2. Ахтирська Н. М. До питання доказової сили кіберінформації в аспекті міжнародного співробітництва під час кримінального провадження / Н. М. Ахтирська. // Науковий вісник Ужгородського національного університету. – 2016. – С. 123–125.

3. Ницевич А. А. Электронный документ как доказательство [Електронний ресурс] / А. А. Ницевич – Режим доступу: http://www.rtpp.com.ua/4business/10

Куцій М.С.
викладач,
Національна академія Служби безпеки України

ЗАБЕЗПЕЧЕННЯ ПОСЕРЕДНИЦЬКОГО ЗВ'ЯЗКУ В КОНФІДЕНЦІЙНОМУ СПІВРОБІТНИЦТВІ

З метою результативного вирішення завдань оперативно-розшукової діяльності (далі – ОРД) на засадах добровільності використовується інститут конфіденційного співробітництва з різними категоріями осіб (конфіденти) [1]. Науковці вітчизняних і зарубіжних правоохоронних відомств у своїх, переважно закритих, працях досліджували питання зазначеного співробітництва та використання сучасних технологій в ОРД. Зокрема, К.В. Антонов, П.П. Артеменко, О.М. Бандурка, Б.І. Бараненко, А.Д. Безруков, М.М. Василина, В.О. Глушков, О.М. Джужа, Є.О. Дідоренко, В.Є. Марічев, С.С. Овчинський, Ю.Ю. Орлов, В.Г. Пилипчук, І.А. Серебряков, І.В. Слюсарчук, І.Ф. Хараберюш, М.О. Шилін та ін.

Але, незважаючи на проведену вказаними й іншими авторами дослідницьку роботу, спрямовану на всебічне вивчення окремих аспектів діяльності негласного апарату, комплексне дослідження процесів правового та організаційного забезпечення зв'язку у конфіденційному співробітництві з використанням сучасної техніки, представниками вітчизняної правової науки не здійснювалось, що і визначає актуальність теми. В контексті з вказаним вище необхідно, на наш погляд, приділити увагу походженню застосованої юридичної термінології, передусім термінам і поняттям, які стосуються ролі таких осіб у забезпеченні конспіративного зв'язку. Запропонований підхід дозволить уникнути термінологічних колізій серед понять, які не визначені в оперативно-розшуковому законодавстві, але широко використовуються в оперативній практиці або не відображені в юридичній науці, однак застосовуються суб'єктами нормотворчої діяльності у відповідних відомчих актах, що мають відношення до сфери конфіденційного співробітництва [2, с. 73].

Як відомо, в оперативній практиці під зв'язком оперпрацівника і конфідента (далі – виконавців завдань ОРД) розуміється їх взаємне сповіщення про необхідність зустрічі, а також конспіративне спілкування, яке надає можливість здійснювати взаємний обмін оперативно-розшуковою інформацією (далі – ОРІ) [3]. Особиста конспіративна зустріч залишається для цих виконавців основним способом їх зв'язку. Однак, при певних негативних умовах, проведення таких зустрічей неможливо внаслідок загроз особистій

безпеці, передусім, конфідента. У непередбачуваних випадках альтернативою «живому» (безпосередньому) конспіративному спілкуванню виконавців завдань ОРД виступає їх зв'язок за допомогою інформаційно-телекомунікаційних систем або через посередників (наприклад, утримувачів т. зв. поштових скриньок, володільців конспіративних телефонів тощо), тобто використовується посередницький зв'язок.

На сьогодні юридична практика визначає посередництво (англ. mediation) як медіацію – дію, що пов'язана із пошуком взаємоприйнятного рішення між жертвою та правопорушником за посередництва компетентної особи (медіатора) [4]. Законодавець пов'язує комерційне посередництво та агентську діяльність у сфері господарювання [5], але жодні його визначення посередництва не стосуються зв'язку виконавців завдань ОРД. Тому, на нашу думку, оперативно-розшукова практика часто вдається до використання спеціально підібраного і підготовленого негласного співробітника – посередника – для забезпечення конспіративності, своєчасності та стійкості зв'язку працівника оперативного підрозділу з конфідентом. Така особа, насамперед, відбирається з оточення конфідента і має можливість тривало контактувати з ним, при цьому не викликати уваги з боку осіб, які знаходяться із конфідентом у певних відносинах, наприклад, є учасниками організованого злочинного угруповання. У конкретних ситуаціях без посередника достатньо складно створити необхідні умови для зв'язку в інтересах ОРД.

На наш погляд, ще на стадії безпосереднього (особистого) зв'язку конфідента з оперативним співробітником, коли використовується єдиний канал передавання ними ОРІ, вже виникають проблеми узгодженості дій щодо взаємного сповіщення цих виконавців завдань ОРД про необхідність зустрічі, їх конспіративного спілкування та обміну матеріалами. В інформатиці під каналом зв'язку або каналом передачі даних (англ. channel чи dataline) розуміють систему технічних засобів та середовище розповсюдження сигналів для односторонньої передачі інформації (даних) від джерела до отримувача [6]. На нашу думку, до каналу зв'язку виконавців завдань ОРД відноситься сукупність засобів і способів, що використовуються конфідентом для пересилання інформації через середовище до оперативного працівника й отримання від останнього інструкцій, завдань, матеріальних засобів на проведення зазначеної діяльності. З огляду на запропоноване вище тлумачення каналу зв'язку з виконавцями завдань ОРД, доцільно віднести до категорії засобів оперативно-розшукової діяльності, так як посередник є тим об'єктом матеріального світу, за допомогою якого конфідент і оперпрацівник користуються для пересилання ОРІ через певне середовище. При цьому, вищезгадана своєчасність посередницького зв'язку забезпечується взаємним сповіщенням виконавців завдань ОРД про його необхідність, тому вона прямо залежить від характеристик обраних каналів (явка зв'язного по паролю, відправлення листа, залишення матеріалів в обумовленому місці тощо). Вважаємо, що стійкість зв'язку пов'язана, передусім, із стійкістю як властивістю цих каналів та, після чого, лише з їх кількістю. Конспіративність же у посередницькому зв'язку взаємопов'язана з надійністю способів передачі інформації по обраних каналах та через підібраних третіх осіб. Отже,

конспіративність, своєчасність і стійкість як складові посередницького зв'язку виконавців завдань ОРД взаємопов'язано залежать від обраних останніми варіантів сповіщення про необхідність обміну інформацією. Зазначене вище, на наш погляд, демонструє можливість використання певних алгоритмів у посередницькому зв'язку. Ці алгоритми розраховані на типові ситуації в системі вимірів, що забезпечують прийняття оптимальних рішень у процесі здійснення виконавцями завдань ОРД зв'язку через посередників. Взагалі конспіративному зв'язку з використанням посередників передує захід (система дій), об'єднаний єдиним задумом та спрямований на досягнення мети скрито передати конфіденційну інформацію, що, як відомо, є різновидом операції [7]. При виникненні конкретної оперативної ситуації співробітник оперативного підрозділу не завжди має достатній практичний досвід, який можна застосувати до неї, а відомчі нормативні документи по цій ситуації носять, як правило, загальний, рекомендаційний характер. Тому, оперативні працівники-початківці намагаються використати здоровий глузд – погляди, що стихійно складаються під впливом повсякденного досвіду людей [8]. Однак, і співробітники із незначним стажем практичної роботи зможуть значно краще вирішувати оперативно-розшукові завдання, якщо будуть опиратися на готові схеми, алгоритми, чим на «здорові міркування» своїх зв'язків, іноді випадкових.

На нашу думку, застосування алгоритмічного підходу при побудові посередницького зв'язку, однаково придатне на практиці як у випадку підтримання спілкування виконавцями завдань ОРД через третіх осіб звичайним, «класичним» способом, так і при використанні замість посередників сучасних технологій. У такій спосіб більш вірогідніше зменшити кількість проблемних ділянок певного вектору зв'язку виконавців завдань ОРД. Наприклад, сучасне програмне забезпечення Telegram [9] із закритим кодом й інші захисні месенджери (англ. Instant messaging – служба миттєвих повідомлень) із задіянням технологій Tor і blockchain сприяють забезпечуванню недосяжного стороннім особам обміну інформацією, чим зумовлюється сьогоднішній інтерес до месенджерів і деяких апаратно-програмних засобів як інструменту створювання належних умов посередницького зв'язку виконавців завдань ОРД. Водночас, так звані оверлейні мережі (оверлейні – англ. Overlay Network – комп'ютерні мережі, що надбудовані над іншими мережами або глобальною мережею для досягнення анонімності) створюють поверх мережі Інтернет скриті від сторонніх осіб канали передачі інформації, що дозволяє проводити відеоконференції та забезпечувати обмін документами з обмеженим доступом [10], тобто практично створювати належні умови проведення виконавцями завдань ОРД особистих зустрічей. Разом з тим, стеганографічне (у перекладі з грецької мови означає «таємне» і «пишу») перетворення (вбудовування інформації в певний об'єкт (контейнер), який передається відкритими каналами зв'язку) і деякі інші технології сучасної стеганографії дозволяють забезпечувати закритий від сторонніх осіб обмін інформацією. На тлі обмеження на використання засобів криптографічного захисту інформації в окремих країнах світу та нових технологічних можливостей для діяльності

спеціальних служб [11] зумовлюється сьогоднішній інтерес до комп'ютерної та, насамперед, цифрової стеганографії як альтернативи створювання належних умов безособистого зв'язку виконавців завдань ОРД.

Взагалі чинник застосування технічних засобів має суттєве значення у забезпеченні стійкого, своєчасного конспіративного зв'язку між виконавцями завдань ОРД у вигляді пересилання інформації конфідента через середовище до оперативного працівника й отримання від останнього інструкцій, завдань, матеріальних засобів на проведення зазначеної діяльності. Техніка невіддільна від законів розвитку суспільства тому, що вона є соціальним феноменом та закономірності розвитку науки і техніки притаманні й для ОРД [12]. Їх уплив виявився у широкому впровадженні в практику технічних засобів. Цей процес знайшов відображення у теорії ОРД, передусім серед вітчизняних науковців, якими визначено технічні засоби як окрему групу серед інших засобів ОРД. Водночас теорія ОРД спрямована на розроблення методів, тактичних прийомів та засобів отримання, передавання, аналізу, оцінки й реалізації ОРІ. Водночас, потребує уточнення саме поняття «технічні засоби» через призму розгляду форми, напрямів та способів використання техніки у забезпеченні зв'язку виконавців завдань ОРД, а також визначення в ньому ролі і місця посередників. Тому й необхідно розробити концептуальні положення підготовки оперпрацівників і конфідентів до використання такої техніки. Під нею, на наш погляд, необхідно розуміти сукупність технічних, програмних засобів, науково обґрунтованих способів і тактичних прийомів їх використання виконавцями завдань ОРД з метою забезпечення конспіративного, своєчасного та стійкого зв'язку між ними.

Список використаних джерел:

1. Глушков В.О., Білічак О.А., Найдьон Ю.О. / Основи оперативно-розшукової діяльності / Підручник – К., НА СБ України: 2014. – 300 с.

2. Бандурка О.М. / Оперативно-розшукова діяльність / Підручник. Ч. 1. – Х., НУ МВС України, 2002. – 245 с., с. 73.

3. Овчинский С.С. / Оперативно-розыскная информация / под ред. А.С. Овчинского и В.С. Овчинского. – М., 2000. – С. 18.

4. О положении жертв преступлений в уголовном судопроизводстве: решение Совета Европейского Союза от 15 марта 2001 г. // Вестник восстановительной юстиции. – М.: Юристъ, 2002. – Вып. 4. – С. 72-77.

5. Господарський кодекс України / Відомості Верховної Ради України (ВВР), 2003, № 18, № 19-20, № 21-22, ст. 144 / [Электронный ресурс] Режим доступа: http://zakon3.rada.gov.ua/laws/show/436-15/page9

6. Толстолуцкий В.Ю. Криминалистическая информатика на современном этапе развития // Криминалистика, криминология и судебные экспертизы в свете системно-деятельностного подхода. Ижевск, 2001. – Вып. 3. – С. 17.

7. Вентцель О.С. «Исследование операцій». – М. / Наука, 2008. – С. 15.

8. Белкин Р.С. Криминалистическая энциклопедия. – М., 1997. – С. 103.

9. Журнал «Хакер», № 3(206), ООО «Эрсиа». – М., 2016. – С. 13.

10. Statistics website for the I2P network: [Електронний ресурс] / Режим доступу: www/ URL: ttp://i2pstats.loria.fr/?sect=historical&subsect_hist=routers

11. Мельник С.В., Кащук В.І. Методи цифрової стеганографії: стан та напрями розвитку / С. В.Мельник, В.І. Кащук // Інформаційна безпека людини, суспільства, держави. – К.: Наук.-вид. відділ НА СБ України, № 3(13) 2013 р. – С. 65-70.

12. Хараберюш І.Ф. Сучасні проблеми використання спеціальної техніки в оперативно-розшуковій діяльності органів внутрішніх справ / І.Ф. Хараберюш // Проблеми правознавства та правоохоронної діяльності – Донецький юридичний інститут МВС України: № 2 2009 р. – С. 237-245.

Перун С.В.
викладач юридичних дисциплін,
Полтавський кооперативний технікум

ЗАСТОСУВАННЯ ДОМАШНЬОГО АРЕШТУ ЯК ЗАПОБІЖНОГО ЗАХОДУ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Кримінальний процесуальний кодекс України (далі – КПК України) [1] вніс суттєві зміни до існуючої системи заходів кримінального процесуального примусу. Не оминули вони і таку важливу складову, як запобіжні заходи. Так, були включені нові запобіжні заходи, що можуть бути застосовані під час кримінального провадження: особисте зобов'язання, домашній арешт. Для вітчизняного кримінального процесуального законодавства особливої уваги заслуговує домашній арешт.

Законодавство багатьох держав світу передбачає застосування домашнього арешту як запобіжного заходу. Зокрема, він передбачений у таких країнах, як Білорусія, Казахстан, Латвія, Литва, Німеччина, Росія, Швеція та в багатьох інших. Однак, практика його застосування в цілому у порівнянні з іншими запобіжними заходами є не значною, що призводить до деяких ускладнень. Цей захід є одним з п'яти запобіжних заходів, передбачених кримінальним процесуальним законодавством і суворішим від нього є лише тримання під вартою. Домашній арешт доволі активно застосовується в нашій державі: згідно статистики він складає близько 20% від усіх обраних запобіжних заходів, при цьому у 90% випадків слідчі судді задовольняють клопотання правоохоронців про його застосування.

Відповідно до ст. 181 КПК України домашній арешт полягає в забороні підозрюваному, обвинуваченому залишати житло цілодобово або у певний період доби. Точна адреса житла, а також час, протягом якого особа зобов'язана знаходитися вдома, визначається суддею в кожному окремому випадку і вказується у відповідній ухвалі. Особі може бути заборонено виходити з дому як цілодобово, так і протягом певного часу (наприклад в нічний час з 23.00 по 07.00). Житло, в якому здійснюється домашній арешт, не обов'язково має належати на праві власності саме підозрюваному. Це може бути будь-яке приміщення пристосоване для проживання, яке знаходиться в постійному чи тимчасовому володінні підозрюваного (наприклад, орендована квартира).

Жодних обмежень щодо занять, зустрічей, телефонних розмов, користування Інтернетом чи іншими засобами зв'язку тощо для особи, яка перебуває під домашнім арештом, законодавством не встановлено. Головним