УДК 343.321.3:303.717

КУЦІЙ М.С., викладач спеціальної кафедри Навчально-наукового інституту контррозвідувальної діяльності Національної академії СБ України

ЦИФРОВА СТЕГАНОГРАФІЯ ДЛЯ ТАЙНИКОВИХ ОПЕРАЦІЙ У КОНФІДЕНЦІЙНОМУ СПІВРОБІТНИЦТВІ

Анотація. *Розглянуто змістовну сутність та призначення тайникових операцій для обміну оперативно-розшуковою інформацією. Наведено різні наукові підходи до поняття “тайник”. Розглянуто перспективи підвищення ефективності особистих конспіративних зустрічей конфідента та оперативного працівника за рахунок впровадження технологій, заснованих на практичному використанні стеганографії. Особливу увагу приділено способам алгоритмізації тайникових операцій, в т.ч. у глобальній мережі.*

Ключові слова: *оперативно-розшукова інформація, конфіденційне співробітництво, тайник, алгоритмізація тайникових операцій, стеганограма.*

Аннотация. *Рассмотрены содержательная суть и предназначение тайниковых операций для обмена оперативно-розыскной информацией. Приведены разные научные подходы к понятию “тайник”. Рассмотрены перспективы повышения эффективности личных конспиративных встреч за счет внедрения технологий, основанных на практическом использовании стеганографии. Особое внимание уделено способам алгоритмизации тайникових операций, в т.ч. в глобальной сети.*

Ключевые слова*: оперативно-розыскная информация, конфиденциальное сотрудничество, тайник, алгоритмизация тайникових операций, стеганограмма.*

Summary. *In the article the author considers the content and function of cache action for the exchange of operational and investigational information. Scientific views of various authors' assessment on the theoretical basis of cache are presented. The prospects of increasing efficiency in personal secret meetings for collaborator and staffer due to the introduction of obtaining technologies based on practical use of steganography are considered. The special attention is given to methods of algorithmization of cache actions in the global network of participants of the operational investigative activity.*

Keywords*: operational and investigative information, confidential collaboration, cache, algorithmization of cache action, steganogram.*

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]. За певних умов неможливе проведення особистої конспіративної зустрічі (основний спосіб зв’язку в ОРД) між конфідентом та оперативним співробітником для обміну оперативно-розшуковою інформацією. Стеганографічне (у перекладі з грецької мови означає “таємне” і “пишу”) перетворення (вбудовування інформації в певний об’єкт (контейнер), який передається відкритими каналами зв’язку) [2] і деякі інші технології сучасної стеганографії дозволяють забезпечувати закритий від сторонніх осіб обмін інформацією. На тлі обмеження на використання засобів криптографічного захисту інформації в деяких країнах світу та нових технологічних можливостей для діяльності спеціальних служб [3, с. 66] і зумовлюється сьогоднішній інтерес до комп’ютерної та, насамперед, цифрової стеганографії (далі – ЦС) як інструменту створювання належних умов безособистого зв’язку учасників ОРД. Тому впровадження алгоритмів і програм, як рекомендацій по застосуванню тих чи інших конспіративних способів зв’язку із

використанням стеганометодів, 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.

Науково-практичному аналізу проблем використання відносин конфіденційного співробітництва у діяльності уповноважених державних органів із розкриття та 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, Е.О. Дідоренко, О.Д. Довгань, О.М. Джужа, В.О. Козенюк, О.Р. Лебедєв, В.Г. Пилипчук, М.О. Шилін, О.Ю. Шумилов та інші. Достатньо значна 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 і конфіденційності виконують завдання ОРД.

Крім зазначеного, за результатами аналізу наукових джерел встановлено, що в теорії ОРД не досліджувані проблеми алгоритмізації зв’язку між учасниками ОРД: оперативним працівником та конфідентом, у т. ч. не встановлено закономірностей використання алгоритмів і програм у конспіративному обміні оперативно-розшуковою інформацією із використанням методів сучасної стеганографії: комп’ютерної і цифрової [3]. Відсутні однозначні погляди до визначення змісту понять “тайник” (як одного із способів зв’язку між учасниками ОРД) та “тайникова операція”.

Метою статті є визначення можливостей використання на практиці методів перетворень ЦС в інтересах ОРД, зокрема, для здійснення її учасниками тайникових операцій зв’язку.

Виклад основних положень. Законодавець визначає інформацію як будь-які відомості та (або) дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [4]. 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. Законодавець визначає документом матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі [4, 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 [5]. За словами О.М. Бандурка – “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” [6]. Учені А.М. Хлус, І.І. Бранчель вважають, що з конфідентами встановлюється співробітництво виключно на негласній основі. Без допомоги конфідентів не можна ефективно боротися зі шпигунством, тероризмом, а також організованою злочинністю [7].

Зв’язок конфідента та співробітника оперативного підрозділу є складовою вищезазначених відносин співробітництва. Під таким зв’язком у практиці ОРД розуміється взаємне сповіщення оперпрацівника та конфідента про необхідність зустрічі, а також саме конспіративне спілкування, що надає можливість здійснювати взаємний обмін інформацією в ході ОРД. Важливішою вимогою до зв’язку конфідента з оперативним працівником є його конспіративність, яка досягається шляхом

використання відповідних способів зв’язку, що відповідають конкретним умовам. Виникнення непередбачуваних ситуацій під час ОРД вимагає від такого зв’язку ще і стійкості. Під нею розуміється певна організація, коли забезпечується регулярність і систематичність спілкування учасників ОРД при виникненні різних труднощів та обставин, що перешкоджають зв’язку. Тобто стійкість зв’язку означає постійну готовність до його здійснення. Поряд із стійкістю наступною вимогою до такого зв’язку є його своєчасність, тобто встановлення зв’язку тоді, коли виникає така необхідність. Своєчасність зв’язку викликається певними обставинами: терміновістю прийняття управлінських рішень по окремих фактах, з якими при виконанні завдань ОРД зіштовхується конфідент, виникненням в нього додаткових питань до оперпрацівника або раптовими змінами ситуації, що потребують корегування подальших заходів ОРД чи відміни поточного завдання тощо. Своєчасність такого 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 та своєчасність є складовими надійності зв’язку оперативного працівника з конфідентом під час вирішення завдань ОРД. В оперативно-розшуковій практиці такий зв’язок здійснюється за двома формами: безпосередньо, шляхом особистого спілкування (тобто, особистий зв’язок) чи за допомогою інформаційно-телекомунікаційних систем, або через посередників. Тому і відрізняють дві форми особистого зв’язку з конфідентами – форму безпосереднього зв’язку та посередницького зв’язку. За кожною формою застосовуються свої способи зв’язку. Безособистий же зв’язок здійснюється за допомогою тайників, телефону, телеграфу, пошти та сучасних телекомунікаційних засобів.

У цій статті розглядаються аспекти безособистого зв’язку між конфідентом та оперативним співробітником, що відбувається через тайник, у т.ч. за допомогою сучасних технологій, зокрема, стеганометодів.

Одразу необхідно зазначити, що законодавець пов’язує поняття “тайник” лише із знаряддями або засобами вчинення злочинів. Наприклад, згідно зі ст. 201 (контрабанда) Кримінального кодексу України, використання тайників пов’язане із переміщенням предметів через митний кордон із приховуванням від митного контролю у вигляді спеціально, з метою вчинення контрабанди, виготовлених або обладнаних схованок в транспортних засобах, устаткуванні, тарі, предметах одягу тощо [8]. Інший приклад, тайник – сховище, виготовлене з метою незаконного переміщення товарів через митний кордон України, а також обладнані та пристосовані з цією метою конструктивні ємності чи предмети, які попередньо піддавалися розбиранню, монтажу тощо (п. 53 ч. 1 ст. 4 Митного кодексу України) [9]. У відкритій вітчизняній науковій літературі відсутнє поняття тайнику як способу безособистого зв’язку між конфідентом та оперативним працівником. Цікаво, що і у військовій літературі, наприклад, у настанові FM 7-93 армійської розвідки Сухопутних військ США Long range surveillance unit operations [10] також відсутнє саме визначення “тайник”, хоча цей документ містить докладні рекомендації щодо використання тайників у бойовій обстановці. Зокрема, настанова FM 7-93 вимагає диверсійно-розвідувальним групам сповіщати командування про підготовку тайника радіограмою із дванадцяти об’ємних пунктів, що містять дані про тип тайнику, його спосіб закладки і зміст, опис контейнерів, район, місце і деталі його приховування тощо. Ця настанова попереджає, що успіх закладки тайнику залежить від деталей, які непрофесіоналу можуть здаватися несуттєвими, потребує твердих знань основних принципів і технічних деталей тайникових операцій, що досягається лише ретельною підготовкою та навчанням. Визначення тайниковим операціям названа

настанова не дає. У вітчизняних законодавчих актах та відкритій науковій літературі взагалі відсутнє поняття “тайникова операція”. Водночас, визначення тайникової операції міститься у Контррозвідувальному словнику КДБ при РМ СРСР (1972 року видання), який у PDF-файлах поширено присутній в мережі Інтернет [11]. Визначення “тайникова операція” (далі – ТО) із цього словника інтерпретується як комплекс заходів при здійсненні безособистого зв’язку між співробітником оперативного підрозділу та конфідентом за допомогою тайнику. ТО умовно поділяють на чотири стадії: підбір та облаштування місця для тайника (1), закладка матеріалів у тайник (2), їх виїмка (3), сигналізація про виїмку (4). Відповідно, під тайником розуміється місце, яке підібране оперпрацівником та обладнане спеціальним контейнером для безпечного зберігання носіїв інформації з обмеженим доступом та прихованого обміну ними із конфідентом без проведення з останнім особистих зустрічей. Уникнення особистого спілкування дозволяє значно зменшити ризик викриття зв’язку співробітника оперативного підрозділу та конфідента. Водночас, використання тайнику ускладнює роботу з негласним помічником, робіть її менш ефективною, насамперед за часом, що може негативно впливати на хід виконання завдань ОРД. При цьому завжди присутня вірогідність виявлення таємного місця сторонніми особами. Тому контейнер у сучасному тайнику є не тільки спеціальним пристроєм зберігання, але і миттєвого знищення інформації (в залежності від її носія – імпульсного, термохімічного, вибухового тощо), якщо ці сторонні особи не уникатимуть із контейнером дій, наслідки яких вони не в змозі заздалегідь передбачити (зняття із запобіжника механізму безпеки контейнера, розміщення його перед розтином у конкретному середовищі (у воді, темноті) та ін.). Тайники споруджуються як в природних укриттях (дуплах дерев, щілинах забудівель, поглибленнях скал тощо), так і спеціально створених укриттях. Розміри тайнику обираються в залежності від розмірів контейнерів і вкладень з інформацією. Кожен тайник перед використанням перевіряється на пробні закладки контейнерів з організацією візуального спостереження за обстановкою навколо нього. Про час закладок контейнерів (їх виїмки) оперативний співробітник і конфідент сповіщають спеціальним сигналом (помітка на стені, припаркування автомобіля у заздалегідь обумовленому місці, зарубка на дереві, горщик із рослиною на вікні та ін.). Зв'язок через тайник в оперативно-розшуковій практиці найбільш доцільний тоді, коли, передусім, особисті зустрічі оперативного працівника з конфідентом сполучені з ризиком викриття негласного співробітника (наприклад, під час його перебування у злочинному угрупованні). Такий зв’язок в інтересах ОРД у більшості випадків також знаходить застосування за кордоном, при перебуванні військовослужбовців на казарменому положенні, території ведення бойових дій або при роботі з негласними співробітниками в районах, тимчасово окупованих противником, тощо. Порівняльним аналізом наведених вище джерел щодо ТО встановлено збіг порядку закладки тайника у настанові FM 7-93 зі стадіями ТО, описаними у словнику. Зазначене, на наш погляд, демонструє можливість використання певних алгоритмів у подібних тайникових операціях. Ці алгоритми розраховані на типові ситуації в системі вимірів, що забезпечують прийняття оптимальних рішень у процесі здійснення учасниками ОРД зв’язку через тайник (див. Таблицю). Взагалі конспіративному звязку з використанням тайника передує захід (система дій), об’єднаний єдиним задумом та спрямований на досягнення певної мети (у нашому випадку приховано передати конфіденціальну інформацію), що, як відомо, і є операцією [12].

На нашу думку, тайникова операція як різновид операції завжди є керованим заходом, тобто від оперпрацівника та конфідента залежить обрання деяких параметрів,

що характеризують організацію цього обміну інформацією як операції. Під організацією слід розуміти набір засобів, що застосовані в цій тайниковій операції. Певний вибір параметрів, залежних від учасників ОРД, буде їх рішенням. Оптимальними називаються рішення, які за різними ознаками мають перевагу перед іншими. Зміст стадій ТО також залежить від середовища її здійснення та вимагає системи, що працює завдяки чіткому алгоритму.

Таблиця.

Збіг порядку здійснення ТО у настанові та словнику

Стадії ТО (за словником)	Підбір і облаштування місця тайника	Закладка контейнера у тайник.	Виїмка носія інформації з контейнеру	Сигналізація про виїмку контейнера
Вимоги до закладки тайника (по настанові)	1. Тип тайника: для кого призначений та характер матер. носія інформації (папір із тайнописом, магнітний носій із зашифр. даними тощо). 2. Спосіб закладки: закопування, маскування, занурення контейнера.	3. Зміст тайника: перелік предметів, закладених у контейнер 4. Опис контейнерів: розмір, вага тощо. 5. Загальний район закладки з прив’язкою до населених пунктів. 6. Безпосередній район закладки з прив’язкою до маршрутів і орієнтирів. 7. Місце закладки тайника (безпосередня відмітка тайника та відстань від неї до контейнеру в одиницях довжини, що зрозумілі для тих, хто шукатиме тайник). 8. Деталі місця закладки контейнера: особливості безпосереднього місця закладки та природні особливості в залежності від способу закладки.	9. Оперативні дані й примітки: потрібне для виїмці обладнання, підходи до тайнику 10. Час закладки та розрахункові терміни зберігання носіїв інформації. 11. Схеми, малюнки фотознімки місця закладки тайника.	12. Радіоповідомлення про виїмку контейнера.
Складові надійності зв’язку	Стійкість зв’язку		Своєчасність зв’язку.	
	Конспіративність зв’язку			

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].

При виникненні 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 носять, 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 із незначним стажем практичної роботи зможуть значно краще вирішувати оперативно-розшукові завдання, якщо будуть спиратися на готові схеми, алгоритми, ніж на “здорові міркування” своїх зв’язків, іноді випадкових. В інформатиці під алгоритмом розуміється точний припис, що визначає обчислювальний процес та веде від варійованих початкових даних до шуканого результату. А програма є описуванням алгоритму на мові програмування [14]. Тому оперативно-розшуковий алгоритм є, на нашу думку, науково обґрунтованим приписом по виконанню оперативним працівником у заданому порядку системи послідовних дій для рішення завдань ОРД певного типу, зокрема, організації зв’язку через тайник із конфідентами. Запропонувати алгоритми у неординарних ситуаціях та запрограмувати нестандартні рішення ТО неможливо. Подібні алгоритми не можуть розглядатися як безумовний припис. Це лише рекомендації про раціональну послідовність дій учасників ОРД при організації обміну інформацією з використанням тайників. На наш погляд, шукане рішення розробки алгоритмів і програм обміну оперативно-розшуковою інформацією через тайник знаходиться у площині взаємозалежності елементів оперативної ситуації та дій. Всі ці елементи індивідуальні саме для цього випадку ТО, незмінні на її протязі та обов’язково враховуються оперпрацівником при підготовці цієї ТО. При цьому, окремі із дій вже достатньо алгоритмізовані, наприклад: збирання інформації стосовно придатності конфідента проводити певні ТО та обраного місця тайника, планування порядку обміну контейнерами при зміні передбачуваних умов навколо місця проведення ТО, засвоєння конфідентом послідовності дій при виникненні загрози захоплення контейнера, розподіл функцій і ролей під час ТО та аналіз даних про конспіративність її здійснення. На нашу думку, такий алгоритм проведення ТО не є вичерпним, але може слугувати “матрицею” для розроблення алгоритмічних дій тайникового зв’язку між конфідентом та оперпрацівником в інших ситуаціях. “Матриця” дозволяє при плануванні ТО, особливо оперативними співробітниками-початківцями, заздалегідь розглянути можливість здійснення окремо взятої такої операції через призму її конспіративності, стійкості та своєчасності.

При цьому, застосування алгоритмічного підходу при побудові тайникового зв’язку, на наш погляд, однаково придатне на практиці як у випадку підтримання спілкування оперпрацівника з конфідентом через тайник звичайним, “класичним” способом, так і при використанні учасниками ОРД способів ЦС для проведення ТО. Пояснимо думку. ЦС як галузь знань розглядає методи організації прихованих каналів передачі і зберігання інформації з використанням різних цифрових об’єктів (засобів і систем зберігання і передачі електронної інформації) та вбудовування спеціальних міток в електронну інформацію з метою її захисту (цифрові водяні знаки, електронні голографічні елементи) [2, с. 67].

Як відомо, ЦС може здійснюватися в різні способи, але загальною рисою для них буде те, що файл із конфіденційною інформацією після її попереднього кодування

перетворюється в інший файл, тобто у певну надлишкову інформацію (далі – НІ), яка вбудовується у контейнер (об’єкт). Процес вбудовування файлу в об’єкт і є стеганоперетворенням (далі – СП). Результатом СП є стеганограма (далі – СГ), тобто заповнений контейнер, що містить приховану інформацію. СГ пересилається по закритому або відкритому каналу зв’язку чи зберігається в отриманому вигляді (наприклад, як GIF-файл – “радіючий” смайлик (☺) під час чату в мережі Facebook, або картинка кошеня (JPG-файл) у локальній комп’ютерній мережі чи аудіофайл у розширенні mp3 на якомусь сайті-фонотеці, що має авторську природу, тобто не містить оригіналу, тощо). При цьому як цифрові, так і всі методи стеганографії і використовують цей надлишок (НІ) в обраній для зміни інформації, за рахунок якого приховується конфіденційна інформація, що не призводить до суттєвої зміни властивостей контейнера та порушення його цільового призначення: аудіофайл як і раніше “співає”, картинка “бачиться” або смайлик продовжує “радіти”. Тобто стеганоалгоритм виявляє певну стійкість до атак проти СГ та конспіративність – здійснення стосовно неї стеганоаналізу. Практично мова йде про проведення тайникової операції – закладки контейнерів у закритих для загального доступу чи, навпаки, відкритих місцях мережевого спілкування або впровадження СГ до колосальних по об’ємах неструктурованих та у різноманітних формах масивів даних, які зберігаються на різних вузлах глобальної мережі [15]. При цьому, ефективність виявлення та зчитування інформації СГ у відкритому та зашифрованому вигляді залежить від статистичного розподілу елементів контейнерів, імовірнісного розподілу самих контейнерів, властивостей стеганограм та криптографічних ключів, якщо і вони використовуються. Взагалі різновиди груп стеганометодів як дій зі стеганоконтейнерами у різних інформаційних середовищах [3, с.70-247] нагадують дії із закопування, маскування, занурення тайникових контейнерів, що описані у настанові FM 7-93. Ще з 2003 року з оперативно-розшукової практики відомі приклади видправлення конфідентами-іноземцями через Інтернет-кафе стеганограм-звітувань із використанням програмних іграшок системи електронних розваг, що забезпечують інтенсивний обмін випадковою електронною інформацією у глобальних комп’ютерних мережах.

Висновки.

Стеганограми відповідають вимогам конспіративності, стійкості і своєчасності передавання інформації між конфідентом і оперативним працівником та в окремих випадках можуть бути використані для обміну оперативно-розшуковою інформацією зазначеними учасниками ОРД. Такі засоби технічного захисту обміну інформацією нагадують “класичні” тайникові операції і мають практичне значення для оперативних підрозділів, тому, на наш погляд, доцільно розробити для учасників ОРД доступною мовою у вигляді брошур відповідні рекомендації щодо застосування окремих сучасних технологій при організації конспіративного зв’язку.

Використана література

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

2. Конахович Г.Ф. Компьютерная стеганография. Теория и практика // Г.Ф. Конахович, А.Ю. Пузыренко – К : “МК-Пресс”, 2006. – 288 с.

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

4. Про інформацію : Закон України // Відомості Верховної Ради України (ВВР). – 1992. – № 48. – Ст. 650.

5. Овчинський С.С. Оперативно-розыскная информация / С.С. Овчинський : под ред. А.С. Овчинського и В.С. Овчинського. – М., 2000. – С. 18.

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

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

8. Кримінальний кодекс України : науково-практичний коментар : у 2 т. ; за заг. ред. В.Я. Тація, В.П. Пшонки, В.І. Борисова, В.І. Тютюгіна та ін. – Х. : Право, 2013. – 1040 с.

9. Митний кодекс України : Закон України // Відомості Верховної Ради України (ВВР). – 2012. – №№ 44 – 48. – Ст. 552.

10. Long range surveillance unit operations. Headquarters, Department of the Army. – Washington, DC, 3 October 1995. – Режим доступу : http://perevod.vrazvedka.ru/index.php?option=com_phocadownload&view=category&download=7:fm-7-93------1995-&id=1:2011-01-17-11-28-41&Itemid=5

11. Контрразведывательный словарь. – М. : ВКШ КГБ при СМ СССР, 1972. – 371 с. – С. 324. – Режим доступа : https://vk.com/doc41072062_187231293?hash=932cfaf9d53cd8febc&dl=72886452c9ba 8a9fd9

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

13. Толстолуцкий В.Ю. Криминалистическая информатика на современном этапе развития // 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. Осипенко А.Л. Новые технологии получения и анализа оперативно-розыскной информации : правовые проблемы и перспективы внедрения // Вестник Воронежского института МВД России. – 2015. – № 2. – С. 15.

Рецензенти: Білічак О.А. доктор юридичних наук, доцент.
Гринь А.К., кандидат технічних наук, доцент.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~