УДК 343.321.3 303.717

# СУЧАСНІ КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ ДЛЯ ПОСЕРЕДНИЦЬКОГО ЗВ'ЯЗКУ В КОНФІДЕНЦІЙНОМУ СПІВРОБІТНИЦТВІ

Куцій М.С., викладач
спеціальної кафедри
*Національна академія Служби безпеки України*

У статті розглянуто змістову сутність і призначення посередницького зв'язку для обміну оперативно-розшуковою інформацією. Наведено різні наукові підходи до поняття «посередник» і запропоновано визначення «посередник» як засіб оперативно-розшукової діяльності. Вивчено перспективи підвищення своєчасності, стійкості й конспіративності передавання інформації за рахунок упровадження технологій, заснованих на практичному застосуванні комп'ютерних програмних продуктів із закритим похідним кодом. Особливу увагу приділено способам алгоритмізації посередницького зв'язку, у т. ч. із застосуванням програмно-апаратних засобів передавання даних у глобальній мережі. Запропоновано визначення поняття «канал зв'язку», що створюється учасниками оперативно-розшукової діяльності.

***Ключові слова:*** *оперативно-розшукова інформація, конфіденційне співробітництво, посередницький зв'язок, посередник, алгоритмізація посередницького зв'язку, канал зв'язку.*

В статье рассмотрены содержательная суть и предназначение посреднической связи для обмена оперативно-розыскной информацией. Приведены разные научные подходы к понятию «посредник» и предложено определение «посредник» как средство оперативно-розыскной деятельности. Изучены перспективы повышения своевременности, стойкости и конспиративности передачи информации за счет внедрения технологий, основанных на практическом применении компьютерных программных продуктов с закрытым исходным кодом. Особое внимание уделено способам алгоритмизации посреднической связи, в т. ч. с применением программно-аппаратных средств передачи данных в глобальной сети. Предложено определение «канал связи», что создается участниками оперативно-розыскной деятельности.

***Ключевые слова:*** *оперативно-розыскная информация, конфиденциальное сотрудничество, посредническая связь, посредник, алгоритмизация посреднической связи, канал связи.*

Kutsii M.S. MODERN COMMUNICATION TECHNOLOGIES FOR THE COMMUNICATION VIA AN INTERMEDIARY BY THE CONFIDENTIAL COLLABORATION

In the article the author considers the content and function of communication via an intermediary for the exchange of operational and investigational information. Scientific views of various authors' assessment on the theoretical basis of intermediator as way of the operational investigative activity are presented. The prospects of increasing timeliness, duration and clandestinely of information transfer for account of technologies implementation witch practical used of PC programs with original code. The special attention is given to methods of algorithmization communication via an intermediary in the global network. The definition of channel of communication is formulated.

***Key words:*** *operational investigative information, confidential collaboration, communication via an intermediary, intermediator, algorithmization of communication via an intermediary, channel of communication.*

**Постановка проблеми.** В оперативно-розшуковій діяльності (далі – ОРД) з метою вирішення її завдань використовується інститут конфіденційного співробітництва. Особи, які залучаються для виконання цих завдань, підлягають захисту [1]. Науково-практичному аналізу проблем використання відносин конфіденційного співробітництва в діяльності уповноважених державних органів із розкриття й розслідування злочинів, а також забезпечення державної безпеки присвячені наукові праці вітчизняних і зарубіжних авторів, серед яких О.М. Бандурка, Б.І. Бараненко, Р.С. Белкін, І.І. Бранчель, Е.О. Дідоренко, О.М. Джужа, В.О. Козенюк, В.Г. Пилипчук, С.С. Овчинський, М.О. Шилін, О.Ю. Шумилов, А.М. Хлус та інші. Більшість праць цих учених мають закритий характер, тому в науці ОРД не спостерігається однозначних підходів до визначення змісту поняття способів зв'язку оперативних працівників уповноважених суб'єктів з особами (конфідентами), які на засадах добровільності й конфіденційності виконують завдання ОРД.

При певних умовах неможливе проведення особистої конспіративної зустрічі (основний спосіб зв'язку в ОРД) між конфідентом і оперативним співробітником для обміну оперативно-розшуковою інформацією. Тому зазначені учасники ОРД використовують посередників, які підбираються співробітниками оперативних підрозділів з оточення конфідентів для підтримання конспіративного зв'язку. У практиці ОРД такий зв'язок називають посередницьким, але він залишається достатньо невизначеним із погляду юридичної науки, як і поняття «канал зв'язку», що створюється учасниками ОРД. Сучасні Telegram й інші захисні месенджери (англ. Instant messaging – служба миттєвих повідомлень) та окремі телекомунікаційні технології дають змогу забезпечувати закритий від сторонніх осіб обмін інформацією. Унаслідок зростання конфіденційності інформаційно-телекомунікаційних технологій і зумовлюється сьогоднішній інтерес до месенджерів і деяких апаратно-програмних засобів як інструмента створювання належних

умов посередницького зв'язку учасників ОРД. Тому впровадження алгоритмів і програм як рекомендацій щодо застосування тих чи інших конспіративних способів зв'язку з використанням посередників для уповноважених законом оперативних підрозділів має практичне значення. Такі рекомендації матимуть вигляд нетаємних документів періодичного видання, що передбачають комплексне використання засобів технічного і криптографічного захисту оперативно-розшукової інформації, технологічний та організаційний аспект зв'язку учасників ОРД.

**Ступінь розробленості проблеми.** За результатами аналізу наукових джерел установлено, що в теорії ОРД не досліджено проблеми алгоритмізації зв'язку між учасниками ОРД – оперативним працівником і конфідентом, у т. ч. не з'ясовано закономірностей застосування алгоритмів і програм у конспіративному обміні оперативно-розшуковою інформацією з використанням посередників. Відсутні однозначні погляди щодо визначення змісту понять «посередницький зв'язок» (як одного зі способів зв'язку між учасниками ОРД), «посередник» і «канал зв'язку».

**Метою статті** є дослідження можливості використання на практиці захисних месенджерів та окремих комп'ютерних програмних засобів в інтересах ОРД, зокрема, для здійснення її учасниками конспіративного посередницького зв'язку.

**Виклад основного матеріалу.** Законодавець визначає інформацію як будь-які відомості й (або) дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [2]. Закон України «Про інформацію» передбачає види інформації за її змістом, у т. ч. соціологічну – будь-які документовані відомості про ставлення до окремих осіб, подій, явищ, процесів, фактів тощо. Законодавство визначає документом матеріальний носій, що містить інформацію, основними функціями якого є її збереження й передавання в часі та просторі [2, ст. 1]. На думку С.С. Овчинського, від інших видів соціальної інформації оперативно-розшукову інформацію відрізняє специфіка джерел, методів і тактичних прийомів отримання та використання [3]. За словами О.М. Бандурки, «конфіденти – це приватні фізичні особи, з якими оперативні підрозділи органів, уповноважених здійснювати ОРД, встановили на платній чи безоплатній основі відносини співробітництва, передбачаючи надання такими громадянами вказаним операпаратам сприяння на конфіденційній основі у виконанні покладених на них завдань» [4]. Учені А.М. Хлус, І.І. Бранчель уважають, що з конфідентами встановлюється співробітництво виключно на негласній основі. Без допомоги конфідентів не можна ефективно боротися зі шпигунством, тероризмом, а також організованою злочинністю [5]. Зв'язок конфідента та співробітника оперативного підрозділу є складовою вищезазначених відносин співробітництва. Під таким зв'язком розуміється взаємне сповіщення учасників ОРД про необхідність зустрічі, а також саме конспіративне спілкування, що надає можливість здійснювати взаємний обмін інформацією. Важливішою вимогою до зв'язку конфідента з оперпрацівником є конспіративність, яка досягається шляхом використання способів зв'язку відповідно до конкретних умов. Виникнення під час ОРД непередбачуваних ситуацій вимагає від такого зв'язку ще й стійкості. Під нею розуміється певна організація, коли забезпечується регулярність і систематичність спілкування учасників ОРД при різних труднощах та обставинах, що перешкоджають зв'язку, тобто стійкість зв'язку означає постійну готовність до його здійснення. Поряд зі стійкістю вимогою до зв'язку учасників ОРД є його своєчасність, тобто встановлення зв'язку тоді, коли виникає така необхідність. Своєчасність зв'язку викликається певними обставинами: терміновістю прийняття управлінських рішень за окремими фактами, з якими під час виконання завдань ОРД зіштовхується конфідент, виникненням додаткових питань до оперпрацівника або раптовими змінами ситуації, що потребує корегування подальших заходів ОРД чи скасування поточного завдання. Своєчасність зв'язку забезпечується обранням надійних способів взаємного термінового сповіщення, а також використанням дублюючих способів зв'язку, тобто впровадженням на практиці односторонніх чи двосторонніх способів екстреного зв'язку. Отже, конспіративність, стійкість і своєчасність є складовими надійності зв'язку оперативного працівника з конфідентом під час вирішення оперативно-розшукових завдань. Зв'язок здійснюється за двома формами: безпосередньо, шляхом особистого спілкування (особистий зв'язок) чи за допомогою дротового телефонного й телеграфного та звичайного поштового зв'язку, сучасних інформаційно-телекомунікаційних систем або через посередників. Тому на практиці відрізняють дві форми особистого зв'язку оперативних співробітників із конфідентами: форму безпосереднього зв'язку та посередницького зв'язку. За кожною формою застосовуються свої способи зв'язку. Але в статті розглядаються аспекти посередницького зв'язку між учасниками ОРД, тобто через третю особу-посередника, у т. ч. з використанням цією особою сучасних інформаційних технологій, зокрема захисних месенджерів. Із практики відомо, що за певних негативних умов особистим зустрічам конфідента й оперпрацівника загрожує викриття факту їх спілкування сторонніми особами. Наприклад, учасниками організованого злочинного угруповання із жорсткою підзвітністю щодо контактів поза угрупованням, до якого під прикриттям уведено цього негласного співробітника. На нашу думку, у наведеному чи подібних випадках посередницький зв'язок більш доцільний із погляду як його конспіративності, так і своєчасності й стійкості. Зокрема, у мегаполісах і великих містах під час проведення антитерористичних операцій (наприклад, листопад 2015 р. в Парижі та березень 2016 р. в Брюсселі) [6] припиняються послуги стільникового телефонного зв'язку й рух громадського транспорту, але Інтернет-провайдерам держава залишає можливість передавати

телекомунікаційними мережами фото-, відеоконтент користувачів із місць подій, тобто в умовах терористичної загрози наявні технічні канали взаємного сповіщення через глобальну мережу. Наприклад, 13 листопада 2015 р. в Парижі терористи організовували шифровані комунікації із задіянням технологій Tor і blockchain, а також використовували Telegram та інші захисні месенджери [7]. Зокрема, розроблене в Санкт-Петербурзі кросплатформове програмне забезпечення Telegram із закритим кодом для передавання повідомлень працює на потужностях кількох американських і німецьких компаній, завдяки його патентуванню на сьогодні майже виявлені уразливості месенджера не дають змоги «зламати» його захист від читання листування в чаті. Інформація в Telegram у зашифрованому вигляді зосереджується на хмаровому хостингу, а сервери розміщено в різних країнах, що надає можливість миттєво розсилати повідомлення. Листування розробником не зберігається заради таємності ключів шифрування, які для кожної пари осіб, що спілкуються за конкретний проміжок часу, лише свої. Ключі зберігаються від інших даних окремо, у різних юрисдикціях і лише на період спілкування осіб. У Telegram передаються файли розміром до 1 Гб і створюються мультичати до 100 осіб. Сьогодні всі ці переваги викликали зростаючу популярність цього месенджера, порівняно з іншими, у США, Чилі, Бразилії, Мексиці, Німеччині, Нідерландах,Іспанії, Італії та країнах Близького Сходу. Водночас бойова обстановка перешкоджає використанню провайдерських послуг. І якщо в оточенні військового формування є діючі дротові телефонні й телеграфні лінії, вони придатні для зв'язку учасників ОРД. Зокрема, з телеграфу населеного пункту конфідент надсилає до штабу військової частини на умовне прізвище телеграму із заздалегідь обумовленим змістом. Через посередника, наприклад, військового листоношу, такі телеграми доставляються до оперативного підрозділу. Інші посередники-власники квартирних телефонів задіяні для організації зв'язку з негласними працівниками. Конфідент дзвонить на відомий номер телефону та передає умовне повідомлення. Посередник не з'ясовує, з ким він спілкується, приймає повідомлення та дослівно й невідкладно доводить його зміст до оперативного співробітника. Як правило, такі особи є завідувачами аптеки, бібліотеки, автомайстерень та інших установ, до яких населення звертається за відповідними послугами. Змістом повідомлення визначається, хто є ініціатором особистої зустрічі. За наявності часу й із урахуванням інших умов учасники ОРД користуються так званими поштовими скриньками (для конспіративного забезпечення роботи скриньок також задіються представники сфери послуг). У приміщенні установи, де працює посередник, конфідент в обумовленому місці залишає в закритому вигляді річ (коробку цукерок, блок цигарок, книгу або конверт із листом (запискою) на умовне ім'я) чи інший закамуфльований контейнер із документом, у т. ч. й електронним. Посередник своєчасно сповіщає оперпрацівника щодо отримання контейнера або особисто доставляє документ до нього. Визначення поштової скриньки міститься в Контррозвідувальному словнику КДБ при РМ СРСР (1972 р. видання), який у PDF-файлах поширено в мережі Інтернет [8]. Зокрема під нею розуміється «конспіративний явочний пункт», на якому конфідент вручає свої повідомлення й інші матеріали посереднику для подальшої їх передачі оперпрацівнику і де він (конфідент) знайомиться з письмовими інструкціями оперативного співробітника. Указаний словник не дає поняття «посередник». Юридична практика визначає посередництво (англ. mediation) як медіацію – дію, що пов'язана з Рішенням Ради Європейського Союзу від 15 березня 2001 р. в пошуку взаємоприйнятного рішення між жертвою та правопорушником за посередництва компетентної особи (медіатора) [9]. Законодавець пов'язує комерційне посередництво й агентську діяльність у сфері господарювання [10], але жодні його визначення посередництва не стосуються зв'язку учасників ОРД. Тому, на нашу думку, оперативно-розшукова практика часто вдається до використання спеціально підібраного й підготовленого негласного співробітника – посередника – для забезпечення конспіративності, своєчасності та стійкості зв'язку працівника оперативного підрозділу з конфідентом. Така особа насамперед відбирається з оточення конфідента й 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 роботи з конфідентом в інтересах ОРД. Зокрема, з практики зафронтової роботи «Смерш» відомо [11], що в 1944 р. підбір і підготовку власних зв'язних у тилу супротивника здійснювали негласні працівники, які й перекидалися через лінію фронту. Тоді з міркувань конспірації перекинення їх на літаках виключалося й негласні співробітники лише пішки перетинали лінію фронту і своїм ходом направляли вже придбаних на місці зв'язних до партизанських таборів або знову відправляли їх через лінію фронту. Двосторонній зв'язок у той час був узагалі під забороною. У 1944 р. конспіративність зв'язку з негласними помічниками ставилася співробітниками «Смерш» понад його стійкості і своєчасності. Тому на визвольній від німецьких загарбників території ці негласні працівники користувалися виключно посередницьким зв'язком [11, с. 474–475] за такими варіантами:

– явка по паролю підготовленого зв'язного до представника «Смерш»;

– відправлення зв'язним листа негласного помічника на домашню адресу придбаного останнім утримувача «поштової скриньки»;

– залишення зв'язним в обумовленому місці матеріалів, зібраних негласним співробітником для передання оперпрацівнику «Смерш»;

– використання «втемну» місцевого жителя, який із прибуттям частин Радянської Армії знаходив співробітника «Смерш» і повідомляв

інформацію щодо нового місцезнаходження негласного помічника та характеру його роботи.

При цьому негласний працівник в обов'язковому порядку та ще до свого перекидання в тил супротивника отримував відповідні паролі на випадок направлення за ним через лінію фронту додаткового зв'язного.

На нашу думку, ще на стадії безпосереднього (особистого) зв'язку конфідента з оперпрацівником, коли присутні дві особи (n=2) та використовується єдиний канал передавання ними оперативно-розшукової інформації (k=1), уже виникають проблеми узгодженості дій щодо взаємного сповіщення цих двох учасників ОРД про необхідність зустрічі, конспіративного їх спілкування та обміну зазначеною інформацією лише через один канал (рис. 1). В інформатиці під каналом зв'язку або каналом передачі даних (англ. channel чи data line) розуміють систему технічних засобів і середовище розповсюдження сигналів для односторонньої передачі інформації (даних) від джерела до отримувача. Як нам видається, до каналу зв'язку учасників ОРД належить сукупність засобів і способів, що використовуються конфідентом для пересилання інформації й матеріалів через середовище до оперативного працівника та отримання від останнього інструкцій, завдань, матеріальних засобів на проведення зазначеної діяльності. З огляду на запропоноване визначення каналу зв'язку утримувача «поштової скриньки», зв'язного чи іншого посередника в підтриманні зв'язку з учасниками ОРД доцільно зарахувати до категорії засобів оперативно-розшукової діяльності, так як посередник є тим об'єктом матеріального світу, за допомогою якого конфідент і оперпрацівник користуються для пересилання оперативно-розшукової інформації через певне середовище.

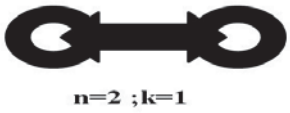


**Рис. 1. Граф обміну інформацією зі взаємним сповіщенням двох учасників ОРД**

У разі використання посередницького зв'язку в ОРД кількість її учасників одразу зростає мінімум до трьох (n=3), у цьому випадку збігається з кількістю каналів передавання інформації (k=3), але водночас припустимо й те, що й кількість проблем узгодженості дій конфідента, посередника та оперпрацівника пов'язана з кількістю каналів при їх зростанні. Наприклад, залучення до взаємного сповіщення трьох учасників ОРД ще й четвертої або п'ятої особи (начальник оперативного співробітника, утримувач «поштової скриньки» чи додатковий зв'язний тощо) призведе до зростання каналів зв'язку (рис. 2) за формулою: $k = (n * (n-1)) / 2$ (1).

(1)

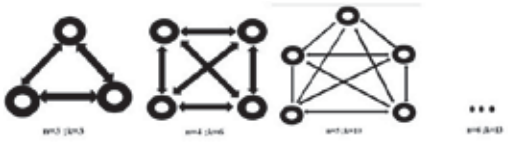

**Рис. 2. Графи обміну інформацією зі взаємним сповіщенням трьох і більше учасників ОРД**

Зокрема, для трьох осіб: n=3 і k=3, чотирьох осіб: n=4 і k=6, п'ятьох осіб: n=5, k=10 і шести осіб: n=6 і k=13. Тому, на нашу думку, у 1944 р. «Смерш» у посередницькому зв'язку із трьох осіб (n=3) вирішив проблеми взаємного сповіщення за рахунок його стійкості і своєчасності й на користь конспіративності (рис. 3), так як існувала реальна загроза виявлення десантування зв'язних. При цьому кількість задіяних каналів (k=3) залишалась незмінною.

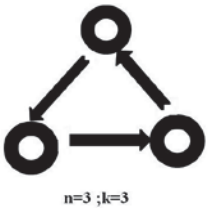


**Рис. 3. Варіант обміну інформацією без взаємного сповіщення для трьох осіб**

Водночас на практиці при використанні посередницького зв'язку обов'язковість взаємного сповіщення трьох чи більше учасників ОРД (конфідент, оперпрацівник, утримувач «поштової скриньки» або зв'язний за телефоном тощо) може регулюватися його ініціатором (конфідентом або оперативним співробітником). Залежно від прийнятого рішення щодо взаємного сповіщення цих учасників знаходиться й кількість обраних каналів зв'язку (рис. 4), яка вже не буде розраховуватись за зазначеною вище формулою (1). Тому ми вважаємо, що обрані варіанти посередницького зв'язку взаємопов'язані з рішенням одного з учасників ОРД. Як, наприклад, наведені у статті варіанти зв'язку «Смерш», що використовувались у 1944 р.

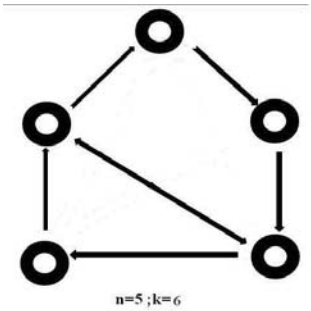


**Рис. 4. Варіант обміну інформацією п'ятьох осіб зі взаємним сповіщенням за одним каналом**

Із вищезазначеного відомо, що своєчасність посередницького зв'язку забезпечу-

ється взаємним сповіщенням учасників 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). На нашу думку, стійкість зв'язку пов'язана передусім зі стійкістю як властивістю цих каналів і після чого лише з їх кількістю. Конспіративність же в посередницькому зв'язку взаємопов'язана з надійністю способів передачі інформації по обраних каналах і підібраних зв'язних (інших посередників). Отже, конспіративність (К.), своєчасність (Св.) і стійкість (Ст.) як складові посередницького зв'язку оперпрацівника з конфідентом під час вирішення оперативно-розшукових завдань взаємопов'язано залежать від обраних учасниками ОРД ★(позначені зіркою) варіантів сповіщення про необхідність обміну інформацією (рис. 5). Зазначене, як нам видається, 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 учасниками ОРД зв'язку через утримувачів поштових скриньок, зв'язних та інших посередників.

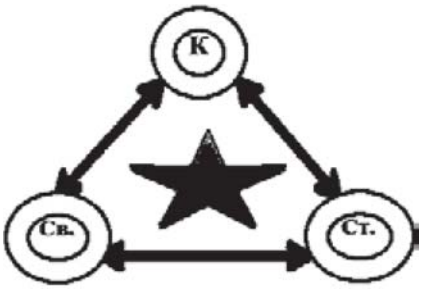


**Рис. 5. Граф складових посередницького зв'язку учасників ОРД**

Узагалі конспіративному зв'язку з використанням посередників передує захід (система дій), об'єднаний єдиним задумом і спрямований на досягнення певної мети (у нашому випадку скрито передати конфіденціальну інформацію), що, як відомо, і є операцією [12]. На нашу думку, проведення посередницького зв'язку як різновиду операції завжди є керованим заходом, тобто від оперпрацівника та конфідента залежить обрання деяких параметрів, що характеризують організацію цього обміну інформацією як операції. Під організацією варто розуміти варіант, що обраний (іншими словами, застосований набір засобів) при передаванні даних за визначеним каналом зв'язку між оперативним співробітником (конфідентом) і посередником. Певний вибір параметрів, залежних від учасників ОРД, буде їх рішенням. Оптимальними називаються рішення, які за різними ознаками є переважними перед іншими. Зокрема, у 1944 р. «Смерш» оптимальним варіантом обрав зв'язок із негласними помічниками через зв'язних, які направлялися пішим порядком через лінію фронту. У такий спосіб посередницький зв'язок підтримувався на той час лише на ділянках відповідальності 1-го та 2-го Білоруських фронтів. Тобто, зміст певних стадій посередницького зв'язку (наприклад, оперпрацівник – зв'язний – конфідент або конфідент – «поштова скринька» – оперативний співробітник тощо) також залежить від середовища його здійснення та вимагає системи, що працює завдяки чіткому алгоритмові. Розроблення такого алгоритму завжди будується на попередніх розрахунках, тобто на дослідженні операцій. Саме попереднє кількісне обґрунтування оптимальних рішень і є дослідженням операцій [12. с. 17]. У разі виникнення конкретної оперативної ситуації співробітник оперативного підрозділу не завжди має достатній практичний досвід, який можна застосувати до неї, а чинні нормативні документи правоохоронного органу по цій ситуації мають, як правило, загальний, рекомендаційний характер. Тому оперативні працівники-початківці намагаються використати здоровий глузд – погляди, що стихійно складаються під впливом повсякденного досвіду людей [13]. Однак і співробітники з незначним стажем практичної роботи зможуть значно краще вирішувати оперативно-розшукові завдання, якщо будуть опиратися на готові схеми, алгоритми, ніж на «здорові міркування» своїх зв'язків, іноді випадкових. В інформатиці під алгоритмом розуміється точний припис, що визначає обчислювальний процес і веде від варійованих початкових даних до шуканого результату. А програма є описуванням алгоритму мовою програмування [14]. Тому оперативно-розшуковий алгоритм є, на нашу думку, науково обґрунтованим приписом щодо виконання оперативним працівником у заданому порядку системи послідовних дій для вирішення завдань ОРД певного типу, зокрема організації посередницького зв'язку з конфідентами. Зрозуміло, що запропонувати алгоритми в неординарних ситуаціях і запрограмувати нестандартні рішення посередницького зв'язку для учасників ОРД неможливо. Подібні алгоритми не можуть розглядатися як безумовний припис. Це лише рекомендації про раціональну послідовність дій конфідента, оперпрацівника з посередниками при організації обміну інформацією. На нашу думку, шукане рішення розробки алгоритмів і програм обміну оперативно-розшуковою інформацією при використанні посередницького зв'язку знаходиться в площині взаємозалежності елементів оперативної ситуації та дій із використанням певного набору засобів. Усі ці елементи індивідуальні саме для цього випадку зв'язку через посередників, незмінні протягом його та обов'язково враховуються оперпрацівником при підготовці такої акції зв'язку. Ученими М. Месконом, М. Альбертом і Ф. Хедоурі пропонується застосовувати так звану циклічну модель для дослідження комунікаційних проблем на основі структури цієї моделі та зв'язків між її елементами [15]. В інтерпретації елементний склад такої моделі дає змогу визначити групи перешкод, які стосуються такого: взаємовідносин учасників ОРД (1), змісту повідомлень з оперативно-розшуковою інформацією (2), їх кодування (декодування) й ідентичності (3) та каналу прямого і зворотного зв'язку (4).

При цьому окремі з дій, що залежать від елементів конкретної оперативної ситуації, уже достатньо алгоритмізовані, наприклад, збирання інформації щодо здатності утримувача «поштової скриньки» забезпечити її надійну роботу й обраного місця для вкладень із повідомленнями в приміщенні, планування порядку обміну закамуфльованого повідомленнями при зміні передбачуваних умов навколо місця розташування «поштової скриньки», засвоєння конфідентом послідовності дій при виникненні загрози захоплення повідомлення, розподіл функцій і ролів під час посередницького зв'язку та аналіз даних про конспіративність обраного варіанта його здійснення. Наукові дослідження [16] визначають дві складові комунікаційних проблем організації, якщо під нею розуміти групу осіб, об'єднаних виконанням певних завдань посередницького зв'язку. До першої належать проблеми структурних комунікацій, пов'язаних із бар'єрами в процесі передавання оперативно-розшукової інформації, а друга складова стосується міжособистісних комунікацій (поведінкових аспектів) учасників ОРД. Якщо міжособистісні комунікації впливають лише на індивідуальні особливості конфідента, оперпрацівника або посередників і контекст передачі цієї інформації, то основним фокусом структурних комунікацій є створення системи її передавання, що, як і було зазначено вище, працює завдяки чіткому алгоритмові. Такий алгоритм проведення акції зв'язку не є вичерпаним, але може слугувати «матрицею» для розроблення алгоритмічних дій посередницького зв'язку між конфідентом та оперпрацівником в інших ситуаціях. «Матриця» дає змогу під час планування акції зв'язку, особливо оперативними співробітниками-початківцями, заздалегідь розглянути можливість здійснення окремо взятої операції зв'язку за участю посередників через призму його конспіративності, стійкості та своєчасності. На нашу думку, збільшення ланцюгів посередницького зв'язку прямо збільшує вірогідність виявів суперечностей між його конспіративністю, стійкістю і своєчасністю. І кожне відхилення від запланованої учасниками ОРД швидкості передавання оперативно-розшукової інформації з пункту А до пункту В та її можливої модифікації посередниками приведе до недосягнення мети зв'язку за визначеним варіантом, тобто призведе до розпаду вектора зв'язку А-В на проблемні ділянки, що досліджуються окремо в методологічному та понятійному планах (рис. 6).

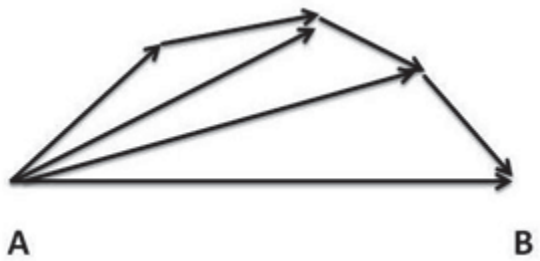


**Рис. 6. Граф варіантів відхилення від запланованої швидкості передавання інформації**

Але, як нам видається, застосування алгоритмічного підходу при побудові посередницького зв'язку однаково придатне на практиці як у випадку підтримання спілкування опер працівника з конфідентом через третю особу звичайним, «класичним» способом, так і при використанні, замість людей-посередників, телекомунікаційних мереж та інших сучасних технологій для проведення зв'язку між конфідентом і оперпрацівником. У такий спосіб вірогідніше зменшити кількість проблемних ділянок вектора зв'язку А-В учасників ОРД або зовсім уникнути їх виникнення (рис. 7). Наприклад, конфідент із числа військовослужбовців прикордонного наряду в лісо-степній смузі патрулювання залишає для оперпрацівника в заздалегідь обладнаному та відомому учасникам ОРД тайнику (дуплі дерева) вкладення (коробку сирників) із повідомленням, яке в зашифрованому вигляді (алфавітний код) містить оперативно-розшукову інформацію.

Посередник-місцевий житель (лісничий) забирає повідомлення та на власному володінні (жилплощі) перетворює його в електронний файл, досягаючи в такій спосіб приховування інформації, і, користуючись Telegram або іншим захисним месенджером, через телекомунікаційні канали доставляє її до оперпрацівника.

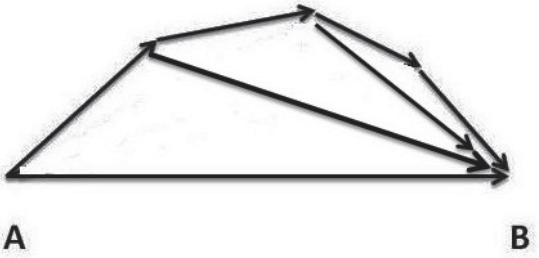


**Рис. 7. Граф варіантів прискорення передавання інформації**

Після отримання з мережі відповіді для конфідента посередник знову перетворює її на цифрові чи літерні позначення на папері та закладає зашифровану інформацію в іншому місці, відомому конфіденту. Обидва негласні співробітники незнайомі між собою, при цьому зміст повідомлення невідомий посереднику. У наведеному прикладі лісничий раптово не залишає місце роботи або оперативний працівник не прибуває до району патрулювання, тобто учасники ОРД знаходяться не в полі зору сторонніх осіб. Наявність у конфідента терміналів стільникового зв'язку чи інших телекомунікаційних пристроїв може викликати підозри в його оточенні. Однак у розглянутому прикладі кількість проблемних ділянок, на яких імовірне розпадання вищезгаданого вектора зв'язку прямо залежить від способу шифрування повідомлень, обраних місць тайників, незмінності графіку патрулювань, стану здоров'я посередника, сили телекомунікаційного сигналу тощо. На нашу думку, на практиці прогалини алфавітного кодування (їх можна порівняти із загрозою виявлення літаків німецькими радарами) швидше за все подолати архівацією з паро-

люванням електронного файлу за програмою WinRAR archiver з одночасним його розділенням на кілька частин за допомогою Hjsplit чи іншої загальновідомої програми та окремим передаванням цих частин різними каналами зв'язку до отримувача.

**Висновки.** Окремі сучасні інформаційно-телекомунікаційні технології відповідають вимогам конспіративності, стійкості і своєчасності передавання закритих відомостей між конфідентом і оперативним працівником та придатні для ефективного використання в обміні оперативно-розшуковою інформацією через посередників. У виправданих випадках технічні й програмні засоби зменшують кількість ланцюгів посередницького зв'язку, роблячи обмін відомостями між учасниками ОРД більш швидким та інформацію, що передається через негласних співробітників, більш захищеною до її модифікації. Поєднання посередницького зв'язку з відібраними телекомунікаційними технологіями має практичне значення для уповноважених законом оперативних підрозділів при організації конспіративного зв'язку з конфідентами. Тому, на нашу думку, доцільно розробити для учасників ОРД відповідні практичні рекомендації щодо застосування окремих сучасних технологій в організації посередницького зв'язку за різними оперативними ситуаціями.

**ЛІТЕРАТУРА:**

1. Про оперативно-розшукову діяльність : Закон України // Відомості Верховної Ради України. – 1992. – № 22. – Ст. 303. – С. 22.

2. Про інформацію : Закон України // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.

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

4. Бандурка О.М. Оперативно-розшукова діяльність : [підручник] / О.М. Бандурка. – Х. : НУ МВС України, 2002. – Ч. 1. – 2002. – 245 с. – С. 73.

5. Хлус А.М. Основы оперативно-розыскной деятельности : [учебник] / А.М. Хлус, И.И. Бранчель. – Минск : БГУ, ТетраСистемс, 2012. – 144 с.

6. Звернення віце-прем'єра Бельгії Олександра де Кру від 22.03.2016 р. до населення Брюсселя через мережу Twitter [Електронний ресурс]. – Режим доступу : https://twitter.com/alexanderdecroo/status/712232253200449537.

7. Журнал «Хакер». – 2016. – № 3 (206). – С. 13.

8. Контрразведывательный словарь. ВКШ КГБ при СМ СССР. – М., 1972. – 371 с. – С. 324. – [Электронный ресурс]. – Режим доступа : https://vk.com/doc 41072062_187231293? hash=932cfaf9d53cd8febc&dl=72886452c9ba8a9fd9.

9. 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.

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

11. Органы государственной безопасности СССР в Великой Отечественной войне : сборник документов / группа авторов-составителей под руков. В.П. Ямпольского. – М. : Куличково поле, 2007. – Т. 5. – Кн. 1. – 2007. – С. 473–474.

12. Вентцель О.С. Исследование операций / О.С. Вентцель. – М. : Наука, 2008. – С. 15.

13. Толстолуцкий В.Ю. Криминалистическая информатика на современном этапе развития / В.Ю. Толстолуцкий // Криминалистика, криминология и судебные экспертизы в свете системно-деятельностного подхода. – Ижевск, 2001. – Вып. 3. – С. 15.

14. Белкин Р.С. Криминалистическая энциклопедия / Р.С. Белкин. – М., 1997. – С. 103.

15. Мескон М.Х. Основы менеджмента / М.Х. Мескон, М. Альберт, Ф. Хедоури ; пер. с англ. – М. : Дело, 1997. – 704 с.

16. Фролов С.С. Социология организаций : [учебник] / С.С. Фролов. – М. : Гардарики, 2001. – 384 с.