УДК 341.123(045)

КНЯЗЄВ Сергій Олександрович

ДОСВІД ПРАВОВОГО РЕГУЛЮВАННЯ ВІДНЕСЕННЯ ІНФОРМАЦІЇ ДО ДЕРЖАВНОЇ ТАЄМНИЦІ У США

Постановка проблеми. Взятий Україною курс на європейську та євроатлантичну інтеграцію поставив перед нашою державою низку завдань щодо приведення державних механізмів до високих стандартів країн – членів ЄС та НАТО. Особливої актуальності серед цих механізмів набуває захист державних інформаційних ресурсів, який повинен забезпечувати інтереси національної безпеки у балансі із дотриманням прав і основоположних свобод людини і громадянина, принципу прозорості у роботі суб'єктів владних повноважень.

Як зазначалось у Стратегії національної безпеки України, яка була затверджена Указом Президента України від 26 травня 2015 року № 287/2015, Революція гідності відкрила перед Україною можливості для побудови нової системи відносин між громадянином, суспільством і державою на основі цінностей свободи і демократії [1].

Зважаючи на новітні загрози в інформаційній сфері, в Стратегії, у тому числі звертається увага на фізичну і моральну застарілість вітчизняної системи охорони державної таємниці та інших видів інформації з обмеженим доступом, що вимагає реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів тощо [1].

У цьому контексті суттєву допомогу щодо подальшого розвитку вітчизняної системи охорони державної таємниці безперечно надає вивчення зарубіжного досвіду провідних країн світу. Враховуючи багаторічний досвід США та достатню ефективність існуючої у цій країні системи захисту секретної інформації, дослідження їх досвіду правового регулювання віднесення інформації до державної таємниці набуває особливої актуальності.

Аналіз останніх досліджень і публікацій. Тема дослідження різних аспектів іноземного досвіду, в тому числі у сфері охорони державної таємниці, в науці не є принципово новою. На необхідність постійного наукового супроводження цієї теми в своїх роботах наголошували І. В. Авдошин, В. Ю. Артемов, С. В. Болдир, В. П. Ворожко, О. В. Гладківська, І. В. Грищенко, А. М. Гуз, В. В. Макаренко, А. І. Марущак, О. Є. Муратов, В. Г. Пилипчук, О. Г. Семенюк, О. М. Солодка, І. М. Сопілко, В. М. Шлапаченко та інші.

Зокрема, І. В. Авдошин зазначав, що вивчення відповідного досвіду країн ЄС і НАТО з практичної точки зору надасть можливість розробити концептуальні підходи для вдосконалення національних правових механізмів адміністративного управління системою охорони державної таємниці в Україні [2, с. 39].

І. В. Грищенко зважала на важливість вивчення досвіду країн Східної Європи, оскільки вони упродовж тривалого часу перебували в соціалістичному таборі, згодом пройшли період «дерадянізації» і реформували свої системи охорони державної таємниці на основі урахування досвіду провідних країн світу [19, с. 19].

А. М. Гуз констатував, що сьогодні міжнародні стандарти інформаційної безпеки все більше стають основою для розробки стандартів безпеки й ефективних методів управління інформаційною безпекою в конкретній організації, на підприємстві, в установі [3, с. 67].

У свою чергу, О. В. Гладківська у своєму дослідженні акцентувала увагу на проблемах і неузгодженості термінології під час укладання нашою країною міждержавних угод про взаємний захист секретної інформації, що суттєво заважає правильному розумінню предмета захисту [4].

Разом з тим О. Г. Семенюк застерігав, що копіювання чужого, нехай і найуспішнішого досвіду, недостатньо продумане перенесення його на наш ґрунт без урахування українських реалій ніколи не приводило до успіху [20, с. 342].

Багатогранність системи охорони державної таємниці, застосування комплексного підходу під час реалізації режимних заходів, врахування новітніх викликів та загроз використанню цієї категорії інформації з обмеженим доступом вимагають постійного наукового супроводження, пошуку нових можливих шляхів підвищення її ефективності.

Метою статті є з'ясування аспектів досвіду правового регулювання віднесення інформації до державної таємниці у США та можливостей його врахування у вітчизняній системі охорони державної таємниці.

Виклад основного матеріалу. Правові основи щодо особливостей використання державної таємниці (далі також – секретної інформації) у США знаходять своє закріплення в низці законодавчих актів, які приймались у різні часи, зважаючи на пріоритети та загрози існуванню цієї інформації.

Варто відмітити нормативно-правові акти, які певною мірою стосуються охорони секретної інформації у США: «Про національну безпеку», «Про атомну енергію», «Про свободу інформації», «Про висвітлення діяльності уряду», «Щодо нагляду за іноземною розвідкою», «Про безпеку комп'ютерних систем», «Про розвідувальні органи», «Про заходи щодо зміцнення контррозвідки і безпеки», «Про удосконалення інформаційної безпеки», «Про внутрішню безпеку» тощо [5–9].

Наприклад, закон «Про національну безпеку» було прийнято після Другої світової війни у 1947 році [7]. Звідти питання використання секретної інформації, які співвідносяться із національною безпекою, були пов'язані

із певною реорганізацією та перебудовою збройних сил США. Зокрема, перепідпорядкування міністерству оборони сухопутних військ та військово-морських сил, які до цього мали окреме керівництво на рівні міністерств, реорганізація військово-повітряних сил тощо.

Також норми закону спрямовані на впорядкування діяльності спеціальних служб *(ЦРУ, Central Intelligence Agency, CIA)*. ЦРУ стало першою у США розвідувальною структурою у мирний час. Створення Ради національної безпеки *(National Security Council, NSC)*, як комітету радників президента США з питань внутрішньої, зовнішньої, а також військової політики, що стосуються державної безпеки.

Безпосередньо зміст поняття «національна безпека» включає національну оборону та/або зовнішні відносини Сполучених Штатів.

З урахуванням закону «Про національну безпеку» розробляються Стратегії національної безпеки США – документи, у яких визначаються пріоритетні напрями внутрішньої та зовнішньої політики США, а також виокремлюються основні загрози безпеці країни та її національним інтересам за кордоном (документ має загальний директивний характер, у подальшому його деталізують та конкретизують інші документи, у тому числі військові стратегії) [9].

Нову Стратегію національної безпеки було представлено президентом США Д. Трампом 18 грудня 2017 року. Подібні стратегії до цього приймались, зокрема у 2002, 2006, 2010 та 2015 роках.

Презентуючи нову стратегію, Д. Трамп наголосив: «Ми усвідомлюємо, що слабкість – це найнадійніший шлях до конфлікту, а неперевершена сила – це найнадійніший засіб для захисту». Крім того, було підкреслено, що такі країни, як Росія, «використовують інформаційні інструменти в спробі підірвати легітимність демократій. Своїм вторгненням до Грузії та України Росія продемонструвала готовність порушувати суверенітет держав регіону» [9].

У свою чергу, закон «Про свободу інформації» закріпив на законодавчому рівні право доступу громадськості до інформації, крім випадків, коли така інформація захищена від публічного (відкритого) використання [6].

30 червня 2016 року президентом Б. Обамою були підписані зміни до закону «Про свободу інформації», які стосувалися декількох істотних та процедурних правок, а також визначення нових вимог щодо звітності міністерств.

Поняття «інформація» тлумачиться як будь-які знання, що можуть бути передані, або документальні матеріали незалежно від їх фізичної форми та характеристик, які створюються, виробляються та належать уряду Сполучених Штатів. «Контроль за використанням інформації» – забезпечується уповноваженими структурами, що можуть створювати відповідну інформацію, або їх правонаступниками з метою забезпечення правомірного доступу до інформації.

Законодавство США визначає своє ставлення й до надмірного, невиправданого засекречування.

Наголошується, що зайва секретність призводить перш за все до підриву суспільної довіри до уряду, особливо, якщо це використовують неправомірно з метою виправдання політичного курсу, приховування зловживань, корупції та неналежного керування.

Якщо суспільство вважає, що уряд враховує лише особисті інтереси і використовує надмірну секретність у цілях втаємничення своєї діяльності або дезінформування громадськості, то це підриває довіру до уряду, викликає сумніви в його легітимності і призводить до того, що завоювання громадської підтримки будь-яких дій уряду буде пов'язане зі значними труднощами [9; 12; 13].

У цьому контексті варто згадати радянську систему охорони державної таємниці, ефективність якої ґрунтувалась на «тотальному засекречуванні інформації та обмеженнях».

Надмірна секретність має й інші негативні наслідки. «Надлишкова засекреченість» інформації може знизити рівень її захищеності. Навіть із «найзасекреченіших файлів» може статися витік інформації, якщо система встановлення грифа секретності не організована належним чином.

Як зазначав суддя Верховного суду США Потер Стюарт у справі «Про документи Пентагону» ще у 1971 році, «тотальна засекреченість перетворюється у відсутність якої б то не було секретності, а система допуску ігнорується циніками і нехлюями і стає об'єктом маніпуляції збоку тих, кого хвилює лише захист власних інтересів та просування по службі» [13].

Під поняттям «секретна інформація» законодавство США визначає інформацію, що отримана чи належить уряду США, яка стосується національної оборони та зовнішніх зв'язків США та яка віднесена до державної таємниці у відповідності до законодавства спеціальним уповноваженим суб'єктом з метою захисту інтересів національної безпеки від несанкціонованого використання [9].

На президента покладається безпосередня відповідальність щодо забезпечення національної безпеки, формування державної інформаційної політики, що включає необхідність розмежування інформації за режимом доступу з метою запобігання завданню шкоди національній безпеці.

Таким чином, деталізація законодавчих норм знаходить своє відображення у низці відповідних розпоряджень президента та інших нормативно-правових актах.

Так, 29 грудня 2009 року президентом США було підписано розпорядження «Засекречування інформації щодо національної безпеки» *(Classified National Security Information),* яке встановлює єдину систему розмежування, захисту та розсекречування інформації, що стосується питань національної безпеки, у тому числі протидії транснаціональному тероризму [9].

Практика підписання подібних документів у США здійснюється з певною періодичністю. Теперішній документ замінив попереднє, аналогічне розпорядження, яке вступило у дію 20 квітня 1995 року, останні зміни до якого вносились у березні 2003 року, до нього використовувалось розпорядження 1982 року [8; 12].

Структура нинішнього розпорядження поділяється на шість частин

і містить питання загального розмежування (класифікації) інформації за режимом доступу (віднесення інформації до державної таємниці), специфіку засекречування, розсекречування та перегляд грифів обмеження доступу матеріальних носіїв інформації, особливості охорони різних категорій інформації з обмеженим доступом, механізми реалізації та застосування цього розпорядження, а також основні терміни та визначення.

Отже, відповідно до законодавства США основними напрямами охорони державної таємниці визначаються наступні:

1. Віднесення інформації до державної таємниці уповноваженими суб'єктами.

2. Засекречування матеріальних носіїв інформації на урядовому та відомчому рівнях.

3. Здійснення спеціальної перевірки осіб, допущених до секретної інформації.

4. Контроль за допуском працівників установ до секретної інформації.

5. Контроль за дотриманням режимних вимог установами та організаціями, де використовується секретна інформація.

6. Регламентування та контроль за виїздом осіб, допущених до секретної інформації, за кордон [14–16].

Як бачимо, визначена структура та основні напрями використання секретної інформації достатньо схожі із вітчизняними вимогами, які окреслені у Законі України «Про державну таємницю» [17].

Для оцінювання ступеня секретності інформації у США введено термін «інформаційна чутливість» *(Information sensitivity)*. «Чутливість» інформації оцінюється за ступенем шкоди, яку може завдати національній безпеці США розкриття цієї інформації.

Таким чином, з метою засекречування інформації у США, що стосується питань національної безпеки, у тому числі протидії транснаціональному тероризму, застосовуються наступні три рівні або ступені секретності:

1) «Цілком таємно» *(«Top Secret»)* – застосовується для засекречування інформації, несанкціоноване розголошення якої може завдати виключно серйозної шкоди національній безпеці;

2) «Таємно» *(«Secret»)* – застосовується для засекречування інформації, несанкціоноване розголошення якої може завдати суттєвої шкоди національній безпеці;

3) «Конфіденційно» *(«Confidential»)* – застосовується для засекречування інформації, несанкціоноване розголошення якої може завдати взагалі шкоду національній безпеці.

Стосовно обрахування шкоди національній безпеці, яка також співвідноситься із поняттям «державна таємниця» в нашій державі, на жаль, доводиться констатувати про відсутність законодавчого закріплення такого механізму.

На теперішній час підставами для обмеження доступу до інформації, що стосується питань національної безпеки, в тому числі протидії транснаціональному тероризму, у США визнається сукупність наступних критеріїв:

А) якщо обмеження здійснив уповноважений на це відповідний орган;

Б) інформація належить установі або створена за її межами, або знаходиться під контролем уряду США;

В) зміст інформації стосується одного або декількох наступних питань:

– військові плани, системи озброєння або військові операції;

– інформація, яка належить уряду іншої держави;

– розвідувальна діяльність (у тому числі таємні операції), джерела або методи розвідки, або криптографія;

– зовнішні відносини або інша іноземна діяльність США, в тому числі конфіденційні джерела;

– наукові, технологічні або економічні питання, які стосуються національної безпеки;

– програми уряду США щодо охорони ядерних матеріалів або об'єктів;

– уразливість або можливості систем, устаткування, інфраструктури, зміст проектів, планів або служб захисту, пов'язаних із національною безпекою;

– розробка, виробництво або використання зброї масового ураження;

Г) уповноважений здійснювати обмеження доступу до інформації орган визначив, що несанкціоноване розкриття інформації завдасть шкоди, яка може бути ідентифікована та обрахована, національній безпеці, у тому числі від транснаціонального тероризму;

Д) при виникненні серйозних сумнівів щодо необхідності засекречування інформації, така інформація не обмежується у доступі. Це положення не передбачає:

– посилення або зміну основних критеріїв, або процедури засекречування;

– створення інших процесуальних дій, що можуть мати юридичні наслідки, та які можуть бути переглянуті у судовому порядку;

Е) засекречена інформація не повинна бути автоматично розсекречена за результатами несанкціонованого розкриття ідентичної або аналогічної інформації;

Є) передбачається, що несанкціоноване розкриття інформації, яка належить уряду іншої країни, завдасть шкоди національній безпеці.

Порівняння із вітчизняною процедурою віднесення інформації до державної таємниці дає підстави для ствердження, що американська модель не обмежується, у нашому розумінні, тільки формуванням загальнодержавного переліку відомостей, що становлять державну таємницю (ЗВДТ). Але пріоритетом для віднесення інформації до державної таємниці у США визнається певна тематика, шкода національній безпеці, власність на інформацію та повноваження відповідних суб'єктів.

Окремо варто назвати суб'єктів, до повноважень яких належить віднесення інформації до державної таємниці:

– президент та віце-президент *(the President and the Vice President)*;

– керівники установ та посадові особи, призначені президентом *(agency heads and officials designated by the President)*;

– делеговані представники органа, уповноваженого засекречувати

інформацію *(Delegation of original classification authority).*

Стосовно останньої категорії, їх кількість повинна бути максимально обмежена із врахуванням доцільності. За визначення достатньої кількості відповідають керівники цих установ звідки делегуються представники.

Призначення таких представників здійснюється за попереднім погодженням із директором управління з нагляду за безпекою інформації *(Director of the Information Security Oversight Office).* Саме з ним вони співпрацюють у подальшому.

Зазначені вище делеговані представники повинні мати відповідні знання із захисту інформації, у тому числі володіти навичками визначення та обрахування шкоди національній безпеці. Вказаний аспект передбачає проведення періодичних навчань, які здійснюються не рідше одного разу на календарний рік.

Посада директора управління із нагляду за безпекою інформації була утворена у 1995 році на підставі розпорядження № 12958 від 17 квітня 1995 року [10].

До повноважень цієї посадової особи відноситься:

– постійний нагляд за загальнодержавною системою засекречування та розсекречування інформації та її реалізація органами виконавчої влади;

– консультування з цих питань президента та політиків вищого рівня, проведення аналітичної роботи щодо ефективності використання секретної інформації;

– підготовка проектів нормативно-правових актів з питань використання та захисту секретних відомостей;

– внесення пропозицій щодо формування бюджету витрат на сферу захисту секретної інформації;

Таким чином, визначення осіб відповідальних за віднесення інформації до державної таємниці у США у багатьох аспектах схоже із вітчизняним призначенням та діяльністю державних експертів з питань таємниць. Проте є й відмінності.

Зокрема, відповідно до Закону України «Про державну таємницю» державний експерт з питань таємниць несе персональну відповідальність за законність і обґрунтованість свого рішення (ст. 9). Разом з тим не визначено, яким чином і хто має право контролювати його діяльність на предмет законності і обґрунтованості.

У вітчизняній системі не передбачено й періодичні проведення занять із державними експертами та членами експертних комісій при них, які повинні знати процедуру віднесення інформації до державної таємниці та вміти обраховувати шкоду національній безпеці України. Хоча доплата за роботу державним експертом або членом експертної комісії при ньому передбачена.

У 2015 році у США суб'єктів, які були уповноважені відносити інформацію до державної таємниці (ОСА), нараховувалось – 2 199. За останні 35 років кількість таких суб'єктів поступово зменшувалась. Наприклад, у 1980 році їх було – 7 149; у 1990 – 6 492; у 2000 – 4 130; у 2010 – 2 378 [12]. Для порівняння, у нашій державі кількість державних експертів, які призначені за посадами Президентом України, не перевищує 150 осіб [18].

Термін засекречування інформації у США визначається органом, який її засекретив. Такий орган повинен встановити точну дату засекречування або подію, після якої буде здійснено розсекречування залежно від уразливості інформації. Після досягнення визначеної дати чи події інформація автоматично розсекречується.

Наприклад, у розпорядженні президента США від 1995 року була визначена вимога щодо розсекречування до грудня 2006 року всієї інформації 25-річної і більше давнини, яка зберегла історичне значення, за винятком даних, спеціально зумовлених і які підлягають додатковій експертизі.

Згідно з цим розпорядженням обов'язок відповідних органів полягав у тому, щоб пояснити причини, за якими та чи інша інформацію не може бути розсекречена, а не причини, за якими гриф секретності може бути знятий.

Створено також паралельну систему нагляду за ходом цього процесу. У період з 1995 по 2001 роки було розсекречено понад 950 мільйонів сторінок (100 мільйонів сторінок лише у 2001 році). Вже у 2015 році шляхом автоматичного розсекречування було переглянуто 85 мільйонів сторінок різних документів [9].

Виключення для автоматичного розсекречування становить інформація, яка повністю розкриває конфіденційне джерело або автора наукової розробки, чи ключові концепції побудови зброї масового знищення. У цьому випадку терміни засекречування встановлюються вище звичайних (25 років).

Якщо уповноважений орган із засекречування не може визначити більш конкретну дату або подію для розсекречування інформації, визначається термін 10 років від дати першого рішення, якщо термін відразу не встановлений – 25 років.

При цьому жодна інформація не може залишатись засекреченою на невизначений термін.

У процесі засекречування інформації визначаються наступні відомості:

1) один з трьох рівнів засекречування *(«Top Secret», «Secret», «Confidential»)*;

2) посадова особа, яка засекретила інформацію;

3) установа, де була визначена ця інформація;

4) вимоги до розсекречування, які містять:

– дату або подію для розсекречування;

– дату, яка становить 10 років з моменту первинного засекречування інформації;

– дату, яка становить 25 років з моменту первинного засекречування інформації, якщо інформація визнається суттєво уразливою (розкриває конфіденційне джерело або автора наукової розробки, чи ключові концепції побудови зброї масового знищення. У цьому випадку терміни засекречування встановлюються вище звичайних);

5) причина засекречування (обґрунтування шкоди).

Наприклад, у 2015 році у США було прийнято рішень щодо віднесення інформації до державної таємниці – 53 425. З них із рівнем «Top Secret» – 2 142; «Secret» – 36 151;

«Confidential» – 15 132. Зазначена й інша, подібна статистична інформація, періодично публікується у відкритому доступі [9].

Стосовно засекреченого документа повинно бути конкретно визначено чи всі його частини підлягають обмеженню, рівні засекречування для кожної частини окремо, відмічена частина документа (якщо така є), яка взагалі не містить інформацію з обмеженим доступом. Процедура такого розмежування документа деталізується в окремих нормативно-правових актах США.

Повне, відкрите, публічне використання засекреченого документа можливо лише за умови розсекречування всіх його частин.

Для порівняння, стаття 15 Закону України «Про державну таємницю» також передбачає, що засекречування документів здійснюється лише в частині відомостей, що становлять державну таємницю. У разі подання запиту на документ, частина якого засекречена, доступ до такого документа забезпечується в частині, що не засекречена [17, ст. 15].

Разом з тим вітчизняне законодавство під час засекречування документа не визначає механізми розмежування і фіксації всіх відомостей у документі за ступенем секретності та, яка інформація у ньому може становити, в тому числі службову інформацію чи взагалі відкриту. Як правило, документ отримує загальний гриф секретності.

Висновки. Проведене дослідження досвіду правового регулювання віднесення інформації до державної таємниці у США дозволяє виокремити наступні важливі напрями, за якими може бути розпочатий перегляд вітчизняної системи охорони державної таємниці з метою підвищення її ефективності:

– *унормування процедури обрахування шкоди національній безпеці* – включає розробку та нормативне закріплення критеріїв визначення та обрахування шкоди національній безпеці України з метою подальшого віднесення інформації до державної таємниці;

– *упорядкування діяльності державних експертів з питань таємниць та експертних комісій при них:*

1) розгляд можливості здійснення контролю за законністю та обґрунтованістю рішень під час віднесення державними експертами інформації до державної таємниці (наприклад, за допомогою РНБО України);

2) організація та періодичне проведення навчань для державних експертів з питань таємниць та експертних комісій при них;

– *врегулювання особливостей засекречування та розсекречування матеріальних носіїв інформації* – деталізація та нормативно-правове закріплення механізмів засекречування матеріальних носіїв інформації не за «загальним» грифом секретності, а своєчасне розмежування всієї інформації, яка міститься у носії за режимом доступу, засекречування інформації не тільки на конкретний термін, але й до настання певної події і т. п., вивчення можливості «автоматичного» розсекречування для окремих категорій секретних відомостей.

Список використаних джерел

1. Стратегія національної безпеки України : Указ Президента України від 26 травня 2015 року № 287/2015.

2. Авдошин І.В. Удосконалення системи адміністративного управління у сфері охорони державної таємниці України з урахуванням досвіду країн ЄС і НАТО // Інформаційна безпека: виклики і загрози сучасності : зб. матеріалів наук.-практ. конф., 5 квіт. 2013 р., м. Київ. – К. : Наук.-вид. центр НА СБ України, 2013. – С. 39–42.

3. Гуз А. М. Становлення та розвиток світових стандартів інформаційної безпеки / А. М. Гуз // Інформаційна безпека: виклики і загрози сучасності: зб. матеріалів наук.-практ. конф., 5 квіт. 2013 р., м. Київ. – К. : Наук.-вид. центр НА СБ України, 2013. – С. 65–68.

4. Гладківська О. В. Інформація з обмеженим доступом: проблема неузгодженості термінології / О. В. Гладківська // Інформація і право. – 2014. – № 1 (10). – С. 49–58.

5. Адабаш О. Охорона державної таємниці: законодавство України та міжнародний досвід / О. Адабаш // Національний університет «Одеська юридична академія». – 2014. – С. 3–7.

6. Freedom of Information Act // Federal Register / Vol. 74, No. 15 / Monday, January 26, 2009 / Presidential Documents.

7. The National Security Act of 1947 – July 26, 1947 Public Law 253, 80th Congress; Chapter 343, 1st Session; S. 758.

8. Classified National Security Information. Federal Register / Vol. 75, No. 2 / Tuesday, January 5, 2010 / Presidential Documents.

9. Report to the President Information security oversight officel – 2015 // National archives end records administration. 700 Pennsylvania avenue, NW, room 100 Washington, DC 20408-0001www. – 42 p.

10. The White House Office of the press secretary For immediate release – April 17, 1995 Executive order 12958 Classified national security information.

11. National Defense Authorization Act for Fiscal Year 2006. Public Law Congress 109–163–JAN. 6, 2006.

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

13. NY Times v. US, 403 US 713 (1971). National Security Archive, The Pentagon Papers Case.

14. Counterintelligence and Security Enhancements Act of 1994. – Public Law 103–359 of October 14, 1994.

15. Information Security Oversight Office, 2004 Report on Cost Estimates for Security Classification Activities, May 2005 [Електронний ресурс]. – Режим доступу : http://www.archives.gov/isoo/reports/2004-cost-report.html.

16. Information Security Oversight Office, 2001 Report to the President, September 2002.

17. Про державну таємницю : Закон України // Відомості Верховної Ради України. – 1999. – № 49. – Ст. 428.

18. Про Перелік посадових осіб, на яких покладається виконання функцій державного експерта з питань таємниць : Указ Президента України від 1 грудня 2009 року № 987/2009.

19. Грищенко І. В. Досвід країн Східної Європи у сфері охорони державної таємниці / І. В. Грищенко // Порівняльно-аналітичне право. – К., 2015. – № 4. – С. 19–22.

20. Семенюк О. Г. Проблеми охорони державної таємниці: кримінально-правові та кримінологічні аспекти : монографія / О. Г. Семенюк. – К. : ТОВ «Видавничий дім «АртЕк», 2017. – С. 342.

Рецензенти:
доктор педагогічних наук
В. Артюшин,
кандидат юридичних наук,
старший науковий співробітник
І. Касперський

Аннотация. В статье исследуется опыт правового регулирования отнесения информации к государственной тайне в США.

Ключевые слова: государственная тайна, отнесение информации к государственной тайне, секретная информация; засекречивание материальных носителей информации.

Abstract. The article deals with practical aspects of legal regulation of state secrets classification in the USA.

Key words: state secret, state secrets classification, classified information, assigning security labels to data media.

УДК 355.40

КРАВЧЕНКО Роман Миколайович

РОЛЬ ЄВРОПЕЙСЬКИХ ПРИНЦИПІВ ПРАВА У ВИЗНАЧЕННІ ПОВНОВАЖЕНЬ ОРГАНІВ ВІЙСЬКОВОЇ КОНТРРОЗВІДКИ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ ЩОДО КОНТРРОЗВІДУВАЛЬНОГО ЗАБЕЗПЕЧЕННЯ ВІЙСЬКОВИХ ФОРМУВАНЬ

Постановка проблеми. Забезпечення ефективного співробітництва і взаємодії України з Євросоюзом та поступове входження до європейського політичного, економічного і правового простору можливе лише за умов наближення джерел вітчизняного права, практики діяльності державних, правоохоронних органів та спецслужб до правових принципів і кращих стандартів, які діють у рамках європейських інтеграційних об'єднань. Здійснення конкретних заходів у цьому напрямку вимагає ґрунтовного та поглибленого вивчення принципів права Євросоюзу та пошуку оптимальних варіантів застосування цих основоположних ідей.