Литература: ***1.*** *Guide to the Expression of Uncertainty in Measurement: First Edition.- ISO, Switzerland, 1993.- 101 p.* ***2.*** *Ціделко В. Д., Яремчик Н. А. Невизначеність вимірювання. Обробка даних і подання результату вимірювання: Монографія.-К.:ІВЦ "Видавництво <Політехніка>", 2002.-176с.* ***3.*** *G. Mauris, V. Lasserre, L. Foulloy. A Fuzzy approach for the expression of uncertainty in measurement. Measurement, 29, 2001.- Elsevier,- p.165-177.* ***4.*** *Е. Т. Володарский, Л. А. Кошевая, А. Н. Карпенко "Взаимосвязь вероятностного подхода и нечеткой логики при оценке неопределенности измерений"// Системи обробки інформації.- Харків, 2006.-с. 19-22. N7.*

УДК 65.012.8

ЩОДО МЕТОДИКИ РЕАЛІЗАЦІЇ ПРОЦЕДУРИ ВІДНЕСЕННЯ ІНФОРМАЦІЇ ДО СЕКРЕТНОЇ

Олександр Архипов, Валерій Ворожко *

*Національний технічний університет України „КПІ", *Інститут захисту інформації з обмеженим доступом Національної академії СБ України*

Анотація: **Розглянуто методичні аспекти реалізації процедури віднесення інформації до секретної, зокрема, виконано формалізацію цієї процедури з представленням її чотириетапною схемою обробки вихідної інформації.**

Summary: **Methodical aspects of realization of information classification procedure to state secret are considered, in particular, there is made formalization of this procedure with its representation by four-stage scheme of the initial information processing.**

Ключові слова: **Державна таємниця, секретна інформація.**

I Вступ

Інформатизація світового суспільства, глобальне розповсюдження нових інформаційних технологій стимулюють загально цивілізаційний процес утворення світового інформаційного простору. Інтеграційні тенденції цього процесу мають спиратися на зростаючу інформаційну відкритість його учасників. Але реалії розвитку та становлення світового інформаційного суспільства вказують на наявність в процесах інформатизації ряду складних та суперечливих тенденцій.

З точки зору розвитку та поширення електронного бізнесу, культурного обміну, технологій дистанційного навчання, доступу до загальносвітових наукових, технічних і культурологічних ресурсів новітні інформаційні та телекомунікаційні технології – це очевидний позитив. Однак одночасно вони – виклик існуючій системі захисту інтелектуальної власності та сегменту національних інформаційних ресурсів, який за своїм характером не є загальнодоступним. Однією з найсуттєвіших складових цього сегменту є державна таємниця (ДТ) – категорія секретних відомостей, умови віднесення інформації до якої чи захист цієї інформації здійснюється відповідно до закону [1]. Процес глобальної інформатизації суспільства приніс для ДТ, як і інших видів інформації з обмеженим доступом (ІзОД), певні проблеми, пов'язані з особливостями захисту ДТ в умовах нового інформаційного середовища.

Для незалежної України, як і для інших держав, що утворилися в пострадянському просторі на початку 90-х років, ці проблеми мали специфічний характер. Справа в тому, що більшість розвинутих країн світу питання регулювання відносин в сфері охорони ДТ розв'язує в межах правового поля, утвореного прийняттям відповідних законодавчих актів. На відміну від цих країн в СРСР не існувало закону про охорону ДТ (як і про регулювання інформаційних відносин взагалі). Практичні питання захисту державних секретів регламентувалися підзаконними нормативними актами, а перелік відомостей, що за своїм змістом мали належати до ДТ, був секретним документом [2]. Фактично мало місце відчуження інституту секретності від суспільства, внаслідок чого не розглядалися та не обговорювалися публічно принципи діяльності цього інституту, його організаційна структура та витрати на функціонування, критично не аналізувався механізм та методи охорони ДТ, їх ефективність та дієвість.

Радикальні зміни політичного та економічного устрою, що сталися в Україні на початку 90-х років та отримали своє законодавче закріплення в різних сферах життєдіяльності особи, суспільства та держави, не обминули і сфери інформаційних відносин. У 1992 р. було прийнято Закон України „Про інформацію", який заклав правові основи інформаційної діяльності. У січні 1994 р. введено в дію Закон України „Про державну таємницю", а в серпні 1995 р. опубліковано „Звід відомостей, що становлять державну таємницю України" (ЗВДТ). З появою цих відкритих документів процес створення механізму віднесення інформації до ДТ можна

вважати завершеним (хоча б у першому наближенні). Чільна роль у функціонуванні цього механізму належить закону „Про державну таємницю", в якому, зокрема, визначено поняття ДТ, процедури віднесення інформації до ДТ, її засекречування та категоріювання за ступенем секретності. Принципово важливою є відсутність в законі вимоги безпосереднього віднесення інформації до ДТ тільки на підставі належності цієї інформації до наведених у ст. 8 закону сфер оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку.

Фактично належність інформації до перерахованих вище сфер реалізує лише необхідні умови віднесення цієї інформації до ДТ. Остаточне рішення у питанні віднесення приймається, виходячи з оцінки рівня шкоди, що може бути завдана національній безпеці України в разі розголошення даної інформації (другий абзац ст. 8 закону „Про державну таємницю"), та при визнанні доцільності такого рішення з боку державного експерта з таємниць (ст. 9). Тобто достатні умови віднесення інформації до ДТ мають комплексний характер та визначаються через критерії можливої шкоди національній безпеці внаслідок розголошення цієї інформації та критерії доцільності їх засекречування.

Треба зауважити, що в законі не висвітлено технологію аналізу достатніх умов та формування остаточного рішення. Є тільки алгоритм, який утворює своєрідний каркас з операцій (дій), що мають бути виконані для реалізації процедури віднесення інформації до ДТ, без деталізації та опису технологічних прийомів для практичного виконання цих операцій: відомо, що треба робити, але не уточнюється, як саме. В цьому сенсі Закон України „Про державну таємницю" сформовано на рівні вимог, що висуваються International Standard Organization (ISO) до змісту міжнародних стандартів та інших нормативних документів, зокрема в галузі інформаційної безпеки [3]. Надмірна конкретизація та деталізація документа є, як правило, наслідком його адаптації до конкретної ситуації та середовища, будь-які зміни в яких обумовлюють необхідність модернізації, переробки всього документу. Така негнучкість, неуніверсальність є вкрай небажаною для нормативних документів, надто – законів. Такі ж негативні наслідки дає однобічна технологічна спрямованість (а фактично технологічна обмеженість) норми.

Слід, однак, зазначити, що своєрідна „рамочна" структура опису процедури віднесення інформації до ДТ, наведена в законі „Про державну таємницю", вимагає від державного експерта, який безпосередньо проводить цю процедуру, вельми високого рівня як фахової кваліфікації, так і загальної підготовки, зокрема, знань з методів, методик, критеріїв експертного оцінювання, економіки, теорії ризиків тощо. Зважаючи на те, що система охорони ДТ в Україні розбудовувалася фактично заново, відсутність належної фахової та загальної підготовки представників корпусу державних експертів могла стати серйозною проблемою. Для її подолання, зокрема саме в площині допомоги державним експертам в організації їх діяльності, в 1998 р. Держкомсекретів України затвердив два документи: „Методичні рекомендації державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня їх секретності" (далі – „Методичні рекомендації...") та „Рекомендації з організації діяльності експертних комісій при державних експертах з питань таємниць" (далі – „Рекомендації...), де було досить детально викладено методичні та практичні аспекти реалізації процедури віднесення інформації до ДТ та встановлення ступеня їх секретності.

II Проблемні аспекти віднесення інформації до державної таємниці

Віднесення інформації до ДТ (або, що те ж саме – секретної інформації) є ключовим елементом реалізації практичних аспектів охорони ДТ. Справа в певних особливостях ДТ. Зокрема, якщо секретну інформацію вже виокремлено, подальші дії із забезпеченням її охорони мають єдиний встановлений згідно з існуючими нормативно-правовими вимогами порядок – так званий режим секретності. Тому саме поділ інформації на секретну та інші види інформації з обмеженим доступом визначає подальшу методологію та методики захисту інформації, його ресурсоємність, вартість, рівні захисту і т. п.

Крім того, вже виділена секретна інформація потребує додаткової деталізації за ступенем секретності відомостей, що їх складають. Ступінь секретності характеризує важливість відповідної інформації, ступінь обмеження доступу до неї та вимоги до її охорони державою. В останньому випадку мається на увазі надійність функціонування задіяних механізмів захисту ДТ, гарантованість забезпечення ними потрібного (заданого) рівня захисту, а відтак – потрібні (граничні) обсяги сукупних витрат на охорону ДТ у кожному конкретному випадку.

Тобто, для конкретного підприємства, організації, установи проблема віднесення інформації до ДТ опосередковано, через проблему забезпечення належного рівня захисту отриманих видів та обсягів секретної інформації, трансформується в проблему економічного забезпечення охорони ДТ. Цей висновок є достатньо очевидним, крім того, він навіть підтверджується кількісними даними. Ще на початку перебудови в СРСР у досить резонансній статті В. А. Рубанова [5] було наведено оцінку витрат з визначення та захисту секретної інформації в США. В цілому ці витрати складали 20 % від загальної суми асигнувань на науково-дослідницькі та дослідницько-конструкторські роботи.

Аналізуючи тогочасну ситуацію в режимно-секретній сфері (друга половина 80-х років 20-го сторіччя), В. А. Рубанов відзначав, що система охорони ДТ в СРСР за своєю суттю виражала лише інтереси політичної влади, її центрального апарату. Керувалася ця система лише зверху, шляхом прямого адміністрування і характеризувалася повною відсутністю економічних важелів (за авторським виразом – „економічних гальм"). Тому, зіштовхнувшись в часи перебудови з реаліями госпрозрахунку і товарно-грошовими відносинами, радянська система охорони секретів стала неефективною. Вирівняти ситуацію мало б врахування в питаннях захисту секретів вимог економічної доцільності їх захисту.

Відносно наведеної вище кількісної оцінки В. А. Рубанова слід зазначити, що її можна вважати вже хронологічно застарілою. До того ж це єдина з кількісних оцінок рівня витрат на захист секретної інформації з наведених у відкритих публікаціях, усі інші [6, 7, 8] зроблено для конфіденційної інформації. Однак аналіз даних саме для конфіденційної інформації, в тому числі з найновіших публікацій, якщо припустити, що максимальні витрати на захист конфіденційної інформації можна розглядати як нижню межу можливих витрат на охорону ДТ, дає приблизно ті ж самі 20 %, підтверджуючи сталість та правдоподібність оцінки В. А. Рубанова [9].

Слід підкреслити, що вище мова йде насамперед про вартісну оцінку функціонування елементів системи охорони ДТ на конкретних об'єктах інформаційної діяльності, де обсяги та ступені секретності інформації, що підлягає охороні, вже визначено. Це, так би мовити, „прямі" витрати на охорону ДТ. І якщо має місце факт необґрунтованого засекречування інформації, то, зрозуміло, що неправомірно утворений додатковий обсяг секретної інформації тягне за собою додаткові об'єктивно невиправдані витрати. Тобто цей механізм виникнення економічно недоцільних витрат в сфері охорони ДТ достатньо прозорий та очевидний. Однак необґрунтоване засекречування інформації може одночасно запустити в дію ще один механізм – механізм втраченої вигоди, який здатний привести до вельми відчутних економічних збитків. За оцінками, наведеними в [10], втрати через необґрунтоване закриття інформації в колишньому СРСР доходили до кількох десятків мільярдів рублів. Ці збитки виникали через втрату вигоди від:

- нереалізованих впроваджень та нереалізованого продажу радянських технологій за кордон;
- заборони продажу промислових виробів, військової техніки та озброєнь;
- припинення робіт за комплексними проектами, технологіями через їх повне чи часткове засекречування та внаслідок цього втрату взаємодії та координації між співвиконавцями.

Крім збитків економічного характеру, які в принципі припускають кількісні оцінки, засекречування інформації, навіть цілком правомірне, може мати негативні наслідки. Частіше за все це пов'язано з встановленням монополії, зокрема, відомчої на певні види інформації, що, наприклад, дозволяє уникнути відповідальності, чи критики за неякісно виконану роботу, приховати бездіяльність, прикрити секретністю порушення та зловживання в неконтрольованих для широкого загалу сферах життя.

III Загальна характеристика процедури віднесення інформації до секретної

Серйозність наслідків безпідставного засекречування інформації вимагає встановлення чіткої процедури віднесення інформації до ДТ. Частково ця процедура визначається Законом України „Про державну таємницю", інші її особливості конкретизуються в „Методологічних рекомендаціях..." [11], та „Рекомендаціях..." [12]. Спробуємо, проаналізувавши ці матеріали, встановити послідовність етапів віднесення інформації до секретної та конкретизувати зміст і задачі кожного з них.

Перший етап процедури віднесення – це встановлення приналежності інформації, що перевіряється, до виділеного Законом України „Про державну таємницю" дозвільного інформаційного сегменту, що охоплює чотири сфери:

а) оборони;

б) економіки, науки і техніки;

в) зовнішніх відносин;

г) державної безпеки та охорони правопорядку.

Тобто це, як вже зазначалося у Вступі, перевірка наявності необхідних умов віднесення інформації до ДТ, попередня селекція інформації, можливо приналежної до секретної. Відповідальність за прийняття правильного рішення на цьому етапі надзвичайно висока, тому цілком правомірним є питання достатності інформаційного обсягу наведеного в законі [1] сегменту а) – б) – в) – г). Зважаючи, що визначальною властивістю ДТ є той факт, що її розголошення веде до спричинення можливої шкоди національній безпеці України, звернемося безпосередньо до змісту Закону України „Про основи національної безпеки України" з метою уточнення характеру шкоди, від якої може потерпати національна безпека. Стаття 7 означеного закону вказує на можливість існування загроз національній безпеці у дев'яти сферах:

1) зовнішньополітичній;

2) держаної безпеки;

3) воєнній та безпеки державного кордону;
4) внутрішньо економічній;
5) економічній;
6) соціальній та гуманітарній;
7) науково-технологічній;
8) екологічній;
9) інформаційній.

Як бачимо, отриманий перелік 1) – 9) суттєво ширший сегменту а) – б) – в) – г). Чи є це свідченням неповноти останнього? Ні. Справа в тому, що в законі [1] мова йде про інформаційні загрози, кожна з яких у відповідних сферах національної безпеки трансформується в свої конкретні загрози. Причому останні можуть бути наслідком як розголошення певної інформації, так і навпаки, результатом неправомірного закриття якихось відомостей. Наприклад, розвідувальна, контррозвідувальна, оперативно-розшукова діяльність вимагають режиму жорсткої конспірації та закриття інформації, тоді як в екологічній та соціально-гуманітарній сферах закриття інформації може бути вкрай небажаним і становити загрозу. Щоб уникнути саме загроз подібного характеру в законі [1] формується інформаційний сегмент обмежень, що містить перелік інформації, яку категорично забороняється відносити до ДТ. Ця заборона стосується відомостей, закриття яких буде звужувати зміст та обсяг конституційних прав та свобод людини і громадянина, завдавати шкоди здоров'ю та безпеці населення. Зокрема, забороняється відносити до ДТ інформацію про:

- стан довкілля, якість харчових продуктів і предметів побуту;
- аварії, катастрофи, небезпечні природні явища, інші надзвичайні події, які сталися або можуть статися і загрожують безпеці громадян;
- стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, соціально-демографічні показники, стан правопорядку, освіти та культури населення;
- факти порушень прав і свобод людини і громадянина;
- незаконні дії органів влади, місцевого самоврядування та їх посадових осіб;
- інші відомості, згода про обов'язковість оприлюднення яких надана Верховною Радою України відповідно до законів та міжнародних угод.

Зіставлення інформації, що перевіряється, зі змістом сегменту обмежень реалізується на другому етапі загальної процедури віднесення інформації до ДТ, із закінченням якого завершується остаточна селекція відомостей, можливо приналежних до секретних (рис. 1). Тобто задача цих двох перших етапів – відсікти будь-яку інформацію, що принципово не може бути віднесена до ДТ.

Що стосується подальшого аналізу інформації, яка залишилася після другого етапу, то в законі [1], ст. 8, 2-й абзац, частина друга визначено лише базовий принцип цього аналізу, де ще раз наголошується на головній властивості ДТ: якщо виділена на другому етапі інформація є секретною, її розголошення має спричиняти шкоду національній безпеці держави. Причому ніяких натяків на те, у який спосіб виконується перевірка головної властивості ДТ, в законі немає. Більш корисним в цьому сенсі є зміст „Методичних рекомендацій..." [11], де викладено як процедуру обчислення шкоди в кількісному вимірі, так і методику визначення ступеня секретності інформації залежно від отриманого кількісного значення шкоди.

В основу використаного в [11] підходу віднесення інформації до ДТ покладено принцип економічної оцінки витрат, обумовлених розголошенням секретної інформації. Він базується на введенні спеціального показника *W* рівня потенційної шкоди, який характеризується величиною економічних збитків, заподіяних розголошенням секретної інформації, тобто *W* отримує певне кількісне значення, причому підрахунок виконується в штучно введених умовних одиницях збитків (у.о.з.) за спеціальною методикою [11]. Для відомостей, шкода від розголошення яких не може бути обчислена в економічній площині прямим застосуванням цієї методики, значення *W* визначається опосередковано. Спочатку шляхом експертного оцінювання співставляються рівні значущості витрат з будь-яким характером збитків. Потім за результатами цього співставлення визначаються економічні еквіваленти втрат довільного характеру в будь-якій сфері національної безпеки.

Таким чином, на третьому етапі процедури віднесення інформації до ДТ вирішується проблема визначення можливих втрат від розголошення інформації, що перевіряється, приведених до єдиної шкали у.о.з. Для полегшення цієї операції в [11] наведено перелік можливих наслідків розголошення секретної інформації в різних сферах діяльності та вказані відповідні економічні еквіваленти обумовлених цими наслідками збитків. Наявність подібного переліку значно спрощує оцінювання інтегрального значення показника *W*, в якому враховуються сукупні збитки в разі комплексного характеру наслідків розголошення інформації.

На останньому четвертому етапі перевірки можливої належності відомостей до секретних (рис. 1) залежно від отриманої величини показника сукупної шкоди *W* приймається рішення про відсутність чи наявність підстав для віднесення відомостей до ДТ, і в разі наявності цих підстав – про визначення ступеня секретності цих

відомостей. Критерієм в останньому випадку є знаходження значень показника W в межах певних позначок шкали сукупної шкоди:

$1 \le W < 10$ → „таємно”,
$10 \le W < 100$ → „цілком таємно”,
$100 \le W$ → „особливої важливості”.

На рис. 1 графічно представлено в достатньо спрощеній формі схему (зміст, послідовність) етапів процедури віднесення інформації до секретної. Аналіз вхідної інформації і визначення за допомогою семантичної фільтрації, чи вважати цю інформацію такою, що може бути віднесена до ДТ, реалізується достатньо прозоро і зрозуміло. Тобто до змісту етапів 1, 2 не виникає більш-менш серйозних та принципових питань. Рішення, що приймаються на 4-ому етапі, хоча і є остаточними (фінальними), базуються на простих і об’єктивних (за умов безпомилкового оцінювання значень показника W) порогових схемах, що дозволяє припустити надійність та правильність отриманих висновків. Критичним місцем процедури віднесення інформації до державної таємниці є третій етап, про що свідчить ряд публікацій за його тематикою, в яких було окреслено певні проблемні питання [13 – 15], що стосуються як принципових засад вирішення завдань цього етапу, так і відповідного математичного забезпечення.

В першу чергу це аспекти, пов’язані з розробкою методики обчислення показника можливої сукупної шкоди W та методики проведення експертної процедури оцінювання конкретних значень W (включно із способом обробки результатів колективної (групової) експертизи). Розгляд цих матеріалів виходить за рамки даної статті і потребує окремого детального викладу.

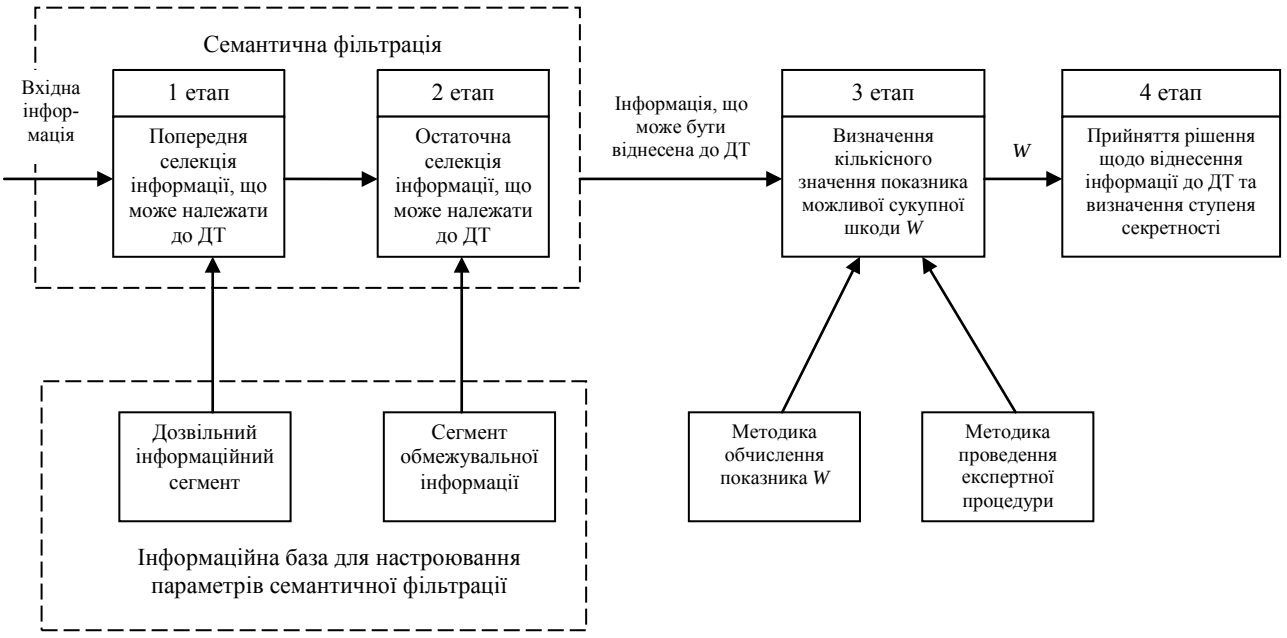

Рисунок 1 - Блок-схема процедури віднесення інформації до секретної

IV Висновки

Виконано формалізацію процедури віднесення інформації до секретної шляхом представлення цієї процедури послідовною чотириетапною схемою обробки інформації включно з елементами попередньої семантичної фільтрації та блоком кількісного оцінювання рівня важливості інформації.

*Література: **1.** Закон України «Про державну таємницю». **2.** Вус М. А., Гусев В. С. Государственная тайна – правовой институт суверенного государства / Конфидент. - № 1(17). – 1996. – с. 17-21. **3.** Галатенко В. А. Стандарты информационной безопасности. М.: Интернет-Университет Информационных технологий, 2004. – 328с. **4.** Государственная программа обеспечения гостайны / Конфидент. - №3(19). – 1996. – с. 13-17. **5.** Рубанов В. А. От «культа секретности» - к информационной культуре / Коммунист. – 13. – 1988. – с. 24-*

*30. **6.** Андрощук Г. А., Крайнев П. П. Экономическая безопасность предприятия: защита коммерческой тайны. – К.: Изд. Дом «Ин Юре», 2000. – 400 с. **7.** Петренко С. А., Симонов С. В. Управление информационными рисками. Экономически опраданная безопасность. М.: Компания Ай Ти; ДМК Пресс, 2004. – 308 с. **8.** Степанов Е. А. Управление персоналом: персонал в системе защиты информации. – М.: ФОРУМ: ИНФА-М, 2002. – 288 с. **9.** Архипов О. Є., Ворожко В. П. Системний підхід до оцінювання ефективності захисту держаної таємниці: // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 10. – К., 2005. – С. 18-22. **10.** Фатьянов А. А. Проблемы защиты конфиденциальной информации, не составляющей государственную тайну / Информационное общество. - №1. – 1997. – С. 49-56. **11.** Методичні рекомендації державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня її секретності. Затверджено наказом Держкомсекретів України від 09.11.1998 №22. **12.** Рекомендації з організації діяльності експертних комісій при державних експертах з питань таємниць. Затверджено наказом Держкомсекретів України від 09.11.1998 №22. **13.** Захист інформаційних ресурсів України: проблеми і шляхи їх розв'язання / Мастяниця Й. У., Соснін О. В., Шиманський Л. Є. Під редакцією О. В. Сосніна. Національний інститут стратегічних досліджень. – К., 2000. – 100 с. **14.** Архипов О. Є., Касперський І. П. Проблеми методичного забезпечення віднесення відомомстей до інформації з обмеженим доступом в Україні / Правова інформатика. - № 3(11). – 2005. – С. 61-66. **15.** Архипов О. Є., Касперський І. П. Проблеми методики отримання та обробки оціночних суджень членів експертних комісій, створених державними експертами з питань таємниць / Правова інформатика. - № 4(12). – 2006. – с. 80-87.*

УДК 65.012.8

ТЕОРЕТИКО-МЕТОДИЧНІ ЗАСАДИ ОЦІНЮВАННЯ ШКОДИ, ОБУМОВЛЕНОЇ РОЗГОЛОШЕННЯМ СЕКРЕТНОЇ ІНФОРМАЦІЇ

Олександр Архипов
Національний технічний університет України «КПІ»

Анотація: **Розглянуто можливість застосування основних положень сучасної теорії вимірювання для обґрунтування теоретико-методичних засад оцінювання шкоди, обумовленої розголошенням секретної інформації.**
Summery: **It is considered possibility of application of measuring modern theory substantive provisions for the substantiation of methodic and theoretical principles of evaluation of harm, caused by the disclosure of secret information**
Ключові слова: **Секретна інформація, шкала вимірювання, захист інформації, охорона державної таємниці.**

І Вступ

Одним з базових положень організації захисту інформації є визначення можливої шкоди, що може бути заподіяна за умови порушення безпеки інформації [1], бо саме реалістична оцінка цієї шкоди дозволяє забезпечити при побудові системи захисту інформації (СЗІ) дотримання принципу адекватності рівня захисту рівню сукупної важливості інформації з обмеженим доступом і, відповідно, оптимізувати витрати на створення системи СЗІ. Особливої ваги принцип адекватності набуває при формуванні системи охорони державної таємниці (ДТ), що в черговий раз обумовлює актуальність проблеми коректного виокремлення секретної інформації та її внутрішньої класифікації за ступенем секретності. Згідно з вимогами закону [2] ця класифікація здійснюється за критерієм можливої шкоди, якої може бути завдано національній безпеці України у разі розголошення секретної інформації.

Оцінка рівня можливої шкоди формується на основі рішень державних експертів з питань таємниць. Ці рішення відносяться із використанням методу експертних оцінок відповідно до Методичних рекомендацій державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня їх секретності, які було затверджено Державним комітетом України з питань державних секретів та технічного захисту інформації [3] (далі – Методичні рекомендації).

За десять років, що минули з часу затвердження Методичних рекомендації, виникло ряд критичних зауважень та побажань до їх змісту [4 – 6]. Одне з них – можливість науково-теоретичного обґрунтування положень Методичних рекомендацій, розглядається в даній статті.