Олександр Семенюк,
кандидат юридичних наук,
заступник начальника
Управління Служби безпеки України

УДК 342:95 (477)

ПОРЯДОК ВІДНЕСЕННЯ ІНФОРМАЦІЇ ДО ДЕРЖАВНОЇ ТАЄМНИЦІ: ПОРІВНЯЛЬНИЙ АНАЛІЗ ВІТЧИЗНЯНОГО ТА ЗАРУБІЖНОГО ЗАКОНОДАВСТВА, ШЛЯХИ УДОСКОНАЛЕННЯ ЦІЄЇ ПРОЦЕДУРИ

У статті проведено аналіз вітчизняної та зарубіжної практики віднесення інформації до державної таємниці, досліджено переваги і недоліки перелікової та персоніфікованої систем засекречування інформації, визначено шляхи вдосконалення цієї процедури.
Ключові слова: *державна таємниця, державний експерт з питань таємниць, засекречування інформації, Звід відомостей, що становить державну таємницю.*

На даний час більшість держав у світі, в тому числі Україна, приділяють значну увагу вдосконаленню механізмів захисту інформації, несанкціоноване розголошення якої може завдати суттєвої шкоди життєво важливим сферам держави, призвести до великих фінансово-економічних витрат, негативно вплинути на існуючі конституційно-правові інститути. Основне завдання законодавця у вирішенні даного питання — створення оптимального підходу, який забезпечить баланс інтересів громадянина в реалізації права на інформацію та обмеження доступу до державної таємниці в інтересах захисту національної безпеки України.

Питання засекречування інформації були предметом досліджень О. Архипова, Ю. Дрейса, І. Касперського, О. Корченко та ін. Проте відсутність однозначного розуміння підстав для віднесення відомостей до державної таємниці та єдиних критеріїв для визначення ступеня їх секретності обумовлює актуальність подальшої розробки даної проблематики.

Метою цієї статті є проведення аналізу вітчизняної та зарубіжної практики віднесення інформації до державної таємниці, дослідження переваг і недоліків перелікової та персоніфікованої систем засекречування інформації, визначення шляхів удосконалення цієї процедури.

Зміст будь-якого виду таємної інформації розкривається через характеристику відомостей, до яких обмежується доступ сторонніх осіб, що дозволяє у кожному конкретному випадку ідентифікувати її предмет та визначити обсяг інформації, що приховується. Здійснюється це у позитивний або негативний спосіб.

Позитивний спосіб полягає у віднесенні відомостей до таємниці шляхом

визначення у нормативно-правовому акті їх змісту або критеріїв. Негативний — у нормативному закріпленні переліку відомостей, які не можуть складати таємницю. Існує і змішаний (комплексний) спосіб, коли дається позитивне визначення обсягу відомостей, які становлять державну таємницю, і одночасно дається перелік відомостей, які не можуть складати таку таємницю.

Стаття 8 Закону України «Про державну таємницю» визначає предмет державної таємниці у змішаний спосіб шляхом одночасного закріплення переліку інформації, яка може бути віднесена до державної таємниці, у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку та переліку відомостей, які заборонено відносити до державної таємниці, якщо будуть звужуватися зміст і обсяг конституційних прав та свобод людини і громадянина, завдаватиметься шкода здоров'ю та безпеці населення [1].

Відповідно до ст. 10 цього Закону віднесення інформації до державної таємниці здійснюється шляхом опублікування мотивованих рішень державних експертів з питань таємниць у Зводі відомостей, що становлять державну таємницю (далі — ЗВДТ) [1]. Крім цього, згідно зі ст. 12 Закону, на підставі та в межах ЗВДТ з метою конкретизації та систематизації даних про секретну інформацію державні органи створюють галузеві або відомчі розгорнуті переліки відомостей, що становлять державну таємницю, а також можуть створювати міжгалузеві або міжвідомчі розгорнуті переліки відомостей, що становлять державну таємницю. Підприємства, установи та організації незалежно від форм власності, що провадять діяльність, пов'язану із державною таємницею, за ініціативою та погодженням із замовником робіт, пов'язаних з державною таємницею, можуть створювати власні розгорнуті переліки відомостей, що становлять державну таємницю (ст. 12) [1].

Таким чином, Закон України «Про державну таємницю» закріплює чотирирівневу перелікову систему віднесення відомостей до державної таємниці.

Так, до першого рівня відноситься інформація, закріплена у ст. 8 цього Закону. Цей перелік не має імперативного характеру та не є вичерпним, оскільки в ньому визначено тільки ті категорії інформації, в яких можуть утворюватися відомості, що становлять державну таємницю. При цьому, як зазначено у цій статті, конкретні відомості можуть бути віднесені до державної таємниці за ступенями секретності «особливої важливості», «цілком таємно» та «таємно» лише за умови, що вони належать до визначених Законом категорій, і їх розголошення завдаватиме шкоди інтересам національної безпеки України.

Другий рівень — це інформація, включена до ЗВДТ за рішеннями державних експертів з питань таємниць.

Третій рівень — галузеві, відомчі, міжгалузеві, міжвідомчі розгорнуті переліки відомостей, що становлять державну таємницю.

Четвертий рівень — власні розгорнуті переліки підприємств, установ, організацій.

Логіка побудови цих переліків полягає у тому, що кожний наступний рівень повинен містити більш конкретизовані (розгорнуті) відомості стосовно інформації, яку засекречено, й не суперечити попередньому. Однак на практиці ці принципи грубо порушуються, що виключає можливість однозначного розуміння змісту категорій секретної інформації та нерідко призводить до їх звуженого або розширеного тлумачення.

У якості прикладу розглянемо норму, закріплену у п. 4 ч. 1 ст. 8 Закону, згідно з якою до державної таємниці відноситься інформація про засоби, зміст, плани, організацію, фінансування та матеріально-технічне забезпечення, форми, методи і результати оперативно-розшукової, розвідувальної і контррозвідувальної діяльності [1]. У ЗВДТ ця норма викладена у статтях 4.4.1 та 4.4.3, але у дещо трансформованому вигляді. Зокрема, відповідно до ст. 4.4.1 державну таємницю становлять відомості за окремими показниками про зміст, форми, методи, організаційні положення, оперативну тактику здійснення ДПС, розвідувальним органом Адміністрації ДПС, ДФС, ГУР, УДО, СЗР; органами СБ, внутрішніх справ; органом, установою виконання покарань,

слідчим ізолятором ДКВС оперативно-розшукової, контррозвідувальної чи розвідувальної діяльності, розголошення яких створює загрозу національним інтересам і безпеці. Згідно зі ст. 4.4.3 ЗВДТ державну таємницю становлять відомості про організацію, завдання, результати оперативно-розшукової, контррозвідувальної діяльності, розголошення яких створює загрозу національним інтересам і безпеці [2]. Як бачимо, закріплені у ЗВДТ норми не тільки не розширюють та деталізують зміст Закону, а навпаки звужують його дію, оскільки у ЗВДТ зникають такі види інформації, як відомості про фінансування та матеріально-технічне забезпечення оперативно-розшукової, розвідувальної та контррозвідувальної діяльності.

Прикладом розширеного тлумачення закріпленого в Законі переліку інформації, що може бути віднесена до державної таємниці, є статті 4.12.4 та 4.12.5 ЗВДТ, відповідно до яких до державної таємниці відносяться відомості про факт або методи проведення негласної слідчої (розшукової) дії та відомості, що дають змогу ідентифікувати особу, місце або річ, щодо якої проводиться чи планується проведення негласної слідчої (розшукової) дії, розголошення яких створює загрозу національним інтересам і безпеці [2].

Слід зазначити, що в Законі взагалі немає жодного натяку на таку категорію інформації, яка давала б підстави для засекречування інформації про негласні слідчі (розшукові) дії, а отже, засекречування цих відомостей прямо суперечить закріпленому в Законі переліку категорій інформації, що може бути віднесена до державної таємниці.

Наведені приклади свідчать про недосконалість перелікового методу засекречування інформації, який не убезпечує від винесення безпідставних рішень про віднесення до державної таємниці певних категорій інформації, що пояснюється відсутністю єдиного підходу до оцінювання можливої шкоди національній безпеці внаслідок розголошення таких відомостей та породжує абсолютно виправдану критику правозахисників щодо безпідставності засекречування значного масиву державних інформаційних ресурсів.

Аналіз законодавства у сфері державної таємниці показує, що, крім перелікового методу засекречування інформації, в деяких країнах застосовується також персоніфікована система віднесення інформації до державної таємниці. Зокрема, персоніфікована система існує в США та ряді інших країн — членах НАТО. Суть цієї системи полягає в тому, що рішення про засекречування, встановлення конкретного грифу секретності, його зниження і розсекречення приймає конкретний уповноважений посадовець.

Якнайповніше цю модель описує директива Президента США від 08.03.1972 № 11652, відповідно до ст. 2 якої правом первинного надання інформації або матеріалам грифа «цілком таємно» можуть користуватися тільки посадовці, уповноважені у письмовій формі Президентом США, а також керівники Виконавчого управління президента, ЦРУ, Державного департаменту, Міністерства оборони, Міністерства фінансів, НАСА і ряду інших федеральних органів. Окрім керівників державних установ та відомств, правом засекречування інформації наділені їх заступники, помічники, керівники провідних підрозділів, яким керівник надає таке право у письмовій формі.

Директива також встановлює, що будь-яке відомство, не зазначене в цій директиві, а також будь-яке нове створене відомство або підрозділ не мають і не матимуть повноважень первинного надання інформації і матеріалам грифа секретності доти, поки не отримають такого права, оформленого спеціальною директивою президента США [4].

З контексту наведених положень випливає, що персоніфікована система віднесення інформації до державної таємниці передбачає делегування цих повноважень виключно по адміністративній вертикалі від Президента США до керівників відомств, а від них — до заступників і керівників підрозділів. Встановлення грифів секретності є винятковою прерогативою виконавчої влади.

Якщо порівнювати між собою перелікову та персоніфіковану системи віднесення інформації до державної таємниці, то можна констатувати, що пе-

реваги однієї системи зворотно пропорційні недоліками іншої.

У персоніфікованої системи є декілька переваг, головна з яких — наявність конкретного суб'єкта, який приймає таке рішення і несе за нього повну юридичну відповідальність. Крім цього, безперечною перевагою є оперативність в ухваленні рішень, оскільки уповноважена особа, виходячи з власного розуміння необхідності засекречування інформації, приймає відповідне рішення самостійно і в такий же спосіб визначає термін збереження відомостей у таємниці. Водночас цей суб'єктивізм має й негативний бік — віднесені до державної таємниці відомості не проходять попередньої оцінки, відсутня будь-яка система їх аналізу, що не виключає можливості прийняття рішення виключно на підставі суб'єктивної оцінки значущості такої інформації для безпеки держави, яка залежить від особливостей характеру конкретної людини, її емоційного стану, професіоналізму тощо.

Переліковий метод засекречування передбачає формальний підхід до вирішення цього питання. При цьому закріплення переліку інформації у різних сферах національної безпеки у найбільш узагальненому вигляді призводить до непоодиноких випадків засекречування інформації, витік якої не завдасть шкоди національній безпеці України, та численних помилок при визначенні її ступеня секретності.

Також суттєвим недоліком перелікової системи є відсутність оперативності в ухваленні рішень про віднесення тієї чи іншої категорії інформації до державної таємниці. Як наслідок, це унеможливлює підтримання цього переліку в актуальному для національної безпеки стані на законодавчому рівні, оскільки коло відомостей, які мають засекречуватися державою, досить динамічне та безпосередньо залежить від зовнішньополітичної й економічної ситуації в країні. Водночас завчасна нормативна визначеність категорій інформації, віднесених до державної таємниці, дозволяє здійснювати аналіз конкретної інформації вже на етапі виготовлення нового інформаційного продукту та його документального закріплення, а отже, запобігти витоку важливої для безпеки держави секретних відомостей.

Правовий інститут державної таємниці повинен виходити з того, що лише обмежений обсяг закритої інформації не підлягає розголошенню і лише в межах терміну дії грифа секретності, тоді як менш секретна інформація повинна мати меншу міру секретності або взагалі бути доступною широкій громадськості. На даний час Методичні рекомендації державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня їх секретності, які затверджено наказом Державного комітету України з питань державних секретів та технічного захисту інформації від 9 лютого 1998 р. № 23 (Методичні рекомендації), є єдиним нормативним актом, який встановлює порядок оцінювання інформації на предмет наявності в них відомостей, що становлять державну таємницю. Проте, як свідчить практика та наукові дослідження з цього питання [5, с. 93; 6; 7], ці рекомендації не знаходять свого застосування внаслідок недосконалості та складності у користуванні.

ЗВДТ формує Служба безпеки України на підставі рішень державних експертів з питань таємниць. Згідно з Переліком посадових осіб, на яких покладається виконання функцій державного експерта з питань таємниць, затверджених Указом Президента України від 01.12.2009 р. № 987/2009, такі функції покладено на 152 посадові особи [8].

Відповідно до п. 120 Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, затвердженого постановою Кабінету Міністрів України від 18.12.2013 р. № 939, державний експерт з питань таємниць здійснює віднесення інформації у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку до державної таємниці, зміни ступеня секретності цієї інформації та її розсекречування з питань, прийняття рішень з яких належить до його компетенції згідно з посадою [9]. Виходячи з цього положення, усі високопосадовці, які обіймають ці

посади, a priori вважаються носіями наукових, технічних або інших спеціальних знань у сфері охорони державної таємниці. Проте, як засвідчила практика, визначальним критерієм при призначенні осіб на такі посади, є наявність у них не стільки фахових, скільки управлінських здібностей та навичок, активна громадська позиція або партійна приналежність. Окремі посади, на які покладено функції державних експертів з питань таємниць, є політичними за своєю сутністю. У більшості державних експертів з питань таємниць відсутні необхідні спеціальні знання у сфері охорони державної таємниці та досвід (навички), необхідні для прийняття виважених рішень щодо віднесення інформації до державної таємниці.

На наше переконання, з метою унеможливлення прийняття одноосібних та необґрунтованих рішень щодо віднесення певних категорій інформації до державної таємниці, має бути змінено процедуру прийняття рішень, на підставі яких формується ЗВДТ. Зокрема, державні експерти з питань таємниць мають бути позбавлені права винесення таких рішень та уповноважені лише на подачу до колегіального органу мотивованих пропозицій щодо віднесення тієї чи іншої категорії інформації до державної таємниці. Таким колегіальним органом, на нашу думку, може бути Рада національної безпеки і оборони України, оскільки саме на неї покладено функції забезпечення національної безпеки. За таких умов найбільш ефективною формою контролю за доцільністю та законністю прийняття цим державним органом рішення щодо віднесення інформації до державної таємниці є парламентський контроль.

Враховуючи викладене, ми можемо зробити наступні ***висновки****.*

Закон України «Про державну таємницю» має містити не перелік категорій інформації, віднесеної до державної таємниці (вичерпний перелік якої a priori сформувати неможливо), а критерії віднесення інформації до державної таємниці, процедуру прийняття відповідних рішень щодо віднесення інформації до державної таємниці, коло осіб (органів), уповноважених на прийняття таких рішень, форми контролю за безпідставним засекречуванням інформації.

Перелік секретної інформації має бути виведений за рамки Закону в окремий нормативний акт, роль якого може виконувати ЗВДТ. Цей перелік має бути єдиним у державі нормативним документом, який визначатиме категорії інформації, віднесені до державної таємниці, у зв'язку з чим всі інші розгорнуті галузеві, відомчі, міжгалузеві, міжвідомчі або власні розгорнуті переліки відомостей, що становлять державну таємницю, мають бути скасовані.

Для визначення ступеня секретності інформації та грифів секретності її матеріальних носіїв необхідно розробити та законодавчо закріпити єдину методику визначення потенційної шкоди для охоронюваних державою суспільних інтересів в інформаційній сфері, що може настати внаслідок розголошення відомостей, які становлять державну таємницю, або втрати її матеріальних носіїв.

Процедура формування ЗВДТ має бути змінена шляхом передачі цих повноважень Раді національної безпеки й оборони України на підставі колегіального розгляду мотивованих подань державних експертів з питань таємниць.

ПРИМІТКИ

1. Закон України «Про державну таємницю» від 21 січня 1994 р. // Відомості Верховної Ради України. — 1994. — № 16. — Ст. 93.

2. Про затвердження Зводу відомостей, що становлять державну таємницю // Служба безпеки України; Наказ, Звід від 12.08.2005 р. № 440 [Електронний ресурс]. — Режим доступу : http://zakon3.rada.gov.ua/laws/show/z0902-05.

3. Кримінальний процесуальний кодекс України // Відомості Верховної Ради України (ВВР). — 2013. — №№ 9—10, 11—12, 13. — Ст. 88.

4. Директива Президента США від 08.03.1972 р. № 11652 / Федеральний регістр США, 1972 [Електронний ресурс]. — Режим доступу : https://www.federalregister.gov/articles/search?conditions%5Bterm%5D=+№+11652+.

5. Касперський І. П. Методичні аспекти і критерії оцінювання інформації на предмет її віднесення до державної таємниці / Ігор Петрович Касперський // Інформаційна безпека людини, суспільства, держави. — 2010. — № 1 (3). — С. 93—97.

6. Архипов О. Є. Проблеми методичного забезпечення віднесення відомостей до інформації з обмеженим доступом в Україні / О. Є. Архипов, І. П. Касперський // Правова інформатика. — 2006. — № 3 (11). — С. 61—66.

7. Архипов О. Є. Проблеми методики отримання та обробки оціночних суджень членів експертних комісій, створюваних державними експертами з питань таємниць / О. Є. Архипов, І. П. Касперський // Правова інформатика. — 2006. — № 4 (12). — С. 80—87.

8. Указ Президента України від 01.12.2009 р. № 987/2009 «Про перелік посадових осіб, на яких покладається виконання функцій державного експерта з питань таємниць» [Електронний ресурс]. — Режим доступу : http://zakon5.rada.gov.ua/laws/show/987/2009.

9. Постанова Кабінету Міністрів України від 18.12.2013 р. № 939 «Про затвердження Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях та визнання такими, що втратили чинність, деяких постанов Кабінету Міністрів України».

Семенюк Александр. Порядок отнесения информации к государственной тайне: сравнительный анализ отечественного и зарубежного законодательства, пути усовершенствования этой процедуры.

В статье проведен анализ отечественной и зарубежной практики отнесения информации к государственной тайне, исследованы преимущества и недостатки перечневой и персонифицированной систем засекречивания информации, определены пути усовершенствования этой процедуры.

Ключевые слова: *государственная тайна, государственный эксперт по вопросам тайны, засекречивание информации, Свод сведений, составляющих государственную тайну.*

Semenyuk Oleksandr. The order for reference of information to state secret: comparative analysis of native and foreign legislation, ways for improvement of this procedure.

The article analyzes native and foreign practice of reference of information to state secret, researches advantages and defects of listing and personified classification systems, defines the ways for improvement of this procedure.

The content of any type of secret information reveals through the description of information the unauthorized persons have limited access to, that allows in each case to identify its object and determine the amount of information that is protected. The Law of Ukraine «On State Secrets» defines the subject of state secret in different ways by simultaneously fixing the list of information that can be classified as a state secret in defense, economy, science and technology, foreign relations, national security and law enforcement, and the list of information that is prohibited to qualify as state secret.

The Law of Ukraine «On State Secrets» establishes a four-level enumerative system of classification of information as a state secret.

The first level concerns information that is enshrined in Art. 8 of this law. This list is not mandatory and is not exhaustive because it defines only those categories of information which can form information constituting a state secret.

The second level is the information included in the Code of information constituting state secret (hereinafter — CISS) by the decisions of state experts on secrets.

The third level is industrial, departmental, cross-sectoral, interdepartmental extended lists of information constituting a state secret.

The fourth level — own extended lists of enterprises, institutions and organizations.

The logic of constructing these lists is that each subsequent level should contain more specific (detailed) information regarding the secret information, and not contradict the previous one. However, in practice, these principles are grossly violated, render impossible unambiguous understanding of the content of categories of classified information and often leads to narrowed or extended interpretation.

Analysis of the legislation on state secrets shows that in addition to enumerative method of information classification in some countries the personalized system of classification of information as state secrets is used. Specifically, personalized system exists in the United

States and other countries — members of NATO. The essence of this system is that the decision on classifying, establishing of specific secrecy, its decline and declassification takes specific authorized public person.
If you compare the enumerative and personalized system of classification of information as state secrets, we can conclude that the benefits of one system are inversely proportional to defects of another one.
A personalized system has several advantages, the main among them is the presence of a specific subject that takes the decision and is legally accountable. In addition, the indisputable advantage is the efficiency in decision-making as person entitled, based on his own understanding of the necessity of classifying information, takes appropriate decisions on his own and in the same manner, determines the period of custody of secret information. However, this subjectivity has also a negative side — classified as state secret information does not conduct a preliminary assessment, there is no system of analysis that does not preclude taking decision solely on the subjective evaluation of the importance of such information for national security, which depends on specific features of the nature of man, his emotional state, professionalism and so on.
Enumerative classification method provides a formal approach to this issue. The consolidation of the list of information in various fields of national security in the most general form leads to numerous cases of classifying information the leak which will not harm the national security of Ukraine and numerous errors in determining the degree of secrecy.
Also significant defect of the enumerative system is the lack of efficiency in taking decisions on the attribution of a category of information as state secret. As a result, it makes it impossible to support this list in important for the national security state at the legislative level, since the range of information that has to be classified by state is quite dynamic and depends directly on the foreign policy and economic situation in the country. At the same time, anticipatory regulatory certainty of information categories classified as state secrets allows to make analysis of specific information on the stage of production of new information products and piece justificative and therefore to prevent the leakage of important for state security secret information.
The author makes the following conclusions.
The Law of Ukraine «On State Secrets» should contain a list of categories of information classified as state secret (a comprehensive list of which a priori cannot be formed) and criteria for classification of information as state secrets, decision-making procedures to classify information as state secrets, the scope of persons (bodies) authorized to make such decisions, forms of control on false classification of information.
The list of secret information has to be removed beyond the law in a separate regulation, which can represent CISS. This list must be the only regulatory document in the country that will determine the categories of information classified as state secrets, and therefore, all other expanded industrial, departmental, cross-sectoral, inter-agency or own extended lists of information constituting state secrets should be repealed.
To determine the degree of secrecy of information and secrecy of its material media we need to develop and legislate exclusive methodology for determining the potential harm to the public interests protected by the state in the information sector, which may occur as a result of disclosure of information constituting a state secret or loss of its material media.
CISS formation procedure should be changed by transferring these powers from state experts on secrets to the National Security and Defense Council of Ukraine, which will be authorized to take appropriate decisions on the basis of collegial review of motivated submissions of state experts on secrets.
***Key words**: state secret, state expert on secret matters, information classification, List of data constituting state secret.*