

ОРГАНІЗАЦІЙНО-ПРАВОВІ ПИТАННЯ БЕЗПЕКИ ІНФОРМАЦІЇ

ОСНОВНІ ПОЛОЖЕННЯ ПОРЯДКУ ЗАСЕКРЕЧУВАННЯ ІНФОРМАЦІЇ У США

Олексій Муратов¹, Валерій Ворожко²

¹Національна академія Служби безпеки України

²Національний авіаційний університет

МУРАТОВ Олексій Євгенович, к.т.н., с.н.с.



Рік та місце народження: 1972 рік, м. Київ, Україна.

Освіта: Київський інститут військово-повітряних сил, 1994 рік.

Посада: начальник науково-дослідної лабораторії з 2003 року.

Наукові інтереси: інформаційна безпека, управління складними системами.

Публікації: більше 20 наукових публікацій, серед яких монографія, словник, наукові статті.

E-mail: amrtv@mail.ru

ВОРОЖКО Валерій Павлович



Рік та місце народження: 1953 рік, м. Гагра, Грузія.

Освіта: Московський державний історико-архівний інститут, 1975 рік.

Посада: доцент кафедри безпеки інформаційних технологій з 2009 року.

Наукові інтереси: інформаційна безпека, конкурентна розвідка, історія України та США.

Публікації: більше 40 наукових публікацій, серед яких монографії, навчальні посібники, наукові статті.

E-mail: wp06vv@gmail.com

Анотація. У статті розглядаються основні положення порядку засекречування та розсекречування інформації, визначеного у нормах виконавчого наказу Президента США 13526, робиться порівняльний аналіз з положеннями законодавства України у сфері охорони державної таємниці.

Ключові слова: інформація, засекречування, розсекречування, підходи, методи, Сполучені Штати Америки.

Вступ

Для забезпечення сталого розвитку країни, підвищення достатку її населення, безпеки особи і суспільства кожна держава вирішує завдання визначення та підтримання необхідної кількості інформації, доступ до якої обмежується. Сучасний етап побудови незалежної, демократичної, соціальної, правової України характеризується низкою проблемних питань у сфері наукового забезпечення державного регулювання віднесення інформації до державної таємниці. Слід зазначити, що в цьому Україна не є винятком. Аналогічні проблеми властиві багатьом, в тому числі, провідним країнам світу.

Оптимальне визначення мінімально необхідної кількості інформації з обмеженим доступом є необхідним для успішного вирішення завдань національної безпеки та сталого розвитку країни. Досягнення кращого балансу між обсягом загально доступної та доступної за спеціальним

порядком інформації у суспільстві гарантуватиме відсутність у суспільстві так званих "зайвих" секретів, що обмежують можливості у розвитку суспільства, з одного боку, а з іншого – те, що до інформації, яка внаслідок свого безконтрольного розповсюдження шкодить національним інтересам, будуть своєчасно вжиті заходи для попередження такого негативного впливу.

Аналіз досліджень і публікацій

Сьогодні можна виокремити декілька підходів, які одночасно застосовуються, доповнюючи один одного, і формують в українському суспільстві погляди на визначення обсягів державної таємниці. Перший підхід представляє собою наукове узагальнення та аналіз практики нормативно-правового регулювання та методичного забезпечення у сфері віднесення інформації до державної таємниці. Дослідження за цим підходом як правило здійснюється за часом (історичний аспект)

та у просторі (за країнами) [1-7]. Такий підхід дозволяє меншими зусиллями одержати результати, достатні для впровадження у практичну діяльність за необхідності удосконалення останньої.

За другим підходом припускається, що ключем до визначення секретної інформації та її необхідної кількості є критерії оцінювання шкоди, яка може бути завдана національній безпеці внаслідок розголошення інформації. Наукове розв'язання завдання з визначення таких критеріїв пов'язане з необхідністю формування загальної моделі держави в існуючому світовому порядку з урахуванням інформаційних потоків, до яких вона залучена. На сьогодні це є проблемою і можна говорити лише про деяке наближення до її практичного розв'язання, коли виокремлюються основні складові таких критеріїв, формалізується механізм заподіяння шкоди розповсюдженням інформації для створення потрібного математичного опису моделі, накопичується досвід вчених інших країн, формується необхідне уявлення про такі категорії як нація, інформація, безпека, національна безпека, шкода національній безпеці тощо [8].

Окрему групу складають дослідження з удосконалення методики та технології автоматизації роботи експертів з питань таємниць [9-11].

Серед зазначених підходів за кількістю публікацій лідирує перший. Предметне поле досліджень цього підходу величезне і до того ж воно зазнає постійних змін. Так, американська система засекречування інформації вже висвітлювалася у статтях В.П.Ворожжа [5, 6]. Однак матеріал цих статей базувався на джерелах та публікаціях 80-х та початку 90-х років минулого сторіччя. У порівнянні з тим часом сучасна світова інформаційна інфраструктура суттєво змінилася, зазнала змін і нормативна база, яка є основою для функціонування американської системи засекречування інформації.

З 1940 року питання віднесення інформації до секретної у загальнодержавному масштабі регулюються нормативно-правовими актами Президента Сполучених Штатів Америки [5]. У 2009 році Президентом Сполучених Штатів був підписаний executive order (виконавчий наказ) 13526 "Classified National Security Information" [12] – "Класифікована інформація у сфері національної безпеки" – (далі – ЕО 13526), який нині встановлює сучасні правила засекречування (класифікації) інформації у Сполучених Штатах Америки.

Інтерес до системи засекречування інформації у Сполучених Штатах Америки обумовлюється значною роллю цієї країни у світі, а також тим, що у зв'язку з опублікуванням великого масиву інформації з обмеженим доступом у мережі Інтернет (Wikileaks.org) американським установам прийшлося за короткий строк переглянути величезний обсяг інформаційних масивів на предмет визначення необхідності їх подальшого засекречування та попередження шкоди національній безпеці, а також удосконалити власну інформаційну політику.

Метою цієї статті є розгляд основних підходів до засекречування інформації та її матеріальних носіїв у сучасній системі засекречування інформації

Сполучених Штатів Америки на основі змісту норм ЕО 13526.

Основна частина дослідження.

Для визначення секретної інформації у Сполучених Штатах використовується термін "класифікована" (classified). Процес засекречування (віднесення до класифікованої або класифікації) інформації визначається за допомогою термінів "первинна" (original) та "похідна" (derivative) класифікація. Якщо спробувати провести аналогію не за загальним змістом слів, а за змістом процесів, що ними позначаються, то можна зазначити, що: первинне засекречування пов'язується зі створенням "нових" секретів і включає дві дії, аналогічні передбаченим українським законодавством щодо віднесення інформації до секретної та засекречування матеріального носія цієї інформації; похідне засекречування не пов'язується зі створенням "нових" секретів і включає тільки засекречування матеріального носія інформації на підставі того, що він містить вже засекречену інформацію, про що зазначено на іншому носіїві інформації або в окремих інструкціях з засекречування (classification guides).

У подальшому для відрізнення первинного засекречування від похідного у межах цієї статті використовуватимуться термінологічні словосполучення "засекречування інформації" та "засекречування носія інформації". Слід ще раз зазначити, що віднесення інформації до державної таємниці ("засекречування інформації") за нормативно-правовими актами Сполучених Штатів збігається з першим засекречуванням носія цієї інформації. В законодавстві ж України такі дії розрізняються і завершене віднесення інформації до державної таємниці може не передбачати одночасної появи першого засекреченого носія цієї інформації.

За законодавством України засекречування інформації здійснюють уповноважені особи, яких визначає Президент України або Голова Верховної Ради України, – експерти з питань таємниць. Нині їх кількість не перевищує двохсот. У Сполучених Штатах Америки діє у загальному схожий підхід. Особи, уповноважені здійснювати засекречування інформації, (original classification authorities або OCAs), яких також називають "класифікаторами" (original classifiers), призначаються Президентом і Віце-Президентом Сполучених Штатів з числа керівників агентств (центральної державних органів) та інших посадових осіб. Президент та Віце-Президент є також особами, уповноваженими здійснювати засекречування інформації. На відміну від українського законодавства, особи, визначені класифікаторами у Сполучених Штатах у системі державної влади, можуть делегувати свої повноваження щодо засекречування інформації підпорядкованим посадовим особам. ЕО 13526 містить норму про необхідність обмеження чисельності осіб, яким делегуються повноваження з засекречування інформації, мінімальною необхідною кількістю. Також зазначається про необхідність обґрунтування таких рішень, їх централізованого

обліку та уникання випадків делегування повноважень для тимчасового, разового використання права з засекречування інформації.

З початку XXI сторіччя кількість осіб, яким було надано право засекречування інформації, була відносно стабільною - близько 4100 осіб. У 2008-2009 роках чисельність ОСАs суттєво зменшилася (майже на 40%). Це пов'язується саме з посиленням вимог до делегування повноважень в ЕО 13526 та зусиллями зі зменшення чисельності таких осіб, що були здійсненими насамперед у Міністерстві закордонних справ (Department of State). У 2010 році таких осіб було 2378 [13].

Посадові особи з делегованими повноваженнями від інших ОСАs розрізняються за своїми правами щодо класифікації інформації різних рівнів засекречування (classification levels). Якщо проводити паралель з українською термінологією сфери охорони державної таємниці, то американським рівням засекречування відповідатимуть вітчизняні ступені секретності. Найвищим (з трьох існуючих) рівнем засекречування є "Top Secret". Цьому рівню відповідає український ступінь секретності "Особливої важливості" [14]. Особам, яких визначено уповноваженими засекречувати інформацію з таким рівнем засекречування, вважаються уповноваженими засекречувати інформацію з нижчими рівнями засекречування "Secret" (відповідає українському ступеню секретності "Цілком таємно" [14]) та "Confidential" (відповідає українському ступеню секретності "Таємно" [14]). Наприклад, у 2010 році осіб, яких було визначено уповноваженими засекречувати інформацію "Top Secret", "Secret" і "Confidential", було 901 (38%), "Secret" і "Confidential" - 1463 (61,5%), "Confidential" - 14 (0,5%) [13].

Для регулювання обсягу засекреченої інформації в ЕО 13526 встановлюються правила засекречування і розсекречування інформації. До основних правил засекречування (крім того, що засекречування інформації здійснюється тільки уповноваженими на це особами) належать наступні, які повинні виконуватись разом:

1) інформація повинна мати відношення до системи державної влади Сполучених Штатів (находитись у її власності, під її контролем або створена нею чи для неї);

2) інформація повинна належати до встановлених законодавством категорій інформації;

3) особа, уповноважена засекречувати інформацію, повинна визначати, що розголошення (в ЕО 13526 використовується словосполучення "unauthorized disclosure" - несанкціоноване розкриття) цієї інформації резонно завдасть шкоди національній безпеці, у тому числі антитерористичній діяльності. При цьому така шкода повинна бути визначеною або описаною цією особою.

Інформацію слід засекречувати за рівнем "Top Secret", якщо її розголошення завдасть надзвичайно тяжкої (exceptionally grave) шкоди національній безпеці, "Secret" - серйозної (serious) шкоди, "Confidential" - шкоди національній безпеці без визначення особливих її ознак.

Під шкодою національній безпеці (damage to the national security) розуміється шкода (harm) національній обороні або міжнародним відносинам Сполучених Штатів. Як можна побачити, сфер державної діяльності, охоплених питаннями національної безпеки, де можлива поява секретної інформації, законодавством США визначено менше ніж в Україні, де до них віднесено: оборона, економіка, наука і техніка, зовнішні відносини, державна безпека та охорона правопорядку (див. Закон України "Про державну таємницю"). З метою засекречування інформації урядів іноземних країн передбачається, що несанкціоноване поширення інформації іноземного уряду завдає шкоди національній безпеці Сполучених Штатів. Наявність суттєвих сумнівів у необхідності засекречування інформації у особи, уповноваженої на це дію, визнається достатньою підставою для залишення інформації некласифікованою.

Законодавство Сполучених Штатів визначає категорії інформації або певні сфери державної діяльності, у яких інформація може бути засекреченою. Це: системи озброєння, воєнні та військові операції та плани; інформація іноземних урядів; заходи, джерела та методи розвідки або криптології; міжнародні відносини або закордонні заходи Сполучених Штатів, включаючи конфіденційні джерела; наукові, технологічні або економічні питання, пов'язані з національною безпекою; програми системи державної влади Сполучених Штатів для забезпечення безпеки ядерних матеріалів та устаткування; уразливість та можливості систем, пристроїв, інфраструктур, проектів, планів або служб захисту, пов'язаних з національною безпекою; розроблення, виробництво або використання зброї масового ураження.

Слід зазначити, що поняттям розвідка у ЕО 13526 охоплюється й контррозвідка. За 2010 рік у Сполучених Штатах було зареєстровано 224734 випадки засекречування інформації, з них за рівнями: "Top Secret" - 4194 (2%), "Secret" - 181045 (81%), "Confidential" - 39495 (17%) [13].

Законодавство Сполучених Штатів (як і українське законодавство) визначає випадки, коли інформацію заборонено засекречувати. Рішення про необхідність засекречування чи розсекречування інформації ні в якому разі не повинні мати за мету: приховування порушення закону, неефективності або помилки державного управління; запобігання складним ситуаціям, у яких може опинитись особа, підприємство або установа; обмеження конкуренції; зупинення чи призупинення поширення інформації, для якої немає підстав для засекречування.

За загальним правилом, інформацію, що вже була розсекреченою, не слід знову засекречувати. Така дія потребує особливого обґрунтування. Не слід також засекречувати інформацію про наукові дослідження, що не стосуються національної безпеки.

Засекречування носіїв інформації (похідне засекречування), не пов'язується зі створенням "нових" секретів, а лише зі збільшенням кількості форм матеріального втілення вже існуючих, тобто кількості носіїв секретної інформації. У 2010 році у Сполучених Штатах було зафіксовано 76,6 мільйонів рішень про

засекречування носіїв інформації, з них за рівнями: "Top Secret" - 21,5 млн. (28%), "Secret" - 36 млн. (47%), "Confidential" - 19,1 млн. (25%). Представляє інтерес те, що у 2009 році було зафіксовано зростання кількості таких рішень більше ніж у двічі, а у 2010 році - ще приблизно на 30%, у 2011 році також очікується їх зростання. Це явище пов'язується з виконанням керівних документів, прийнятих у 2009 році та спрямованих на підвищення пильності у фіксуванні рішень з засекречування носіїв інформації особливо у сфері електронного документообігу [13].

Положення ЕО 13526 містять вимоги про обов'язкове навчання осіб, які мають право засекречувати інформацію, (раз на рік) та осіб, які засекречують носії інформації, (раз на два роки). Осіб, які не пройшли таке навчання, керівникам агентств наказується позбавляти права засекречувати інформацію чи носії інформації. Також ЕО 13526 містить деякі вимоги до змісту такого навчання, що повинне включати вивчення порядку засекречування та розсекречування інформації та її носіїв з акцентуванням уваги на попередження зайвого засекречування. Крім того навчання повинно передбачати порядок забезпечення безпеки секретної інформації (порядок забезпечення режиму секретності) та санкції, які застосовуватимуться до порушників порядку засекречування та розсекречування інформації та її носіїв і порядку забезпечення режиму секретності. Серед таких санкцій визначено: догана, тимчасове утримання заробітної плати, звільнення з посади, обмеження у правах із засекречування, позбавлення права допуску чи відмову у наданні доступу до секретної інформації тощо.

Невід'ємною складовою системи засекречування (security classification system) визнається розсекречування. Важливими правилами розсекречування інформації є припущення про те, що ніяка інформація не може залишатись засекреченою невизначено довго, і те, що факт розголошення інформації не є підставою для її автоматичного розсекречування.

Прийнято виокремлювати чотири шляхи, за якими інформація та її носії можуть бути розсекречені: внаслідок автоматичного розсекречування (Automatic Declassification), внаслідок систематичного перегляду для розсекречування (Systematic Declassification Review), внаслідок дискреційного ("на власний розсуд") перегляду для розсекречування (Discretionary Declassification Review), внаслідок мандатного ("за запитом") перегляду для розсекречування (Mandatory Declassification Review). Автоматичне розсекречування є загальним правилом розсекречування інформації, за яким через 25 календарних років після засекречування інформація повинна бути розсекреченою. У зв'язку з існуванням великої кількості винятків із загального правила розсекречування ЕО 13526 передбачає необхідність здійснення систематичного перегляду інформації для розсекречування. Організація такого перегляду вимагає створення у кожному агентстві переліків секретної інформації та її носіїв, яких виключено з

автоматичного розсекречування, та відповідних планів (програм) з їх перегляду.

Протягом 2010 року у Сполучених Штатах було переглянуто 45,4 млн. сторінок документів у рамках автоматичного розсекречування та 5,8 млн. сторінок документів у рамках систематичного перегляду. За результатами першого було розсекречено 24,2 млн. сторінок документів і другого - 4,6 млн. сторінок документів [13].

Слід зазначити, що строк засекречування інформації може бути як менший так і більший 25 років. Найтриваліші строки (50 та 75 років) засекречування як правило встановлюються для інформації, яка може розкрити особу, яка є конфіденційним чи розвідувальним джерелом інформації, або концепції (ноу хау) створення зброї масового ураження.

Дискреційний ("на власний розсуд") перегляд здійснюється у випадках, коли з точки зору особи, яка засекретила інформацію, або агентства, в якому було засекречено інформацію, з'явилися підстави вважати, що ця інформація може бути розсекреченою до встановленого під час її засекречування терміну. За таким типом розсекречування протягом 2010 року у Сполучених Штатах було переглянуто 1,9 млн. сторінок документів, з яких розсекречено приблизно 181,6 тис. [13].

До цього типу розсекречування законодавство Сполучених Штатів визначає відносно новий в Україні привід для розгляду доцільності обмеження доступу до інформації "підвищений суспільний інтерес". Перевага шкоди від оприлюднення інформації над суспільним інтересом в її отриманні встановлюється сучасним українським законодавством (див. частину 2 статті 6 Закону України "Про доступ до публічної інформації") однією з необхідних умов для обмеження доступу до інформації.

У Сполучених Штатах підвищений суспільний інтерес також не є достатньою підставою для розсекречування інформації. Його можна вважати обставиною, яка може виникати і яку необхідно враховувати під час прийняття рішення про необхідність залишення інформації засекреченою чи ні. Поява такої обставини становить підставу для організації позапланового розгляду інформації, до якої такий інтерес виник, особою, яка засекретила цю інформацію, на предмет можливого її розсекречування з огляду на те, що незадоволення суспільного інтересу також може мати шкідливі наслідки для національної безпеки. Якщо така шкода перевищуватиме шкоду від розголошення секретної інформації, то інформацію слід розсекречувати. Треба зазначити, що в ЕО 13526 рекомендується розсекречувати інформацію, до якої виник суспільний інтерес.

Перегляд класифікованої інформації "за запитом" на її можливе розсекречування (Mandatory Declassification Review) є відносно новим шляхом розсекречування інформації у Сполучених Штатах, але як визнається дуже дієвим і перспективним. Він здійснюється у відповідь на письмовий запит

зовнішнього для агентства суб'єкта про розсекречування певної інформації. У 2010 році було опрацьовано 67726 запитів про розсекречування, за якими було переглянуто 331782 сторінки. У результаті такого перегляду тільки 22089 сторінок (7%) залишилися засекреченими, 213425 сторінок (64%) були розсекреченими у повному обсягу, 96268 сторінок (29%) були розсекреченими частково [13]. ЕО 13526 встановлює обмеження щодо можливості невідкладного проведення перегляду інформації для її розсекречування. Ці обмеження можуть бути пов'язаними з неможливістю ідентифікації інформації у державному органі за ознаками, зазначеними у запиті, а також з тимчасовою заборонаю у доступі до інформації з метою невідкладного проведення її перегляду для розсекречування, у визначених законодавством випадках.

Зважаючи на значущість та необхідність централізації заходів з розсекречування, в ЕО 13526 передбачається створення Національного центру з розсекречування (National Declassification Center) у структурі Адміністрації національних архівів та документації (National Archives and Records Administration) для спрямування процесів розсекречування, сприяння заходам, гарантуючим якість розсекречування, та впровадження одноманітного профільного навчання. Керівник Національного центру з розсекречування призначається керівником зазначеної адміністрації (Архівістом Сполучених Штатів) за погодженням з керівниками декількох державних органів (Міністерства закордонних справ, оборони, енергетики, внутрішньої безпеки, Генеральним прокурором, Директором Національної розвідки).

ЕО 13526 зобов'язує керівників державних органів забезпечувати директора Національного центру з розсекречування методичною документацією з розсекречування, а також за посередництвом керівництва Адміністрації національних архівів та записів визначати частину особового складу цього Центру, якому делегувалися б повноваження з перегляду, розсекречування (залишення засекреченою) інформації, яка була створена у підпорядкованих цим керівникам державних органах.

Повноваження щодо розсекречування інформації, одержаної від інших державних органів (агентств), які у подальшому були ліквідованими, встановлюються за такими правилами: якщо було визначено державного органу, якому передано функції ліквідованого, то зазначені повноваження переходять до нього; якщо такого державного органу не було визначено, то зазначені повноваження переходять до кожного державного органу, який має секретні носії інформації, що були створеними у ліквідованому державному органі. При цьому розсекречування таких документів слід здійснювати за погодженням з іншими державними органами, які володіють примірниками таких документів. Річне фінансування діяльності, пов'язаної з засекречуванням інформації та забезпеченням її безпеки, у Сполучених Штатах, наприклад, у 2009

році складало близько 8,8 мільярдів доларів США [15].

Висновки

Системи засекречування (розсекречування) інформації США та України у загальному є схожими: наявність класифікаторів або державних експертів з питань таємниць, рівнів засекречування або ступенів секретності, строків засекречування, подібність загальних підходів до засекречування (розсекречування) інформації тощо. Але, звичайно, є й відмінності. Особливістю українського законодавства у сфері охорони державної таємниці є передбачення наявності єдиного державного нормативного акта – зводу відомостей, що становлять державну таємницю, – який об'єднує результати застосування всіх правил засекречування інформації у цілому у державі. Цей акт створює підґрунтя для централізації та уніфікації роботи всіх державних експертів з питань таємниць. У Сполучених Штатах робота посадових осіб, уповноважених з засекречування інформації, має більш відокремлений та незалежний характер. Поряд з цим уряд докладає зусиль щодо підвищення ступеня уніфікації роботи зазначених посадовців, що виражається у наявності планів зі створення єдиних правил засекречування (розсекречування) інформації. Деякі методичні підходи з засекречування носіїв інформації, що застосовуються у Сполучених Штатах, можуть бути використаними і в Україні.

На кожному засекреченому носії інформації (у випадку похідного засекречування) зазначаються ідентифікатори того носія інформації, використання інформації з якого стало підставою для засекречування першого. Застосуванням таких позначок можна суттєво зменшити витрати коштів на пошук і прийняття рішення про розсекречування окремого носія інформації у випадках, коли частину носіїв однієї інформації вже розсекречено. Система відміток з засекречування на носіях інформації дозволяє також завжди ідентифікувати посадову особу, яка здійснила засекречування цієї інформації. Виокремлення спеціальними позначками місць у документах, де наведено секретну інформацію, також сприятиме зручності виконання дій з розсекречування чи перегляду документів для розсекречування. Оцінювання результатів перегляду з розсекречування інформації та документів, що містять таку інформацію, за сторінками (аркушами) документів, а не за окремими одиницями обліку – документами, справами і т.п., сприяє більш ґрунтовному аргументуванню розсекречування. До того ж такий підхід точніше відображає витрати праці на виконання такої роботи.

Заслугує на увагу положення щодо визначення підстав для заборони не тільки засекречування інформації, а також її розсекречування та зміни ступеня секретності. При цьому слід звернути увагу на те, що визначається не сама інформація (наприклад, "відомості про...", "інформація про..."), а мета діянь, заради досягнення якої очікуються намагання суб'єктів змінити порядок доступу до будь-якої інформації.

При організації заходів з засекречування (розсекречування) інформації у США застосовується поєднання принципів централізації та колегіальності. З одного боку при Адміністрації національних архівів та документації визначено центральний орган виконавчої влади, уповноважений за цими питаннями, а з іншого – до складу цього органу входять представники всіх державних органів, в яких створюється основна частина "секретів". Особлива увага приділяється питанню підвищення кваліфікації всіх посадових осіб, яких залучено до виконання завдань з засекречування (розсекречування) інформації, та автоматизації (комп'ютеризації) обліку засекреченої інформації та її носіїв, а також інформації, яка була розсекреченою.

Література

- [1] Ботвінкін О.В. Історія охорони державної таємниці в Україні: монографія / О.В. Ботвінкін, В.М. Шлапаченко, В.П. Ворожко, А.С. Пашков. – К.: Наук.-вид. відділ Національної академії Служби безпеки України, 2008. – 155 с.
- [2] Мاستяниця Й.У. Охорона державних секретів незалежної України (Історично-правові нариси) / Й.У. Мاستяниця, Л.Є. Шиманський, О.В. Олійник, В.П. Ворожко // За заг. ред. П.О. Мисника, О.В. Зайчука. – К.: Інститут законодавства Верховної Ради України, 2010. – 128 с.
- [3] Бернадський Б.В. Охорона державної таємниці як складова частина контрозвідувальної діяльності департаменту поліції МВС Російської імперії (на прикладі українських губерній) / Б.В. Бернадський. – К.: Наук.-вид. відділ Національної академії Служби безпеки України, 2010. – 274 с.
- [4] Ворожко В.П. Нарис історії охорони державної таємниці в Україні / В.П. Ворожко, Б.В. Бернадський, О.В. Ботвінкін. – К.: Лазурит-Поліграф, 2012. – 188 с.
- [5] Ворожко В.П. Система засекречивання і рассекречивання информации в США / В.П. Ворожко // Безопасность информации. – 1997. – №1(8). – С. 48-53.
- [6] Ворожко В.П. Область государственной тайны в США / В.П. Ворожко // Защита информации. Сборник научных трудов. Киевский международный

университет гражданской авиации. – Вып.1. – 1995. – С. 97-102.

[7] Авдошин І.В. Охорона державної таємниці в постсоціалістичних країнах: Естонська Республіка, Румунія, Чеська Республіка: навчальний посібник / І.В. Авдошин, В.В. Макаренко, С.М. Сидоренко. – К.: Наук.-вид. відділ НА СБУ, 2011. – 166 с.

[8] Архипов О.Є. Критерії визначення можливої шкоди національній безпеці України у разі розголошення інформації, що охороняється державою: моногр. / О.Є. Архипов, О.Є. Муратов. – К.: Наук.-вид. відділ НА СБУ, 2011. – 195 с.

[9] Архипов О.Є. Оцінювання якості роботи експертів за даними багатооб'єктної експертизи / О.Є. Архипов, С.А. Архіпова // Захист інформації. – №4 (53) – 2012. – С. 45-54.

[10] Корченко О.Г. Система підтримки прийняття рішень державних експертів з питань таємниць у сфері оборони / О.Г. Корченко, Ю.О. Дрейс // Збірник матеріалів IV-ої науково-технічної конференції "Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення", 22-23 жовтня 2008 р., м. Київ. – К.: ВПНГУУ "КІП", 2008. – С. 188.

[11] Корченко О.Г. Удосконалення проведення процедури прийняття рішень державних експертів з питань таємниць у сфері оборони засобами інформаційних технологій / О.Г. Корченко, Ю.О. Дрейс // Збірник матеріалів міжвідомчої науково-практичної конференції "Сучасні проблеми захисту інформації з обмеженим доступом": 20-21 листопада 2008р, м.Київ. – К.: НАУ, Національна академія Служби безпеки України, 2008. – С. 62-63.

[12] Classified National Security Information. Executive Order 13526. Presidential Documents. // Federal Register. – Vol. 75. – No 2. – P. 707-731.

[13] ISOO Report to the President for FY 2010. – Washington: NARA, 2011. – 27 p.

[14] Угода між Урядом України та Урядом Сполучених Штатів Америки про охорону секретної інформації у сфері оборони // Відомості Верховної Ради України. – 2004. – №36. – ст.441.

[15] CRS – Classified Information Policy and Executive Order 13526 // Електронний ресурс. Режим доступу: <http://web.docuticker.com/go/docubase/62605>.

УДК 654.028.4:004.01 (73) (045)

Муратов А.Е., Ворожко В.П. Основные положения порядка засекречивания информации в США

Аннотация. В статье рассматриваются основные положения порядка засекречивания и рассекречивания информации, установленного нормами исполнительного приказа Президента США 13526, делается сравнительный анализ с положениями законодательства Украины в сфере охраны государственной тайны.

Ключевые слова: информация, засекречивание, рассекречивание, подходы, методы, Соединенные Штаты Америки.

Muratov O.Ye., Vorozhko V.P. The basic provisions of information classification order in the USA

Abstract. The basic provisions of information classification and declassification order are considered, the article is focused on US Executive Order 13526 content, comparative analysis with Ukrainian statutory provisions is presented.

Keywords: information, classification, declassification, ways, methods, United States of America.

Отримано 19 квітня 2012 року, затверджено редколегією 04 червня 2012 року

(рецензент д.т.н., професор О.Є. Архипов)