ISSN 1995-6134

УДК 343.1:65.012.8
О.В. МАНЖАЙ, канд. юрид. наук, Харківський національний університет внутрішніх справ

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОПЕРАТИВНО-РОЗШУКОВОЇ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ ІНСТИТУТУ ДЕРЖАВНОЇ ТА СЛУЖБОВОЇ ТАЄМНИЦІ В ОКРЕМИХ КРАЇНАХ СВІТУ

Ключові слова: *державна таємниця, оперативно-розшукова діяльність, світовий досвід, інформаційна безпека, аналіз законодавства*

08.07.2009 р. Президент України Указом № 514/2009 затвердив «Доктрину інформаційної безпеки України» [1], в якій відзначається, що за сучасних умов інформаційна складова набуває дедалі більшої ваги і стає *одним із найважливіших елементів забезпечення національної безпеки*. Водночас у ст.7 Закону України «Про основи національної безпеки України» [2] визначено загрози національній безпеці України в інформаційній сфері, однією з яких є розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю.

Одним із напрямів правоохоронної діяльності, яка захищена за допомогою інституту таємниць [3, с.10], є оперативно-розшукова діяльність, і це не є випадковістю. Адже держава завжди убезпечувала найбільш чутливі сторони свого існування саме за допомогою обмеження доступу до інформації про них. Тим більш, що в оперативно-розшуковій діяльності особливе місце займає принцип забезпечення конспірації її провадження.

Взагалі дослідженням проблем охорони державної таємниці займалися небагато вчених, серед яких слід виділити О.Є. Архіпова, Р.В. Корсуна, В.М. Лопатіна, В.В. Макаренка, А.С. Пашкова, М.В. Шлапаченка.

Проблеми охорони державної таємниці за межами країн СНД висвітлені в Україні недостатньо, а такий аспект, як світовий досвід захисту за її допомогою оперативно-розшукової інформації розглядається лише поверхово. Все наведене зумовило написання даної роботи, метою якої є порівняльний аналіз захисту оперативно-розшукової інформації в різних країнах за допомогою інституту таємниць, зокрема державної.

В Україні інформація за порядком доступу поділяється як на рис.1.

Базовим законодавчим актом, який регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки є Закон України «Про державну таємницю» від 21.01.1994 р. [4].

Організаційну структуру охорони державної таємниці в Україні умовно можна представити, як на рис.2.

Відповідно до п.4 ст.8 Закону України «Про державну таємницю» інформація про засоби, зміст, плани, організацію, фінансування та матеріально-технічне забезпечення, форми, методи і результати оперативно-розшукової діяльності; про осіб, які співпрацюють або раніше співпрацювали на конфіденційній основі з органами, що проводять таку діяльність; про склад і конкретних осіб, що є негласними штатними працівниками органів, які здійснюють оперативно-розшукову діяльність, відноситься до державної таємниці.

Законом встановлюється три ступеня секретності для відомостей, які містять державну таємницю: «особливої важливості», «цілком таємно» та «таємно».

Інформація вважається державною таємницею з часу опублікування Зводу відомостей, що становлять державну таємницю, до якого включена ця інформація, чи зміни до нього у порядку, встановленому Законом «Про державну таємницю».

На даний момент в Україні діє Звід відомостей, що становлять державну таємницю (далі ЗВДТ), затверджений наказом Служби безпеки України № 440 від 12.08.2005 р. [5].

ISSN 1995-6134

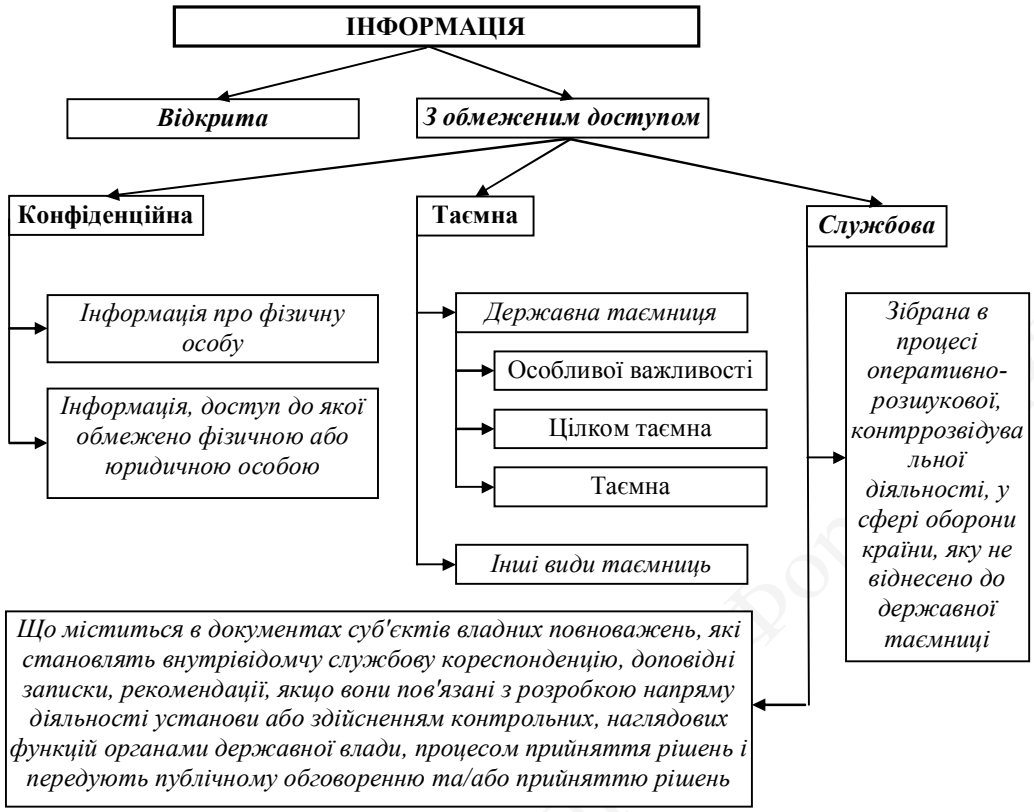

Рисунок 1 – Законодавча класифікація видів інформації в Україні

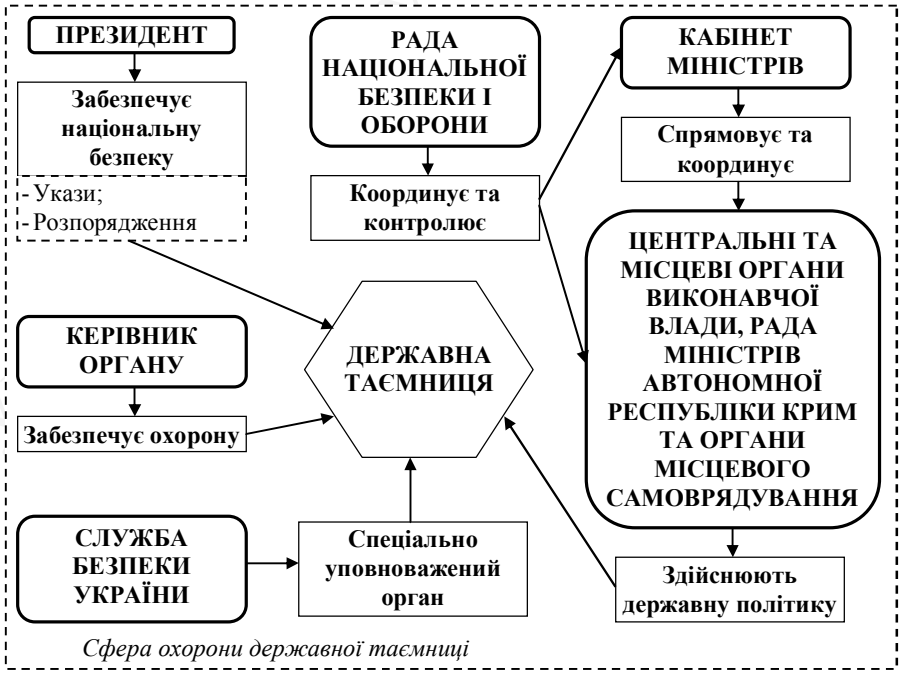

Рисунок 2 – Компетенція органів державної влади, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці

ISSN 1995-6134

Надання грифу секретності документам, що містять інформацію, яка є державною таємницею, здійснюється на підставі ЗВДТ. Відповідно до цього нормативно-правового акту для окремих відомостей щодо провадження оперативно-розшукової діяльності встановлені різні ступені секретності.

Так, наприклад, відомості про організацію, завдання, результати оперативно-розшукової, контррозвідувальної чи розвідувальної діяльності, розголошення яких створює загрозу національним інтересам і безпеці за сукупністю всіх показників у цілому щодо Служби зовнішньої розвідки мають ступінь секретності – «особливої важливості»; за окремими показниками в цілому щодо Служби безпеки України – «цілком таємно»; за окремими показниками в цілому щодо оперативного підрозділу органів внутрішніх справ – «таємно».

Окремі відомості оперативно-розшукової діяльності, які не містять державної таємниці, можуть становити службову інформацію, тоді документам, які містять такі відомості надається гриф обмеження доступу «для службового користування». Порядок роботи з такими документами регулюється Інструкцією про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію, затвердженою Постановою Кабінету Міністрів України від 27.11.1998 р. № 1893 [6].

Приблизно так само, як і в Україні, врегульовано питання захисту державної таємниці та службової інформації обмеженого поширення, зокрема, і оперативно-розшукового характеру, в Російській Федерації.

Основна нормативно-правова база обмеження доступу до окремих відомостей оперативно-розшукової діяльності складається з Федерального Закону «Про державну таємницю» від 21.07.1993 р. [7]; Указу Президента Російської Федерації № 1203 «Про затвердження переліку відомостей, віднесених до державної таємниці» від 30.11.1995 р.; Положення про порядок поводження зі службовою інформацією обмеженого поширення у федеральних органах виконавчої влади, затверджене Постановою Уряду РФ № 1233 від 03.11.1994 р. [8]; Указу Президента Російської Федерації № 188 «Про затвердження переліку відомостей конфіденційного характеру» від 06.03.1997 р. [9].

Відмінність законодавства Росії в цій сфері від українського полягає в тому, що в указаному вище Указі Президента РФ № 1203 вказується лише перелік відомостей, які становлять державну таємницю, а відповідні ступені секретності цим відомостям надають уповноважені Президентом органи державної влади у розгорнутих переліках відомостей, що підлягають засекречуванню. Так, наприклад, щодо відомостей, в яких розкриваються сили, засоби, джерела, методи, плани, результати оперативно-розшукової діяльності такими повноваженнями наділено Міністерства внутрішніх справ, оборони, юстиції, економічного розвитку Росії; Службу зовнішньої розвідки, Федеральну службу безпеки Росії тощо [10].

У США система обмеження доступу до певних відомостей регулюється Указом Президента «Секретна інформація в сфері національної безпеки», відповідно до якого в США існують три ступені секретності «цілком таємно» («Top Secret»), «таємно» («Secret») та «конфіденційно» («Confidential»).

Причому, до інформації зі ступенем секретності «цілком таємно» відносяться відомості, несанкціоноване розкриття яких може завдати тяжкої шкоди національній безпеці, до інформації зі ступенем секретності «таємно» – відомості, несанкціоноване розкриття яких може завдати значної шкоди національній безпеці, та до інформації зі ступенем секретності «конфіденційно» – відомості, несанкціоноване розкриття яких може завдати шкоди національній безпеці (Section 1.2 [11]).

До категорій інформації, яка може бути засекречена відносяться відомості про військові плани, озброєння або операції; інформація

ISSN 1995-6134

іноземних урядів; *відомості про розвідувальні заходи (включаючи спеціальні заходи), розвідувальні джерела чи методи* або криптологію; іноземні відносини або закордонні заходи США, включаючи конфіденційні джерела; наукову, технологічну або економічну діяльність щодо забезпечення національної безпеки, яка забезпечує захист від міжнародного тероризму; програми США щодо безпеки ядерних матеріалів та обладнання; вразливості та можливості систем, установок, інфраструктур, проектів, планів або захисних служб національної безпеки, які забезпечують захист від міжнародного тероризму або зброї масового знищення.

Всі інші категорії інформації засекречувати забороняється.

На базі вищезгаданого Указу Президента США відповідні державні органи розробляють власні інструкції щодо роботи з державною таємницею.

Як правило, окремі відомості щодо проведення оперативно-розшукових заходів відносять до державної таємниці на підставі їх належності до відомостей про розвідувальні заходи (включаючи спеціальні заходи), розвідувальні джерела чи методи.

При розгляді в суді кримінальних справ може виникнути необхідність у розкритті окремих секретних аспектів оперативно-розшукової діяльності. В такому разі суди США користуються Законом «Про процедури з секретною інформацію» («Classified Information Procedures Act») (18 U.S.C. App. IV) 1980 року. Відповідно до цього закону в разі, якщо суддя вважатиме, що розкриття секретних відомостей є необхідним для вирішення питання про невинність підсудного, то він має право вимагати розкриття таких відомостей. Якщо в розкритті таких відомостей буде відмовлено відповідним державним органом, то судове переслідування припиняється. Як показує практика, в більшості випадків, коли виникали подібні ситуації, судове переслідування було припинено.

Крім зазначеного вище указу слід також відзначити, прийнятий 07.10.2011 року Президентом США Указ № 13587 «Про структурну реформу щодо підтримання безпеки секретних мереж та обґрунтованого поширення та убезпечення секретної інформації» («Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information»), який присвячено захисту секретної інформації, що циркулює в комп'ютерних мережах.

У Великій Британії закон з охорони державної таємниці також має назву «Про державну таємницю» («Official Secrets Act»). Він був прийнятий у 1989 році. Однак, історія законодавства з охорони державної таємниці у Великобританії значно довша. Вона бере початок ще у 1889 році, коли було вперше прийнято закон з аналогічною назвою.

Систему охорони державної таємниці викладено в Настанові з охорони державної таємниці (Manual of Protective Security), на базі якої міністерства розробляють власні настанови.

Згідно чинного законодавства Великобританії інформація з обмеженим доступом може мати чотири ступені секретності: «цілком таємно» (Top Secret); «таємно» (Secret); «конфіденційно» (Confidential); «для службового користування» (Restricted).

До інформації зі ступенем «цілком таємно» відносяться відомості, несанкціоноване розголошення яких може обернутися безпосередньою загрозою внутрішній стабільності Об'єднаного Королівства або дружніх йому країн; значними людськими втратами; може завдати тяжкої шкоди ефективності або безпеці британських чи союзницьких сил або розвідувальним операціям; заподіяти тяжку шкоду взаєминам з дружніми урядами або нанести довгострокові збитки економіці Королівства.

Прикладом правоохоронної інформації, яка відноситься до цієї категорії відомостей у Великій Британії є перелік потенційних мі-

ISSN 1995-6134

шеней терористів, база даних інформаторів та кримінальної розвідки тощо.

До інформації зі ступенем «таємно» відносяться відомості, несанкціоноване розголошення яких може обернутися підвищенням рівня міжнародної напруженості; серйозно зашкодити відносинам з дружніми урядами; безпосередньо загрожувати життю або завдати значної шкоди громадському порядку або безпеці та свободам особистості; завдати значної шкоди ефективності або безпеці британських чи союзницьких сил або розвідувальним операціям; спричинити істотну матеріальну шкоду національним фінансам чи економіці та комерційним інтересам.

Прикладом правоохоронної інформації, яка відноситься до цієї категорії відомостей у Великій Британії, є об'єкти спеціальних операцій; інформація, яка розшифровує особу інформатора, оскільки її розголошення може загрожувати його життю.

До інформації зі ступенем «конфіденційно» відносяться відомості, несанкціоноване розголошення яких може завдати матеріальної шкоди дипломатичним стосункам, що матиме наслідком офіційний протест або інші санкції; заподіяти шкоду безпеці та свободам особистості; завдати шкоди ефективності або безпеці британських чи союзницьких сил або розвідувальним операціям; спричинити шкоду національним фінансам чи економіці та комерційним інтересам; істотно підірвати фінансову спроможність основних (крупних) організацій; перешкодити розслідуванню або полегшити вчинення тяжкого злочину тощо.

Прикладом правоохоронної інформації, яка відноситься до цієї категорії відомостей у Великій Британії є відомості про інформаторів, які не розкривають їх справжньої особи, проте розголошення яких може загрожувати безпеці інформаторів; відомості про спеціальні операції, розкриття яких може зашкодити розслідуванню по тяжким злочинам; відомості про характер злочинної діяльності та можливі методи її припинення.

До інформації зі ступенем «для службового користування» відносяться відомості, несанкціоноване розголошення яких може зашкодити міжнародним стосункам, ускладнити забезпечення ефективності або безпеки британських чи союзницьких сил; завдати шкоди розслідуванню або полегшити скоєння злочину; завдати фінансової шкоди фізичним або юридичним особам, підірвати належний рівень управління державним сектором тощо.

Прикладом правоохоронної інформації, яка відноситься до цієї категорії відомостей у Великій Британії може бути інформація, отримана від поліції іншої країни, якщо така передача інформації не була загальновідомою, покази осіб у справі, розголошення яких може зашкодити розслідуванню тощо.

У Німеччині система захисту державних секретів перетинається із загальною системою захисту значущих секретів у сфері промисловості й торгівлі (промислове шпигунство) та регулюється нормами низки законів, до яких відносяться: Кримінальний кодекс, Закон про боротьбу з недобросовісною конкуренцією, Постанова про боротьбу з підкупом не посадових осіб, Федеральний закон про охорону даних тощо. Кримінальний кодекс Німеччини, наприклад, містить положення про те, що державною таємницею є факти, об'єкти й інформація, доступні лише обмеженому колу осіб, які повинні зберігатися в секреті від іноземних держав з метою недопущення нанесення шкоди зовнішній безпеці Федеративної республіки.

Удосконалення захисту державних секретів здійснюється за трьома напрямами: вдосконалення законодавства у сфері захисту державних секретів і секретів фірм; посилення органів контррозвідки та надання їм великих повноважень, у тому числі й у сфері захисту державних секретів; створення організацій «самодопомоги» в промисловості та розгортання їх діяльності.

Важливим у вдосконаленні захисту секретів під час проведення науково-дослідних ро-

ISSN 1995-6134

біт військового призначення в Німеччині є посилення органів контррозвідки, і, зокрема, тих її підрозділів, які покликані вести боротьбу зі шпигунством і займатися питаннями захисту державних секретів, у тому числі й у промисловості.

У системі забезпечення захисту державних секретів у питаннях боротьби з «промисловим шпигунством» іноземних держав важлива роль відводиться об'єднанням промисловців, так званим організаціям «самодопомоги». До таких організацій відноситься, наприклад, «Координаційний центр по забезпеченню безпеки в промисловості», створений у Кельні в 1969 році, який вирішує проблеми забезпечення режиму секретності в промисловості держави [12].

У ФРН інформація з обмеженим доступом може мати три ступені секретності: «цілком таємно» (Streng Geheim); «таємно» (Geheim); «конфіденційно» (VS-Vertraulich);

Слід зазначити, що у ФРН до державної таємниці відносяться лише відомості, які необхідно зберігати в секреті від іноземних держав з метою недопущення нанесення шкоди зовнішній безпеці Федеративної республіки. В той же час відомості, які містять інформацію про проведення оперативно-розшукових заходів, належать до службової таємниці та охороняються відповідним законодавством. Зокрема відповідальність за порушення службової таємниці встановлена у 28 Розділі Кримінального кодексу ФРН. Відповідні документи, що містять службову таємницю, позначають грифом «Для службового користування» (VS nur fur den dienstgebrauch).

Якщо документи для службового користування обробляються в автоматизованих системах, то мають бути дотримані певні вимоги безпеки. А саме автоматизовану систему має бути обладнано фаєрволом, у випадку підключення до мережі Інтернет, має бути затверджений перелік осіб, які мають доступ до автоматизованої системи, використовуватися механізми автентифікації та ідентифікації (ім'я користувача та пароль), обов'язковою є наявність Інструкції з IT-безпеки тощо [13, Section II (1)].

Систему захисту державної таємниці у Китайській Народній Республіці представлено Законом КНР «Про захист державної таємниці» (中华人民共和国保守国家秘密法) від 29.04.2010 р.

Згідно ст. 9 даного закону до державної таємниці відносяться, зокрема, окремі відомості, що стосуються діяльності з охорони державної безпеки та розслідування кримінальних злочинів. Саме ця категорія відомостей охоплює сферу оперативно-розшукової діяльності у класичному її розумінні.

Державна таємниця у Китаї за ступенем секретності поділяється на три рівні: цілком таємна (绝密); таємна (机密); конфіденційна (秘密).

Цілком таємна інформація – це найважливіша державна таємниця, розголошення якої може завдати дуже значну шкоду національній безпеці та національним інтересам.

Таємна інформація – це важлива державна таємниця, розголошення якої може завдати значну шкоду національній безпеці та національним інтересам.

Конфіденційна інформація – це державна таємниця, розголошення якої може завдати шкоду національній безпеці та національним інтересам (Article 10 [14]).

Конкретні сфери та категорії державної таємниці, визначаються державним відділом з охорони державної таємниці, спільно з міністерствами закордонних справ, відділом громадської безпеки, відділом державної безпеки та іншими відповідними центральними органами (Article 11 [14]).

На підставі досліджених матеріалів доходимо висновку, що на відміну від КНР, ФРН, а також країн пострадянського простору для США та Великобританії характерними є більш докладні приписи щодо віднесення тієї чи іншої правоохоронної інформації до державної таємниці. Дана обставина зумовлена

ISSN 1995-6134

прецедентною системою права, яка тяжіє до якомога більшої конкретизації рішень, що можуть бути прийняті в рамках тих чи інших суспільних відносин.

Серед розглянутих систем захисту оперативно-розшукової інформації за допомогою інституту таємниць найбільш схожими до української є системи Російської Федерації, КНР та Великобританії, хоча існує і певна структурна різниця у загальному підході до захисту державних секретів. Незважаючи на різницю в законодавчому регулюванні захисту інформації, яка є державною таємницею у Великобританії, КНР, Росії, США, ФРН та Україні бачимо, що інформація про проведення конкретних оперативно-розшукових заходів та залучення осіб до конфіденційного співробітництва має обмежений доступ в усіх цих країнах. Для неї передбачено окремий, особливий порядок отримання, обробки, зберігання, захисту та розсекречування. Процедурні питання роботи з такою інформацією мають приблизно однаковий характер в усіх цих країнах.

ЛІТЕРАТУРА

1. Доктрина інформаційної безпеки України / затв. Указом Президента України : від 08.07.2009 р. № 514/2009 // Офіційний вісник України. – 2009. – № 52. – Ст. 1783.

2. Закон України «Про основи національної безпеки України» : від 19.06.2003 р. // Офіційний вісник України. – 2003. – № 29. – Ст. 1433.

3. Носов В. В. Організація та забезпечення інформаційної безпеки : навч. посібник / В. В. Носов, О. В. Манжай. – Х. : Вид-во Харк. нац. ун-ту внутр. справ, 2007. – 216 с.

4. Закон України «Про державну таємницю» : від 21.01.1994 р. // ВВР України. – 1994. – № 16. – Ст. 93.

5. Звід відомостей, що становлять державну таємницю / затв. наказом Служби безпеки України : від 12.08.2005 р. № 440 // Офіційний вісник України. – 2005. – № 34. – Ст. 2089.

6. Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію / затв. Постановою Кабінету Міністрів України : від 27.11.1998 р., № 1893 // Офіційний вісник України. – 1998. – № 48. – Ст. 1764.

7. Федеральный закон РФ «О государственной тайне» : от 21.07.1993 г. // Российская газета. – 21.09.1993. – №182.

8. Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти / утв. Постановлением Правительства РФ : от 03.11.1994 г., № 1233 // Собрание законодательства РФ. – 2005. – № 30 (ч. II). – Ст. 3165.

9. Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера» : от 06.03.1997 г., №188 // Собрание законодательства РФ. – 1997. – № 10. – Ст. 1127.

10. Перечень сведений, отнесенных к государственной тайне / утв. Указом Президента РФ : от 30.11.1995 г., № 1203 // Российская газета. – 27.12.1995. – № 246.

11. Executive Order 13526 Classified National Security Information, December 29, 2009 [Електронний ресурс]. – Режим доступу: http://edocket.access.gpo.gov/2010/pdf/E9-31418.pdf.

12. Шавкеро А. Зарубежный опыт защиты государственной тайны и возможности его использования в России / А. Шавкеро // Право и жизнь. – 2008. – № 124 (7) [Електронний ресурс]. – Режим доступу: http://www.law-n-life.ru/arch/124/124-17.doc.

13. Instruction sheet on the Handling of Protectively Marked Information Classified VS-NUR FÜR DEN DIENSTGEBRAUCH (RESTRICTED) [Електронний ресурс]. – Режим доступу: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/VS-MerkblattEnglisch_pdf.pdf?__blob=

ISSN 1995-6134

publicationFile.

14. Law of the People's Republic of China on Guarding State Secrets (2010 Revision) [Електронний ресурс]. – Режим доступу: http://en.pkulaw.cn/display.aspx?id=8039&lib=law&SearchKeyword=&SearchCKeyword=.

Манжай О. В. Порівняльний аналіз забезпечення безпеки оперативно-розшукової інформації за допомогою інституту державної та службової таємниці в окремих країнах світу / О. В. Манжай // Форум права. – 2012. – № 1. – С. 593–600 [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/e-journals/FP/2012-1/12movokc.pdf

Проаналізовано нормативно-правову базу у сфері захисту державної та службової таємниці в окремих країнах Європи, Америки і Азії. Розкрито поділ інформації за ступенем секретності та надано визначення інформації, яка відноситься до кожного ступеню. Визначено механізм захисту оперативно-розшукової інформації за допомогою інституту таємниць.

***

Манжай А.В. Сравнительный анализ обеспечения безопасности оперативно-розыскной информации с помощью института государственной и служебной тайны в некоторых странах мира

Проанализирована нормативно-правовая база отдельных стран Европы, Америки и Азии в сфере защиты государственной и служебной тайны. Раскрыта классификация информации по степени секретности и дано определение информации, которая относится к каждой степени. Определен механизм защиты оперативно-розыскной информации с помощью института тайн.

***

Manzhai O.V. Comparative Analysis of Safety Providing of Information about Special Investigative Methods by the Institute of Protective Security in the Separate Countries of the World

The legal base of separate countries of Europe, America and Asia in the field of official secrets security is analyzed. Classification of information is exposed on the levels of secrecy and the definition of information which behaves to every level is given. The mechanism of defence of information about special investigative methods is certain by the official secrets institute.