розшукових) дій, у пошуковій діяльності ОВС, а також для подолання протидії розслідуванню [30].

Зазначене положення цілком кореспондується з вимогами Закону України «Про телекомунікації», в ч. 4 ст. 39 якого передбачено, що оператори телекомунікацій зобов'язані за власні кошти закуповувати та встановлювати на своїх телекомунікаційних мережах технічні засоби, необхідні для здійснення уповноваженими органами оперативного-розшукових заходів, і забезпечувати функціонування цих технічних засобів, а також у межах своїх повноважень сприяти проведенню оперативного-розшукових заходів та недопущенню розголошення організаційних і тактичних прийомів їх проведення. Оператори телекомунікацій зобов'язані забезпечувати захист зазначених технічних засобів від несанкціонованого доступу [31].

Слід додати, що оператори телекомунікацій під час виконання своїх службових обов'язків мають доступ до інформації про персональні дані, переміщення (місцезнаходження), контакти (особисті зв'язки) користувачів тощо, яка може бути цінною в розслідуванні економічних злочинів.

Так, наприклад, операторами систем мобільного зв'язку оброблюється (приймається, реєструється, зберігається тощо) такі відомості: 1) розрахункові дані – відомості, на основі яких системами операторів здійснюється облік наданих послуг і наступні розрахункові операції з абонентами: абонентські номери, що беруть участь у з'єднанні, отриманні послуг (MSISDN); вид послуги, напрям з'єднання тощо; час початку, завершення та тривалість з'єднання, надання послуги тощо; телекомунікаційні картки, що використовувалися для розрахунків із оператором; 2) службові дані – відомості суто технічного характеру, що забезпечують функціонування систем операторів і терміналів щодо надання та споживання послуг, підтримки з'єднання тощо: міжнародний ідентифікаційний номер рухомого абонента (IMSI); міжнародний ідентифікаційний номер терміналу (IMEI); постійне місцезнаходження споживача відносно підсистеми базових станцій (BSS) оператора [32, с. 7].

Основними взаємодіючими об'єктами в процесі встановлення з'єднання абонентів за допомогою систем мобільного зв'язку є програми, бази даних, апаратно-програмний комплекс (мобільний телефон, мережі базових станцій і комутатор), що являють собою своєрідний банк цифрових даних. Добування з використанням елементів розвідки та аналітична обробка зазначених даних дозволяють здійснювати контроль за основними аспектами приватного життя кожного абонента (групи абонентів).

На основі загальних положень теорії інформації, структури побудови, функціонування, а також специфіки збереження і передачі інформації, можна зробити висновок, що системи мобільного зв'язку є потенційним джерелом інформації оперативного-розшукового чи доказового значення, що в пізнавальному плані представляє криміналістичний інтерес. При цьому, як зазначає В.А. Козінін, інформація, що оброблюється в мережах мобільного зв'язку, може носити характер як потенційно, так і актуально криміналістично значущої [33, с. 17-19].

Апелюючи до твердження О.О. Матвєєва, слід звернути увагу на універсальний

характер в доказовому плані категорії «обліково-звітні документи». Адже такі документи, утворені в результаті використання інформаційно-телекомунікаційних технологій, можуть містити інформацію, що представляє інтерес не лише в межах протидії економічним злочинам (як вважає О.О. Матвєєв), але й використовуватися в цілях виявлення, попередження та припинення злочинів різної спрямованості, у т.ч. комп'ютерних або, навіть, загальнокримінальних злочинів.

Процес виявлення та припинення злочину економічної спрямованості уточнюється та конкретизується залежно від того, яким способом і на які сфери функціонування економічної структури впливає злочинна діяльність. Слід погодитися з І.І. Рожковим, який пропонує початкову схему виявлення в межах ОРД злочинів економічної спрямованості за напрямком «мотив – особистість – мета», а також схему подальшого розслідування злочинів у сфері економіки «мета – засоби – об'єкти впливу – слідова інформація» [16, с. 113, 115]. Разом з тим важливо встановити всі обставини кримінальної події та інші дрібні деталі вчиненого за допомогою інформації, що містяться в обліково-звітних документах. Тому важливим і актуальним завданням підрозділів ОВС по боротьбі з економічною злочинністю є виявлення метаслідів, а особливо слідів метадезінформування в сфері економічної діяльності, утворених у результаті використання інформаційно-телекомунікаційних технологій.

Автоматизовані комп'ютерні системи оперують у своїй роботі інформацією в бінарному вигляді, багаторазово змінюючи її форму та зміст. Саме через те, що інформація не є матеріальною об'єктом, а лише може бути матеріально зафіксована у різній формі, класичне розуміння слідів та процесу слідоутворення, у розрізі злочинів, що вчиняються в інформаційно-телекомунікаційній мережі, не є співвідносним. При цьому визначальна роль у процесі слідоутворення в комп'ютерній мережі належить процесу інкапсуляції – важливому інструменті об'єктно-орієнтованого програмування, що обмежує доступ до компонентів (методів і властивостей), які складають об'єкт, та робить їх приватними (доступними лише всередині об'єкта).

При вчиненні економічного злочину за допомогою застосування інформаційно-телекомунікаційних технологій відбувається зміна матеріального стану елементів телекомунікаційної системи мобільного зв'язку або Інтернет, що утворює системи електронних слідів-відображень, придатних до сприйняття за допомогою відповідних програмно-технічних засобів. Це показує корисну властивість телекомунікаційних систем (мереж) щодо фіксації обліково-звітних даних про факт передачі та зміст переданої телекомунікаційними мережами інформації в формі електронного документа, завдяки чому цей процес можна назвати унікальним способом виявлення, попередження та припинення сучасних способів учинення злочинів у сфері економіки.

Зазначені технології мають перевагу в отриманні підрозділів ОВС по боротьбі з економічною злочинністю криміналістично значущої інформації при оперативнорозшуковому документуванні та розслідуванні кримінальних правопорушень, а тому повинні використовуватись під час виявлення, попередження та припинення злочинів цими підрозділами за конкретними напрямками, обумовленими виконанням завдань кримінального провадження, згідно визначеної КПК процедури шляхом зняття інформації з транспортних телекомунікаційних мереж та електронних інформаційних систем, а також встановлення контролю за місцезнаходженням злочинців з урахування специфіки протидії злочинам економічної спрямованості.

Говорячи про унікальну властивість обліково-звітних даних про факт передачі та зміст переданої телекомунікаційними мережами інформації, при використанні її за певним

напрямок (в ОРС або кримінальному провадженні) слід враховувати криміналістичну цінність такої інформації, можливість її законного отримання та виходити з розвідувальних можливостей (стратегічного становища) оперативного підрозділу. Для цього, в першу чергу, слід переглянути положення, що змінюють усю специфіку процесу взаємодії оперативного працівника зі слідчим у процесі розслідування кримінальних проваджень. Необхідно касувати положення ч. 2 ст. 41 КПК України та п. 1.8 міжвідомчої Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні, якими обмежено можливість оперативних працівників самостійно організувати свою роботу. Адже творча ініціатива оперативного працівника (в межах законодавства), має бути попереду процедурних обмежень, даючи можливість розвиватися творчому потенціалу оперативно-розшукової діяльності.

ЛІТЕРАТУРА:

1. Реформа МВС триватиме й надалі // Інтернет-представництво Президента України; новина від 08.09.2013 [Електронний ресурс]. – Режим доступу: <http://www.president.gov.ua/news/28713.html>.
2. Финансовая полиция: своевременно ли ее создание в Украине? (пост-релиз) <http://www.lfr.org.ua/cu/events/pressrelease/701-2013-04-04.html>.
3. Всесвітній огляд економічних злочинів – 2011. Україна [Електронний ресурс]. – Режим доступу: http://www.pwc.com/ua/en/services/forensic/assets/-gecs_2011_report_ukraine_ukr.pdf.
4. Лук'яничков Є.Д. Інформаційне забезпечення розслідування злочинів (правові і тактико-криміналістичні аспекти) : дис. ... докт. юрид. наук ; спец. 12.00.09 / Є.Д. Лук'яничков. – Київ: НАВС, 2005. – 429 с.
5. Фролова О.Г. Сучасне інформаційно-методичне забезпечення управління в органах внутрішніх справ : дис... докт. юрид. наук ; спец. 12.00.07 / Олена Григорівна Фролова. – Харків: ХНУВС, 2002. – 433 с.
6. Про Національну програму інформатизації : Закон України від 04.02.1998 № 74/98-ВР // ВВР від 17.07.1998. – К., 1998. – № 27. – Ст. 181.
7. Про організацію діяльності підрозділів державної служби боротьби з економічною злочинністю Міністерства внутрішніх справ України : наказ МВС України від 03.09.2012 № 769 // Офіційний вісник України від 05.10.2012. – К., 2012. – № 73. – С. 71.
8. Шарихин А.Е. Научные основы обеспечения экономической безопасности России посредством оперативно-розыскной деятельности : дис. ... докт. юрид. наук ; спец. 12.00.09 / А.Е.Шарихин. – М.: РУДН, 2007. – 497 с.
9. Шарихин А.Е. Научные основы обеспечения экономической безопасности посредством оперативно-розыскной деятельности : автореф. дис... докт. юрид. наук ; спец. 12.00.09 / А.Е. Шарихин. – М., 2007. – 52 с.
10. Свенссон Б. Экономическая преступность / БуСвенссон ; пер. со шведск. – М.: Прогресс, 1987. – 160 с.
11. Яковлев А.М. Социология экономической преступности / Александр Максимович Яковлев ; Отв. ред. В.Н. Кудрявцев. – М.: Наука, 1988. – 256 с.
12. Матвеев А.А. Использование экономической информации при выявлении и предупреждении организованных преступлений : дис. ... канд. юрид. наук ; 12.00.09 / Алексей Александрович Матвеев. – Н. Новгород: Нижегородский юрид. ин-т МВД РФ, 1999. – 208.
13. Умаров М.Н. Криминалистическая теория слеодообразования и применение ее выводов в практике раскрытия экономических преступлений : дис. ... канд. юрид. наук ; спец. 12.00.09 / Муса Нажмуудинович Умаров. – Ижевск, 2001. – 171 с.
14. Каминский М.К. Технично-криминалистические средства создания условий, способствующих возникновению информации. – М.: Академия МВД СССР, 1974.
15. Куликов В.И. Основы криминалистической теории организованной преступной деятельности. Ульяновск : Филиал МГУ, 1994.
16. Рожков И.И. Родовая криминалистическая модель процесса раскрытия экономических преступлений и ее практическое использование : дис. ... канд. юрид. наук ; 12.00.09 / Иван Иванович

Рожков. — Ижевск, 2001. — 176 с.

17. Семейные теневые банки // Обзор Интерпола за июль 2000 г. № 23; Бюллетени інформаційного центра МВД РФ за май-сентябрь 2000 г.

18. Каминский М.К. Расследование хищений государственного и общественного имущества, совершенных путем присвоения, растраты, злоупотребления служебным положением : (лекция). — Горький: ГВШ МВД СССР, 1978. — 16 с.

19. Ільницький О.В. Оперативне обслуговування об'єктів і галузей економіки підрозділами Державної служби боротьби з економічною злочинністю (ДСБЕЗ) МВС України / О.В. Ільницький // Віче : (теоретичний і громадсько-політичний журнал). — К., 2009. — № 22. — С.7-10.

20. Предборський В.А. Економічна безпека держави : (монографія) / Валентин Антонович Предборський. — К.: Кондор, 2005. — 391 с.

21. Литвинов М.Ю. Розкриття оперативними підрозділами ДСБЕЗ МВС України злочинів у сфері використання комп'ютерної інформації : дис. ... канд. юрид. наук ; спец. 12.00.09 / М.Ю. Литвинов. — Х.: ХНУВС, 2010. — 300 с.

22. Про затвердження Положення про здійснення банками фінансового моніторингу : Постанова Правління Національного банку України від 14.05.2003 № 189 // Офіційний вісник України від 13.06.2003. — К., 2003. — № 22. — С. 9.

23. Савченко О.О. Програмне забезпечення банківських установ : (лекція) / О.О. Савченко, М.Ю. Литвинов // курс «Інформаційні технології банківської діяльності». — Донецьк: ДЮІ МВС України, 2012. — 48 с.

24. Савченко О.О. Оперативно-розшукова профілактика й розкриття злочинів у сфері діяльності банківських і кредитно-фінансових установ. Курс лекцій : (навчальний посібник) / Олександр Олександрович Савченко. — Донецьк: ДЮІ ЛДУВС ім. Е.О. Дідоренка, 2011. — 292 с.

25. Івахненков С.В. Інформаційні технології в організації бухгалтерського обліку та аудиту : (навчальний посібник) / С.В. Івахненков. — 4-е вид., випр. і доп. — К.: Знання, 2008. — 343 с.

26. Виявлення та розслідування злочинів у сфері комп'ютерних технологій : (метод. рекомендації). http://www.naiu.kiev.ua/tslc/pages/arm/operatpr/metod_rek/r14.html.

27. Кримінальний процесуальний кодекс України від 13.04.2012 № 465-1-VI // Голос України від 19.05.2012. — К., 2012. — № 90-91.

28. Інструкція про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні, затверджена спільним наказом Генеральної прокуратури України, Міністерства внутрішніх справ України, Служби безпеки України, Міністерства фінансів України, Адміністрації Державної прикордонної служби України, Міністерства юстиції України від 16.11.2012 № 114/1042/516/1199/936/1687/5.

29. Розовский Б.Г. Дамоклов меч над ОРД / Б.Г. Розовский // Боротьба з Інтернет-злочинністю : матеріали міжнар. наук.-практ. конф. (м. Донецьк, 12-13 червня 2013 р.). — Донецьк : ДЮІ МВС України, 2013. — 266 с. — С. 83-86.

30. Отримання інформації з телекомунікаційних мереж мобільного зв'язку та її використання у кримінальному провадженні : [науково-практичний посібник] / О.В. Меживой, О.І. Хараберюш, Д.В. Безруков, І.Ф. Хараберюш ; за ред. професора І.Ф. Хараберюша. — Донецьк: Вид-во «Нюлідж» (донецьке відділення), 2013. — 297 с.

31. Про телекомунікації : Закон України від 18.11.2003 р. № 1280-IV // Відомості Верховної Ради України від 19.03.2004. — К., 2004. — № 12. — Ст. 155, ч. 4 ст. 39

32. Сулацький Д.В. Відомості щодо наданих телекомунікаційних послуг як предмет інформаційної безпеки людини та джерело оперативно значимої інформації : науково-практичні рекомендації / Г.О. Маркарян, Д.В. Сулацький. — Донецьк : ДЮІ МВС України, 2011. — 28 с.

33. Козинкин В.А. Использование в расследовании преступлений информации, обнаруживаемой в средствах сотовых систем подвижной связи : автореф. дис... канд. юрид. наук ; спец. 12.00.09 // Владислав Анатольевич Козинкин. — Москва: Московский университет МВД России, 2009. — 28 с.