УДК: 342.1+355/359

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

РЕФОРМУВАННЯ СИСТЕМИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ: ПРАВОВІ АСПЕКТИ

Анотація. *У статті аргументується необхідність якнайшвидшого перегляду поглядів та усталених традицій до існуючих у національній практиці напрямів охорони державної таємниці з урахуванням досвіду держав-учасниць НАТО та ЄС, а також наводяться та описуються основні напрями такого перегляду.*

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

Summary. *The article grounds the necessity of prompt reassessment of approaches and established traditions towards existing in national practice directions of protection of classified information taking into consideration the experience of the NATO and EU member states, and also presents and describes the main directions of such reassessment.*

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

Аннотация. *В статье аргументируется необходимость скорейшего пересмотра взглядов и упроченных традиций к существующим в национальной практике направлениям охраны государственной тайны с учетом опыта государств-членов НАТО и ЕС, а также определяются и описываются основные направления такого пересмотра.*

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

Постановка проблеми. Події, які спостерігаються на світовій арені, супроводжуються процесом перерозподілу зон впливу у світовому просторі, розвитком інформаційних технологій, що породжують нові способи заволодіння інформацією. У зв’язку з цим, питання убезпечення секретної інформації є актуальними та потребують від держав, незалежно від їх розвитку та впливовості, постійного зміцнення власної системи охорони секретної інформації, а також вимагають спроможності не лише відбити загрози безпеці інформації, а й мінімізувати ризики, у разі реального витоку секретних відомостей.

Незмінність курсу нашої держави у євроатлантичний простір, незважаючи на військову агресію Російської Федерації на сході України, окупацію частини нашої суверенної території, а також проведення нею різноманітних спеціальних інформаційних операцій, направлених, зокрема, і на розхитання світового устрою, вимагає від України відійти від традиційних підходів до охорони державної таємниці, які тягнуться з часів СРСР, та виробити зовсім новий погляд на безпеку інформації, спираючись як на власні напрацювання українських вчених, так і на євроатлантичний досвід із зазначеного питання.

Результати аналізу наукових публікацій. На науковому рівні питання, пов’язані з реформуванням системи охорони державної таємниці, досліджували такі науковці як С. Князєв, І. Мейдич, О. Розвадовський, О. Семенюк, Т. Ткачук, В. Шлапаченко та інші. Разом з тим, події XXI сторіччя, пов’язані з витоками секретних відомостей, наштовхують на необхідність ще раз з’ясувати цінність інформації у вільному суспільстві та спробувати оцінити наслідки від її розголошення. Задля мінімізації ризиків витоку такої інформації,

робота з виокремлення та ґрунтовного вивчення напрямів системи охорони державної таємниці, які потребують удосконалення, має вестися на постійній основі як з урахуванням набутого Україною власного досвіду забезпечення безпеки інформації під час протистояння збройній агресії Російської Федерації, так і наявних напрацювань держав-учасниць НАТО та ЄС.

Метою статті є визначення окремих аспектів реформування системи охорони державної таємниці (перегляд функціонування дозвільного порядку провадження діяльності пов’язаної з державною таємницею, допускної системи, а також окремих питань інженерно-технічного захисту інформації) з огляду на євроатлантичні прагнення нашої держави.

Виклад основного матеріалу. Адаптація законодавства до норм Європейського Союзу є однією з найважливіших складових політики європейського вибору України та будь-якої іншої держави, яка йде шляхом європейської інтеграції. За даними міжнародних експертів, для входження України в правове поле Європи необхідно прийняти нові або внести відповідні зміни майже в чотири тисячі законів та інших нормативно-правових актів. Це означає, що все законодавство України повинне бути модифіковане відповідно до міжнародних принципів і стандартів [1, с. 32].

Не є винятком і національне законодавство у сфері охорони державної таємниці та службової інформації. Зазначене обумовлено, передусім, наявністю певних розбіжностей у підходах до захисту інформації з обмеженим доступом у державах євроатлантичної спільноти та в Україні.

Разом з тим, слід зазначити, що реформування законодавства має відбуватися на основі всебічного вивчення досвіду провідних держав світу у сфері безпеки інформації. Однак, потрібно зауважити, що копіювання чужого, нехай і найуспішнішого досвіду, недостатньо продумане перенесення його на наш ґрунт без урахування українських реалій ніколи не приводило до успіху [2, с. 342].

Слід зазначити, що окремі напрями реформування системи охорони державної таємниці та службової інформації (пов’язані із процедурами віднесення інформації до такої, що потребує обмеження у доступі; визначення на законодавчому рівні Національного органу безпеки; питання технічного захисту інформації) було висвітлено у минулому науковому дослідженні [3, с. 79].

Поряд з цим, на увагу заслуговують й інші питання у сфері безпеки інформації, що стосуються дозвільного порядку провадження діяльності, пов’язаної з державною таємницею; процедур перевірки громадян у зв’язку з допуском до державної таємниці, а також окремих питань інженерно-технічного захисту інформації, та потребують подальшого удосконалення в рамках реформування системи охорони державної таємниці та службової інформації. Пропонуємо розглянути кожен із напрямів більш детально.

З огляду на євроінтеграційні прагнення нашої держави, одним з першочергових напрямів, що потребує змін, є дозвільна система провадження діяльності, пов’язаної з державною таємницею.

Відповідно до статті 20 Закону України “Про державну таємницю” державні органи, органи місцевого самоврядування, підприємства, установи, організації мають право провадити діяльність, пов’язану з державною таємницею, після надання їм Службою безпеки України спеціального дозволу на провадження діяльності, пов’язаної з державною таємницею (далі – Спеціальний дозвіл) [4].

Водночас, законодавець повинен визначитись з доцільністю надання такого дозволу державним органам, враховуючи мету їх створення – здійснення функцій держави.

При вирішені вказаного питання слід враховувати, що суб’єктами режимно-секретної діяльності в більшості є державні органи, зупинення чи скасування яким відповідного Спеціального дозволу призведе до припинення їх діяльності. Наведене є неприпустимим з огляду на необхідність забезпечення сталого функціонування певних галузей діяльності держави особливо за умов ведення воєнних (бойових) дій.

Якщо звернутися до міжнародного досвіду із зазначеного питання, зокрема, до законодавства держав-учасниць НАТО та ЄС, можемо пересвідчитися, що державним органам дозвіл на роботу з класифікованою інформацією не оформлюється, оскільки їх діяльність безпосередньо пов’язана з реалізацією та виконанням функцій держави у т.ч. у сфері оборони, державної безпеки та охорони правопорядку тощо.

З огляду на міжнародний досвід, а також з метою мінімізації ризиків уникнення нестабільного виконання органами державної влади своїх функцій, пропонується досконало вивчити питання щодо можливості відмови від оформлення такого дозволу державним органам, які відповідно до покладених завдань виконують секретні роботи, а належний стан режиму секретності на такій категорії суб’єктів режимно-секретної діяльності підтримувати за допомогою заходів офіційного контролю.

Залишається невирішеним і питання щодо процедури надання, переоформлення Спеціального дозволу державним органам, підприємствам, установам, організаціям (далі – Установи), керівником яких є іноземний громадянин.

Сьогодні у процес реформування різноманітних сфер діяльності держави залучаються іноземні громадяни, шляхом призначення їх на керівні посади Установ, у тому числі і на ті, які провадять діяльність, пов’язану з державною таємницею. Водночас, як вже зазначалося вище, такі Установи мають право провадити відповідну діяльність після надання їм Службою безпеки України відповідного Спеціального дозволу. Разом з тим, частиною десятою статті 20 Закону наголошено, що Спеціальний дозвіл не надається, якщо керівник Установи не є громадянином України або не має допуску до державної таємниці [4].

Одним із шляхів вирішення вказаного питання є надання можливості уповноваженому органу СБУ здійснювати заходи з надання, переоформлення Спеціального дозволу Установам, у разі призначення іноземця на керівну посаду, за умови взяття ним письмового зобов’язання щодо збереження державної таємниці та надання йому на підставі відповідного розпорядження Президента України та за дозволом СБУ доступу до державної таємниці.

Стандартами безпеки НАТО та ЄС приділено неабияку увагу й питанням захисту інформації під час виконання підприємствами недержавної форми власності контрактів або робіт, пов’язаних із секретними відомостями.

Так, з метою зниження рівня ймовірності реалізації загроз, пов’язаних із розголошенням інформації з обмеженим доступом, яка використовується промисловими підприємствами під час виконання секретних контрактів, застосовуються заходи і процедури з її охорони. Таким чином, у стандартах безпеки НАТО та ЄС уводиться поняття “промислова безпека”, яке наразі у національному законодавстві відсутнє, в рамках якої і здійснюються відповідні заходи щодо захисту інформації. Разом з тим, для виконання секретних контрактів або роботи над секретним дослідженням з використанням інформації з обмеженим доступом з грифом CONFIDENTIAL (еквівалент грифу секретності “Таємно”) чи вище, підприємству має бути надано відповідний Спеціальний дозвіл [5; 6].

Крім того, вже на стадії попередніх переговорів або проведення тендерів щодо укладення секретних контрактів від підприємств вимагається вжиття відповідних заходів з охорони інформації з обмеженим доступом, а співробітники підприємства до

надання відповідного Спеціального дозволу повинні у встановленому порядку отримати доступ та пройти інструктаж з питань безпеки.

Впровадження зазначеного євроатлантичного досвіду у національне законодавство у частині забезпечення ефективної системи захисту інформації на підприємствах недержавної форми власності, які провадять секретні роботи, а також уведення відповідного поняття, еквівалентного “промисловій безпеці” із відповідним змістовним наповненням надасть змогу, на нашу думку, деякою мірою мінімізувати ті ризики, що виникають під час виконання такими суб’єктами державного замовлення чи передачі секретної інформації від замовника до виконавця тощо.

Поряд із дозвільним порядком провадження діяльності, пов’язаної з державною таємницею, враховуючи умови сьогодення, потребують перегляду і підходи до забезпечення функціонування допускної системи у цій сфері.

Так, у рамках цієї роботи проаналізовано основні положення і вимоги нормативних приписів у зазначеній сфері НАТО, ЄС та окремих держав-учасниць цих міжнародних організацій, формування безпекового законодавства яких відбувалося за схожих з існуючими в Україні умов (Польща, Румунія, Болгарія, Словаччина, Чехія тощо).

За результатами дослідження визначено, що принциповим підходом до можливості надання доступу особам до секретної інформації, закріпленим стандартами НАТО та ЄС, є визначення необхідності доведення до особи секретних відомостей у зв’язку з виконанням нею службових обов’язків (принцип “need-to-know” – “необхідного знання”, як правило, встановлюється керівником суб’єкта режимно-секретної діяльності), наявність свідоцтва про проходження необхідних процедур з питань безпеки, спрямованих на встановлення лояльності та надійності особи (“Personnel Security Clearance” – найближчим еквівалентом в українському законодавстві є “допуск”), а також проведення навчання та інструктажу з питань безпеки, що проводяться відносно особи, якій надається доступ до секретної інформації.

Вбачається, що законодавство України у зазначеній сфері не повною мірою узгоджується зі стандартами безпеки НАТО та ЄС, а також з системою надання доступу до секретної інформації держав-учасниць цих міжнародних організацій.

Відповідно до статті 1 Закону України “Про державну таємницю” – допуск до державної таємниці – оформлення права громадянина на доступ до секретної інформації.

При цьому слід зазначити, що прямий переклад відповідного терміну, що застосовується у стандартах безпеки НАТО та ЄС (“Personnel Security Clearance Certificate”), означає – “сертифікат очистки персоналу з питань безпеки”, “свідоцтво про проходження персоналом процедур безпеки”, тобто мається на увазі, що особі надається сертифікат, який свідчить про позитивний результат перевірки особи щодо її лояльності, міри довіри до неї, що дає можливість надавати їй доступ до секретної інформації [5; 6].

Такі сертифікати, згідно з національним законодавством держав-учасниць НАТО та ЄС (зокрема Польщі, Румунії, Болгарії, Чехії, Словаччини тощо), видаються уповноваженим державним органом, що здійснює (або організовує) відповідну перевірку з питань безпеки, на певний термін залежно від ступеня секретності інформації, з якою особа планує працювати. При цьому, такий сертифікат залишається чинним незалежно від ситуативної потреби особи у роботі з секретними документами.

Необхідно зауважити, що національним законодавством Польщі, Румунії, Болгарії, Чехії, Словаччини тощо передбачено, що глибина перевірки безпосередньо залежить від ступеня секретності інформації, до якої планується надати доступ особі.

Так, відповідно до законів Польщі, Румунії, Болгарії перевірка поділяється на “базову” (для доступу до інформації зі ступенем секретності, еквівалентному “Таємно”),

“розширену” (для доступу до інформації із ступенями секретності, еквівалентними “Цілком таємно”, “Особливої важливості”), а також “контрольну” (здійснюється у разі встановлення підстав для скасування дії такого сертифікату, зокрема таких як нелояльність, ненадійність, неправдивість тощо) [7 – 9].

Разом з тим, залежно від глибини перевірки особи та її оточення застосовуються наступні критерії, які ґрунтуються на визначенні ступеня її надійності, лояльності та рівні довіри до неї. Таким чином, для побудови уявлення про особу враховується інформація щодо:

- можливих протиправних вчинків у сфері шпіонажу, тероризму, саботажу, зради або заколоту;
- алкогольної, наркотичної, лікарської залежності;
- психічних або емоційних розладів;
- здійснення несанкціонованих дій у комунікаційно-інформаційних системах;
- можливої вразливості осіб до тиску з боку родичів та близьких їй осіб, на яких можуть впливати служби іноземних розвідок, терористичні групи чи інші підривні організації або особи [5; 6].

На нашу думку, зазначені критерії перевірки особи та членів її сім’ї чи осіб, які з нею проживають в рамках надання їй доступу до інформації з обмеженим доступом визначеного ступеня секретності вбачаються такими, що охоплюють майже увесь спектр тих рушійних сил, що можуть вплинути на особу та, як наслідок, на безпеку інформації, що їй була довірена.

Крім цього, законодавством Чехії, Словаччини передбачено можливість при перевірці у зв’язку з необхідністю роботи з відомостями зі ступенем секретності, еквівалентним “Особливої важливості”, застосовувати як оперативні, так і оперативно-технічні заходи, спрямовані не лише на об’єкт перевірки, а й на його оточення [10; 11].

У зв’язку з цим, важливим аспектом є строки проведення безпекової перевірки, від яких безпосередньо залежить якість результатів перевірочних заходів (індикативні терміни перевірки, встановлені законодавством окремих держав-учасниць НАТО та ЄС, наведено у таблиці 1).

Таблиця 1

Еквівалентність ступеня секретності інформації, у зв’язку з доступом до якої проводиться безпекова перевірка	**Строки проведення перевірки**			
	Польща	**Чехія**	**Болгарія**	**Румунія**
TOP SECRET – “Особливої важливості”	до 3 місяців	до 6 місяців	30 днів	30 днів
SECRET – “Цілком таємно”			45 днів	60 днів
CONFIDENTIAL – “Таємно”			60 днів	90 днів

Вбачається, що саме диференційований та поглиблений підхід до перевірки осіб у зв’язку з їх доступом до секретної інформації дає уповноваженим органам зазначених держав-учасниць НАТО та ЄС можливість видання вказаних сертифікатів про безпекову перевірку без необхідності їх скасування у зв’язку з відсутністю потреби особи у роботі із секретною інформацією.

Під час збору, обробки та зберігання інформації про особу та її оточення в ході проведення перевірки мають запроваджуватися відповідні заходи щодо її схоронності. Таке збереження зазвичай здійснюється із застосуванням, технічних засобів захисту інформації. Як свідчить вітчизняна практика, в більшості державних органів

використовується програмне забезпечення та інструментальні засоби іноземного виробництва, оскільки на державному рівні недостатньо приділено увагу створенню, удосконаленню та впровадженню власного як технічного, так і програмного забезпечення. Зазначене може спричинити порушення таких властивостей інформації, як цілісність та конфіденційність, що може завдати шкоди інтересами громадян та держави.

Також необхідно зауважити, що законодавством зазначених держав-учасниць НАТО та ЄС не передбачено процедур, аналогічних погодженню “номенклатури посад, перебування на яких потребує оформлення допуску та надання доступу до державної таємниці” на кожному підприємстві, установі, організації, як це визначено в українському законодавстві.

Нормативно-правові акти у сфері охорони інформації з обмеженим доступом окремих країн передбачають складання на підприємствах, установах, організаціях “переліків посад, перебування на яких потребує роботи з відомостями з обмеженим доступом”, що затверджуються керівниками таких суб’єктів режимно-секретної діяльності.

При цьому, Національні органи безпеки мають право контролювати правомірність віднесення посад до такого переліку.

Також, законодавство держав-учасниць НАТО та ЄС не передбачає грошової компенсації особам за роботу в умовах режимних обмежень. Як правило, підвищена грошова винагорода таким особам визначається залежно від тарифікації посад, перебування на яких потребує доступу до секретної інформації.

З огляду на наведене, пропонується основні зусилля у рамках реформування існуючої допускної системи скерувати за такими напрямами:

1. Відмовитись (шляхом внесення змін до законодавчих актів або видання нової редакції відповідного закону) від терміну “допуск до державної таємниці”, який є спадщиною режимних вимог колишнього СРСР та призводить до обмежень застосування органами СБУ усіх можливих підстав для відмови в його наданні або скасуванні, впровадити на його заміну визначення “сертифікат про безпекову перевірку” (або споріднене з ним).

2. Встановити диференційований обсяг (що відповідатиме вимогам стандартів НАТО та ЄС) безпекової перевірки громадян в залежності від ступеня секретності такої інформації.

3. З метою забезпечення якості перевірочних заходів передбачити строк проведення безпекової перевірки до 3 місяців (з урахуванням досвіду Польщі).

4. Розглянути питання щодо можливості встановлення норми, згідно з якою безпекова перевірка здійснюватиметься відносно осіб, які претендують на заняття посади, що передбачає доступ до секретної інформації, тобто ще до їх призначення (зазначені положення існують у законодавстві Польщі, Болгарії тощо).

5. Передбачити, що сертифікат за результатами такої перевірки видається на встановлений строк залежно від ступеня обмеження доступу до інформації та не потребує скасування у разі відсутності потреби у громадянина доступу до секретної інформації (на відміну від норми, встановленої у статті 26 Закону України “Про державну таємницю”).

6. Від грошової компенсації за роботу в умовах режимних обмежень перейти на диференційовану тарифікацію посад, які передбачають роботу із секретною інформацією, оскільки існуюча система провокує необґрунтоване віднесення посад до таких, що передбачають роботу із секретними документами, та призводить до невиправданого розширення кола осіб, що матимуть доступ до секретної інформації.

7. Відмовитися від підготовки підприємствами, установами, організаціями номенклатур посад, перебування на яких потребує оформлення допуску та надання доступу до державної таємниці, та їх погодження органами СБУ. Натомість встановити, що керівники підприємств, установ, організацій здійснюють погодження переліку посад, перебування на яких передбачає доступ до секретної інформації, правильність складання якого перевірятиметься органами СБУ у ході проведення заходів офіційного контролю.

Крім того, надійне функціонування дозвільного та допускного порядку провадження діяльності, пов’язаної з державною таємницею, не може оминати питань застосування заходів та засобів фізичного захисту безпеки інформації та забезпечення контролю доступу до режимних Приміщень (зон, територій).

Так, приписами Закону України “Про державну таємницю” передбачено комплекс заходів, спрямованих на охорону державної таємниці, одним із яких є інженерно-технічний захист відомостей, який досягається відповідними засобами охорони [4].

Зокрема, національним законодавством визначено, що до інженерно-технічних засобів охорони належать інженерні споруди, загорожі, пристрої, обладнані технічними засобами охорони і призначені для запобігання несанкціонованому чи безконтрольному доступу сторонніх осіб в режимні Приміщення (зони, території).

В науковій літературі аспекти інженерно-технічного захисту інформації розглядаються як такі, що загалом спрямовані не безпосередньо на інформацію, а на системи, об’єкти та носії, на яких інформація збирається, обробляється й розповсюджується [12, с. 220].

Разом з тим, варто зазначити, що фінансування питання впровадження надійних заходів та засобів інженерно-технічного захисту суб’єктами режимно-секретної діяльності у більшості випадків здійснюється за залишковим принципом.

Однак, зазначене питання як ніколи набрало своєї значимості, оскільки в умовах військового протистояння відсутність ґрат, залізних дверей чи іншого спеціалізованого обладнання, призначеного для забезпечення режиму секретності на об’єкті, не дозволить, навіть на деякий час, зупинити супротивника та здійснити заходи, передбачені на випадок виникнення надзвичайної ситуації. При цьому, ціна інформації в умовах ведення воєнних дій є вкрай високою, а її неконтрольований витік може спричинити невиправних наслідків для подальшого планування та проведення військових операцій.

Звертаючись до євроатлантичного досвіду із зазначеного питання, слід зазначити, що стандартами безпеки НАТО та ЄС передбачено дещо інший підхід до інженерно-технічного захисту інформації.

Зокрема, уведено поняття “фізична безпека”, зміст якого полягає у застосуванні фізичних захисних заходів щодо місць, будівель та Приміщень, в яких знаходиться інформація, яка потребує захисту від втрати або розголошення [5; 6].

При цьому, зазначені заходи безпеки залежать від загроз, ступенів обмеження доступу і кількості матеріальних носіїв інформації, що захищатимуться.

Тобто для забезпечення фізичної безпеки в усіх Приміщеннях, будинках, офісах, кімнатах (далі – Приміщення) та на територіях, де зберігається та/або обробляється інформація з обмеженим доступом передбачено встановлення зон безпеки інформації відповідного класу (клас I, клас II, адміністративна зона) [5; 6].

Зони безпеки класу I та II призначені для обробки та зберігання інформації зі ступенем NATO CONFIDENTIAL (еквівалент “Таємно”) та вище. Разом з тим, вхід до зони класу I для всіх практичних цілей розглядається як доступ до секретної інформації. При цьому, усі входи та виходи Приміщення обладнуються відповідними системами вхідного контролю, що дозволяють доступ лише тих осіб, яким у встановленому порядку надано допуск та які мають Спеціальний дозвіл до цієї зони.

У зоні безпеки класу ІІ можливо охороняти інформацію з обмеженим доступом визначеного вище ступеня секретності від доступу сторонніх осіб шляхом встановлення внутрішнього контролю. Вхід до цієї зони можливий як особам, яким надано допуск та які мають Спеціальний дозвіл, так і іншим особам, які пропускаються за умовами наявності супроводження або еквівалентного контролю [5; 6].

Навколо або на підходах до зон безпеки класу І та ІІ може встановлюватися адміністративна зона. Така зона вимагає наявності візуально визначеного периметра, усередині якого є можливість здійснювати контроль за персоналом та транспортними засобами. При цьому, в адміністративних зонах може оброблятися та зберігатися тільки інформація із ступенем обмеження доступу не вище NATO RESTRICTED (еквівалент “Для службового користування”) [5; 6].

Тобто встановлення у Приміщеннях або на території відповідної зони безпеки відповідного класу залежить від інформації, яка в них циркулює (ступінь її секретності, кількість і форма обробки, її зберігання), категорії співробітників, які підпадають під дію принципу “необхідного знання” (доступ до інформації обумовлено виконанням службових обов’язків), а також оцінки загроз інформації.

Слід зазначити, що у національній практиці присутній аналог зонування, водночас відмінність полягає у висунутих вимогах до їх обладнання, які більшою мірою залежать тільки від природи виникнення носія інформації, заходи із захисту якої планується здійснювати.

Таким чином, в рамках комплексного підходу до зміцнення системи охорони державної таємниці, вбачається доцільним розглянути питання щодо впровадження диференційованих підходів до застосування фізичних та технічних заходів захисту інформації залежно від наданого грифу обмеження доступу до інформації. Вказане дозволить запобігти, своєчасно виявити, перешкодити протиправній діяльності іноземних спеціальних служб, спрямованій на здобування секретних відомостей, посяганням на інформацію з боку окремих організацій, нелояльних співробітників чи їх груп, полегшити процес розмежування доступу до секретної інформації, з урахуванням принципу “необхідного знання”, що звузить коло обізнаних осіб, а також надасть можливість удосконалити діяльність з виявлення порушень встановлених правил безпеки.

Крім того, слід наголосити, що з огляду на необхідність підвищення рівня захисту державної таємниці, а також приведення законодавства України у вказаній сфері діяльності у відповідність до стандартів безпеки НАТО та ЄС, з метою сприяння подальшій інтеграції України в європейське співтовариство, питання реформування системи охорони державної таємниці та службової інформації є доволі важливим та потребують залучення до їх вирішення різних інституцій держави та громадськості.

Висновки.

Підсумовуючи зазначене, можна дійти висновку, що наразі державна таємниця розглядається як один із найважливіших видів інформації з обмеженим доступом, а розголошення її може призвести до породження нових загроз державній безпеці. Таким чином, охорона державної таємниці є однією із складових частин загальної системи забезпечення національної безпеки України. А подальший розвиток та постійне вдосконалення системи охорони державної таємниці та службової інформації забезпечуватиме адекватне і гнучке реагування на можливі загрози її безпеці.

Саме тому метою зазначеної статті було визначення окремих напрямів реформування системи охорони державної таємниці, а також надання відповідних пропозицій, зокрема:

- Спеціальний дозвіл на провадження діяльності, пов’язаної з державною таємницею державним органам, які відповідно до покладених завдань виконують секретні роботи не

оформлювати, а належний стан режиму секретності на такій категорії суб’єктів режимно-секретної діяльності підтримувати за допомогою заходів офіційного контролю;

- на заміну терміну “допуск до державної таємниці” впровадити визначення “сертифікат про безпекову перевірку” (або споріднене з ним);

- відмовитися від підготовки підприємствами, установами, організаціями номенклатур посад, перебування на яких потребує оформлення допуску та надання доступу до державної таємниці, та їх погодження органами СБУ;

- встановити диференційований обсяг (що відповідатиме вимогам стандартів НАТО та ЄС) безпекової перевірки громадян в залежності від ступеня секретності такої інформації;

- впровадити диференційовані підходи до застосування фізичних та технічних заходів захисту інформації залежно від наданого грифу обмеження доступу до інформації.

На нашу думку, реалізація висвітлених напрямів реформування системи охорони державної таємниці докорінно змінять підходи до забезпечення безпеки інформації та нададуть змогу убезпечити власну таємницю.

Використана література

1. Нормативно-правове забезпечення стратегічного курсу України на європейську та євроатлантичну інтеграцію : навчальний посібник-хрестоматія : у 2-х ч. ; уклад. і коментар І.В. Артьомов, Д.В. Вітер, Л.І. Загайнова, О.М. Казакевич, О.М. Руденко. – Ужгород : Ліра, 2007. – Ч. 1. – С. 32.

2. Семенюк О.Г. Проблеми охорони державної таємниці : кримінально-правові та кримінологічні аспекти : монографія. – К. : ТОВ “Видавничий дім “АртЕк”, 2017. – С. 342.

3. Болдир С.В. Перспективи реформування системи охорони державної таємниці та службової інформації // Інформація і право. – № 4(23)/2017. – С. 79-85.

4. Про державну таємницю : Закон України від 21.01.94 р. № 3855-XII // Відомості Верховної Ради України (ВВР). – 1994. – № 16.

5. Security within the North Atlantic Treaty Organisation (C-M(2002)49). – Available as : http://arhives.nato.int/amendments-to-nato-document-security-within-nato-c-m-55-15-final

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

7. The Act of 5 August 2010 on the Protection of Classified Information (Poland). – Available as : http://www.infor.pl/akt-prawny/194475,metryca,ustawa-o-ochronie-informacji-niejaw nych.html

8. National standarts on the protection of classified information in Romania, Government decision no 585/2002 [Online tool]. – Available as: http://www.orniss.ro/en/legislatie/pdf/GD585.pdf.

9. Classified Information Protection Act (Bulgaria) [Online tool]. – Available as : http://www.dksi.bg/NR/rdonlyres/070CA55F-EAD3-435D-BE41A01-AC62A005D/-/0/-CLASSIFIEDINFORMATIONPROTECTIONACT.doc

10. Czech Republic: Act No. 412 of 21 September 2005 on the Protection of Classified Information [Online tool]. – Available as : http://www.right2info.org/laws/Chech_Protection_classified_info.pdf/at_download/file

11. Slovakia : Act No. 215/2004 Coll. On the Protection of Classified Information and on Amendments to Certain Acts (as amended up to July 1, 2013) [Online tool]. – Available as : http://www.wipo.int/wipolex/en/details.jsp?id=15574

12. Кормич Б.А. Інформаційне право : підручник / Б.А. Кормич. – Харків : “Бурун і К”, 2011. – С. 220.

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