4. Положення про Державну судову адміністрацію України : Рішення Ради суддів України від 22 жовтня 2010 р. № 12 [Електронний ресурс]. – Режим доступу : http://court.gov.ua/dsa/.

5. Про Державну судову адміністрацію України : Указ Президента України від 29 серпня 2002 р. № 780 [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/780/2002.

6. Про визнання такими, що втратили чинність, деяких указів Президента України : Указ Президента України від 23 червня 2009 р. № 477 [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/477/2009.

7. Створення Державної судової адміністрації України та її територіальних управлінь [Електронний ресурс]. – Режим доступу : http://court.gov.ua/tu12/20/10/10/.

8. Экономика и право : энциклопедический словарь Габлера ; [пер. с нем. / под ред. А.П. Горкина, Н.Л. Тумановой, Н.Н. Шаповаловой и др.] – М. : Большая Российская Энциклопедия, 1998. – 432 с.

9. Положення про територіальні управління Державної судової адміністрації України : Наказ Державної судової адміністрації України від 5 березня 2011 р. [Електронний ресурс]. – Режим доступу : http://court.gov.ua/tu16/norm/pol2/polojennia/.

БЛІНОВА Г. О.,
кандидат юридичних наук, доцент,
завідувач кафедри цивільно-правових дисциплін
(ВНПЗ «Дніпропетровський гуманітарний університет»)

УДК 349.2

ДЖЕРЕЛА НЕБЕЗПЕКИ ДЛЯ РЕЖИМУ СЛУЖБОВОЇ ІНФОРМАЦІЇ В ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

У статті характеризується правове регулювання інформаційної безпеки правоохоронних органів та джерела небезпеки для режиму службової інформації в їх сучасній практичній діяльності.

Ключові слова: *інформація з обмеженим доступом, службова таємниця, правоохоронні органи, режим, інформаційна безпека.*

В статье характеризуется правовое регулирование информационной безопасности правоохранительных органов и источники опасности для режима служебной информации в их современной практической деятельности.

Ключевые слова: *информация с ограниченным доступом, служебная тайна, правоохранительные органы, режим, информационная безопасность.*

Characterized by legal regulation of information security law enforcement agencies and sources of danger to the regime of official information in their modern practice.

Key words: *restricted access information, official secret, law enforcement, treatment, information security.*

Вступ. Функціонування державних інститутів неможливе без використання певного обсягу службової інформації, яка забезпечує потреби організації їх роботи. Службова інформація призначена для забезпечення конфіденційності відомостей, утворених чи отриманих працівниками при виконанні своїх службових обов'язків, від незаконного розголошення, використання, зміни чи знищення, забезпечення прав і законних інтересів фізичних та юридичних осіб. Інтенсивний інформаційно-технологічний розвиток привів до створення можливостей відносно легкого та швидкого отримання будь-яких відомостей. Як зазначено у Концепції технічного захисту інформації в Україні, на сучасному етапі розвитку інформаційних технологій створилися можливості витоку інформації, порушення її цілісності та блокування. У свою чергу витік інформації, яка становить державну та іншу передбачену законом таємницю, службову інформацію, – це одна з основних можливих загроз національній безпеці України в інформаційній сфері [10]. Тому законодавець вважає одним з головних принципів технічного захисту інформації захист відомостей, що становлять службову інформацію на рівні з державною та іншими видами таємниць. Яскравим прикладом термінологічної неузгодженості у сфері обігу інформації з обмеженим доступом є використання в законодавстві на одному рівні таких термінів, як «службова таємниця» та «службова інформація». Така негативна термінологічна невизначеність законодавства, що регулює інформаційні відносини з приводу використання службових відомостей, є свідченням перебудови системи інформації з обмеженим доступом, що розпочалась із прийняттям Закону України «Про доступ до публічної інформації».

Постановка завдання. Мета статті – з'ясування змісту поняття та кола джерел небезпеки для режиму службової інформації в практичній діяльності працівників правоохоронних органів. Предмет розгляду цього наукового дослідження – правові норми, наукові теорії, що визначають зміст та правовий режим службової інформації, порядок її формування, зберігання та межі використання у правоохоронних органах, а також результати опитування працівників правоохоронних органів.

Результати дослідження. Відповідно до чинного законодавства службовою інформацією є інформація, що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень, а також інформація, що зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці [10]. Документам, що містять інформацію, яка становить службову інформацію, присвоюється гриф «для службового користування». Доступ до таких документів обмежується за умови поєднання таких вимог: 1) забезпечення інтересів національної безпеки, територіальної цілісності; 2) забезпечення громадського порядку та запобігання заворушенням чи злочинам; 3) забезпечення охорони здоров'я населення; 4) забезпечення захисту репутації або прав інших людей; 5) запобігання розголошенню інформації, одержаної конфіденційно; 6) підтримання авторитету і неупередженості правосуддя; 7) якщо розголошення інформації може завдати істотної шкоди цим інтересам; 8) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні [9]. Конкретизований перелік відомостей, що складають службову інформацію в органах державної влади, органах місцевого самоврядування, інших суб'єктів владних повноважень, у тому числі на виконання делегованих повноважень, не може бути обмеженим у доступі.

Аналогічні законодавчі положення щодо використання конфіденційної інформації, що є власністю держави, існували і до прийняття Закону України «Про доступ до публічної інформації». Фактично має місце заміна назви «конфіденційна інформація, що є власністю держави» на термін «службова інформація», про що пише і Я.Д. Скиба. Цей науковець однією з проблем правового регулювання використання службової інформації

вбачає те, що пунктом 3 ст. 21 Закону «Про інформацію» та ст. 9 Закону «Про доступ до публічної інформації» визначено, що порядок доступу до службової інформації регулюється законом. Я.Д. Скиба зазначає, що жодного єдиного порядку віднесення інформації до службової не встановлено чинними законами України [14, с. 335]. Слід погодитись, що основні правила правового режиму використання службової інформації, визначені не у законі, а в підзаконному нормативно-правовому акті «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію» [11]. Зміна назви цього акта, а також заміна терміна «конфіденційна інформація, що є власністю держави» на термін «службова інформація» у значній кількості правових документів відбулась відповідно до Постанови Кабінету Міністрів України від 7 вересня 2011 р. № 938 [8], прийняття якої пов'язано із Законом України «Про доступ до публічної інформації».

Тепер заборона розголошувати конфіденційну інформацію, що є власністю держави, замінена на заборону розголошувати службову інформацію. На сучасному етапі розвитку вітчизняного законодавства система нормативного забезпечення режиму службової інформації перебуває на гідному рівні, оскільки визначена основна частина правил формування, зберігання, використання, передання, знищення відомостей, що складають службову інформацію, та передбачені норми, які визначають підстави та порядок притягнення до юридичної відповідальності службових осіб за порушення правил використання службової інформації.

Оскільки режим службової таємниці нами було визначено як елемент інформаційної безпеки правоохоронних органів [15], доречно буде навести наукові підходи до визначення загроз інформаційній безпеці. Так, О.К. Юдін та В.М. Богуш виділяють два види загроз за критерієм їх місця відносно системи інформаційної безпеки: зовнішні та внутрішні.

Зовнішніми загрозами, що становлять найбільшу небезпеку для об'єктів забезпечення інформаційної безпеки, а відповідно, і забезпечення службової таємниці у правоохоронній сфері, є: 1) розвідувальна діяльність спеціальних служб іноземних держав, міжнародних злочинних угруповань, організацій і груп, пов'язана зі збором відомостей, що розкривають завдання, плани діяльності, технічне оснащення, методи роботи та місця дислокації спеціальних підрозділів і органів внутрішніх справ України; 2) діяльність іноземних державних і комерційних структур, що прагнуть одержати несанкціонований доступ до інформаційних ресурсів правоохоронних і судових органів.

Внутрішніми загрозами, що становлять найбільшу небезпеку для об'єктів системи інформаційної безпеки правоохоронних органів, є: 1) порушення встановленого регламенту збору, обробки, зберігання і передачі інформації, що міститься в картотеках та автоматизованих банках даних і використовується для розслідування злочинів; 2) недостатність законодавчого та нормативного регулювання інформаційного обміну в правоохоронній і судовій сферах; 3) відсутність єдиної методології збору, обробки та зберігання оперативно-розшукової, довідкової, криміналістичної та статистичної інформації; 4) недоліки технічних засобів і збої програмного забезпечення в інформаційних і телекомунікаційних системах; 5) умисні дії та помилки персоналу, безпосередньо зайнятого формуванням і веденням картотек і автоматизованих банків даних [16, с. 489].

Продовжуючи думку В.П. Мельникова, логічно розмежувати, на наш погляд, такі види загроз 1) за підставою виникнення: випадкові і цілеспрямовані загрози; 2) за реальністю існування: потенційні та реальні; 3) за можливими наслідками – перелічені вище. Вид загроз залежить від об'єкта інформаційної безпеки. Так, для держав зовнішніми загрозами в основному є загострення міжнародної конкуренції за володіння інформаційними технологіями, діяльність міжнародних терористичних організацій, діяльність різних засобів розвідки інших країн тощо, а внутрішніми – криміногенна ситуація, недостатнє врегулювання інформаційних відносин, неповне фінансування заходів, спрямованих на забезпечення інформаційної безпеки держави, тощо [7, с. 33–34].

Розголошення інформації, що становить службову таємницю, є порушенням її режиму, а його причини можна розглядати як загрози для цілісності та недоторканості службової таємниці. Так, одним з основних мотивів отримання чи розголошення службової інформації є дезорганізація роботи державних органів, зокрема правоохоронних органів, оскільки це дає можливість безпосередньо впливати на процес розслідування кримінальних справ. Окрім корисливого мотиву, як зазначали В.С. Кузьмічов та В.Г. Лісогор, особами, які причетні до незаконного розголошення службової таємниці, керує острах за себе (шантажування, погроза, фізичний або психічний вплив); страх за своїх близьких (погроза, різні види насильства); зведення рахунків з певними особами (компрометація, заздрість, неприязнь, помста) [4, с. 174].

При цьому особи, які отримують чи розголошують інформацію, що становить службову таємницю, мають на меті отримання матеріальної винагороди за надану інформацію; уникнення розголошення певних відомостей; уникнення певного впливу (тиску); отримання відомостей про хід і результати оперативно-розшукових заходів та розслідування злочинів, про учасників кримінального процесу, про заходи безпеки, що здійснюються відносно осіб, які беруть участь у кримінальному судочинстві, з метою протидії, погроз, шантажу, підкупу і т. ін. [4, с. 174].

Для отримання інформації, що цікавить, злочинні елементи використовують будь-яку помилку в системі захисту, якою найчастіше є нераціональний вибір засобів захисту. Г.В. Загіка наводить такі аргументи: комп'ютерні злочини, в тому числі й ті, внаслідок яких можливий витік інформації, відбуваються через: помилку персоналу – 55%, проблеми фізичного захисту – 20%; нечесних співробітників – 10%; скривджених співробітників – 9%; віруси – 4%; зовнішні напади – 1–3%. Таким чином, констатує науковець, найбільш уразливим елементом будь-якої комп'ютерної системи є люди [3, с. 144]. Відповідно, основні засоби, заходи та методи забезпечення службової таємниці повинні застосовуватись саме з урахуванням цього висновку.

Найбільш імовірними джерелами витоку службової інформації є постійні та тимчасові користувачі інформації, які мають доступ до її носіїв: документів, технічних засобів та систем обробки інформації. Як зазначав В.П. Лавров, розголошення, втрата відомостей, що становлять слідчу таємницю, яка є частиною службової, стають можливими з таких причин: а) недбалість, необережність посадових осіб, поінформованих про хід розслідування; б) випадковий збіг обставин; в) дії злочинців, спрямовані на отримання такої інформації [5, с. 81]. Способами розголошення інформації, що становить службову таємницю, усіма особами, які будь-яким чином стикалися з нею, можуть бути: 1) безпосереднє розголошення; 2) по телефону; 3) у листі; 4) у пресі; 5) по радіо; 6) по телебаченню і т. ін.

Збільшення обсягів інформації, що надходить та обробляється, розвиток технічних засобів обробки інформації зумовили необхідність використання сучасних засобів комп'ютерної техніки та новітніх інформаційних технологій у правоохоронних органах з метою підвищення ефективності їх роботи. При цьому у своїй діяльності підрозділи правоохоронних органів використовують відомості, які містять службову, державну таємницю, іншу інформацію, доступ до якої повинен бути обмежений за допомогою засобів інформаційної безпеки. Тому захисту комп'ютерів і комп'ютерних мереж від несанкціонованого доступу необхідно приділяти особливу увагу.

Існує така класифікація каналів несанкціонованого доступу, якими можна здійснити викрадення, викривлення або знищення інформації: 1) через людину такими шляхами: викрадення носіїв інформації, читання інформації з екрану або клавіатури, читання інформації з роздрукованого тексту; 2) через програму: перехват паролів, розшифровка зашифрованої інформації, копіювання інформації з носія; 3) через апаратуру: підключення спеціально розроблених апаратних засобів, що забезпечують доступ до інформації, перехоплення побічних електромагнітних випромінювань від апаратури, ліній зв'язку, мережі електроживлення тощо.

Проведеним Д.І. Бєдняковим дослідженням було встановлено, що джерела отримання інформації злочинцями розподілилися так: колишні оперативні працівники – 53%; засоби масової інформації – 43%; раніше судимі особи – 35%; оперативні працівники – 15%; слідчі – 14%; адвокати – 30%; колишні слідчі – 22%; інші працівники правоохоронних органів – 38%; злочинці, які самостійно розкрили методи ОРД, – 11%; товариші по службі, знайомі, родичі – 6%; неуміле проведення оперативних заходів – 12% [1, с. 73]. Однак ситуація змінюється, і, за даними наших досліджень, серед різних груп осіб, які мають доступ до службової таємниці, її розголошення найчастіше вчинюється: керівництвом ОВС, прокуратури, податкової міліції тощо – 28,8%; співробітниками ОВС – 35,3%; працівниками прокуратури – 23,0%; працівниками податкової адміністрації, податкової міліції – 6,5%; працівниками внутрішньої безпеки МВС України – 11,2%; суддями – 14,4%; свідками, потерпілими, підозрюваними – 30,3%; адвокатами (захисниками) – 24,7%; засобами масової інформації – 42,6%; працівниками інших наглядових та контролюючих органів – 9,7%.

Загрози інформації у більшості випадків спрямовані на її негласне отримання, знищення (поновлення) чи внесення певних змін (модифікацію) [6, с. 9]. Окремими вченими розглядаються три основні групи способів негласного отримання інформації: 1) незаконне вилучення носіїв інформації; 2) несанкціоноване отримання інформації; 3) неправомірне маніпулювання інформацією [6, с. 63].

Нами з'ясовано, що основними причинами розголошення інформації, яка становить службову таємницю, були названі: обговорення працівниками у колі друзів службових питань – 46,5%, намагання працівника заробити гроші у будь-який спосіб – 36,2%, відсутність чітких правил використання інформації, що становить службову таємницю – 24,1%, звичка ділитися досвідом та давати поради – 13,8%, неконтрольоване використання копіювальної техніки – 20,3%, психологічні конфлікти між співробітниками та керівництвом – 20,8%, низька фінансова компенсація за роботу з інформацією з обмеженим доступом – 0,8%.

Отже, основними джерелами витоку службової інформації є люди (працівники) та відсутність чітких правил користування службовою таємницею в правоохоронних органах. А.М. Благодарний визначає аналогічні причини вчинення адміністративних порушень законодавства про державну таємницю: недостатнє знання деякими особами, котрі мають допуск та доступ до державної таємниці, норм чинного законодавства про державну таємницю; нехтування цими особами нормами чинного законодавства; недостатнє фінансування заходів, спрямованих на захист державної таємниці [2, с. 5].

Певний негативний вплив на збереження конфіденційної інформації може здійснити неправильна організація праці співробітників правоохоронних органів України, в тому числі й робочого місця. Наприклад, В.Г. Лісогор зазначає, що поширеними є випадки, особливо для районних органів внутрішніх справ, роботи декількох слідчих в одному кабінеті [6, с. 39]. За даними Р.Ю. Савонюка, вдвох в одному кабінеті працюють 37,8% слідчих, утрьох – 17,6% й учотирьох – 16,8%. Як зазначає автор, «зрозуміло, що за таких умов про забезпечення таємниці слідства … важко вести мову» [13, с. 481]. У рішенні Колегії МВС України підкреслюється, що окремі робочі кабінети мають менше половини слідчих, а окремі абонентні номери телефонного зв'язку – тільки 30% [12]. Слідчі також загострюють увагу на незадовільній звукоізоляції кабінетів – 84% опитаних [13, с. 482].

Однією з причин розголошення службової таємниці ОВС України може бути неналежний рівень порядку зберігання службових матеріалів, тобто допускається їх тримання у столах працівників. Тому ми погоджуємося з думкою В.Г. Лісогора про те, що надзвичайно важливо, яким чином і в яких умовах зберігаються ці документи [6, с. 40]. Як зазначається в науковій літературі, «найсуворіші накази про збереження кримінальних справ не допоможуть, якщо не забезпечити слідчого сейфом» [6, с. 482].

У приміщеннях правоохоронних органів, особливо в тих, де розміщені оперативні та слідчі підрозділи, діє пропускний режим. Цей режим полягає в обмеженні доступу сторонніх осіб, він служить одним із бар'єрів на шляху витоку інформації. Співробітник має зустрічати та супроводжувати відвідувачів, які до нього прибули. Але інколи ця вимога не дотримується, що сприяє можливості негласного доступу до службової таємниці. Трапляються випадки, коли розголошення службової таємниці відбувається з вини технічних працівників правоохоронних органів, які мають доступ до цих матеріалів, до листування у справі як на паперових, так і на електронних носіях.

Розголошенню службової таємниці також сприяє і розповсюдження працівниками правоохоронних органів службової інформації у позаслужбовому, побутовому спілкуванні або у службовому спілкуванні без належного дотримання вимог нерозголошення інформації тощо. Це підтверджується результатами анкетування: всього 28,8% опитаних працівників ніколи в своїй діяльності не зустрічались із витоком службової інформації, а всі інші (71,2%) мали справу з такими випадками.

У діяльності, наприклад, дільничних інспекторів, слідчих та оперативних працівників є поширеною практика залучення активістів (помічників, нештатних співробітників), які допомагають їм. Оскільки ці особи отримують службову інформацію у ході виконання тих чи інших дій, то існує певна можливість її розголошення, тим більше що законодавством та відомчими нормативними актами не передбачено підписки про нерозголошення службової таємниці такими особами.

Мають місце також великий обсяг документообігу, нечіткі строки виконання документів, затягування їх виконання, що призводить до збільшення небезпеки розголошення службової таємниці.

Негативними наслідками розголошення службової таємниці в правоохоронних органах були: погіршення розслідування кримінальних справ – 30,8%; ускладнення проведення оперативних заходів – 44,7%; знищення зацікавленими особами речових доказів – 28,8%; штучні перепони у винесенні справедливого рішення – 21,5%; інші негативні наслідки – 1,5%. Отже, в переважній більшості випадків шкода завдавалась особі, що здійснювала розслідування або проводила оперативно-розшукові заходи, і зводилась до різного роду перепон у винесенні справедливого рішення. Однак, незважаючи на те що при розголошенні службової таємниці шкода завдавалась майже в усіх випадках, винні у розголошенні особи виявлялись завжди у 2,3% випадках, інколи – 50,0%, ніколи – 33,8%, і 12,7% опитаних не знають про такі факти.

Висновки. Така висока латентність цих правопорушень працівниками правоохоронних органів пояснюється: невизнанням незаконного розголошення службової таємниці протиправним діянням – 15,0%, невизначеністю в законодавстві всіх елементів режиму службової таємниці – 27,3% та замовчуванням таких випадків керівництвом органу – 35,3%. Щодо відповідальності тієї невеликої групи осіб, які були виявлені і були винні у розголошенні службової таємниці ОВС України, то 44,1% з них взагалі не були покарані, 44,7% були притягнені до дисциплінарної відповідальності, понесли адміністративну відповідальність 5,6%, кримінальну – 2,9%, і відшкодували завдану шкоду у порядку цивільного провадження 2,6%. Таким чином, розголошення службової таємниці у правоохоронних органах України за чинним законодавством та реальним станом справ є безкарним у 44 – 45 випадках із 100.

Режим службової таємниці в правоохоронних органах, як і режим будь-якої з таємниць, передбачає охорону та захист конфіденційної інформації, що становить службову таємницю, за допомогою організаційно-правових, інженерно-технічних, криптографічних, оперативних і навіть психологічних заходів. Механізм адміністративно-правового забезпечення службової таємниці в ОВС України по суті і є комплексом заходів адміністративно-правового характеру, спрямованих на досягнення інформаційної безпеки правоохоронних органів України. І, як свідчить наведена інформація, цей механізм потребує подальшого вдосконалення.

Список використаних джерел:

1. Бедняков Д.И. Непроцессуальная информация и расследование пре ступлений / Д.И. Бедняков. – М. : Юр. лит., 1991. – 208 с.

2. Благодарний А.М. Адміністративна відповідальність за порушення законодавства про державну таємницю: автореф. дис. ... канд. юрид. наук : спец. 12.00.06 «Земельне право, аграрне право, екологічне право, природоресурсне право» / А.М. Благодатний ; Ін-т законодавства Верховної Ради України. – К., 2006. – 20 с.

3. Загіка Г.В. Деякі питання забезпечення безпеки інформаційної системи в ОВС на транспорті / Г.В. Загіка // Вісн. Одеськ. ін-ту внутр. справ. – 2000. – № 3. – С. 143–147.

4. Кузьмічов В.С. Розголошення інформації, що становить таємницю досудового слідства / В.С. Кузьмічов., В.Г. Лісогор // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2001. – № 4. – С. 173–183.

5. Лавров В.П. Проблема обеспечения следственной тайны в условиях развития демократии и гласности / В.П. Лавров // Проблемы демократизации предварительного следствия : сб. науч. тр. / отв. ред. Ф. В. Глазырин и др. – Волгоград : ВСШ МВД СССР, 1989. – С. 82–86.

6. Лісогор В.Г. Криміналістичне забезпечення збереження таємниці досудового слідства : наук.-практ. посібник / В.Г. Лісогор. – Дніпропетровськ : Юрид. акад. М-ва внутр. справ. – 2005. – 156 с.

7. Мельников В.П. Информационная безопасность: учеб. пособие для средн. проф. образования / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова. – М. : Издательский центр «Академия», 2005. – 336 с.

8. Про внесення змін до деяких постанов Кабінету Міністрів України з питань доступу до інформації : Постанова Кабінету Міністрів України від 7 вересня 2011 р. № 938 [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/938-2011-%D0%BF.

9. Про доступ до публічної інформації : Закон України від 13 січня 2011 р. № 2939-VI // Відомості Верховної Ради України. – 2011. – № 32. – ст. 314 – ст. 6.

10. Про доступ до публічної інформації: інформаційний прорив в Україні : Роз'яснення Міністерства юстиції України від 13 травня 2011 р. // Дебет-Кредит (Галицькі контракти). – 2011 р. – № 31. – С. 57.

11. Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію : Постанова Кабінету Міністрів України від 27 листопада 1998 р. № 1893 // Урядовий кур'єр від 10.12.1998.

12. Про заходи щодо вдосконалення діяльності органів досудового слідства : Рішення Колегії МВС України № 8 км/1 від 19 липня 2002 р.

13. Савонюк Р.Ю. Слідча діяльність: детермінанти і проблеми // Проблеми боротьби з корупцією, організованою злочинністю та контрабандою. Президенту України, Верховній Раді України, Уряду України, органам центральної та місцевої виконавчої влади. Аналітичні розробки, пропозиції наукових і практичних працівників : міжвідомч. наук. зб. / під ред. А.І. Комарової, В.В. Медведчука, В.О. Євдокимова, В.Ф. Бойка, О.О. Крикуна. – К., 1999. – Т. 18. – С. 478–484.

14. Скиба Я.Д. Порядок визначення службової інформації: проблеми теорії та практики / Я.Д. Скиба // Митна справа. – № 2(80). – 2012. – Ч. 2. – Кн.2. – С. 334–340.

15. Шлома Г.О. Адміністративно-правове забезпечення службової таємниці в органах внутрішніх справ України : автореф. дис... канд. юрид. наук. : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / Г.О. Шлома ; Дніпропетр. держ. ун-т внутр. справ. – Д., 2008. – 20 с. – С. 15.

16. Юдін О.К. Інформаційна безпека держави : навч. посіб. / О.К. Юдін, В.М. Богуш. – Х. : Консум, 2005. – 576 с.