УДК: 342.1+355/359

БОЛДИР С.В., начальник Департаменту охорони державної таємниці та ліцензування Служби безпеки України

ПЕРСПЕКТИВИ РЕФОРМУВАННЯ СИСТЕМИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА СЛУЖБОВОЇ ІНФОРМАЦІЇ

Анотація. *У статті на основі наявного досвіду та проведеного аналізу норм законодавства іноземних держав у сфері безпеки інформації розкриваються окремі питання, пов’язані з практичними аспектами реалізації вказівок керівництва держави, задекларованих у різних нормативних актах щодо реформування національного законодавства у згаданій сфері діяльності.*

Ключові слова: *реформування законодавства, система охорони державної таємниці та службової інформації, безпека інформації, стандарти НАТО та ЄС.*

Summary. *The article discloses certain questions related to practical aspects of implementation of the state leadership instructions declared in various normative acts, concerning the reform of the national legislation in the mentioned area of activity, based on actual experience and analysis of the legislative acts in the sphere of information security of foreign countries .*

Keywords: *legislation reforming, system of protection of state secrets and official information, information security, NATO and EU standards.*

Аннотация. *В статье на основе имеющегося опыта и проведенного анализа норм законодательства иностранных государств в сфере безопасности информации раскрываются некоторые вопросы, связанные с практическими аспектами реализаций указаний руководства государства, задекларированных в различных нормативных актах по реформированию национального законодательства в упомянутой сфере деятельности.*

Ключевые слова: *реформирование законодательства, система охраны государственной тайны и служебной информации, безопасность информации, стандарты НАТО и ЕС.*

Постановка проблеми. Одним із пріоритетних напрямів державної політики національної безпеки України, виходячи із положень Стратегії національної безпеки України, яку затверджено Указом Президента України від 26.05.2015 № 287/2015, є реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом з урахуванням практики держав-членів Організації Північноатлантичного договору та Європейського Союзу [1].

Необхідність формування нових підходів до забезпечення функціонування вказаної системи зумовлена передусім взятим Україною курсом на інтеграцію у світове співтовариство та розширенням міжнародного співробітництва у політичній, оборонній, науково-технічній та інших сферах діяльності, а також певною фізичною та моральною застарілістю національного законодавства у сфері охорони інформаційних ресурсів, сформованого значною мірою на основі нормативних актів колишнього СРСР.

При цьому закритість сфери охорони державної таємниці призвела до збереження у своїй основі засад побудови та функціонування радянського механізму захисту державних секретів, який утратив свою ефективність і перестав відповідати сучасним реаліям, що суттєво вплинуло на принципи захисту інформації [2, с. 335].

З урахуванням викладеного та зважаючи на важливість зазначеного питання, яке безпосередньо стосується національної безпеки України, очевидним є те, що впровадження певних новацій потребує виваженого підходу та ретельного вивчення практики їх застосування в інших державах.

Результати аналізу наукових публікацій. Дослідженню питань, пов’язаних з реформуванням системи охорони державної таємниці та службової інформації, присвячені роботи таких науковців як С. Князєва, І. Мейдича, О. Розвадовського, О. Семенюка, В. Шлапаченка та інших. Проте і на сьогодні, у зв’язку з відсутністю єдиного державного бачення щодо шляхів реалізації певних реформаторських започаткувань, окреслена проблема не отримала належного теоретичного осмислення.

Метою статті є аналіз сучасного стану системи охорони державної таємниці та іншої інформації з обмеженим доступом з урахуванням практики держав-членів НАТО та ЄС, окреслення основних перспективних шляхів її удосконалення для кардинального підвищення ефективності національних спроможностей щодо забезпечення гарантованого рівня безпеки таких відомостей.

Виклад основного матеріалу. Цілком зрозуміло, що визначенню основних перспективних напрямів реформування системи охорони державної таємниці та службової інформації має передувати вивчення досвіду держав-учасниць НАТО та ЄС з розбудови та впровадження дієвої системи захисту інформації. Результати опрацювання цього питання засвідчили, що національне законодавство таких країн у цій сфері базується на мінімальних стандартах безпеки, встановлених зазначеними міжнародними організаціями.

Тому, поряд з розглядом національних нормативно-правових актів держав євроатлантичної спільноти, ґрунтовного вивчення та дослідження вимагають підходи до захисту інформації саме НАТО та ЄС, оскільки, як влучно зазначив Розвадовський О.Б., вони є результатом спільних зусиль, формувалися під впливом і за участю розвинутих країн світу, містять обов’язкові для всіх країн-членів універсальні приписи [3, с. 163].

Аналіз іноземної нормативної бази довів, що вітчизняне законодавство у сфері охорони державної таємниці та службової інформації не повною мірою узгоджується зі стандартами безпеки НАТО та ЄС, що може вплинути як на міжнародні партнерські взаємовідносини у сфері захисту інформації, так і ускладнити інтеграційні процеси нашої держави.

На наш погляд, одним із найважливіших напрямів, за яким має здійснюватися реформування української системи охорони державної таємниці та службової інформації, є кардинальний перегляд “філософії” віднесення інформації до такої, що потребує обмеження у доступі.

На сьогодні первісним законодавчим актом, що регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації, є Закон України “Про інформацію”, який, зокрема, визначає порядок доступу до інформації, поділяючи її на відкриту та з обмеженим доступом [4].

Разом з тим, у контексті впливу зовнішніх та внутрішніх чинників на стале функціонування держави найбільш уразливою є інформація, доступ до якої обмежується виключно в інтересах, передбачених статтею 6 Закону України “Про доступ до публічної інформації” [6], та яка підлягає охороні державою, тобто державна таємниця та службова інформація.

Водночас, на сьогодні склалась ситуація, коли недостатнє нормативно-правове врегулювання окремих аспектів захисту інформаційних ресурсів призвело до значної втрати впливу держави на забезпечення схоронності саме службової інформації.

Як зазначив Мейдич І.М., визначення службової інформації в законодавстві України на сьогодні відсутнє. У ст. 9 Закону України “Про доступ до публічної інформації” подається лише перелік відомостей (до того ж не вичерпний), які можуть до неї належати, який не містить чітких критеріїв віднесення інформації до службової.

Узагальнений Перелік відомостей, що становлять службову інформацію (на кшталт ЗВДТ), законодавством не передбачений. Відомості, що становлять службову інформацію, у відомчих переліках визначаються без чіткої структуризації та недостатньо конкретно. Зазначені чинники не сприяють правильному встановленню службової інформації, як предмета кримінально-правової охорони [5, с. 164].

Дійсно, згідно з положеннями наведеного законодавчого акта відомості, що становлять службову інформацію, визначаються у відповідних переліках, які складаються органами державної влади, органами місцевого самоврядування, іншими суб’єктами владних повноважень, у тому числі на виконання делегованих повноважень [6].

Проте, на законодавчому рівні єдині вимоги щодо таких переліків не встановлені, тому розпорядники інформації відносять її до службової, у більшості випадків, на свій розсуд. При цьому контроль за цим процесом здійснюється лише для інформації, зібраної в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Відсутність належної уваги з боку суб’єктів владних повноважень до процедури складання переліку відомостей, що становлять службову інформацію, може викликати безпідставне оприлюднення зазначеної інформації та завдати значної шкоди національній безпеці держави, а також призвести до порушення конституційних прав та свобод людини і громадянина.

Тому, першочерговим є вирішення питання щодо впровадження нових комплексних підходів та створення уніфікованої системи безпеки як державної таємниці, так і службової інформації, яка б забезпечувала в усіх сферах надійний та ефективний захист чутливих відомостей, спеціальний режим доступу до яких встановлюється, виходячи з інтересів держави.

Слід зазначити, що така позиція співпадає з висновками Мейдича І. М., на думку якого ґрунтовною проблемою удосконалення кримінально-правової охорони службової інформації є переосмислення її статусу як виду таємної інформації та закріплення в законодавстві її визначення, за аналогією з державною таємницею, яке б конкретизувало її тлумачення та сприяло правильній кваліфікації як предмету злочинних посягань [5, с. 164].

Безумовно, при вирішенні цього проблемного питання має бути враховано, що у стандартах безпеки НАТО та ЄС, а також нормативній базі більшості країн-членів цих міжнародних організацій відсутні поняття “державна таємниця”, “службова інформація”, натомість передбачено застосування єдиного терміну для позначення відомостей з еквівалентними ступенями обмеження доступу, а саме – “classified information”, прямим перекладом якого є “класифікована інформація” (саме у такому написанні вказаний термін поширено використовується в україномовних ресурсах).

Зокрема, на нормативному рівні впроваджено чотирьохрівневу систему обмеження доступу до вказаної інформації, ступені якої розподіляються за рівнем шкоди, яку може бути заподіяно інтересам міжнародних організацій та країн-членів у разі розголошення класифікованих відомостей [7; 8].

З огляду на викладене, вбачається, що закріплення на законодавчому рівні встановлених політикою безпеки НАТО та ЄС стандартів та процедур щодо застосування системи ступенів обмеження доступу до інформації дозволить демократизувати цей процес, забезпечивши його прозорість, сприятиме оптимізації роботи з визначення ступенів секретності матеріальних носіїв інформації, а також гармонізації та адаптації національного законодавства до вимог політики безпеки євроатлантичного суспільства.

Саме тому, з метою виокремлення секретної та службової інформації з-поміж інших категорій інформації з обмеженим доступом (до яких відноситься конфіденційна та інша таємна інформація, що містить професійну, банківську таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю), пропонується об’єднати державну таємницю та службову інформацію в єдину категорію інформації, доступ до якої обмежується виключно в інтересах, передбачених статтею 6 Закону України “Про доступ до публічної інформації” [6], та яка підлягає охороні державою.

При цьому, з огляду на відсутність у законодавстві України аналогу впровадженого у стандартах безпеки НАТО та ЄС терміну “класифікована інформація”, еквівалентне поняття, що відповідатиме належному його розумінню з урахуванням традиційних та сталих форм застосування (наприклад “засекречена інформація”, “секретна інформація”) має бути закріплено на законодавчому рівні.

Поряд із цим, потребують правового врегулювання й інші питання у сфері безпеки інформації, зокрема, визначення на законодавчому рівні Національного органу безпеки.

Відповідно до стандартів безпеки НАТО та ЄС однією з умов євроатлантичної інтеграції держав-партнерів в загальноєвропейську систему обміну інформацією з обмеженим доступом є створення Національного органу безпеки [7; 8].

Так, згідно з вимогами стандартів безпеки НАТО та ЄС у державах-учасницях створюються Національні органи безпеки, основною функцією яких є впровадження стандартів безпеки інформації, здійснення інспектувань умов захисту інформації з обмеженим доступом у всіх національних організаціях на всіх рівнях, забезпечення проведення перевірки з визначення надійності громадян, які потребують доступу до секретної інформації, видачу дозволів на провадження діяльності, пов’язаної з інформацією з обмеженим доступом [7; 8].

Статус та підпорядкованість такого органу визначаються державами-учасницями вказаних міжнародних організацій самостійно з урахуванням традиційних підходів та практики забезпечення охорони інформації з обмеженим доступом.

Поширеною є також практика створення Національних органів безпеки при окремих державних органах (при Міноборони – Великобританія, Естонія, Кіпр, Норвегія, Франція; Нідерланди, при МЗС – Бельгія, Фінляндія, Швеція, при МВС – Німеччина, при Раді Міністрів – Італія, Португалія). У деяких країнах функції Національних органів безпеки покладаються на національні спецслужби (Греція, Польща, Румунія – законодавство гармонізовано зі стандартами НАТО та ЄС) або діяльність такого органу скеровується керівником спеціальної служби (Іспанія).

Разом з тим, статтею 2 Адміністративних домовленостей щодо охорони інформації з обмеженим доступом між Урядом України та Організацією Північноатлантичного договору на Службу безпеку України як орган безпеки покладено впровадження мінімальних стандартів охорони та поводження з такою інформацією, обмін якою здійснюється між Україною та НАТО, узгоджених у цих Домовленостях, та забезпечення нагляду за їхнім дотриманням [9].

Водночас, вказане має знайти своє відображення, як цього вимагають стандарти безпеки НАТО, у національному законодавстві у сфері охорони державної таємниці в частині визначення Служби безпеки України як Національного органу безпеки.

Відповідно до стандартів безпеки НАТО та ЄС, окрім забезпечення виконання усіх заходів та процедур безпеки, а також контролю за охороною інформації, обмін якою здійснюється, передбачено наділення Національного органу безпеки функціями з комунікаційно-інформаційної безпеки, у т.ч. і з питань технічного захисту інформації [7; 8].

Вказаний підхід, на нашу думку, сприяє ефективному вирішенню нагальних завдань у сфері безпеки інформації, створює необхідні умови для удосконалення державного контролю і координації діяльності державних органів з питань технічного захисту інформації.

У свою чергу, в Україні питання щодо реалізації державної політики у сферах криптографічного та технічного захисту інформації наразі покладено на Державну службу спеціального зв’язку та захисту інформації України [10].

При цьому забезпечення охорони державної таємниці відповідно до статті 2 Закону України “Про Службу безпеки України” покладається на Службу безпеки України у межах визначеної законодавством компетенції [11].

Так, дійсно: покладання повноважень з питань забезпечення технічної та криптографічної складової охорони державної таємниці на інший орган свідчить про комплексний підхід до забезпечення охорони державної таємниці. Однак в умовах протистояння збройній агресії Російської Федерації на сході України функціональна розгалуженість з питань охорони державної таємниці, зокрема неналежне забезпечення технічного захисту інформації може призвести до значного погіршення ефективності функціонування загальнодержавної системи охорони державної таємниці.

Слід наголосити, що невідповідність стану технічного захисту інформації вимогам сьогодення може призвести до суттєвого підвищення уразливості інформації з обмеженим доступом, яка накопичується, зберігається й обробляється в автоматизованих системах, через що спостерігається зростання загроз безпеці держави, суспільства та особистості.

Тому впровадження ефективних заходів з технічного захисту інформації, як невід’ємної складової охорони інформації з обмеженим доступом, сприятиме надійному функціонуванню системи національної безпеки держави. З огляду на викладене, пропонується запровадити нові підходи до визначення повноважень державних органів з функцій контролю за технічним захистом інформації у сфері охорони державної таємниці.

Крім того, потребують удосконалення і такі напрями охорони державної таємниці, як порядок провадження діяльності, пов’язаної з державною таємницею, процедури перевірки громадян у зв’язку з допуском до державної таємниці, а також питання впровадження диференційованих підходів до застосування фізичних та технічних заходів захисту інформації залежно від наданого грифу обмеження доступу до інформації. Виклад вказаної проблематики є достатньо осяжним, у зв’язку з чим доцільно продовжити науковий дискурс концептуальних питань реформування системи охорони державної таємниці та службової інформації.

Висновки.

Система охорони державної таємниці та службової інформації потребує постійного удосконалення, оскільки виклики сьогодення, у т.ч. і в інформаційній сфері, вимагають якнайшвидшого реагування та протидії. Відповідно, робота щодо виокремлення саме “чутливих” напрямів охорони державної таємниці та службової інформації, які потребують змін, має проводитися пропорційно розвитку у сфері інформаційної безпеки.

Зокрема, основні зусилля у ході здійснення заходів з реформування системи охорони державної таємниці та службової інформації мають бути зосереджені на вирішенні наступних питань:

- об’єднання державної таємниці та службової інформації в єдину категорію інформації, доступ до якої обмежується виключно в інтересах, передбачених статтею 6

Закону України “Про доступ до публічної інформації”, та яка підлягає охороні державою; здійснення заходів щодо впровадження нових комплексних підходів та створення уніфікованої системи безпеки як державної таємниці, так і службової інформації, яка б забезпечувала в усіх сферах надійний та ефективний захист чутливих відомостей, спеціальний режим доступу до яких встановлюється, виходячи з інтересів держави;

- закріплення на законодавчому рівні встановлених політикою безпеки НАТО та ЄС стандартів та процедур щодо застосування системи ступенів обмеження доступу до інформації;
- визначення у вітчизняному законодавстві у сфері охорони державної таємниці Служби безпеки України як Національного органу безпеки.

Крім того, враховуючи, що на Службу безпеки України покладено впровадження мінімальних стандартів безпеки НАТО та ЄС, пропонується запровадити нові підходи до визначення повноважень державних органів з функцій контролю за технічним захистом інформації у сфері охорони державної таємниці.

Також слід зазначити, що наведені пропозиції щодо реформування системи охорони державної таємниці та службової інформації узгоджуються з напрацюваннями та висновками робочої групи, за результатами діяльності якої розроблено пропозиції до проектів Концепції реформування системи охорони державної таємниці та службової інформації, а також відповідних нормативних актів щодо введення її у дію в рамках виконання пункту 4.12 Стратегії національної безпеки України, затвердженої Указом Президента України від 26.05.2015 р. № 287/2015 [1], а також задля усунення наявних розбіжностей у підходах до захисту інформації з обмеженим доступом у державах євроатлантичної спільноти та в Україні.

Переконані, що реалізація зазначених напрямів має здійснюватися на підставі ґрунтовного вивчення досвіду країн євроатлантичної спільноти щодо охорони їх класифікованої інформації.

Використана література

1. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року “Про Стратегію національної безпеки України” : Указ Президента України від 26.05.15 р. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/287/2015

2. Семенюк О.Г. Проблеми охорони державної таємниці: кримінально-правові та кримінологічні аспекти : монографія / О.Г. Семенюк. – К. : “Видавничий дім “АртЕк”, 2017. – С. 335.

3. Розвадовський О.Б. Забезпечення охорони державної таємниці та службової інформації: теоретичний, правовий та організаційний аспекти : моногр. : у 2-х ч. – Ч. 1 / О.Б. Розвадовський. – К. : Центр навч.-наук. та наук.-практ. видань НА СБ України, 2014. – С. 163.

4. Про інформацію : Закон України від 02.01.92 р. № 2658-XII. – Режим доступу : http://zakon.rada.gov.ua/laws/show/2657-12

5. Мейдич І.М. Кримінально-правова охорона службової інформації : підходи до удосконалення : матеріали науково-практичної конференції, 08 червня 2016 р. ; упорядн. В.М. Фурашев, С.Ю. Петряєв., 2016. – С. 164.

6. Про доступ до публічної інформації : Закон України від 13.01.11 р. № 2939-VI. – Режим доступу : http:// zakon3.rada.gov.ua/laws/show/2939-17

7. Security within the North Atlantic Treaty Organisation (C-M(2002)49). – Режим доступу : http://arhives.nato.int/amendments-to-nato-c-m-55-15-final;isad

8. Council Decision of 23 September 2013 on the security rules for protecting EU classified information (2013/488/EU). – Режим доступу : http://publications.europa.eu/en/publication-detail/-/publication/d43001e3-356d-11e3-806a-01aa75ed71a1

9. Адміністративні домовленості щодо охорони інформації з обмеженим доступом між Урядом України та Організацією Північноатлантичного договору : ЗаконУкраїни від 24.05.17 р. № 2068-VIII . – Режим доступу : http://zakon5.rada.gov.ua/laws/show/950_035-16

10. Про Державну службу спеціального зв’язку та захисту інформації України : Закон України від 23.02.06 р. № 3475-І. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/3475-15

11 Про Службу безпеки України : Закон України від 25.03.92 р. № 2230-XII. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2229-12

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~