НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

О. Г. Корченко, О. Є. Архипов, Ю. О. Дрейс

ОЦІНЮВАННЯ ШКОДИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ У РАЗІ ВИТОКУ ДЕРЖАВНОЇ ТАЄМНИЦІ

Монографія

Київ – 2014

УДК 004.891:65.012.8
ББК 66.4(0)
О-93

Рекомендовано до друку Вченою радою Національної академії СБ України
(*протокол №14 від 26.06.2014 року*)

Р е ц е н з е н т и:

А.І. Марущак – лауреат Державної премії України в галузі науки і техніки, доктор юридичних наук, професор, перший заступник директора інституту Національної академії СБ України;
Ю.І. Грицюк – доктор технічних наук, професор, завідувач кафедри управління інформаційною безпекою Інституту цивільного захисту Львівського державного університету безпеки життєдіяльності;
О.А. Смірнов – доктор технічних наук, професор, професор кафедри програмного забезпечення Кіровоградського національного технічного університету.

О-93 Оцінювання шкоди національній безпеці України у разі витоку державної таємниці : Монографія / О.Г. Корченко, О.Є. Архипов, Ю.О. Дрейс. – К.: наук.-вид. центр НА СБ України, 2014. – 332 с.: іл.
ISBN 978-617-7092-26-0

Охорона державної таємниці є окремим сегментом національної безпеки України, визначеним чинною політикою інформаційної безпеки, де одним із основних її положень є виділення окремої категорії відомостей, що складають державну таємницю. Дана процедура пов'язана з аналізом і оцінкою важливості секретної інформації саме у контексті загроз національній безпеці України та можливої шкоди від їх реалізації. Існуюча процедура визначення цієї шкоди базується на емпіричних підходах, яким властивий високий рівень суб'єктивізму та низька точність отриманих результатів. Тому актуальною є задача розроблення науково обґрунтованої методології оцінювання шкоди, заподіяної витоком секретної інформації, зокрема моделей, методів, критеріїв і систем, що застосовуються для цього і врахувати існуючі в цій сфері напрацювання, що базуються на осмисленні багаторічного позитивного досвіду у сфері охорони державної таємниці.

Розглянуті нормативно-правові та соціально-організаційні аспекти охорони державної таємниці, проведено критичний аналіз чинних методичних настанов, рекомендацій та процедур оцінювання можливої шкоди у разі розголошення державної таємниці або втрати її матеріальних носіїв, запропоновано оригінальні експертно-аналітичні підходи до визначення цінності секретної інформації та обсягів втрат у разі її витоку.

Видання призначене для фахівців сфери забезпечення охорони державної таємниці, студентам, аспірантам, здобувачам, науковцям, викладачам, які надають послуги за освітніми напрямами, пов'язаними з забезпеченням національної та інформаційної безпеки.

УДК 004.891:65.012.8
ББК 66.4(0)

ISBN 978-617-7092-26-0

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ……. 6
ВСТУП…….. 8

Розділ 1. ОХОРОНА ДЕРЖАВНОЇ ТАЄМНИЦІ В УКРАЇНІ…… 10
1.1. Базова термінологія у сфері охорони державної таємниці…... 10
1.2. Система охорони державної таємниці …… 12
Хронологія становлення державної таємниці…….. 12
Організація системи охорони державної таємниці……... 19
Державний експерт з питань таємниць, експертні комісії……... 23
Режимно-секретні органи, особливості їх діяльності…… 29
1.3. Віднесення інформації до державної таємниці……... 35
Порядок віднесення інформації до державної таємниці……... 35
Методичні рекомендації державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня їх секретності …….... 40
Загальна характеристика та проблемні аспекти процедури віднесення інформації до державної таємниці……. 45
1.4. Засекречування та розсекречування носіїв інформації…… 53
Вимоги до засекречування та розсекречування матеріальних носіїв інформації…… 53
Методичні рекомендації щодо порядку організації та проведення експертиз на предмет наявності чи відсутності у матеріальних носіях інформації відомостей, що становлять державну таємницю……... 55

Розділ 2. СПОСОБИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ В ІНОЗЕМНИХ КРАЇНАХ …… 60
2.1. Визначення шкоди внаслідок розголошення державної таємниці в Російській Федерації…….. 60
Система органів захисту державної таємниці …… 60
Переліковий підхід до організації захисту державної таємниці…. 70
Критерії віднесення відомостей до державної таємниці ……... 73
Визначення величини шкоди від поширення інформації і збитку, що наноситься у результаті їх засекречування…….. 83
Ліцензування діяльності у галузі захисту державної таємниці…. 99
Організація захисту інформації, що становить державну таємницю, на підприємствах, в організаціях та установах…… 103
Загальна характеристика та проблемні аспекти…….. 106
2.2. Порядок засекречування класифікованої інформації в США… 108
2.3. Організація охорони державної таємниці країн-членів НАТО (Естонії, Румунії, Чехії, Словаччини, Болгарії)…….. 116

Розділ 3. ТЕОРЕТИЧНІ ПОЛОЖЕННЯ ВИЗНАЧЕННЯ ЦІННОСТІ ІНФОРМАЦІЇ…… 128
3.1. Методичні основи та способи визначення цінності інформації…….. 128
Поняття цінності інформації…… 128
Моделі цінності інформації…….. 130
Інформація: цінність чи важливість? …… 138
3.2. Практичні аспекти визначення цінності інформації…… 140
3.3. Застосування ноніусного методу для визначення цінності інформації……. 147
Ноніусний підхід до визначення цінності інформації …….. 148
Онтологічна ієрархія …… 150
Методика побудови онтологічної ієрархії визначення цінності інформації……... 151
3.4. Застосування системи комбінованих шкал для оцінки інформаційних втрат…….. 156
Узагальнена задача вимірювання й типологія комбінованих шкал для визначення цінності (значущості) інформації…… 156
Експертно-аналітична процедура оцінювання значущості інформаційних ресурсів в загальному випадку…….. 160
3.5. Проблеми методики обробки оціночних суджень членів групової експертизи……167
Експертне оцінювання, загальні відомості……..167
Отримання та обробка оціночних суджень членів експертних комісій при державних експертах з питань таємниць…… 170
Способи формування групових експертних оцінок……173
Оцінювання якості роботи експертів за даними багатооб'єктної експертизи…….. 179

Розділ 4. ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ СИСТЕМИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ В УКРАЇНІ ……188
4.1. Загрози інформації, обумовлені використанням засобів обчислювальної техніки для обробки секретної інформації…. 190
4.2. Системні аспекти захисту інформації……196
4.3. Дослідження і оцінка стану охорони державної таємниці…… 203
Визначення критерію стану охорони державної таємниці…… 203
Показники кількісної оцінки захищеності державної таємниці… 204
Методика кількісної оцінки стану охорони державної таємниці… 206
4.4. Практичні аспекти реалізації оцінювання впливу стану охорони державної таємниці на національну безпеку…….. 214
4.5. Приклад використання методики розрахунку ефективності системи охорони державної таємниці……220

Розділ 5. МОДЕЛІ ТА МЕТОДИ ОЦІНЮВАННЯ ШКОДИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ У РАЗІ ВИТОКУ ДЕРЖАВНОЇ ТАЄМНИЦІ…….. 227
5.1. Моделі оцінювання шкоди національній безпеці України у разі витоку державної таємниці……... 227
Класифікація інформації з обмеженим доступом……. 227
Модель складної орієнтованої інформаційної мережі Зводу відомостей, що становлять державну таємницю…… 231
Модель складної орієнтованої інформаційної мережі Переліку відомостей, що становлять службову інформацію…….. 235
Модель оцінювання шкоди національній безпеці як складова експертизи матеріальних носіїв інформації…….. 239
Базова модель інтегрованого представлення параметрів шкоди національній безпеці у сфері охорони державної таємниці…..... 243
5.2. Методи оцінювання шкоди національній безпеці України у разі витоку державної таємниці…… 244
Метод аналізу і оцінки величини можливої шкоди національній безпеці у сфері охорони державної таємниці…… 244
Метод оцінювання важливості відомостей за визначеними сферами державної таємниці ……. 256
Метод нечіткої класифікації відомостей, що становлять державну таємницю за встановленими критеріями…… 260
Сценарний метод оцінювання шкоди, заподіяної витоком секретної інформації…… 266
Метод визначення рівня компетентності членів експертної комісії при державних експертах з питань таємниць…… 277

Розділ 6. СИСТЕМА ОЦІНЮВАННЯ ШКОДИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ У РАЗІ ВИТОКУ ДЕРЖАВНОЇ ТАЄМНИЦІ…….. 284
6.1. Методологія синтезу системи оцінювання шкоди національній безпеці у разі витоку державної таємниці…… 284
Структурна схема системи оцінювання шкоди національній безпеці у разі витоку державної таємниці …… 288
Базовий алгоритм роботи системи…… 290
6.2. Програмна реалізація та експериментальне дослідження системи оцінювання шкоди національній безпеці України у разі витоку державної таємниці…….. 292

ВИСНОВОК…… 302
СПИСОК ЛІТЕРАТУРИ…… 304
ДОДАТКИ…… 320

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АС	автоматизована система
АСО	апріорний словник об’єктів
АСПО	апріорний словник показників об’єктів
БД	база даних
БІАС	біологічна інформаційно-аналітична система
БЛВ	блок логічного виводу
БОЕ	багатооб’єктна експертиза
ВВСЧО	відносна вартість складової частини об’єкта
ВІР	внутрішній інтелектуальний ресурс
ВРУ	Верховна Рада України
ГС	гриф секретності
ДЕТ	державний експерт з питань таємниць
ДСК	для службового користування
ДТ	державна таємниця
ДТЗС	допоміжні технічні засоби і системи
ДТК РФ	державна технічна комісія РФ
ЕК	експертна комісія
ЕСВ	емпірична система з відношенням
ЕШ	економічна шкода
ЗВДТ	звід відомостей, що становлять державну таємницю
ЗІР	зовнішній інформаційний ресурс
ЗОТ	засоби обчислювальної техніки
ІАС	інформаційно-аналітична система
ІзОД	інформація з обмеженим доступом
ІППШ	інтегроване представлення параметрів шкоди
ІР	інформаційні ресурси
ІТС	інформаційно-телекомунікаційна система
КЗІ	криптографічний захист інформації
КМУ	Кабінет Міністрів України
МАІ	метод аналізу ієрархії
МВК РФ	міжвідомча комісія із захисту державної таємниці РФ
МГЗ	модуль генерації звіту
МНІ	матеріальні носії інформації
МНСІ	матеріальні носії секретної інформації
МО РФ	Міністерство оборони РФ
МПВ	модуль процесу вибірки
НКДТ	нечіткий класифікатор відомостей, що становлять ДТ
НСД	несанкціонований доступ
ОВ	особливої важливості
ОДТ	охорона державної таємниці

ОІД	об’єкт інформаційної діяльності
ПЕМВН	побічне електромагнітне випромінювання і наводки
ПЗ	програмне забезпечення
РНБОУ	Рада національної безпеки і оборони України
РПВДТ	розгорнутий перелік відомостей, що становлять ДТ
РС	режим секретності
РСО	режимно-секретні органи
РФ	Російська Федерація
СБУ	Служба безпеки України
СВІ	система відновлення інформації
СД	секретне діловодство
СЗІ	система захисту інформації
СЗР РФ	Служба зовнішньої розвідки РФ
СІ	секретна інформація
СОД	ступінь обмеження доступу
СОДТ	система охорони державної таємниці
СОІМ	складна орієнтована інформаційна мережа
СРСД	суб’єкт режимно-секретної діяльності
СС	ступінь секретності
СТЗІ	система технічного захисту інформації
СЧО	складова частина об’єкта
Т	таємно
ТЗІ	технічний захист інформації
ТП	технологічні процеси
ФСБ РФ	Федеральна служба безпеки РФ
ЦТ	цілком таємно
ЧСВ	числова система з відношенням

ВСТУП

На сучасному етапі міжнародної активної співпраці в інформаційній сфері однією із основних реальних та потенційних загроз національній безпеці України є розголошення інформації, яка становить державну таємницю, чи втрата матеріальних носіїв секретної інформації, спрямованої на забезпечення державних потреб та національних інтересів. Тому в умовах підвищення рівня розвідувальної діяльності іноземних спецслужб досить гостро постає питання удосконалення напрямів забезпечення інформаційної безпеки як однієї з найважливіших функцій держави, зокрема, щодо забезпечення охорони державної таємниці, що є комплексом організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв.

Згідно до вимог Закону України «Про державну таємницю» охороні державою підлягають відомості таємної інформації, які визнані державною таємницею (або секретною інформацією) у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці. Відомості становлять державну таємницю з часу опублікування Зводу відомостей, що становлять державну таємницю, до якого вони включені за процедурою прийняття державним експертом з питань таємниць рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з встановленням ступеня їх секретності шляхом обґрунтування та визначення можливої шкоди національній безпеці держави у разі розголошення відомостей, що становлять державну таємницю, чи втрати матеріальних носіїв секретної інформації.

Слід зазначити, що здійснення заходів щодо віднесення відомостей до секретної інформації, засекречування, розсекречування та охорони матеріальних носіїв секретної інформації, криптографічний та технічний захист та інші витрати, пов’язані з державною таємницею, в державних підприємствах, установах, організаціях фінансуються за рахунок Державного бюджету України. Тому наявне зростання витрат на заходи охорони державної таємниці та збитків, що пов’язані з наслідками розголошення державної таємниці чи втратою матеріальних носіїв секретної інформації та їх ліквідацією, підвищують вимоги до прогнозування й інформаційно-аналітичної підтримки процесів прийняття рішень щодо забезпечення інформаційної безпеки України при отриманні, зберіганні, використанні і розповсюдженні суспільно значущої інформації, особливо секретної інформації, стосовно:

удосконалення методичних рекомендацій державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до ДТ та ступеня їх секретності; експертизи матеріальних носіїв інформації на предмет наявності відомостей, що становлять державну таємницю, та присвоєння їм грифу секретності; встановлення строків засекречування та розсекречування матеріальних носіїв секретної інформації; визначення параметрів оцінювання економічної шкоди та інших тяжких наслідків як величини можливої сукупної шкоди національній безпеці України в інформаційній сфері; організації формування Зводу відомостей, що становлять державну таємницю та розгорнутих переліків відомостей, що становлять ДТ (РПВДТ); порядку забезпечення режиму секретності суб'єкта режимно-секретної діяльності; оцінювання ефективності системи охорони державної таємниці у цілому, обумовлюють необхідність розробки моделей та методів оцінювання шкоди національній безпеці у сфері охорони державної таємниці.

Однак у зазначеній сфері залишається низка завдань, вирішення яких має важливе наукове та практичне значення. З цих позицій розробка моделей та методів оцінювання шкоди національній безпеці у разі розголошення відомостей, що становлять державну таємницю, чи втрати матеріальних носіїв секретної інформації для оцінювання ефективності функціонування системи охорони державної таємниці та результативного розв'язання відповідних задач на основі як статистичних даних, так і експертних оцінок, *є актуальним науковим завданням.*

Розділ 1. ОХОРОНА ДЕРЖАВНОЇ ТАЄМНИЦІ В УКРАЇНІ

1.1. Базова термінологія у сфері охорони державної таємниці

На сьогодні однією із основних реальних і потенційних загроз національній безпеці України у інформаційній сфері є розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави [1]. Тому, завжди залишаються актуальними питання щодо удосконалення існуючих систем захисту інформації, зокрема, і у сфері охорони державної таємниці, із законодавчим врегулюванням її нормативно-правових обмежень в інтересах держави для однієї з найважливіших її функцій – забезпечення інформаційної безпеки [2, 3]. Адже у цій сфері суспільні відносини, пов'язані з віднесенням відомостей до державної таємниці, засекречуванням, розсекречуванням та охороною матеріальних носіїв секретної інформації з метою захисту національної безпеки України регулюються законодавством, що визначає наступні базові поняття та визначення [3]:

державна таємниця (ДТ) (далі також – *секретна інформація* (СІ)) – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у встановленому порядку ДТ і підлягають охороні державою;

віднесення інформації до ДТ – процедура прийняття (державним експертом з питань таємниць) рішення про віднесення категорії відомостей або окремих відомостей до ДТ з установленням ступеня їх секретності шляхом обґрунтування та визначення можливої шкоди національній безпеці України у разі розголошення цих відомостей, включенням цієї інформації до Зводу відомостей, що становлять ДТ, та з опублікуванням цього Зводу, змін до нього;

гриф секретності (ГС) – реквізит матеріального носія СІ, що засвідчує ступінь секретності даної інформації;

державний експерт із питань таємниць (ДЕТ) – посадова особа, уповноважена здійснювати відповідно до вимог віднесення інформації до ДТ у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, зміни ступеня секретності цієї інформації та її розсекречування;

допуск до ДТ – оформлення права громадянина на доступ до СІ;

доступ до ДТ – надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною СІ та проведення

діяльності, пов'язаної з ДТ, або ознайомлення з конкретною СІ та провадження діяльності, пов'язаної з ДТ, цією посадовою особою відповідно до її службових повноважень;

засекречування матеріальних носіїв інформації (МНІ) – введення у встановленому законодавством порядку обмежень на поширення та доступ до конкретної СІ шляхом надання відповідного ГС документам, виробам або іншим матеріальних носіїв цієї інформації;

звід відомостей, що становлять державну таємницю (ЗВДТ), – акт, в якому зведено переліки відомостей, що згідно з рішеннями державних експертів із питань таємниць становлять ДТ у визначених сферах;

категорія режиму секретності – категорія, яка характеризує важливість та обсяги відомостей, що становлять ДТ, які зосереджені в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях;

криптографічний захист СІ – вид захисту, що реалізується шляхом перетворення інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

матеріальні носії секретної інформації (МНСІ) – матеріальні об'єкти, в тому числі фізичні поля, в яких відомості, що становлять ДТ, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо;

охорона державної таємниці (ОДТ) – комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню СІ та втратам її матеріальних носіїв;

режим секретності (РС) – встановлений згідно вимогами закону та інших нормативно-правових актів єдиний порядок забезпечення ОДТ;

розсекречування МНСІ – зняття в установленому законодавством порядку обмежень на поширення та доступ до конкретної СІ шляхом скасування раніше наданого ГС документам, виробам або іншим матеріальним носіям цієї інформації;

спеціальна експертиза щодо наявності умов для провадження діяльності, пов'язаної з ДТ, – експертиза, що проводиться з метою визначення в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях наявності умов, для провадження діяльності, пов'язаної з ДТ;

ступінь секретності (СС) (особливої важливості (ОВ), цілком таємно (ЦТ), таємно (Т)) – категорія, яка характеризує важливість СІ, ступінь обмеження доступу до неї та рівень її охорони державою.

технічний захист СІ – вид захисту, спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності та унеможливлення блокування інформації.

1.2. Система охорони державної таємниці

Хронологія становлення державної таємниці

Національна система ОДТ (СОДТ) створювалась з урахуванням досвіду розвинених демократичних країн та випробуваних на практиці традиційних засобів і методів. Значною мірою сучасна Україна є спадкоємцем системи захисту СІ, яка існувала за часів Радянського Союзу (СРСР). Напрацювання того часу було покладено в основу функціонування системного захисту державних секретів (таємниць).

Історію становлення СОДТ умовно можна поділити на *радянський період* (1921-1990 рр.) і *період незалежної України* (1991 р. – по нині).

Радянський період має три етапи (періоди) [4-7]:

Перший (1921-1927 рр.) – період становлення радянської системи захисту державних секретів, створення культу таємності та встановлення державного РС:

1921 р. – створено Державне політичне управління у складі НКВС;

1922 р. – створено Секретно-оперативного управління, сформовано Фельд'єгерський корпус при Державному політичному управлінні; прийнято постанову ЦК РКП(б) «Про порядок збереження і руху секретних документів» (організація та ведення секретного діловодства) і перший Кримінальний кодекс РСФРР;

1923 р. – створено Об'єднане державне політичне управління при Раді Народних Комісарів СРСР та спеціальне міжвідомче бюро по дезінформації (Дезінформбюро);

1924 р. – створено спецвідділ у складі Державного політичного управління УСРР (об'єднував шифрувальну справу в усіх народних комісаріатах і центральних установ республіки);

1926 р. – спецвідділом Об'єднаного державного політичного управління видано «Інструкцію з ведення секретного і шифрувального діловодства», «Інструкцію про порядок стенографування на секретних нарадах і засіданнях», «Інструкцію про порядок ведення і зберігання секретного листування» тощо, а також прийнято постанову РНК СРСР «Про затвердження Переліку відомостей, що є за своїм змістом ДТ, яка спеціально охороняється» (перший відкритий загальносоюзний перелік відомостей, що становив ДТ, який містив відомості ЦТ, Т і ті, що не підлягають розголошенню);

1927 р. – Об'єднаним державним політичним управлінням введено в дію систему заходів із засекречування роботи підприємств військової промисловості, посилюється кримінальна відповідальність посадових осіб за невжиття заходів із забезпечення збереження державних секретів.

Другий (1928-1953 рр.) – період військово-мобілізаційної моделі розвитку економіки та тоталітарного політичного режиму, де набуває важливого значення захист СІ економічного та оборонного характеру.

1928 р. – Спецвідділом Об'єднаного державного політичного управління введено «Інструкцію з секретного діловодства» (закладено основні принципи РС);

1929 р. – прийнята «Інструкція місцевим органам Об'єднаного державного політичного управління щодо спостереження за станом секретного і мобілізаційного діловодства установ і організацій»;

1934 р. – ліквідовано Об'єднане державне політичне управління і створено Головне управління державної безпеки у складі НКВС СРСР, де захист СІ входив до обов'язки Особливого (до якого входив контрозвідувальний відділ), Економічного, Транспортного та Спеціального (з 1938 р. 9-й спецвідділ) відділів;

1936 р. – ліквідовано Економічний відділ, а Особливий поділено на: Особливий та, з частиною розформованого Економічного відділу, на Контрозвідувальний відділи;

1938 р. – ліквідовано Головне управління державної безпеки, реорганізовано НКВС на три управління: перше – Управління державної безпеки, друге – Управління особливих відділів, третє – Управління транспорту і зв'язку. Діяльністю, пов'язаною із захистом СІ займалися друге і третє управління, а також окремі відділи першого управління (контрозвідувальний; оперативної роботи в органах міліції, пожежної охорони і військкоматах; оперативної роботи на підприємствах оборонної промисловості; та ін.) та Спеціальний (шифрувальний) відділ НКВС СРСР;

1938 р. – (наркомом став Л.П. Берія) відновлено Головне управління державної безпеки і складалося з семи відділів з яких протидією шпигунства та захистом СІ займалися третій (контрозвідувальний), четвертий (особливий), сьомий (шифрувальний, оперативна робота з ОДТ) відділи;

1940 р. – введено контроль поштово-телеграфної кореспонденції, яким займався другий спеціальний відділ НКВС СРСР;

1941 р. – функції збереження ДТ в установах і на підприємствах, а також ведення шифрувальної і дешифрувальної роботи покладено на 5-й відділ НКДБ (Народний комісаріат державної безпеки);

1943 р. – завершено утворення НКДБ, реформовано окремі управління та відділи, створено Головне управління контррозвідки «Смерш» СРСР;

1946 р. – створено Друге головне (контррозвідувальне) управління, перейменування НКДБ в Міністерство державної безпеки (МДБ) СРСР;

1947 р. – затверджено «Перелік відомостей, що становлять ДТ, розголошення яких карається законом», що замінив перелік 1926 р., але й сам проіснував менше року; видано Указ «Про відповідальність за розголошення ДТ та втрату документів, що містять ДТ», який значно посилював покарання за розголошення ДТ та диференціював санкції залежно від суб'єкта злочину (посадова особа, військовослужбовець, приватна особа);

1948 р. – затверджено «Перелік найголовніших відомостей, що становлять ДТ» та «Інструкцію із забезпечення збереження ДТ в установах і на підприємствах СРСР», що встановлювала три СС (ЦТ ОВ, ЦТ, Т). Перелік містив такі розділи: мобілізаційні питання та відомості про резерви, відомості військового та економічного (промисловість, корисні копалини, транспорт і зв'язок тощо) характеру, фінанси, зовнішня політика і зовнішня торгівля, питання науки і техніки (атомна енергія, радіолокаційна техніка, реактивна техніка, відкриття і винаходи, відомості з картографії, геології, гідрології), відомості про Арктику, різні відомості;

1949 р. – прийнято постанову «Про порядок пересування по території СРСР дипломатичних і консульських представників в СРСР іноземних держав і службовців іноземних посольств і місій» (посилення агентурного спостереження і оперативного стеження за ними, перевірка зв'язків іноземців серед радянських громадян, що працювали на особливо важливих об'єктах, маскування цих об'єктів і т.п.);

1953 р. – реорганізація органів, що проводять діяльність з охорони ДТ, а саме МДБ об'єднали з МВС та окремо виділено Головне управлінням Уповноваженого Ради Міністрів СРСР по охороні військових і державних таємниць у пресі (Головліт).

Третій (1954-1991 рр.) – період становлення та діяльності радянських спецслужб у їх монументальному вигляді, закладення основ для СОДТ незалежної України.

1954 р. – утворено Комітет державної безпеки (КДБ) при Раді Міністрів СРСР, до складу якого увійшли головні управління та окремі відділи колишнього МДБ;

1958 р. – прийнято ряд постанов щодо посилення РС, а саме: «Про заходи по збереженню ДТ», «Про заходи з посилення секретності робіт зі спеціального озброєння і оборонної тематики» та ін.;

1959 р. – відповідно до наказу голови КДБ «Про зміни в структурі КДБ при РМ УРСР та його місцевих органах» 5-е управління в центрі і відповідні відділи-відділення-групи об'єднали в самостійний контррозвідувальний підрозділ;

В середині 60-х років стає очевидним, що багато відомостей секретного характеру про об'єкти оборонної галузі промисловості іноземні розвідки отримують у результаті радіоперехоплення і використання інших технічних засобів збирання інформації. З цього часу почала активно складатися система протидії технічним розвідкам.

1963 р. – прийнято постанову «Про посилення РС робіт, що проводяться»;

1964 р. – «Про заходи щодо подальшої зашифровки діючих, та тих, що будуються, об'єктів оборонних галузей промисловості»;

1965 р. – «Інструкція по забезпеченню збереження ДТ і РС робіт, що проводяться» (№ 00150-65);

1968 р. – створені штатні аналітичні підрозділи із захисту ДТ, які дістали назву «спеціальні науково-технічні (науково-дослідні) підрозділи» у Міністерстві середнього машинобудування СРСР;

1970 р. – «Про заходи щодо посилення РС», де діяльність із забезпечення ДТ вперше стала одним з найголовніших завдань КДБ;

1972 р. – прийнято «Інструкцію щодо забезпечення збереження ДТ і РС робіт, що проводяться в установах і на підприємствах СРСР» (№ 00166-72) та постанову «Про протидію іноземним технічним розвідкам», яка створила комплексну протидію технічним розвідкам противника на чолі з загальнодержавним органом – Державною технічною комісією СРСР з протидії іноземним технічним розвідкам, створеною на базі існуючих підрозділів МО і КДБ СРСР;

1974 р. – затверджено «Положення про Держтехкомісію», яка 1975 р. затвердила «Положення з комплексної протидії іноземним технічним розвідкам при розробці, виробництві і випробуваннях озброєння і військової техніки на підприємствах»;

1978 р. – затверджено «Інструкцію по забезпеченню РС в міністерствах, відомствах, на підприємствах, в установах і організаціях СРСР» (№ 0126-87), яка діяла частково в Україні і після розпаду СРСР до жовтня 2003 р.

1990 р. – Головліт перейменовано у Головне управління з охорони ДТ (ГУОТ) у пресі й інших засобах масової інформації, а згодом у 1991 р. скасовано з передачею своїх функцій до Міністерства інформації і преси СРСР;

Період незалежної України має два етапи [4-8]:

Перший (1991-1999 рр.) – період становлення нормативно-правового забезпечення у сфері ОДТ, визначення органів забезпечення захисту ДТ:

1991 р. – розпад СРСР, Верховна Рада УРСР проголосила незалежність України і прийняла ряд постанов на підпорядкування Верховній Раді України (ВРУ), спрямованих на зміцнення суверенітету України, зокрема, на підпорядкування ВРУ Збройних Сил, Внутрішніх військ, органів і військ КДБ, інших військових формувань;

1991 р. – постановою ВРУ «Про Службу національної безпеки» ліквідовувався КДБ України з передачею повноважень на Службу національної безпеки (СНБ) України;

1992 р. – СНБ перетворено на Службу безпеки України (СБУ); Указом Президента створено Державну службу України з питань технічного захисту інформації (ДСТЗІ); створено Головне управління по охороні державних таємниць у пресі та інших засобах масової інформації (ГУОТ) при Кабінеті Міністрів України (КМУ), а також Державний комітет по охороні державних таємниць у пресі та інших засобах масової інформації (Держкомтаємниць) на базі ГУОТ; введено в дію Закони «Про Службу безпеки України», «Про інформацію», «Про оперативно-розшукову діяльність», внесено зміни до окремих кодексів;

1993 р. – постановою КМУ створено Державний комітет України з питань державних секретів (Держкомсекретів); прийнято Закон «Про організаційно-правові основи боротьби з організованою злочинністю»;

1994 р. - постановою ВРУ введено в дію Закон «Про державну таємницю», «Про захист інформації в автоматизованих системах»; затверджено «Положення про державного експерта з питань таємниць», «Положення про порядок і механізм формування та опублікування Зводу відомостей, що становлять ДТ» (ЗВДТ), «Види, розміри і порядок надання компенсацій громадянам у зв'язку з роботою, яка передбачає доступ до ДТ», «Положення про порядок і умови надання органам державної виконавчої влади, підприємствам, установам і організаціям дозволу (ліцензії) на здійснення діяльності, пов'язаною з ДТ, та про особливий режим цієї діяльності», «Положення про технічний захист інформації в Україні»;

1995 р. - між Урядом України та НАТО в м. Брюсселі підписано перший міжнародний правовий акт з питань взаємної охорони державних секретів – «Угода про безпеку», яка передбачала охорону інформації обмеженого доступу, якою сторони будуть обмінюватися в процесі виконання програми «Партнерство заради миру»; затверджено «Положення про режимно-секретні органи в міністерствах, відомствах, Уряді Автономної республіки Крим, місцевих органах державної виконавчої влади, на підприємствах, в установах і організаціях», що замінило вимоги розділу 2 Інструкції № 0126-87 і реалізовувало вимоги закону «Про державну таємницю» щодо РС робіт, пов'язаних з ДТ; визначено НТУУ «КПІ» як базовий вищий навчальний заклад з

підготовки, перепідготовки, підвищення кваліфікації спеціалістів РСО та системи технічного захисту інформації (ТЗІ) в Україні; затверджено «ЗВДТ» наказом Держкомсекретів № 47 від 30.07.1995 р.; прийнято Закон «Про боротьбу з корупцією»;

1996 р. – прийнято Конституцію України; затверджено «Інструкцію про порядок ОДТ, а також іншої інформації з обмеженим доступом (ІзОД), що є власністю держави, під час прийому іноземних делегацій, груп та окремих іноземців і проведення роботи з ними»; Указом Президента України ліквідовано Держкомсекретів та ДСТЗІ України і створено Державний комітет України з питань державних секретів та технічного захисту інформації; затверджено «Положення про порядок надання, скасування та переоформлення допуску громадян України до ДТ», який замінив розділ 3 Інструкції № 0126-87 і визначив єдиний порядок оформлення та надання допуску до ДТ; затверджено Перелік напрямів та спеціальностей, за якими здійснювалася підготовка фахівців у вищих навчальних закладах, до якого включено напрям «Комп'ютеризовані системи, автоматизація управління», що передбачав підготовку спеціалістів за спеціальністю «Захист інформації з обмеженим доступом та автоматизація її обробки», відкрито нову галузь підготовки фахівців з вищою освітою «Національна безпека» та новий напрям підготовки «Інформаційна безпека»;

1997 р. – Указами Президента України затверджені «Положення про порядок оформлення дозволів за розпорядженням Президента України на передачу іншій державі інформації, що становить ДТ, та матеріальних носіїв такої інформації», «Положення про порядок оформлення дозволів за розпорядженням Президента України на передачу іншій державі інформацію, що становить ДТ, та носіїв такої інформації»; постановою ВРУ схвалена «Концепція (основи державної політики) національної безпеки України»; постановою КМУ затверджена «Концепція технічного захисту інформації в Україні»;

1998 р. – Державним комітетом України з питань державних секретів та технічного захисту інформації затверджені «Методичні рекомендації ДЕТ щодо визначення підстав для віднесення відомостей до ДТ та ступеня їх секретності» та «Рекомендації з організації діяльності експертних комісій при ДЕТ»; постановою КМУ затверджено «Положення про забезпечення РС під час обробки інформації, що становить ДТ, в автоматизованих системах»; Указом Президента України визначені першочергові заходи з проведення нового етапу адміністративної реформи; прийнято закон «Про Раду національної безпеки і оборони»; видано «Інструкцію про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв

інформації, які містять конфіденційну інформацію, що є власністю держави»;

1999 р. – Указом Президента України ліквідовано Державний комітет України з питань державних секретів та технічного захисту інформації, а його функції щодо розробки та забезпечення реалізації політики у сфері ОДТ та ТЗІ передано СБУ на новостворене Управління охорони державної таємниці (УОДТ) та Департамент спеціальних телекомунікаційних систем та захисту інформації (ДСТСЗІ); внесені відповідні зміни до Закону України «Про державну таємницю».

Другий (2000 р. - по нині) – період удосконалення нормативно-правового забезпечення у сфері ОДТ, конкретизації діяльності та окремих функцій підрозділів СБУ [4-8]:

2000 р. – наказами СБУ затверджено «Положення про контроль за функціонуванням системи ТЗІ», «Положення про державну експертизу у сфері криптографічного захисту інформації (КЗІ)»;

2001 р. – наказами СБУ затверджено «ЗВДТ» № 52; «Положення про державну експертизу у сфері КЗІ», «Про затвердження зобов'язання громадянина України у зв'язку з допуском до ДТ та анкети для оформлення допуску до ДТ», прийнято Кримінальний кодекс України;

2002 р. – наказами СБУ затверджено «Положення про дозвільний порядок проведення робіт з ТЗІ для власних потреб», «Перелік психічних захворювань (розладів), які можуть завдати шкоди ОДТ і за наявності яких допуск до ДТ громадянинові не надається», «Положення про порядок розроблення, прийняття, перегляду та скасування міжвідомчих нормативних документів системи ТЗІ», «Інструкцію про організацію та здійснення органами СБУ діяльності щодо надання, переоформлення, зупинення дії або скасування спеціального дозволу на провадження діяльності, пов’язаної з ДТ» та ін.;

2003 р. – прийнято Закони України «Про боротьбу з тероризмом», «Про контррозвідувальну діяльність»; наказом СБУ затверджено «Порядок організації та забезпечення РС в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях» № 1561, який повністю замінив Інструкцію № 0126-87;

2004 р. – видано Указ Президента «Про деякі питання передачі ДТ іноземній державі чи міжнародній організації» та ряд наказів СБУ з грифом «Для службового користування» (ДСК);

2005 р. – внесено зміни до Закону «Про захист інформації в автоматизованих системах» і прийнято у його редакції «Про захист інформації в інформаційно-телекомунікаційних системах»; наказами СБУ затверджено «ЗВДТ» № 440, «Положення про експертні комісії з питань ДТ», «Про забезпечення ОДТ та Інструкції щодо заповнення форми звіту про стан забезпечення ОДТ та порядку його подання»;

2006 р. – прийнято Закони України «Про загальну структуру і чисельність СБУ», «Про Державну службу спеціального зв'язку та захисту інформації України», видано Указ Президента «Про Положення про порядок підготовки документів щодо надання доступу до ДТ іноземцям та особам без громадянства», наказом СБУ затверджено «Інструкцію про порядок оформлення матеріалів про адміністративні правопорушення у сфері ОДТ та конфіденційної інформації, що є власністю держави», «Інструкцію про порядок здійснення СБУ контролю за обігом документів, які містять конфіденційну інформацію, що є власністю держави»;

2007-2013 рр. – прийнято Закони України «Про доступ до публічної інформації», «Про захист персональних даних», видано Указ Президента «Про Перелік посадових осіб, на яких покладається виконання функцій державного експерта з питань таємниць», затверджено «Положення про державну експертизу в сфері ТЗІ», «Положення про державну експертизу в сфері КЗІ», «Порядок державного обліку секретних науково-дослідних, дослідно-конструкторських робіт і дисертацій», видано накази СБУ «Про затвердження форм звіту про стан забезпечення ОДТ та інструкцій щодо порядку їх заповнення та подання», «Щодо порядку організації та проведення експертиз на предмет наявності чи відсутності у матеріальних носіях інформації відомостей, що становлять ДТ» та ряд наказів з грифом ДСК, змінено «Інструкцію про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію» тощо.

Організація системи охорони державної таємниці

Аналіз історії захисту та ОДТ [4-7] показує, що на початку 90-х років для незалежної України, як і для інших держав, що утворилися в пострадянському просторі, практичні питання захисту регламентувалися закритими для загального користування підзаконними нормативними актами, тобто фактично мало місце відчуження питання ОДТ від суспільства, внаслідок чого не розглядалися та не обговорювалися публічно принципи діяльності, її елементи, організаційну структуру та витрати на функціонування, критично не аналізувався механізм і методи, їх ефективність і дієвість.

Сьогодні формування державно-правової сфери ОДТ базується на основних засадах Конституції України [2] і реалізується за допомогою законів ВРУ [1-3; 9-16], Указів Президента України [17-23], рішень Ради національної безпеки і оборони України, постанов КМУ [24-28], наказів

СБУ [29-33] та інших нормативно-правових документів [34-42], якими регулюється цей вид суспільних відносин. На основі Закону України «Про державну таємницю» [3] розроблено і введено в дію ряд загальнодержавних, відомчих нормативно-правових актів, що дозволило в цілому створити *систему* для забезпечення стану сфери ОДТ та її функціонування, як одну з складових забезпечення національної безпеки з метою недопущення нанесення шкоди у разі розголошення відомостей, що становлять ДТ.

Система охорони державної таємниці (СОДТ) – комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню СІ та втратам її матеріальних носіїв [43].

СОДТ – організована державою сукупність суб'єктів, що провадять діяльність, пов'язану з ДТ, повноваженнями яких, згідно чинного законодавства України, є розробка і реалізація організаційно-правових, інженерно-технічних, криптографічних, оперативно-розшукових та інших заходів, спрямованих на запобігання розголошенню відомостей, що становлять ДТ та втратам МНСІ і використання цієї інформації на шкоду безпеці держави [44-48].

До організаційно-правових заходів ОДТ відносяться [3, 43]:

- єдині вимоги до виготовлення, користування, збереження, передачі, транспортування та обліку МНСІ;
- дозвільний порядок провадження державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями діяльності, пов'язаної з ДТ;
- обмеження оприлюднення, передачі іншій державі або поширення іншим шляхом СІ;
- обмеження щодо перебування та діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, їх доступу до ДТ, а також розташування і переміщення об'єктів і технічних засобів, що їм належать;
- особливості здійснення державними органами їх функцій щодо державних органів, органів місцевого самоврядування, підприємств, установ і організацій, діяльність яких пов'язана з ДТ;
- РС державних органів, органів місцевого самоврядування, підприємств, установ і організацій, що провадять діяльність, пов'язану з ДТ;
- спеціальний порядок допуску та доступу громадян до ДТ;
- технічний та криптографічний захисти СІ.

СОДТ складає [44-48] сукупність структурних елементів *трьох рівнів*, які знаходяться у взаємозв'язках один з одним, мають усі разом представництво спеціально уповноваженого органу у сфері забезпечення

ОДТ – СБУ, і поділяються на *чотири підсистеми*: управління (керуючу), виконання, інформаційну, забезпечення.

До підсистеми *управління* (керуючої) відносяться два рівні:

1) вищі державної органи (визначення політики ОДТ та напрямків її реалізації, координація дій):

- Президент України є Верховним Головнокомандувачем Збройних Сил України (ЗСУ); призначає на посади та звільняє з посад вище командування ЗСУ, інших військових формувань; здійснює керівництво у сферах національної безпеки та оборони держави; забезпечує державну незалежність, національну безпеку і правонаступництво держави; очолює Раду національної безпеки і оборони України [2].
- Рада національної безпеки і оборони України (РНБОУ) є координаційним органом з питань національної безпеки і оборони при Президентові України (координує і контролює діяльність органів виконавчої влади у сфері національної безпеки і оборони);
- ВРУ (визначає державну політику щодо ДТ як складову засад внутрішньої та зовнішньої політики);

2) центральні державної органи (здійснюють державну політику в сфері ОДТ в межах своїх повноважень):

- КМУ (спрямовує та координує роботу міністерств, інших органів виконавчої влади щодо забезпечення здійснення державної політики у сфері ОДТ);
- Конституційний суд України (вирішує питання відповідності законів та інших правових актів до [2] у сфері ОДТ);
- суди загальної юрисдикції (здійснюють правосуддя у сфері ОДТ);
- Прокуратура України (здійснює представництво державних інтересів щодо ОДТ у судах);
- ЗСУ, СБУ, Служба зовнішньої розвідки України (СЗРУ), Державна прикордонна служба України (ДПСУ), Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІУ) та інші військові формування, утворені відповідно до законів України;

3) місцевий рівень – підсистема *виконання* (виконання державної політики у сфері ОДТ):

- державні органи, органи місцевого самоврядування, підприємства, установи і організації, що провадять діяльність, пов'язану з ДТ;
- режимно-секретний орган (РСО) (розроблення та здійснення заходів щодо забезпечення РС, постійного контролю за їх додержанням).

До підсистеми *забезпечення* належать державні установи, що здійснюють доставку та транспортування МНСІ: ДССЗЗІУ та Державна фельд'єгерська служба України.

Під *інформаційною* підсистемою слід розуміти сукупність структурних елементів СОДТ, які отримують та надають відомості, щодо зовнішнього та внутрішнього середовища, стану елементів, ресурсів та результатів функціонування системи. До таких елементів належать СБУ та СРСД (разом з РСО) у якості постачальника самої інформації про стан ОДТ.

Головне завдання або призначення СОДТ – *запобігання розголошенню ДТ чи втратам її МНСІ.*

Призначення СОДТ реалізується за допомогою вирішення низки завдань, до яких можна віднести [42-50]:

- розробка державної політики ОДТ та механізмів її реалізації;
- розробка законодавчої та нормативної бази у сфері ОДТ;
- виявлення, оцінка та прогнозування джерел загроз у сфері ОДТ;
- розробка спеціальних методів і алгоритмів, а також організаційно-правових, інженерно-технічних, криптографічних, оперативно-розшукових та інших заходів по забезпеченню ОДТ;
- координація діяльності державних органів, органів місцевого самоврядування, підприємств, установ і організацій по забезпеченню ОДТ;
- стандартизація, сертифікація і державне ліцензування діяльності пов'язане із забезпеченням ОДТ.

Відповідно до норм закону [3] та інших виданих до нього нормативно-правових актів, встановлено єдиний порядок забезпечення ОДТ – РС, який включає у себе наступні порядки [3, 19, 20]:

- віднесення інформації до ДТ; дозвільний порядок провадження діяльності, пов'язаної з ДТ, та РС; порядок засекречування та розсекречування МНСІ; порядок надання, переоформлення та скасування громадянам допуску до ДТ [3];
- передачі ДТ іноземній державі чи міжнародній організації [19];
- підготовки документів щодо надання доступу до ДТ іноземцям та особам без громадянства [20];
- технічного та криптографічного захисту СІ [22; 23];
- надання компенсації громадянам у зв'язку з роботою, яка передбачає доступ до ДТ [24];
- проведення експертизи цінності документів [25];
- організації та проведення експертиз на предмет наявності чи відсутності у МНІ відомостей, що становлять ДТ [32];
- проведення державної експертизи в сфері ТЗІ [34];
- організації та проведення державної експертизи у сфері КЗІ [35];
- державного обліку секретних науково-дослідних робіт, дослідно-конструкторських робіт і дисертацій [37];
- інші порядки.

Державний експерт з питань таємниць, експертні комісії

Державний експерт з питань таємниць (ДЕТ) здійснює відповідно до вимог Закону України «Про державну таємницю»[3] віднесення інформації у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку до ДТ, зміни СС цієї інформації та її розсекречування.

Державний експерт у своїй діяльності керується Конституцією і законами України, постановами ВРУ, указами і розпорядженнями Президента України, постановами КМУ, наказами СБУ, іншими нормативно-правовими документами у сфері забезпечення ОДТ.

Державними експертами є особи, які займають у відповідних галузях державної діяльності посади, перелічені Указом [21] Президента України. Виконання функцій ДЕТ на конкретних посадових осіб покладається [3]: у ВРУ – Головою ВРУ; в інших державних органах, Національній академії наук України, на підприємствах, в установах і організаціях – Президентом України за поданням СБУ на підставі пропозицій керівників відповідних державних органів, Національної академії наук України, підприємств, установ і організацій.

Втручання в діяльність ДЕТ особи, якій за посадою його підпорядковано, не допускається.

Державний експерт відносить інформацію до ДТ з питань, прийняття рішень з яких належить до його компетенції згідно з посадою. У разі, коли прийняття рішення про віднесення інформації до ДТ належить до компетенції кількох експертів, його ухвалюють простою більшістю голосів. При цьому кожен експерт має право викласти свою думку [17].

ДЕТ відповідно до покладених на нього *завдань* [3]:

1) визначає: підстави, за якими інформацію має бути віднесено до ДТ; підстави та доцільність віднесення до ДТ інформації про винаходи (корисні моделі), призначені для використання у сферах, зазначених у частині першій статті 8 Закону [3]; доцільність віднесення до ДТ інформації про винаходи (корисні моделі), що мають подвійне застосування, на підставі порівняльного аналізу ефективності цільового використання та за згодою автора (власника патенту); СС інформації, віднесеної до ДТ; державний орган (органи), якому надається право приймати рішення щодо кола суб'єктів, які матимуть доступ до СІ;

2) готує висновок щодо завданої національній безпеці України шкоди у разі розголошення СІ чи втрати МНСІ;

3) установлює та продовжує строк дії рішення про віднесення інформації до ДТ із зазначенням дати її розсекречення;

4) дає СБУ рішення про зміну СС інформації та скасування рішення про віднесення її до ДТ у разі, якщо підстави, на яких цю інформацію було віднесено до ДТ, перестали існувати;

5) затверджує за погодженням із СБУ розгорнуті переліки відомостей, що становлять ДТ, зміни до них, контролює відповідність змісту цих переліків ЗВДТ;

6) розглядає пропозиції державних органів, органів місцевого самоврядування, підприємств, установ, організацій, об'єднань громадян та окремих громадян щодо віднесення інформації до ДТ та її розсекречування;

7) затверджує висновки щодо обізнаності з ДТ громадян, які мають чи мали допуск до ДТ;

8) контролює обґрунтованість і правильність надання документам, виробам та іншим МНІ, які містять відомості, включені до ЗВДТ, відповідного ГС, своєчасність зміни такого грифа та розсекречування цих носіїв із наданням їм реквізиту «розсекречено»;

9) бере участь у розробленні критеріїв визначення шкоди, яку може бути завдано національній безпеці України у разі розголошення СІ чи втрати матеріальних носіїв такої інформації.

ДЕТ під час виконання покладених на нього *функцій* зобов'язаний [3]:

1) погоджувати за посередництвом СБУ свої висновки про скасування рішень щодо віднесення інформації до міждержавних таємниць з відповідними посадовими особами держав - учасниць міжнародних договорів України про взаємне забезпечення збереження міждержавних таємниць та повідомляти їх про прийняті рішення щодо віднесення інформації до ДТ, на яку поширено чинність цих договорів;

2) подавати СБУ не пізніш як через десять днів з моменту підписання рішення про віднесення відомостей до ДТ або про скасування цих рішень, а розгорнуті переліки відомостей, що становлять ДТ (РПВДТ), - у той же строк з моменту їх затвердження;

3) розглядати протягом одного місяця пропозиції СБУ про віднесення інформації до ДТ, скасування чи продовження терміну дії раніше прийнятого рішення про віднесення інформації до ДТ;

4) надавати відповідний ГС рішенням про віднесення інформації до ДТ та про скасування цих рішень залежно від важливості їх змісту;

5) брати участь у засіданнях ДЕТ;

6) ініціювати питання щодо притягнення до відповідальності посадових осіб, які порушують законодавство України про ДТ.

ДЕТ має *право* [3]:

1) безперешкодно проводити перевірку виконання державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями, що перебувають у сфері його діяльності,

рішень про віднесення інформації до ДТ, скасування цих рішень, додержання порядку засекречення інформації та у разі виявлення порушень давати обов'язкові для виконання приписи про їх усунення;

2) створювати експертні комісії з фахівців і науковців, які мають допуск до ДТ, для підготовки проектів рішень про віднесення інформації до ДТ, зниження її СС та скасування зазначених рішень, висновків щодо обізнаності з ДТ громадян, які мають чи мали допуск до ДТ, а також для підготовки відповідних висновків у разі розголошення СІ чи втрати матеріальних носіїв такої інформації;

3) скасовувати безпідставні рішення про надання носію інформації ГС, зміну або скасування цього грифа;

4) клопотати про притягнення до відповідальності посадових осіб, які порушують законодавство України у сфері ОДТ;

5) одержувати в установленому порядку від державних органів, органів місцевого самоврядування, підприємств, установ та організацій відомості, необхідні для виконання своїх функцій.

ДЕТ, а також фахівцям, які залучаються до підготовки рішень та висновків ДЕТ, встановлюються додаткові виплати у порядку і розмірах, що визначаються у [24] постановою КМУ. ДЕТ несе персональну відповідальність за законність і обґрунтованість свого рішення про віднесення інформації до ДТ або про зниження СС такої інформації чи скасування рішення про віднесення її до ДТ, а також за умисне неприйняття рішення про віднесення до ДТ інформації, розголошення якої може завдати шкоди інтересам національної безпеки України [3].

Рішення державного експерта про віднесення інформації до ДТ підлягає реєстрації СБУ у ЗВДТ. Висновок державного експерта про скасування рішення про віднесення інформації до ДТ є підставою для вилучення інформації із ЗВДТ. Цей висновок набирає чинності з моменту внесення змін до ЗВДТ. Винесення рішення і дачу висновків державний експерт здійснює за формами (див. *Додаток 1, 2*) [17].

ДЕТ у разі потреби видає разом з іншими державними експертами спільні рішення про віднесення інформації до ДТ та спільні висновки про скасування цих рішень. Рішення (висновок) державного експерта (експертів), видане в межах його (їх) повноважень і зареєстроване у ЗВДТ, є обов'язковим для виконання на території України. Рішення державного експерта про віднесення інформації до ДТ та його висновок про скасування цього рішення може бути змінено або скасовано Президентом України [17].

Відповідно до постанови [24] КМУ ДЕТ встановлено надбавку в розмірі 20 % посадового окладу, а також фахівцям, які входять до складу експертних комісій та залучаються до підготовки рішень та висновків ДЕТ, надбавку за фактично виконану роботу в розмірі до 20 %

посадового окладу. Конкретний розмір надбавки визначається керівником відповідного державного органу, органу місцевого самоврядування, підприємства, установи, організації в межах фонду оплати праці залежно від обсягу, складності та тривалості роботи над [24]:

1) пропозиціями щодо:

прийняття рішень про віднесення інформації до ДТ, продовження строку дії чи скасування таких рішень, зміну СС інформації;

встановлення СС науково-дослідної, дослідно-конструкторської або проектної роботи, яка проводиться в інтересах забезпечення національної безпеки та оборони держави, її складових частин і етапів;

наявності чи відсутності у МНІ, які є предметом експертизи, відомостей, що становлять ДТ;

2) проектами рішень про віднесення інформації до ДТ, продовження строку дії чи скасування таких рішень, зміну СС інформації;

3) проектами висновків про СС науково-дослідної, дослідно-конструкторської або проектної роботи, яка проводиться в інтересах забезпечення національної безпеки та оборони держави, її складових частин і етапів;

4) проектами експертних висновків про наявність чи відсутність відомостей, що становлять ДТ.

Експертні комісії (ЕК) створюються за рішенням ДЕТ, керівників підприємств, установ, організацій, що провадять діяльність, пов'язану з ДТ, з метою [30, 39]:

- сприяння виконанню ДЕТ, керівниками підприємств, установ, організацій покладених на них завдань у сфері ОДТ;
- забезпечення вимог законодавства під час провадження підприємством, установою, організацією діяльності, пов'язаної з ДТ;

запобігання розголошенню відомостей, що становлять ДТ.

Основним завданням ЕК, які створюються ДЕТ, є розгляд матеріалів та підготовка пропозицій про [30, 39]:

1) віднесення інформації до ДТ, продовження терміну дії рішення про віднесення інформації до ДТ та скасування рішення про віднесення інформації до ДТ;

2) визначення та зміну СС інформації, віднесеної до ДТ.

Основними завданнями ЕК, які створюються на підприємствах, в установах і організаціях, є [30, 39]:

1) підготовка пропозицій про віднесення інформації до ДТ, визначення СС науково-дослідних, дослідно-конструкторських, проектних робіт та їх складових частин, а також відомостей, які містяться в документах та інших МНІ, підготовка проектів рішень про зміну чи скасування ГС, наданих МНСІ;

2) проведення експертної оцінки документів, інших МНІ, які плануються для передачі іноземним делегаціям, групам чи окремим іноземцям під час здійснення міжнародного співробітництва та тих, що передбачається використовувати працівниками підприємства, установи, організації у закордонних відрядженнях (текстові чи технічні документи, відео-, аудіо-, аудіовізуальні матеріали тощо), а також матеріалів, які готуються для публікації у друкованих виданнях, передачі на телебаченні та радіо, оголошенні на міжнародних, зарубіжних і відкритих загальнодержавних з'їздах, конференціях, нарадах, симпозіумах, публічного захисту дисертацій, демонстрації в кінофільмах, відеофільмах, діафільмах, діапозитивах та слайд-фільмах, експонування в музеях, на виставках, ярмарках, депонування рукописів тощо (відкрите опублікування);

3) визначення фактичної обізнаності громадян у відомостях, що становлять ДТ, яким було надано допуск та доступ до ДТ в порядку, установленому законодавством, та які порушили клопотання про виїзд на постійне проживання в іноземну державу;

4) проведення експертизи цінності документів та інших МНСІ з метою їх відбору для передачі до секретних архівних підрозділів на зберігання або для знищення;

5) надання пропозицій щодо підготовки номенклатури секретних справ, а також інші завдання, визначені законодавством.

До складу ЕК включаються найбільш кваліфіковані фахівці підприємств, установ, організацій, яким надано допуск до ДТ відповідної форми, а також фахівці РСО. У разі потреби, для проведення експертизи можуть залучатися фахівці інших підприємств, установ, організацій за наявності письмової згоди їх керівників.

Загальна чисельність членів ЕК повинна становити не менше ніж три особи. Персональний склад ЕК затверджується ДЕТ, керівником підприємства, установи, організації.

Голова ЕК організовує роботу комісії та забезпечує для цього необхідні умови.

Секретар ЕК за вказівками голови забезпечує скликання засідань комісії, складає протоколи, акти, описи, готує проекти рішень, актів та висновків.

Основною формою роботи ЕК є засідання, необхідність проведення якого та перелік питань для розгляду визначає голова комісії. Він завчасно призначає доповідача з членів комісії для розгляду окремого питання та забезпечує можливість висловити свою думку всім присутнім на засіданні членам комісії. Засідання ЕК є правомочним, якщо на ньому присутні не менш як дві третини її членів. Рішення комісії приймається простою більшістю голосів. У разі розподілу

голосів ухвальним є голос голови ЕК. За результатами розгляду на засіданні поданих на експертизу документів, інших МНІ ЕК приймається рішення, яке оформляється протоколом за відповідною формою (див. *Додаток 3*).

У протоколі фіксуються питання для обговорення та їх результати, запитання, зауваження та пропозиції членів ЕК. Кожен член комісії має право внести до протоколу свою особисту думку щодо питання, яке розглядалося на засіданні. Протокол підписується головою та присутніми на засіданні членами ЕК.

ЕК має *право* [30]:

одержувати в установленому порядку від структурних підрозділів підприємства, установи, організації, інших підприємств, установ, організацій та громадян інформацію, необхідну для виконання покладених на неї завдань;

надавати ДЕТ, керівнику підприємства, установи, організації пропозиції щодо вдосконалення СОДТ.

Якщо експертиза документів, інших МНІ проводилася у зв'язку з підготовкою їх для відкритого опублікування або із запланованою передачею матеріалів іноземним делегаціям, групам чи окремим іноземцям, використанням МНІ працівниками підприємства, установи, організації у закордонному відрядженні, крім протоколу, також складається акт експертизи за відповідною формою (див. *Додаток 4*).

В акті експертизи викладається перелік документів, інших МНІ, які подані для експертизи, та висновок про наявність чи відсутність у них СІ.

У разі наявності такої інформації в акті експертизи зазначаються, які саме відомості становлять ДТ, з посиланням на статті ЗВДТ, пункти РПВДТ, та, у разі необхідності, їх стислий зміст, а також робляться посилання на сторінки, пункти, абзаци, речення тощо, у яких вони містяться.

При відсутності в документах, інших МНІ, яка становить ДТ, відповідно до встановленого порядку проводиться подальша оцінка цих носіїв інформації щодо наявності в них службової інформації та згідно з вимогами законодавства готуються пропозиції щодо їх використання.

Гриф обмеження доступу протоколу та акта експертизи встановлюється відповідно до вимог законодавства.

ДЕТ та керівники підприємств, установ, організацій повинні здійснювати контроль за дотриманням членами ЕК вимог чинного законодавства про ДТ.

Методичне забезпечення роботи експертних комісій здійснює СБУ.

Режимно-секретні органи, особливості їх діяльності

В державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, що провадять діяльність, пов'язану з ДТ (або суб'єкти режимно-секретної діяльності (СРСД)), з метою розроблення та здійснення заходів щодо забезпечення РС, постійного контролю за їх додержанням створюються на правах окремих структурних підрозділів *режимно-секретні органи* (РСО), які підпорядковуються безпосередньо керівнику державного органу, органу місцевого самоврядування, підприємства, установи, організації.

Створення, реорганізація чи ліквідація РСО здійснюються за погодженням із СБУ. У своїй роботі РСО взаємодіють з органами СБУ.

До складу РСО входять підрозділи режиму, секретного діловодства та інші підрозділи, що безпосередньо забезпечують ОДТ, залежно від специфіки діяльності державного органу, органу місцевого самоврядування, підприємства, установи та організації [3]:

- із значним обсягом робіт, пов'язаних з ДТ, вводиться посада заступника керівника з питань режиму, на якого покладаються обов'язки та права керівника РСО;

- з незначним обсягом робіт, пов'язаних з ДТ, де штатним розписом не передбачено створення РСО, облік і зберігання секретних документів, а також заходи щодо забезпечення РС здійснюються особисто їх керівниками або спеціально призначеним наказом керівника працівником після створення необхідних умов, що забезпечують РС. На них поширюються обов'язки та права працівників РСО.

Призначення осіб на посади заступників керівників з питань режиму, начальників РСО та їх заступників, а також видання наказу про покладення на окремого працівника обов'язків щодо забезпечення РС здійснюється за погодженням з органами СБУ та РСО вищестоящих державних органів, органів місцевого самоврядування, підприємств, установ і організацій. РСО комплектуються спеціалістами, яким надано допуск до ДТ із СС «ЦТ», якщо характер виконуваних робіт не вимагає допуску до ДТ із СС «ОВ». Якщо державний орган, орган місцевого самоврядування, підприємство, установа або організація не провадить діяльність із СІ, що має СС «ЦТ» та «ОВ», РСО такого органу, підприємства, установи або організації комплектується спеціалістами, яким надано допуск до ДТ зі СС «Т».

Основними *завданнями* РСО є [3]:

а) недопущення необґрунтованого допуску та доступу осіб до СІ;

б) своєчасне розроблення та реалізація разом з іншими структурними підрозділами державних органів, органів місцевого

самоврядування, підприємств, установ і організацій заходів, що забезпечують ОДТ;

в) запобігання розголошенню СІ, випадкам втрат матеріальних носіїв цієї інформації, заволодінню СІ іноземними державами, іноземними юридичними особами, іноземцями, особами без громадянства та громадянами України, яким не надано допуску та доступу до неї;

г) виявлення та закриття каналів просочення СІ в процесі діяльності державних органів, органів місцевого самоврядування, підприємства, установи, організації;

д) забезпечення запровадження заходів РС під час виконання всіх видів робіт, пов'язаних з ДТ, та під час здійснення зовнішніх відносин;

е) організація та ведення секретного діловодства;

є) здійснення контролю за станом РС в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях та на підпорядкованих їм об'єктах.

РСО мають *право* [3]:

а) вимагати від усіх працівників державного органу, органу місцевого самоврядування, підприємства, установи та організації, а також відряджених неухильного виконання вимог законодавства щодо забезпечення ОДТ;

б) брати участь у розгляді проектів штатних розписів державного органу, органу місцевого самоврядування, підприємства, установи та організації та підвідомчих їм установ, підприємств у частині, що стосується РСО, вносити пропозиції щодо структури та чисельності працівників цих органів;

в) брати участь у проведенні атестації працівників, що виконують роботи, пов'язані з ДТ, а також у розгляді пропозицій щодо виплати в установленому нормативними актами порядку компенсації за роботу в умовах режимних обмежень;

г) залучати спеціалістів державного органу, органу місцевого самоврядування, підприємства, установи та організації до здійснення заходів щодо ОДТ;

д) здійснювати перевірки стану й організації роботи з питань захисту ДТ і забезпечення РС у підрозділах державного органу, органу місцевого самоврядування, підприємства, установи та організації, а також у підвідомчих їм установах та підприємствах, давати відповідні рекомендації;

е) здійснювати перевірки додержання РС на робочих місцях працівників, що мають допуск до ДТ, вмісту спецсховищ (приміщень, сейфів, металевих шаф, спецчемоданів, спецпапок тощо), наявності документів, виробів та інших МНСІ;

є) порушувати перед керівником державного органу, органу місцевого самоврядування, підприємства, установи та організації питання про призначення службових розслідувань за фактами порушень РС та секретного діловодства, про притягнення осіб до відповідальності згідно з законом, а також давати рекомендації щодо обов'язкових для виконання вказівок керівникам підрозділів державного органу, органу місцевого самоврядування, підприємства, установи та організації та підвідомчих їм установ, підприємств з питань забезпечення РС;

ж) брати участь у службових розслідуваннях, у встановленому порядку вимагати від працівників державного органу, органу місцевого самоврядування, підприємства, установи та організації письмових пояснень щодо фактів розголошення ними секретних відомостей, втрати МНСІ, інших порушень РС;

з) вносити пропозиції керівникові державного органу, органу місцевого самоврядування, підприємства, установи та організації про припинення робіт, пов'язаних з ДТ, в структурних підрозділах, якщо умови для їх виконання не відповідають вимогам РС; опечатувати приміщення, де ведуться такі роботи або зберігаються МНСІ;

и) одержувати від громадян, яким оформляються документи на допуск до ДТ, анкетні дані;

і) використовувати засоби зв'язку та вести в установленому порядку поштово-телеграфне листування з іншими державними органами, органами місцевого самоврядування, підприємствами, установами і організаціями та їх РСО з питань забезпечення РС;

ї) мати печатку з найменуванням РСО, а також інші печатки та штампи установленої форми.

Передача функцій РСО будь-яким іншим підрозділам державного органу, органу місцевого самоврядування, підприємства, установи та організації не допускається.

Чисельність РСО повинна бути достатньою для якісного виконання покладених на них завдань за умови оптимальних витрат коштів на їх утримання. Умовно всі завдання РСО можливо розділити на завдання з забезпечення: секретного діловодства; РС; технічного захисту інформації. Для визначення чисельності працівників РСО необхідно провести розрахунок загальної річної трудомісткості робіт РСО. Тобто визначити обсяг часу, необхідного для виконання всіх завдань РСО, який потім ділиться на фонд робочого часу одного працівника за рік. Таким чином отримується число, на основі якого приймається рішення про чисельність працівників РСО. Для розрахунку загальної річної трудомісткості робіт РСО необхідно [51]:

- провести класифікацію витрат робочого часу працівників РСО,
- визначено роботи РСО, що займають найбільше часу;

- визначено розрахункові залежності витрат часу співробітників РСО за основними напрямками роботи.

Для нормування роботи РСО щодо виконання інженерно-технічних заходів можливо використати той самий підхід, який був застосований і для підрозділів секретного діловодства та РС. Роботи з ТЗІ можуть проводити або організації, що мають ліцензії на право провадження господарської діяльності у галузі ТЗІ, або підрозділи органів державної влади, органи місцевого самоврядування, які мають дозвіл на проведення робіт з ТЗІ для власних потреб. Для запровадження заходів з ТЗІ у складі РСО може створюватися підрозділ ТЗІ, який формулює загальні вимоги до ТЗІ, розроблює політику безпеки, створює модель загроз, розроблює технічне завдання на створення комплексу засобів захисту або комплексної системи захисту інформації. Підрозділ ТЗІ супроводжує розробку проектів систем ТЗІ, проведення будівельно-монтажних, пусконалагоджувальних робіт, проведення випробувань, дослідної експлуатації. Також на цей підрозділ РСО покладається розробка інструкцій щодо порядку застосування засобів ТЗІ, навчання користувачів та підготовка документації для проведення державної експертизи. З урахуванням наведених особливостей необхідно провести дослідження діяльності підрозділів ТЗІ, результатом якого має бути встановлення нормованих видів робіт з ТЗІ. Наявність цих даних дозволить більш точно планувати роботи РСО з урахуванням завдань ТЗІ. При цьому необхідно пам’ятати, основними носіями інформації у будь-якій сфері діяльності залишаються люди, тому питання забезпечення захисту СІ залишається нагальним і потребує постійного контролю та належного його вирішення з РСО та відповідних органів ОДТ СБУ.

У зв’язку з цим та з метою формування концептуальних основ щодо визначення порядку здійснення аналітичної роботи РСО щодо організації захисту СІ від можливих загроз її витоку, у [52] пропонується окреслити загальні підходи *визначення понятійно-категорійного апарату аналітичної роботи РСО*, його елементів, критеріїв, принципів і завдань, наприклад, щодо визначення понять [52]:

аналітична робота РСО – процес, в результаті якого факти стосовно загроз витоку СІ перетворюються в логічно закінчену продукцію режимної діяльності, яка призначена для керівництва установи та органів, що здійснюють або виробляють відповідні позиції забезпечення державної безпеки;

інформаційно-аналітична діяльність РСО – особливий вид аналітичної діяльності, основним змістом якої є дослідження загроз витоку СІ та її складових елементів. При цьому поняття інформаційно-аналітичної роботи охоплює всі види діяльності, яка здійснюється представниками, що отримали завдання скласти інформаційний документ

з будь-якого питання стосовно виявлення та закриття каналів витоку СІ про стан виробничої, науково-дослідної, дослідно-конструкторської та іншої діяльності державного органу, підприємства, установи, організації;

інформація як продукт діяльності РСО (оперативна інформація) – осмислені відомості, які ґрунтуються на зібраних, оцінених і розтлумачених фактів, викладених таким чином, що ясно відображають їх значення для вирішення будь-якого конкретного завдання поточної ситуації;

зміст аналітичної інформації – представляє собою відомості відносно можливостей, вразливих позицій та вірогідного каналу витоку СІ стосовно можливих загроз як внутрішнього, так і зовнішнього характеру. Така інформація в першу чергу призначена для відповідних органів СБУ та РНБОУ та інших органів відповідальних за вироблення загальної політики безпеки нашої держави. Вона необхідна головним чином для того, щоб допомогти відповідальним керівникам розробити та здійснити режимно-секретні заходи по забезпеченню національної безпеки та створення надійних правових механізмів протидії можливого витоку СІ;

вразливість режимних позицій – наявність у державного органу, підприємства, організації, установи в її СОДТ слабких місць, які роблять її чутливою до різних дій (впливів) як внутрішнього, так і зовнішнього характеру здатних ослабити її режимний потенціал і підірвати СОДТ;

інформаційно-аналітична оцінка – документ, в якому або аналізується існуюче у даний момент становище, або робиться прогноз про розвиток подій в майбутньому. Будь-які прогнози, що містяться в інформаційному документі, є оцінкою. В оцінках часто, але не завжди мова йде про можливі майбутні події;

потенційні можливості СОДТ – прогнозовані можливості системи режимних заходів, які можуть адекватно забезпечити протидію можливого витоку СІ;

корисність – інформаційно-аналітичний документ переслідує одну ціль: він має бути корисним для забезпечення державних інтересів. Корисність аналітичної інформації РСО визначається багатьма якостями як: *повнота* та *точність* інформації. Водночас іноді повнота та точність можуть бути частково принесені в жертву заради її *своєчасності*. А також – *достовірність*, оскільки недооцінка або переоцінка різних фактів або вільне їх тлумачення при висвітленні реального становища можуть призвести до помилкових дій та рішень і нанести шкоду всій СОДТ.

Принципи роботи РСО [52]*:*

1) *З'ясування змісту фактів (подій)*. Цей принцип вимагає чіткого розкриття дійсного значення та суті отриманих фактів. Як правило цього можна досягти шляхом порівняння аналогічних даних в процесі здійснення режимних заходів у діяльності РСО. З'ясовуючи дійсне

значення та зміст фактів, тим самим збільшується рівень його корисності, оскільки факти рідко говорять самі за себе.

2) *Встановлення причин і наслідків.* Цей принцип вимагає від співробітника РСО визначити причинно-наслідкові зв'язки між різними явищами при вирішення будь-якого інформаційного завдання. Виявлення дійсних причин та наслідків відповідних подій і обставин є дієвим засобом, що сприяє з'ясуванню рушійних сил таких подій та убезпечить нас від помилкових суджень. Такий підхід дослідження питання допомагає знайти головний фактор. Вказуючи причини тих або інших явищ РСО тим самим полегшують використання поданої до відповідного підрозділу СБУ інформації.

3) *Врахування характеру та особливостей діяльності організації* (*установи*)**.** Цей принцип вимагає, щоб особливий характер діяльності підприємства, установи, організації або державного органу розглядався у якості фактора першочергової важливості при оцінці відповідних інформаційних потоків стосовно конкретних фактів, подій, обставин. Принцип вимагає також врахування існуючих адміністративно-правових механізмів протидії можливим загрозам витоку СІ, впровадження організаційно-правових елементів взаємодії усіх суб'єктів задіяних в процесі забезпечення режимних заходів та їх злагодженої роботи. Зазначене відповідно збільшує або зменшує уявні можливості режимної системи протидіяти загрозам витоку СІ на конкретному об'єкті з урахуванням особливостей діяльності підприємства, організації, установи, державного органу.

4) *Визначення тенденцій розвитку СОДТ***.** Цей принцип базується на врахуванні розвитку та форм людських взаємовідносин, оскільки людський фактор є найбільш вразливим у цій системі. Він вимагає оцінки можливого напрямку розвитку подій в майбутньому. Необхідно встановити, чи розвивається досліджуване явище по висхідній або низхідній лінії і з якою швидкістю. Чи є тенденція розвитку подій стійкою, циклічною або незмінною. Врахування тенденцій тісно пов'язане з передбачуваністю, яка є доволі важливим елементом інформаційної роботи.

5) *Ступінь достовірності.* У відповідності з цим принципом необхідно враховувати достовірність отриманих даних, точність цифрового матеріалу і ступінь правильності оцінок і висновків. Вказані три моменти подібні між собою, але не тотожні. Всі вони є елементами поняття «ступінь достовірності». У кожному конкретному випадку ступінь достовірності отриманих даних, точності цифрового матеріалу і правильності оцінок та висновків може бути різним – високий, малий або середній. Такі розбіжності мають важливе значення. Тому представник РСО шляхом ретельного аналізу повинен точно встановити

ступінь достовірності, точності і правильності кожного важливого факту або висновку підготовленого ним інформаційного документу, а потім зробити його абсолютно ясним набувачу. При такому підході значно підвищується корисність будь-якого інформаційного документу.

6) *Обґрунтованість висновків.* Висновки необхідні для того, щоб інформаційний документ набув завершеного вигляду міг бути максимально корисним. «Висновки» є природнім наслідком досягнення поставленої «цілі». Щоб зробити висновки, необхідно відповісти на питання: «Що означає досліджуване явище щодо можливих загроз витоку СІ»? Як правило, в багатьох документах читаються і запам'ятовуються лише висновки. Тому, необхідно звертати увагу на те, щоб у висновках найважливіші моменти викладались коротко і чітко, однак при цьому не допускаючи помилкового уявлення про предмет дослідження. Складання висновків вимагає від співробітника РСО високої фахової майстерності.

Отже, організаційно-правове регулювання ОДТ в частині, що стосується аналітичної роботи РСО з виявлення та закриття каналів можливого витоку СІ в будь-якій сфері діяльності здійснюється на підставі формально визначених норм, які містяться у відповідних нормативно-правових актах України. Водночас, окремі напрями такої діяльності здійснюється на підставі суб'єктивних уявлень відповідних РСО на свій розсуд, хоча виконання та реалізація таких заходів здебільшого стримується через відсутність належного механізму правового регулювання такої діяльності, а за низкою напрямів взагалі становить пряму загрозу витоку ІзОД. Крім того, відсутність належного механізму правового регулювання аналітичної роботи РСО з виявлення та закриття каналів можливого витоку СІ не сприяє створенню належних умов захищеності СОДТ та призводить до розпорошеності і не ефективного застосування законодавства України щодо захисту ІзОД, а також підвищує можливості діяльності спеціальних служб інших держав з отримання розвідувальної інформації, при цьому певною мірою, знижуючи можливості протидії спеціальних служб України.

1.3. Віднесення інформації до державної таємниці

Порядок віднесення інформації до державної таємниці

До ДТ у порядку, встановленому статтею 8 Законом України «Про державну таємницю», *відноситься* інформація [3]:

1) *у сфері оборони*:

про зміст стратегічних і оперативних планів та інших документів бойового управління, підготовку та проведення військових операцій, стратегічне та мобілізаційне розгортання військ, а також про інші найважливіші показники, які характеризують організацію, чисельність, дислокацію, бойову і мобілізаційну готовність, бойову та іншу військову підготовку, озброєння та матеріально-технічне забезпечення Збройних Сил України та інших військових формувань;

про напрями розвитку окремих видів озброєння, військової і спеціальної техніки, їх кількість, тактико-технічні характеристики, організацію і технологію виробництва, наукові, науково-дослідні та дослідно-конструкторські роботи, пов'язані з розробленням нових зразків озброєння, військової і спеціальної техніки або їх модернізацією, а також про інші роботи, що плануються або здійснюються в інтересах оборони країни;

про дислокацію, характеристики пунктів управління, зміст заходів загальнодержавного та регіонального, у разі необхідності міського і районного рівня, щодо приведення у готовність єдиної державної системи цивільного захисту населення і територій до виконання завдань в особливий період та про організацію системи зв’язку (оповіщення) в особливий період, можливості населених пунктів, регіонів і окремих об'єктів щодо евакуації, розосередження населення і забезпечення його життєдіяльності; забезпечення виробничої діяльності об’єктів національної економіки у воєнний час;

про геодезичні, гравіметричні, картографічні та гідрометеорологічні дані і характеристики, які мають значення для оборони країни;

2) *у сфері економіки, науки і техніки:*

про зміст мобілізаційних планів державних органів та органів місцевого самоврядування, мобілізаційні потужності, заходи мобілізаційної підготовки і мобілізації та обсяги їх фінансування, запаси та обсяги постачання стратегічних видів сировини і матеріалів, а також зведені відомості про номенклатуру та рівні накопичення, загальні обсяги поставок, відпуску, закладення, освіження, розміщення і фактичні запаси державного матеріального резерву;

про використання транспорту, зв’язку, потужностей інших галузей та об’єктів інфраструктури держави в інтересах забезпечення її безпеки;

про плани, зміст, обсяг, фінансування та виконання державного оборонного замовлення;

про плани, обсяги та інші найважливіші характеристики добування, виробництва та реалізації окремих стратегічних видів сировини і продукції;

про державні запаси дорогоцінних металів монетарної групи, коштовного каміння, валюти та інших цінностей, операції, пов'язані з

виготовленням грошових знаків і цінних паперів, їх зберіганням, охороною і захистом від підроблення, обігом, обміном або вилученням з обігу, а також про інші особливі заходи фінансової діяльності держави;

про наукові, науково-дослідні, дослідно-конструкторські та проектні роботи, на базі яких можуть бути створені прогресивні технології, нові види виробництва, продукції та технологічних процесів, що мають важливе оборонне чи економічне значення або суттєво впливають на зовнішньоекономічну діяльність та національну безпеку України;

3) *у сфері зовнішніх відносин:*

про директиви, плани, вказівки делегаціям і посадовим особам з питань зовнішньополітичної і зовнішньоекономічної діяльності України, спрямовані на забезпечення її національних інтересів і безпеки;

про військове, науково-технічне та інше співробітництво України з іноземними державами, якщо розголошення відомостей про це завдаватиме шкоди національній безпеці України;

про експорт та імпорт озброєння, військової і спеціальної техніки, окремих стратегічних видів сировини і продукції;

4) *у сфері державної безпеки та охорони правопорядку:*

про особовий склад органів, що здійснюють оперативно-розшукову діяльність або розвідувальну чи контррозвідувальну;

про засоби, зміст, плани, організацію, фінансування та матеріально-технічне забезпечення, форми, методи і результати оперативно-розшукової, розвідувальної і контррозвідувальної діяльності; про осіб, які співпрацюють або раніше співпрацювали на конфіденційній основі з органами, що проводять таку діяльність; про склад і конкретних осіб, що є негласними штатними працівниками органів, які здійснюють оперативно-розшукову, розвідувальну і контррозвідувальну діяльність;

про організацію та порядок здійснення охорони адміністративних будинків та інших державних об’єктів, посадових та інших осіб, охорона яких здійснюється відповідно до Закону України «Про державну охорону органів державної влади України та посадових осіб»;

про систему урядового та спеціального зв’язку;

про організацію, зміст, стан і плани розвитку криптографічного захисту СІ, зміст і результати наукових досліджень у сфері криптографії;

про системи та засоби криптографічного захисту СІ, їх розроблення, виробництво, технологію виготовлення та використання;

про державні шифри, їх розроблення, виробництво, технологію виготовлення та використання;

про організацію РС в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, державні програми, плани та інші заходи у сфері ОДТ;

про організацію, зміст, стан і плани розвитку технічного захисту СІ;

про результати перевірок, здійснюваних згідно з законом прокурором у порядку відповідного нагляду за додержанням законів, та про зміст матеріалів оперативно-розшукової діяльності, досудового розслідування та судочинства з питань, зазначених у цій статті сфер;

про інші засоби, форми і методи ОДТ.

Конкретні відомості можуть бути віднесені до ДТ за СС «ОВ», «ЦТ» та «Т» лише за умови, що вони належать до вищезазначених сфер і їх розголошення завдаватиме шкоди інтересам національної безпеки України.

Порядок віднесення інформації до ДТ.

Віднесення інформації до ДТ здійснюється мотивованим рішенням ДЕТ за його власною ініціативою, за зверненням керівників відповідних державних органів, органів місцевого самоврядування, підприємств, установ, організацій чи громадян.

ДЕТ відносить інформацію до ДТ з питань, прийняття рішень з яких належить до його компетенції згідно з посадою. У разі, якщо прийняття рішення про віднесення інформації до ДТ належить до компетенції кількох ДЕТ, воно за ініціативою ДЕТ або за пропозицією СБУ приймається колегіально та ухвалюється простою більшістю голосів. При цьому кожен експерт має право викласти свою думку.

Інформація вважається ДТ з часу опублікування ЗВДТ, до якого включена ця інформація, чи зміни до нього відповідно до [3].

У рішенні ДЕТ про віднесення інформації до ДТ зазначаються [3]:

- інформація, яка має становити ДТ, та її відповідність категоріям і вимогам статті 8 Закону України «Про державну таємницю» [3];
- підстави для віднесення інформації до ДТ та обґрунтування шкоди національній безпеці України у разі її розголошення;
- СС зазначеної інформації;
- обсяг фінансування заходів ОДТ;
- державний орган, орган місцевого самоврядування, підприємство, установа, організація чи громадянин, який вніс пропозицію про віднесення цієї інформації до ДТ, та державний орган (органи), якому надається право визначати коло суб'єктів, які матимуть доступ до цієї інформації;
- строк, протягом якого діє рішення про віднесення інформації до ДТ.

Рішення про віднесення інформації до ДТ, продовження строку дії раніше прийнятого рішення про віднесення інформації до ДТ, зміну СС інформації, скасування раніше прийнятого рішення про віднесення інформації до ДТ приймаються ДЕТ протягом одного місяця з часу надходження звернення державного органу, органу місцевого самоврядування, підприємства, установи, організації чи громадянина. Такі рішення підлягають реєстрації СБУ та є підставою для формування

ЗВДТ, і внесення змін до зазначеного Зводу, до галузевих або відомчих РПВДТ. Порядок реєстрації рішень ДЕТ визначається КМУ.

Звід відомостей, що становлять державну таємницю (ЗВДТ).

ЗВДТ, формує СБУ на підставі рішень ДЕТ. Зазначений Звід та зміни до нього набирають чинності з моменту опублікування в офіційних виданнях України. Зміни до ЗВДТ вносяться не пізніше трьох місяців з дня одержання СБУ відповідного рішення ДЕТ. Зразки форм рішень ДЕТ, порядок та механізм формування ЗВДТ, і його опублікування визначаються КМУ. На підставі та в межах ЗВДТ, з метою конкретизації та систематизації даних про СІ державні органи створюють галузеві або відомчі РПВДТ, а також можуть створювати міжгалузеві або міжвідомчі РПВДТ. Підприємства, установи та організації незалежно від форм власності, що провадять діяльність, пов'язану із ДТ, за ініціативою та погодженням із замовником робіт, пов'язаних з ДТ, можуть створювати власні РПВДТ. Такі переліки погоджуються із СБУ, затверджуються ДЕТ та реєструються у СБУ. РПВДТ, не можуть суперечити ЗВДТ. У разі включення до ЗВДТ, або до РПВДТ інформації, яка не відповідає категоріям і вимогам, передбаченим статтею 8 закону [3], або порушення встановленого порядку віднесення інформації до ДТ заінтересовані громадяни та юридичні особи мають право оскаржити відповідні рішення до суду. З метою недопущення розголошення ДТ судовий розгляд скарг може проводитися в закритих засіданнях.

Строк дії рішення про віднесення інформації до ДТ.

Строк, протягом якого діє рішення про віднесення інформації до ДТ, встановлюється ДЕТ з урахуванням СС інформації, критерії визначення якого встановлюються СБУ, та інших обставин. Він не може перевищувати для СІ і із СС: «ОВ» – 30, «ЦТ» – 10, «Т» – 5 років.

Після закінчення передбаченого строку дії рішення про віднесення інформації до ДТ ДЕТ приймає рішення про скасування рішення про віднесення її до ДТ або приймає рішення про продовження строку дії зазначеного рішення в межах зазначених строків. Президент України з власної ініціативи або на підставі пропозицій ДЕТ чи за зверненням державних органів, органів місцевого самоврядування, підприємств, установ, організацій чи громадян може встановлювати більш тривалі строки дії рішень про віднесення інформації до ДТ.

Зміна СС інформації та скасування рішення про віднесення її до ДТ.

Підвищення або зниження СС інформації та скасування рішення про віднесення її до ДТ здійснюються на підставі рішення ДЕТ або на підставі рішення суду у випадках передбачених законодавством, та оформляються СБУ шляхом внесення відповідних змін до ЗВДТ.

Інформація вважається ДТ з більш високим чи нижчим СС або такою, що не становить ДТ, з часу опублікування відповідних змін до ЗВДТ.

Здійснення права власності на СІ та її матеріальні носії.

Власник СІ або МНСІ здійснює своє право власності з урахуванням обмежень, установлених в інтересах національної безпеки України. Якщо обмеження права власності на СІ або МНСІ завдають шкоди їх власнику, відшкодування здійснюється за рахунок держави у порядку та розмірах, що визначаються у договорі між власником такої інформації або її матеріальних носіїв і державним органом (органами), якому ДЕТ надається право приймати рішення щодо суб'єктів, які матимуть доступ до цієї інформації та її матеріальних носіїв. Зазначеним договором також визначаються порядок та умови ОДТ, включаючи РС під час користування і розпорядження СІ та МНСІ, обумовлюється згода власника цієї інформації та її матеріальних носіїв на здійснення права власності з урахуванням обмежень, встановлених відповідно до закону [3], взяття власником на себе зобов'язання щодо збереження ДТ та ознайомлення його з мірою відповідальності за порушення законодавства про ДТ. Якщо власник СІ або МНСІ відмовляється від укладення договору чи порушує його, за рішенням суду ця інформація або її матеріальні носії можуть бути вилучені у власність держави за умови попереднього і повного відшкодування власникові їх вартості.

Фінансування витрат на здійснення діяльності, пов'язаної з ДТ.

Витрати на здійснення заходів щодо віднесення інформації до ДТ, засекречування, розсекречування та охорони матеріальних носіїв такої інформації, її криптографічного та технічного захисту, інші витрати, пов'язані з ДТ, на недержавних підприємствах, в установах, організаціях фінансуються на підставі договору з замовником робіт, пов'язаних з ДТ.

Методичні рекомендації ДЕТ щодо визначення підстав для віднесення відомостей до ДТ та ступеня їх секретності

Правовий інститут ДТ є найбільш розвинутим у порівнянні з іншими видами ІзОД. Механізм ідентифікації відомостей, що становить ДТ із загального масиву інформації, що може бути віднесена до СІ, наведений у [38, 40] як «Методичні рекомендації ДЕТ щодо визначення підстав для віднесення відомостей до ДТ та ступеня їх секретності» (далі – «Рекомендації…»).

Дані «Рекомендації» мають такий основний зміст [38, 40]:

1. *Загальні положення.* Методичні рекомендації призначені для ДЕТ та створених при державних експертах ЕК і містять порядок визначення підстав для віднесення відомостей до ДТ та надання цим

відомостям відповідного СС за методом експертних оцінок. Застосований у «Рекомендаціях...» принцип експертних оцінок дозволяє визначити в однакових умовних одиницях величину економічної шкоди та тяжкості інших негативних наслідків, що можуть бути завдані життєво важливим інтересам України внаслідок розголошення відомостей, які віднесені чи повинні бути віднесені до ДТ, та надати цим відомостям відповідного СС [38, 40].

2. *Визначення основних понять* [38, 40]:

економічна шкода (ЕШ)– матеріальні збитки держави у сферах оборони, економіки, зовнішніх відносин, державної безпеки і охорони правопорядку у кількісному виразі, які спричинені чи які можуть бути спричинені внаслідок розголошення конкретних відомостей, що становлять ДТ;

інші тяжкі наслідки (ІТН) – негативні зміни у зазначених сферах (головним чином у сферах зовнішніх відносин, державної безпеки і охорони правопорядку), які відбулися чи можуть відбутися внаслідок розголошення конкретних відомостей, що становлять ДТ, і які не піддаються економічному обрахунку у кількісному (вартісному) виразі;

сукупна шкода (СШ) – ЕШ та ІТН, що завдані чи можуть бути завдані державі внаслідок розголошення конкретних відомостей, які становлять ДТ;

об'єкт – система, зразок, виріб, розробка військового або народногосподарського призначення, що містить відомості, які віднесені або можуть бути віднесені до ДТ;

складова частина об'єкта (СЧО) – елемент об'єкту, на функціонування якого безпосередньо впливають прогнозні дії сторони, що оволоділа відомостями, які віднесені, або можуть бути віднесені до ДТ.

3. *Підстави для віднесення відомостей до ДТ* [38, 40]:

3.1.Підставою для віднесення відомостей до ДТ є наявність потенційної СШ (*W*) державі у сферах, зазначених у статті 6 Закону України "Про державну таємницю" [3], від втрати цих відомостей, тобто [38, 40]:

$$W = W_{ек} + W_{ін}, \qquad (1.1)$$

де $W_{ін}$ – показник, який характеризує шкоду державі від ІТН, що не можуть бути обраховані в економічному кількісному (вартісному) виразі. Рівень шкоди від таких наслідків (п. 3.2) встановлюється на підставі попередньої експертної оцінки за участю відповідних фахівців; $W_{ек}$ – показник, що характеризує ЕШ державі як рівень зниження ефективності використання виділених коштів для забезпечення

діяльності (створення, функціонування) об'єкта внаслідок розголошення відомостей про цей об'єкт [38, 40]:

$$W_{ек} = W_1 - W_2, \tag{1.2}$$

де W_1 – показник, який характеризує ефективність використання виділених коштів для забезпечення діяльності (створення, функціонування, використання) об'єкта за умови відсутності розголошення відомостей, що підлягають експертизі на предмет віднесення до ДТ; W_2 - той самий показник за умови розголошення цих відомостей.

Розрахунок значення величини W_1 проводиться без урахування витрат на організацію та здійснення режимно-секретної діяльності, пов`язаної з захистом цих відомостей, а розрахунок значення величини W_2 здійснюється для випадку, коли імовірність втрати цих відомостей приймається за одиницю.

Таким чином, значення $W_{ек}$ визначає рівень шкоди, яка зумовлена повною або частковою втратою ефективності подальшого використання (створення) об'єкта внаслідок розголошення відомостей про цей об'єкт.

З метою уникнення впливу факторів, пов`язаних зі зміною цінових показників, підрахунок коштів виконується в умовних одиницях – балах. Кількість балів, яка характеризує «питому вагу» окремих важливих об`єктів (див. *Додаток 5*).

3.2. *Перелік важливих ІТН* для інтересів держави від розголошення відомостей, упорядкований за ступенем їх тяжкості в балах, становить [38, 40]:

3.2.1. Наслідки *першої* категорії - більше 200 балів:

- повний розрив дипломатичних відносин, що може призвести до озброєного нападу на Україну чи її союзників або воєнних дій;
- повний контроль державного шифрованого листування з боку іншої держави;

3.2.2. Наслідки *другої* категорії - 100-200 балів :

- розрив дипломатичних відносин з однією або з кількома розвиненими державами;
- повне або часткове (30 % і більше) розкриття розвідувальних можливостей держави за кордоном;
- загроза життю чи свободі особам, які виконують розвідувальні чи контррозвідувальні завдання;

3.2.3. Наслідки *третьої* категорії - 70-100 балів :

- розрив дипломатичних відносин з іншими державами (державою);
- закриття посольства (представництва) України у будь-якій країні;
- зниження рівня представництва України у будь-якій країні;

- повне або часткове (30 % і більше) зниження ефективності оперативно-стратегічних планів;

- повна або часткова (30 % і більше) втрата бойового управління військами, необхідність розробки нових алгоритмів систем управління військами, створення нових пунктів управління;

- часткове (до 30 %) розкриття розвідувальних можливостей держави за кордоном.

3.2.4. Наслідки *четвертої* категорії - 50-70 балів :

- зрив укладення Україною міжнародного договору;

- зрив чи неможливість виконання розвідувальної, контррозвідувальної чи іншої спеціальної операції;

- часткове (до 30 %) зниження ефективності оперативно-стратегічних планів;

- часткова (до 30 %) втрата бойового управління військами, необхідність розробки нових алгоритмів системи бойового управління військами;

- розкриття даних про особу, яка виконує на негласній основі розвідувальне, контррозвідувальне чи інше оперативне завдання;

- розкриття сил чи засобів негласного оперативного контролю, що застосовуються державними органами для виконання оперативно-розшукової діяльності.

3.2.5. Наслідки *п'ятої* категорії - 10-50 балів :

- зрив переговорів з питань озброєння-роззброєння;

- економічні санкції проти України;

- розрив торговельно-економічних зв`язків з іншими державами;

- несанкціонований доступ (проникнення) на об'єкти, де впроваджено режим спеціального допуску і охорони.

3.3. Підставою для прийняття рішення про віднесення відомостей до ДТ є наявність у бальному обрахуванні суми ЕШ та шкоди від ІТН у разі розголошення цих відомостей, тобто [38, 40]:

$$W > 0. \tag{1.3}$$

У ряді випадків можливо, що шкода від розголошення відомостей визначатиметься лише економічним показником або показником ІТН.

4. *Визначення СС відомостей* [38, 40]:

Критерієм визначення СС відомостей є знаходження значення СШ від її розголошення у межах:

- *від 1 до 10 балів* – для відомостей зі СС «Т»;

$$1 \le W < 10, \tag{1.4}$$

- *від 10 до 100 балів* – для відомостей зі СС «ЦТ»;

$$10 \le W < 100, \tag{1.5}$$

- 100 балів і більше – для відомостей зі СС «ОВ».

$$W \ge 100. \tag{1.6}$$

5. *Проведення експертних оцінок* [38, 40]:

Процедура експертизи організується і здійснюється ДЕТ у порядку, вказаному у (див. *Додаток 6*).

Для проведення експертних оцінок ДЕТ, відповідно до Положення про ДЕТ [17], може створювати ЕК у складі 5-7 або більше провідних фахівців і науковців, які мають допуск до ДТ і працюють у сфері, що належать до компетенції ДЕТ. Із числа членів ЕК призначається секретар комісії. Склад ЕК затверджується наказом керівника відповідного міністерства, відомства, підприємства, установи, організації, де працює ДЕТ, за його поданням. Оновлення складу ЕК також здійснюється за поданням ДЕТ і затверджується відповідним наказом керівника. Засідання ЕК проводяться як правило під головуванням ДЕТ. В окремих випадках, за рішенням ДЕТ, до роботи комісії можуть залучатися також фахівці, які не входять до складу ЕК, але мають відповідний допуск до ДТ.

Порядок формування і діяльності ЕК викладений у «Рекомендаціях з організації діяльності ЕК при ДЕТ» [39]. Якщо відомості, визначені для проведення експертизи, стосуються двох чи більше сфер діяльності, вони підлягають розгляду кількома ДЕТ, до компетенції яких належать ці відомості. У такому випадку приймається спільне рішення ДЕТ згідно з порядком, визначеним [3] та [17].

5.1. Послідовність проведення експертизи.

ДЕТ ставить завдання перед ЕК у формі листів опитування (див. *Додаток 7*), до графи 1 яких внесені відомості, що підлягають експертизі. Кожному члену ЕК видається лист опитування для заповнення.

Члени ЕК спільно, на основі завдання, виданого ДЕТ, визначають і вносять в листи опитування :

- сферу (сфери) діяльності, до якої (яких) належать відомості, що підлягають експертизі (графа 2 листа опитування);
- об’єкт, який містить відомості, що підлягають експертизі, його «питома вага» у балах (графа 3) (див. *Додаток 5*);
- прогнозні дії сторони, що оволоділа відомостями, з метою зниження ефективності функціонування (створення) об’єкта (графа 4);
- СЧО, що безпосередньо підпадає під прогнозні дії сторони, яка оволоділа відомостями, її відносна вартість від вартості об’єкта (графа 4).

У разі, якщо зазначені дії стосуються об'єкта в цілому, у графі 5 вказується назва об'єкта і його відносна вартість - 1,0.

У разі, якщо відомості стосуються об'єкта, який знаходиться за межами таблиці (див. *Додаток 5*), ІТН від розголошення відомостей - за межами п.3.2, рішення щодо них, у т.ч. відносно їх «питомої ваги», приймається членами ЕК спільно.

Кожний член ЕК незалежно один від одного [38, 40]:

- визначають рівень (у відносних одиницях) зниження ефективності використання СЧО або об'єкта у цілому внаслідок дії сторони, що оволоділа відомостями (графа 6);
- здійснюють оцінку ЕШ від дій іноземної держави (графа 7) шляхом множення «питомої ваги» об'єкта (графа 3) на відповідну вартість СЧО (графа 5), а також на рівень зниження ефективності функціонування (використання) СЧО (графа 6);
- визначають рівень шкоди від ІТН (графа 8) відповідно до переліку, що наведений у п.3.2. При визначенні тяжкості кількох наслідків до кожного з них визначається свій рівень шкоди;
- проводять оцінку рівня СШ шляхом підсумування рівня ЕК та шкоди від ІТН (графа 9).

Секретар ЕК [38, 40]:

- на підставі аналізу листів опитування визначає остаточну величину СШ як суму оцінок, зроблених кожним членом ЕК, які заповнили листи опитування, поділену на кількість членів ЕК, які заповнили відповідні листи опитування;
- на підставі величини СШ визначає СС відомостей;
- оформляє протокол засідання ЕК за формою (див. *Додаток 8*);
- готує проект рішення (висновку, експертного висновку) ДЕТ.

Приклади проведення експертизи визначення належності відомостей до ДТ та їх ступеня секретності наведені у додатках (див. *Додаток 9, 10*).

Загальна характеристика та проблемні аспекти процедури віднесення інформації до державної таємниці

Серйозність наслідків безпідставного засекречування інформації вимагає встановлення чіткої процедури віднесення інформації до ДТ. Частково ця процедура визначається Законом України «Про державну таємницю» [3], інші її особливості конкретизуються в «Рекомендаціях...» [38, 39] Спробуємо, навівши та проаналізувавши [53-61] ці матеріали, встановити послідовність етапів віднесення інформації до секретної та конкретизувати зміст і задачі кожного з них.

Перший етап процедури віднесення – встановлення приналежності інформації, що перевіряється, до виділеного Законом України «Про державну таємницю» [3] 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 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 [3] 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» [1] з метою уточнення характеру шкоди, від якої може потерпати національна безпека. Стаття 7 означеного закону [1] 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 [3] мова йде про інформаційні загрози, кожна з яких у відповідних сферах національної безпеки трансформується у 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, законом [3] 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 [3]:

- 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 ВРУ відповідно до законів та міжнародних угод.

Зіставлення інформації, що перевіряється, зі змістом сегменту обмежень реалізується на *другому етапі* загальної процедури віднесення інформації до ДТ, з 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 ж стосується подальшого аналізу інформації, яка залишилася після другого етапу, то в законі [3] визначено лише базовий принцип цього аналізу, де ще раз наголошується на головній властивості ДТ: якщо виділена на другому етапі інформація є секретною, то її розголошення має спричиняти шкоду національній безпеці держави. Причому ніяких натяків на те, у який спосіб виконується перевірка головної властивості ДТ немає. Більш корисним в цьому сенсі є зміст «Рекомендацій...» [38], де викладено як процедуру обчислення шкоди у кількісному вимірі, так і методику визначення СС інформації залежно від отриманого кількісного значення шкоди.

В основу використаного в [38] підходу віднесення інформації до ДТ покладено принцип економічної оцінки витрат, обумовлених розголошенням СІ. Він базується на введені спеціального показника *W* рівня потенційної шкоди, який характеризується величиною ЕШ, заподіяних розголошенням СІ, тобто *W* отримує певне кількісне значення, причому підрахунок виконується в штучно введених умовних одиницях збитків (у.о.з.) за спеціальною методикою [38].

Дана методика визначення підстав для віднесення відомостей до ДТ та їх СС передбачає вирішення цих питань шляхом розрахунків рівня потенційної СШ (ЕШ та ІТН) у разі розголошення цих відомостей.

Рис. 1. Блок-схема процедури віднесення інформації до ДТ та визначення її СС

Під час обрахування шкоди використовуються однакові у.о.з. (бали). Імовірна повна вартість відомостей, віднесених до ДТ чи повинні бути віднесені до ДТ, визначається також умовним коефіцієнтом, який приймається за одиницю. При частковій втраті відомостей (окремих елементів об’єкта) підрахунки шкоди здійснюються у відсотках від умовного коефіцієнта (одиниці) помноженого на «питому вагу» об’єкта (бали). Розглянута методика у процесі визначення підстав для

віднесення відомостей до ДТ не передбачає урахування витрат на організацію та здійснення режимно-секретної діяльності, пов'язаної з захистом цих відомостей та сфери їх обігу [61].

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 у 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 [38] наведено перелік можливих наслідків (перелік ІТН) розголошення СІ 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 СШ (W) приймається рішення про відсутність чи наявність підстав для віднесення відомостей до ДТ, і в разі наявності цих підстав – про визначення СС цих відомостей. Критерієм в останньому випадку є знаходження значень показника W в межах певних позначок шкали сукупної шкоди: $1 \le W < 10 \rightarrow$ «Т»; $10 \le W < 100 \rightarrow$ «ЦТ»; $100 \le W \rightarrow$ «ОВ».

На рис. 1 графічно представлено у 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 ДТ є третій етап, про що свідчить ряд публікацій за його тематикою, в яких було окреслено певні проблемні питання [53-61], що стосуються як принципових засад вирішення завдань цього етапу, так відповідного математичного забезпечення. В першу чергу, це аспекти пов'язані з

розробкою методики обчислення показника можливої сукупної шкоди *W* та методика проведення експертної процедури оцінювання конкретних значень *W* (включно із способом обробки результатів колективної (групової) експертизи).

Проблемні аспекти. Віднесення інформації до ДТ (або СІ) є ключовим елементом реалізації практичних аспектів ОДТ. Справа в певних особливостях ДТ, а також і термінологічного забезпечення цієї процедури [59]. Зокрема, якщо СІ вже виокремлено, подальші дії із забезпеченням її охорони мають єдиний встановлений згідно з існуючими нормативно-правовими вимогами порядок – РС. Тому саме поділ інформації на секретну та інші види ІзОД визначає подальшу методологію та методики захисту інформації, його ресурсоємність, вартість, рівні захисту і т.п.

Крім того, вже виділена СІ потребує додаткової деталізації за СС відомостей, що їх складають. СС 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 СІ, гарантованість забезпечення ними потрібного (заданого) рівня захисту, а відтак – потрібні (граничні) обсяги сукупних витрат на ОДТ у кожному конкретному випадку.

Тобто, для конкретного СРСД проблема віднесення інформації до ДТ опосередковано, через проблему забезпечення належного рівня захисту отриманих видів та обсягів СІ, трансформується в проблему економічного забезпечення ОДТ. Цей висновок є достатньо очевидним, крім того, підтверджується окремими кількісними даними, наприклад, у статті [60] було наведено оцінку витрат із визначення та захисту СІ в США, що складали 20 % від загальної суми асигнувань на науково-дослідні та дослідно-конструкторські роботи. Це єдина з кількісних оцінок рівня витрат на захист СІ з наведених у відкритих публікаціях, усі інші зроблено для конфіденційної інформації. Однак аналіз даних саме для конфіденційної інформації, якщо припустити, що максимальні витрати на захист конфіденційної інформації можна розглядати як нижню межу можливих витрат на ОДТ, дає приблизно ті ж самі 20 %, підтверджуючи сталість та правдоподібність оцінки В.Рубанова у [60].

Принциповим питанням, яке обов’язково підлягає врахуванню в процесі віднесення відомостей до ДТ, є врахування можливих економічних втрат, обумовлених засекречуванням інформації, що має перспективу так званого подвійного використання.

Тобто, діяльність пов’язана з ДТ має чітко виражені економічні, вартісні показники у багатьох сферах. *Віднесення відомостей до ДТ* – це важлива складова державної економічної політики. Встановленням

обмежень доступу до відомостей, що становлять ДТ у галузях науки, науково-дослідних, дослідно-конструкторських робіт, промислового виробництва, звужуються сфери застосування цієї інформації. Особливо це стосується такої чутливої сфери, як технології подвійного призначення, нових видів виробництва та технологічних процесів, що мають важливе не тільки для економіки та суттєво впливають на зовнішньоекономічну діяльність. Тільки всебічне економічне обґрунтування всіх факторів дозволить об'єктивно оцінювати необхідність віднесення відомостей до ДТ на підставі ЕШ у разі їх розголошення та враховувати важливі переваги відкритого використання таких відомостей. А також забезпечувати раціональне використання бюджетних коштів для захисту тих відомостей, які дійсно необхідно приховувати в інтересах національної безпеки [61].

Економічне обґрунтування підстав для віднесення відомостей до ДТ доцільне щоб включало розгляд у сферах які піддаються обрахунку у вартісному виразі, наступних факторів [61]:

- ЕШ від розголошення відомостей, які віднесені чи повинні бути віднесені до ДТ, у вартісному виразі;
- визначення переваг відкритого використання відомостей, які віднесені чи повинні бути віднесені до ДТ, також у вартісному виразі можливої економічної вигоди;
- визначення обсягів витрат бюджетних коштів на захист відомостей, що повинні бути віднесені до ДТ.

При цьому слід враховувати те, що кваліфікований розгляд наведених факторів, сприятиме позитивній оцінці можливих потенційної, реальної і попередженої ЕШ державі внаслідок протиправних дій проти ДТ [61]:

Потенційна ЕШ – це можливі матеріальні збитки державі, які можуть бути спричинені внаслідок розголошення відомостей, які віднесені чи повинні бути віднесені до ДТ. Потенційна ЕШ є одним із важливих критеріїв віднесення відомостей до ДТ.

Реальна ЕШ – це матеріальні збитки державі, спричинені внаслідок розголошення відомостей, віднесених до ДТ. На підставі визначення у вартісному виразі реальної економічної шкоди до винних посадових осіб та громадян застосовуються правові (цивільно-правові, адміністративні, кримінальні) санкції за розголошення відомостей, що становлять ДТ, а також вживаються заходи для ліквідації негативних наслідків цих дій.

Попереджена ЕШ – це своєчасна запобіжними заходами ліквідовані умови для розголошення відомостей, віднесених до державної таємниці, що могло спричинити матеріальні збитки державі. На підставі сукупності фактів попередження ЕШ оцінюється стан захисту ОДТ у відповідних галузях та ефективність роботи керівників державних

органів, органів місцевого самоврядування, підприємств, установ і організацій та їх спеціальних підрозділів і служб щодо забезпечення захисту ДТ.

Цей аспект уже розглядався в [60], де вказано на односторонність у ставленні до цієї проблеми у ході експертизи, коли визначається лише достатність важливості інформації для її засекречування без урахування обсягу економічного ефекту від використання даних у народному господарстві, який буде втрачено внаслідок засекречування. Ці та подібні їм оцінки можуть бути отримані лише за умови участі в експертних комісіях фахівців з економіки, достатньо обізнаних у прикладних аспектах відповідних сфер діяльності.

Слід підкреслити, що вище мова йде насамперед про вартісну оцінку функціонування елементів СОДТ на конкретних об'єктах інформаційної діяльності, де обсяги та СС інформації, що підлягає охороні, вже визначено. Це, так би мовити, «прямі» витрати на ОДТ. І якщо має місце факт необґрунтованого засекречування інформації, то, зрозуміло, неправомірно утворений додатковий обсяг СІ тягне за собою додаткові об'єктивно невиправдані витрати. Тобто цей механізм виникнення економічно недоцільних витрат у сфері ОДТ достатньо прозорий та очевидний. Однак необґрунтоване засекречування інформації може одночасно «запустити» в дію ще один механізм – механізм втраченої вигоди, який здатний призвести до вельми відчутних економічних збитків. За оцінками, наведеними у [62], втрати через необґрунтоване закриття інформації у колишньому СРСР доходили до кількох десятків мільярдів рублів. Ці збитки виникали через втрату вигоди від [62]:

- 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 із 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 у неконтрольованих для широкого загалу сферах життя.

Загалом можна зробити *висновок*: запропонована у «Рекомендаціях…» [38] методика віднесення відомостей до ДТ не є універсальною і вимагає доопрацювання для формування диференційованого підходу до різних видів об'єктів, відомості про які складають предмет експертизи, із урахуванням особливостей їх функціонування, експлуатації тощо.

Поряд з тим стає зрозумілим, що за такої постановки завдання кількість ймовірних варіантів розвитку подій, обумовлених витоком СІ, необмежено зростає. Це робить неможливим розробку єдиної типової процедури визначення СШ (*W*), тобто спроба побудови певного шаблону дій, придатного для обчислення рівня *W* за будь-яких обставин, є нездійсненною. Якщо не можна скласти шаблону дій, треба дати експерту методологію оцінювання рівня *W*, знання якої дозволить у кожній конкретній ситуації самостійно визначити спосіб обчислення *W* (при цьому не виключається розроблення однієї чи декількох типових галузево орієнтованих методик обчислення *W* або проміжних рішень на зразок типових переліків «питомої ваги» об'єктів (*див. Додаток 5*), які допомогли б експерту у вирішенні його завдання).

Окрім того, доцільне, щоб вказані правила враховували не тільки СШ у разі розголошення відповідних відомостей, а й фактори, пов'язані з і перевагою їх відкритого використання, а також витрати на захист таких відомостей [61].

Таким чином, найпершим кроком у проблемі визначення рівня шкоди, якої може бути завдано національній безпеці України у разі розголошення ДТ чи втрати МНСІ, має бути розробка теоретико-методологічних засад вимірювання СШ (*W*).

1.4. Засекречування та розсекречування носіїв інформації

Вимоги до засекречування та розсекречування МНІ

Засекречування матеріальних носіїв інформації (МНІ) здійснюється шляхом надання на підставі ЗВДТ (РПВДТ), відповідному документу, виробу або іншому матеріальному носію інформації ГС посадовою особою, яка готує або створює документ, виріб або інший матеріальний носій інформації.

ГС кожного МНСІ повинен відповідати СС інформації, яка у ньому міститься, згідно із ЗВДТ, - «ОВ», «ЦТ» або «Т». Реквізити кожного МНСІ складаються із: ГС; номера примірника; статті ЗВДТ, на підставі якої здійснюється засекречення; найменування посади та підпису особи, яка надала ГС. Якщо реквізити, зазначені у частині другій цієї статті,

неможливо нанести безпосередньо на МНСІ, вони мають бути зазначені у супровідних документах.

Забороняється надавати ГС, передбачені законом [3], матеріальним носіям іншої таємної інформації, яка не становить ДТ, або конфіденційної інформації. Перелік посад, перебування на яких дає посадовим особам право надавати МНСІ ГС, затверджується керівником СРСД.

СС науково-дослідних, дослідно-конструкторських і проектних робіт, які виконуються в інтересах забезпечення національної безпеки та оборони держави, встановлюються шляхом винесення відповідного висновку ДЕТ, який виконує свої функції у сфері діяльності замовника, разом з підрядником.

Після закінчення встановлених строків засекречування МНІ та у разі підвищення чи зниження визначеного ДЕТ СС такої інформації або скасування рішення про віднесення її до ДТ керівники державних органів, органів місцевого самоврядування, підприємств, установ, організацій, у яких здійснювалося засекречування МНІ, або керівники державних органів, органів місцевого самоврядування, підприємств, установ, організацій, які є їх правонаступниками, чи керівники вищого рівня зобов'язані протягом шести місяців забезпечити зміну ГС або розсекречування цих МНСІ та письмово повідомити про це керівників державних органів, органів місцевого самоврядування, підприємств, установ, організацій, яким були передані такі МНСІ.

Строк засекречування МНІ. Строк засекречування МНІ має відповідати строку дії рішення про віднесення інформації до ДТ, встановленого рішенням ДЕТ. Перебіг строку засекречування МНІ починається з часу надання їм ГС.

Оскарження рішення щодо засекречування МНІ. Громадяни та юридичні особи мають право внести посадовим особам, які надали ГС МНСІ, обов'язкову для розгляду мотивовану пропозицію про розсекречування цього носія інформації. Зазначені посадові особи повинні протягом одного місяця дати громадянину чи юридичній особі письмову відповідь з цього приводу.

Рішення про засекречування МНІ може бути оскаржено громадянином чи юридичною особою в порядку підлеглості вищому органу або посадовій особі чи до суду. У разі незадоволення скарги, поданої в порядку підлеглості, громадянин або юридична особа мають право оскаржити рішення вищого органу або посадової особи до суду.

Методичні рекомендації щодо порядку організації та проведення експертиз на предмет наявності чи відсутності у МНІ відомостей, що становлять ДТ

Відповідно до вимог Законів України [1, 3, 9], Порядку організації та забезпечення РС в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях, затвердженого постановою КМУ від 02.10.2003 № 1561, Положення [17], інших нормативно-правових актів у сфері ОДТ розроблені методичні рекомендації у якій запропоновано порядок організації та проведення експертиз щодо встановлення наявності чи відсутності у МНІ відомостей, що становлять ДТ, та визначення їх СС (далі – експертиза).

У рекомендаціях терміни вживаються у значеннях [32]:

експертиза – організоване ДЕТ комплексне вивчення МНІ на предмет наявності чи відсутності у них відомостей, що становлять ДТ, їх достовірності, актуальності та повноти, визначення ступеня обмеження доступу до цих відомостей, встановлення та обґрунтування шкоди, яка може бути завдана державним інтересам внаслідок їх витоку. За результатами експертизи ДЕТ приймається рішення щодо доцільності вжиття суб'єктами правовідносин України додаткових заходів, спрямованих на охорону МНІ. Результати експертизи оформлюються експертним висновком ДЕТ;

оцінка – комплексне вивчення МНІ на предмет наявності чи відсутності у них відомостей, що становлять ДТ, їх достовірності, актуальності та повноти, визначення ступеня обмеження доступу до цих відомостей, встановлення та обґрунтування шкоди, яка може бути завдана державним інтересам внаслідок їх витоку. За результатами оцінки подаються пропозиції щодо необхідності вжиття заходів, спрямованих на обмеження доступу до МНІ, а також доцільності проведення експертизи. Результати оцінки оформлюються протоколом, висновком, актом тощо, що затверджується керівником органу державної влади, підприємства, установи, організації, які є ініціатором її проведення.

Експертизи проводяться за ініціативою ДЕТ, звернення органів державної влади, підприємств, установ, організацій або громадян у випадках [32]:

- втрати МНСІ;
- розголошення відомостей, що становлять ДТ;
- надання МНІ іноземній державі, міжнародній організації чи її представникам;
- в інших випадках за рішенням ДЕТ.

Експертизи організовуються ДЕТ відповідно до компетенції згідно до займаної посади, визначеної у [21] за законом [3]. Компетенція ДЕТ визначається законодавчими та відомчими нормативно-правовими актами, посадовими обов'язками тощо, які визначають сферу його діяльності згідно із займаною посадою. До експертизи та оцінки залучаються особи, які мають відповідну форму допуску до ДТ. Для проведення експертиз за рішенням ДЕТ можуть створюватися ЕК, засади діяльності яких визначаються Положенням [30].

Порядок організації експертизи.

Експертизі передує оцінка (вивчення) МНІ, що плануються для проведення їх експертизи (матеріали експертизи), на предмет наявності чи відсутності у них відомостей, що становлять ДТ.

Попередню оцінку організовує ініціатор її проведення. До проведення оцінки ініціатор залучає компетентних фахівців, які мають відповідний рівень професійної підготовки та знань для надання об'єктивних даних щодо достовірності, актуальності, повноти інформації, що міститься у матеріалах, які підлягали вивченню. Оцінка може не проводитися у випадках, якщо проведення експертизи ініційовано ДЕТ. Результати оцінки оформлюються окремим документом, у якому ідентифікуються МНІ, що підлягали оцінці (реєстраційний номер, дата, назва, кількість аркушів, номер примірника), а також вказується, які саме відомості (сторінка, абзац, пункт) становлять ДТ з посиланням на конкретні статті ЗВДТ, пункти РПВДТ, можливість завдання ймовірної шкоди національній безпеці та її обґрунтування у випадку розголошення зазначених відомостей. Такий документ підписується фахівцями, які здійснили оцінку (зазначаються посади, прізвища, ініціали і дата), та затверджується керівником органу державної влади, підприємства, установи чи організації.

Грифи обмеження доступу на матеріалах експертизи приводяться РСО відповідно до прийнятого рішення за результатами проведення їх оцінки. Гриф обмеження доступу завіряється печаткою, підписом працівника РСО з розшифруванням його посади. При цьому зазначається реєстраційний номер та дата документа, на підставі якого проставлено гриф обмеження доступу.

У разі необхідності проведення оцінки із залученням інших суб'єктів правовідносин перелічені матеріали надсилаються до органу державної влади, підприємства, установи чи організації, що є замовниками робіт, стосовно яких проводилася оцінка, або до сфери управління яких належить ініціатор експертизи.

Для проведення експертизи ініціатор надсилає ДЕТ за компетенцією МНІ, що підлягали оцінці, із супровідним листом та документ про її результати. У разі, якщо прийняття рішення про наявність у матеріалах

експертизи відомостей, що становлять ДТ, належить до компетенції кількох ДЕТ, такі матеріали ініціатор може надіслати цим ДЕТ. У супровідному листі зазначаються результати оцінки, підстави для проведення експертизи, перспективи реалізації чи використання її результатів.

ДЕТ доручає проведення експертизи ЕК при ДЕТ чи спеціально для цього створеній ЕК. У разі необхідності ДЕТ проводить експертизу самостійно. ЕК вивчає подані на експертизу матеріали на предмет наявності у них відомостей, що становлять ДТ. У разі необхідності ЕК вносить пропозиції ДЕТ щодо отримання необхідної для проведення експертизи додаткової інформації. У разі потреби необхідну для проведення експертизи інформацію ДЕТ одержує в установленому порядку від державних органів, підприємств, установ, організацій або громадян.

За результатами розгляду поданих на експертизу матеріалів ЕК приймається рішення, яке оформляється протоколом, де зазначаються [32]:

- повні ідентифікаційні ознаки МНІ, щодо яких проводилася експертиза (назва, дата, реєстраційний номер, ГС, номер примірника носія інформації та ін.);
- прийняте за розглядом матеріалів експертизи рішення із зазначенням назви, реєстраційного номеру, конкретної сторінки, пункту, абзацу, речення тощо, які містять відомості, що становлять ДТ, з посиланням на статті ЗВДТ, пункти РПВДТ, під дію яких вони підпадають, та ступінь їх секретності;
- коротке описання інформації, розголошення якої може завдати шкоду національній безпеці;
- обставини розголошення інформації, за яких може бути завдано шкоду національній безпеці;
- обґрунтування шкоди національній безпеці України, яку може завдати (чи вже завдав) витік інформації, що міститься у матеріалах експертизи (наслідки витоку цієї інформації);
- пропозиції для прийняття ДЕТ відповідного рішення.

У протоколі фіксуються поставлені членам ЕК питання для обговорення та його результати, а також висловлені запитання, зауваження та пропозиції. До протоколу може бути внесена інша інформація, необхідна для розгляду питання по суті. Протокол підписується головою, присутніми на засіданні членами ЕК та затверджується ДЕТ.

За результатами розгляду матеріалів експертизи, протоколів засідання ЕК, інших необхідних матеріалів ДЕТ виносить *експертний висновок* про наявність чи відсутність у матеріалах експертизи відомостей, що становлять ДТ, де зазначається:

- посада, прізвище, ініціали ДЕТ;
- ініціатор проведення експертизи (назва, дата, реєстраційний номер документу, що був підставою для проведення експертизи);

- за чиєю пропозицією винесено експертний висновок (назва, дата, реєстраційний номер протоколу ЕК);

- повні ідентифікаційні ознаки матеріалів експертизи (назва, дата, реєстраційний номер, ГС , номер примірника носія інформації та ін.);

- назви та вид документів, інших МНІ, їх реєстраційні номери, сторінка, пункт, абзац та інші дані, які містять відомості, що становлять ДТ;

- до якої сфери забезпечення життєдіяльності належить інформація, яку віднесено до ДТ;

- стаття ЗВДТ, під дію якої підпадає інформація, що становить ДТ;

- СС інформації;

- коротке описання інформації, розголошення якої може завдати шкоди національній безпеці;

- обставини розголошення інформації, за яких може бути завдано шкоди національній безпеці;

- обґрунтування шкоди національній безпеці України, яку може завдати (чи вже завдав) витік інформації, що міститься у матеріалах експертизи (наслідки витоку цієї інформації).

Якщо відомості, щодо яких проводилася експертиза, відповідно до прийнятого ДЕТ рішення не становлять ДТ, вони вивчаються на предмет віднесеності їх до службової інформації. У разі необхідності та за умови, якщо прийняття рішення про наявність у матеріалах експертизи відомостей, що становлять ДТ, належить до компетенції кількох ДЕТ, розгляд таких матеріалів може виноситися на спільні засідання цих ДЕТ (*спільні засідання*).

Спільне засідання ініціюється одним з ДЕТ, що планують приймати у ньому участь, чи СБУ. За згодою ДЕТ, що планують приймати участь у спільному засіданні, з їх числа визначається головуючий цього засідання, який забезпечує роботу спільного засідання та призначає його секретаря. Передує спільному засіданню розгляд матеріалів ЕК, створеними ДЕТ, що приймають участь у спільному засіданні. Результати роботи ЕК оформляються протоколом. До спільного засідання кожен з ДЕТ подає затверджений ним протокол засідання ЕК чи документ, у якому викладається мотивована думка ДЕТ про наявність чи відсутність у матеріалах експертизи відомостей, що становлять ДТ. У разі необхідності, для розгляду матеріалів експертизи на спільному засіданні, ДЕТ, що приймають у ньому участь, можуть створювати спільні ЕК. Результати роботи цих комісій оформляються протоколами, які подаються на затвердження кожному з ДЕТ, що приймають участь у спільному засіданні. У разі відсутності необхідності у роботі ЕК ДЕТ , що приймають участь у спільному засіданні, можуть їх не створювати. Результати спільного засідання оформляються протоколом, який підписується ДЕТ, що приймали у ньому участь. При цьому, кожен з

ДЕТ має право викласти свою думку. Рішення приймається колегіальне та ухвалюється простою більшістю голосів, кожен з яких є рівнозначним. По завершенню роботи спільних засідань виноситься експертний висновок, який підписується ДЕТ, що приймали участь у проведенні експертизи та завіряється печаткою органу державної влади, підприємства, установи, організації.

Експертний висновок складається у необхідній кількості примірників, які підписуються ДЕТ і завіряються печаткою органу державної влади, підприємства, установи, організації. РСО обліковує експертний висновок у журналі. Після підпису ДЕТ експертного висновку РСО приводить грифи обмеження доступу на матеріалах експертизи відповідно до прийнятого рішення за результатами проведення їх експертизи. Гриф обмеження доступу завіряється печаткою, підписом працівника РСО з розшифруванням його посади. При цьому зазначається реєстраційний номер та дата експертного висновку, на підставі якого проставлено гриф обмеження доступу. Експертний висновок у необхідній кількості примірників надсилається на реєстрацію до СБУ та для опрацювання на предмет його відповідності вимогам законодавства і за його результатами приймає рішення щодо його реєстрації. У разі невідповідності експертного висновку вимогам законодавства СБУ повертає його без реєстрації. Після прийняття рішення щодо реєстрації експертного висновку, один його примірник залишається в СБУ, інші надсилаються на адресу ДЕТ.

Після надходження зареєстрованого в СБУ експертного висновку РСО у місячний термін письмово повідомляє про прийняте рішення щодо розсекречування або зміну ГС матеріалів експертизи керівників органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, яким були передані такі МНСІ, чи на зберіганні у яких вони знаходяться.

У разі потреби ДЕТ надсилає експертний висновок та матеріали експертизи ініціатору експертизи (якщо не визначено іншого).

Розділ 2. СПОСОБИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ В ІНОЗЕМНИХ КРАЇНАХ

2.1. Визначення шкоди внаслідок розголошення державної таємниці в Російській Федерації

Система органів захисту державної таємниці

Законодавче визначення поняття інформації наведено у Законі РФ «Про інформацію, інформатизацію і захист інформації», чинному з лютого 1995 р. Відповідно до цього закону, *інформація* – це «відомості про осіб , предмети, факти , події, явища і процеси незалежно від форми їх подання». ДТ є одним з видів інформації, тому необхідно враховувати всі особливості при захисту ДТ, як інформації унікального феномену. Визначення поняття «ДТ» дано в Законі РФ «Про державну таємницю» .

Державна таємниця (ДТ) – захищені відомості у його військової, зовнішньополітичної, економічної, розвідувальної , контррозвідувальної та оперативно-розшукової діяльності, поширення яких може завдати шкоди безпеці РФ (ст. 2 Закону РФ від 21 липня 1993 «Про державну таємницю») .

З цього визначення випливає, що до ДТ відносяться відомості , що задовольняють таким *ознакам*:

по-перше, – відомості у строго встановлених сферах діяльності держави (військової, зовнішньополітичної, економічної, розвідувальної, контррозвідувальної та оперативно-розшукової діяльності);

по-друге, – відомості, що не відомі широкому, точніше - невизначеному неконтрольованого колу осіб, і, що представляють цінність саме в силу такої невідомості;

по-третє, – відомості , поширення яких може завдати шкоди безпеці РФ. Слід підкреслити, що збиток стосується не окремих фізичних чи юридичних осіб, а держави в цілому. При цьому величина збитку така, що впливає на безпеку держави;

по-четверте, – відомості, щодо яких вживаються спеціальні заходи захисту, спрямовані на запобігання їх неконтрольованого розповсюдження.

При наявності всіх чотирьох ознак відомості відносяться до ДТ.

Носіями відомостей, що становлять ДТ, можуть бути матеріальні об’єкти, у тому числі фізичні поля, у яких відомості, що становлять ДТ, знаходять своє відображення у вигляді символів, образів, сигналів, технічних рішень і процесів.

Деякі приклади таких носіїв:

- паперові документи ;

- магнітні носії інформації в електронно-обчислювальній машині;

- електромагнітне поле, створюване радіостанцією при передачі інформації;

- фізичні прояви об'єктів (зразків зброї, промислових підприємств та інші), що мають охоронювані відомості, у вигляді різноманітних полів і слідів діяльності;

- та інші носії .

Особливу роль, як носії відомостей, в сучасних умовах мають технічні засоби збору, передачі, обробки, зберігання та інформації. З їх використанням обробляється майже 100 % інформації, що становить ДТ. При безсумнівних перевагах таких носіїв, їх негативною рисою є вразливість для широкого спектру загроз несанкціонованого розповсюдження інформації, що захищається. До захисту інформації на таких носіях приділяється особливе значення.

Слід відмітити, що людина у чинному Законі РФ «Про державну таємницю» не розглядається як специфічний носій відомостей, хоча він у своїй пам'яті і зберігає ці відомості. Тим самим людина не ставиться на один рівень з технічними носіями. Людина у проблемі забезпечення захисту ДТ розглядається як суб'єкт суспільних відносин, що виникають у процесі захисту ДТ.

Забезпечення інформаційної безпеки є однією з складових частин суперництва (конфлікту, боротьби) в інформаційній сфері. Іншою складовою частиною цього суперництва є вплив на інформаційну сферу суперника. Обидві із зазначених складових частин інформаційного суперництва взаємопов'язані і являють собою активну і пасивну компоненту системи заходів щодо забезпечення національної безпеки в інформаційній сфері.

Основними напрямками діяльності щодо забезпечення інформаційної безпеки є:

- виявлення загроз інформаційної безпеки та їх джерел;

- формування , накопичення і раціональне управління державними інформаційними ресурсами;

- забезпечення інформаційних прав особистості, суспільства, органів державної влади, їх захист від негативних інформаційних впливів;

- захист інформації, віднесеної у законному порядку до категорії обмеженого доступу (що становить таємницю), від загроз її витоку до недружніх суб'єктів;

- захист інформації (незалежно від категорії доступу до неї та форми подання) від загроз небажаних несанкціонованих і ненавмисних впливів на інформацію.

Роль і місце забезпечення інформаційної безпеки в інформаційному суперництві представлено на рис. 2 [68].

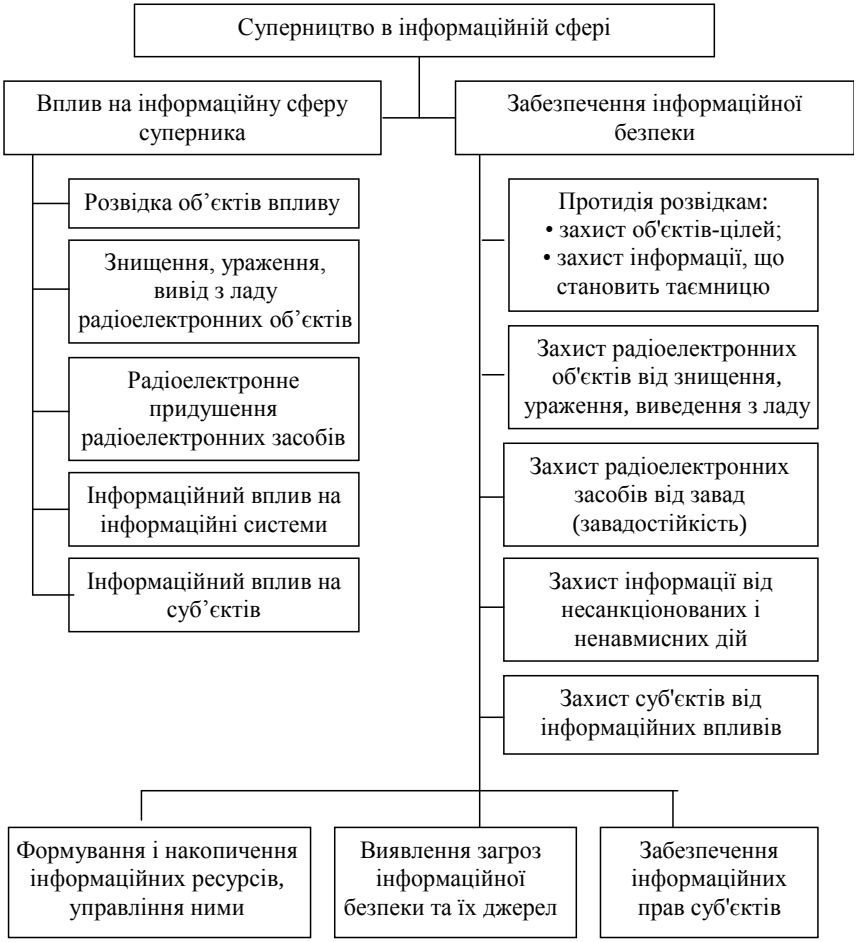


Рис. 2. Роль і місце забезпечення інформаційної безпеки в інформаційному суперництві

Різноплановість і взаємозв’язок напрямків діяльності щодо забезпечення інформаційної безпеки і складність науково-технічних і соціально-економічних проблем у цій сфері потребує скоординованих дій щодо їх вирішення. Така координація здійснюється *Міжвідомчою комісією з інформаційної безпеки Ради безпеки РФ*.

Важливою складовою частиною інформаційної безпеки є захисту інформації, що становить державну таємницю. Тому питання захисту державної таємниці постійно перебувають у полі зору Міжвідомчої комісії з інформаційної безпеки періодично, обговорюються на засіданнях і знаходять своє відображення в рішеннях Ради безпеки РФ.

Відповідно до Закону РФ «Про безпеку» на міжвідомчі комісії і апарат Ради безпеки РФ (у тому числі на міжвідомчу комісію з інформаційної безпеки, у сфері її компетенції) покладаються:

- оцінка внутрішніх і зовнішніх загроз життєво важливим інтересам об'єктів безпеки, виявлення джерел небезпеки;
- підготовка науково обґрунтованих прогнозів зміни внутрішніх і зовнішніх умов і факторів, що впливають на стан безпеки РФ;
- розробка та координація федеральних програм щодо забезпечення безпеки РФ і оцінка їх ефективності;
- накопичення, аналіз і обробка інформації про функціонування системи забезпечення безпеки РФ, вироблення рекомендацій щодо її вдосконалення;
- інформування Ради безпеки РФ про хід виконання його рішень;
- організація наукових досліджень у галузі забезпечення безпеки;
- підготовка проектів рішень Ради безпеки РФ, а також проектів указів Президента РФ з питань безпеки;
- підготовка матеріалів для доповіді Президента РФ Верховній Раді РФ про забезпечення безпеки РФ.

Міжвідомча комісія із захисту ДТ РФ (МВК РФ) – колегіальний орган, основною функцією якого є координація діяльності федеральних органів державної влади та органів державної влади суб'єктів РФ щодо захисту ДТ в інтересах розробки та виконання державних програм, нормативних та методичних документів, які забезпечують реалізацію федерального законодавства про ДТ.

МВК РФ утворена відповідно до Закону РФ «Про державну таємницю» та Указом Президента РФ «Про Міжвідомчу комісію із захисту ДТ».

МВК РФ при здійсненні своєї діяльності має право:

- формувати перелік посадових осіб органів державної влади, які наділяються повноваженнями щодо віднесення відомостей до ДТ;
- формувати перелік відомостей, віднесених до ДТ;
- надавати пропозиції щодо організації розроблення та виконання державних програм, нормативних та методичних документів, які забезпечують реалізацію федерального законодавства про ДТ, і представляти їх у встановленому порядку до Уряду РФ;
- розглядати і подавати в установленому порядку Президентові і Уряду РФ пропозиції щодо правового регулювання питань захисту ДТ та удосконалення системи захисту ДТ в РФ;
- визначати порядок розсекречення носіїв відомостей, що становлять ДТ, у разі ліквідації організації - фондоутворювача і відсутності її правонаступника;
- організовувати роботу міжвідомчих експертних груп з

розсекречення і продовженню термінів засекречування документів КПРС, Уряду СРСР та інших архівних документів у разі відсутності організації - фондоутворювача та її правонаступника;

- розглядати у випадках, передбачених Законом РФ «Про державну таємницю», запити органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій та громадян про розсекречення відомостей, віднесених до ДТ;

- підготовлювати експертні висновки на документи, що містять відомості, віднесені до ДТ, з метою вирішення питання про можливість передачі зазначених відомостей іншим державам і представляти ці висновки у встановленому порядку в Уряд РФ для прийняття рішення;

- приймати рішення про передачу органом державної влади, органом місцевого самоврядування, підприємством, установою та організацією відомостей, що становлять ДТ, у випадках зміни їх функцій, форм власності, ліквідації або припинення робіт, пов'язаних з використанням відомостей, що становлять ДТ, іншому органу державної влади, органу місцевого самоврядування, підприємству, установі, організації;

- готувати і подавати в установленому порядку до Уряду РФ пропозиції щодо порядку визначення розмірів шкоди, що може бути нанесено безпеці РФ внаслідок несанкціонованого поширення відомостей, що становлять ДТ, а також збитку, що наноситься підприємствам, установам, організаціям і громадянам у зв'язку з засекречуванням інформації, що знаходиться у їх власності;

- готувати і подавати в установленому порядку до Уряду РФ пропозиції до правил віднесення відомостей, що становлять ДТ, до різних СС;

- розглядати за дорученнями Президента та Уряду РФ експертні висновки з метою визначення розмірів можливої шкоди, яку може бути нанесено безпеці РФ внаслідок несанкціонованого поширення відомостей, що становлять ДТ, а також шкоди, завданої підприємствам, установам, організаціям і громадянам у зв'язку з засекречуванням інформації, що знаходиться у їх власності;

- розглядати за дорученнями Президента та Уряду РФ проекти міжнародних договорів РФ про спільне використання та захист відомостей, що становлять ДТ, надавати відповідні пропозиції та експертні висновки, брати участь у міжнародному співробітництві з цих питань;

- давати висновки на рішення керівників органів державної влади, пов'язані із зміною діючих в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях переліків відомостей, що підлягають засекречуванню, які можуть призвести до зміни переліку відомостей, віднесених до ДТ, припиняти чи опротестовувати їх вирішення;

- координувати роботи з організації сертифікації засобів захисту інформації;

- координувати в установленому порядку щодо проведення робіт з ліцензування діяльності підприємств, установ і організацій, пов'язаної з використанням відомостей, що становлять ДТ, створенням засобів захисту інформації, а також здійсненням заходів та (або) наданням послуг із захисту ДТ;

- вирішувати питання про продовження 30-річного терміну засекречування відомостям, що становлять ДТ;

- розглядати за дорученнями Президента та Уряду РФ інші питання відповідно до Закону РФ «Про державну таємницю».

До МВК РФ входять керівники федеральних органів виконавчої влади, Адміністрації Президента РФ, Апарату Уряду РФ або їх заступники. Склад МВК за посадами затверджується Президентом, а персональний склад – Урядом РФ.

Відповідальним секретарем МВК за посадою є заступник голови Державної технічної комісії при Президентові РФ. Організаційно-технічне забезпечення діяльності МВК здійснює центральний апарат Державної технічної комісії, у якому створюється структурний підрозділ для виконання цих функцій.

Голова МВК РФ:

- запитує та одержує в установленому порядку від державних органів, органів місцевого самоврядування, підприємств, установ, організацій, посадових осіб і громадян необхідні для здійснення діяльності МВК інформацію, документи і матеріали;

- створює міжвідомчі робочі та експертні групи для забезпечення діяльності МВК;

- залучає на договірній основі державні та недержавні підприємства, організації та установи, а також окремих фахівців для виконання аналітичних, дослідницьких та експертних робіт.

Рішення МВК РФ, прийняті відповідно до її повноважень є обов'язковими для виконання органам державної влади, органам місцевого самоврядування, підприємствам, установам, організаціям, посадовим особам та громадянам.

Члени МВК мають рівні права при прийнятті рішення. У разі незгоди з прийнятим рішенням кожен член МВК РФ має право викласти письмово свою окрему думку з даного питання, яке підлягає обов'язковому внесенню до протоколу засідання.

Рішення не може бути прийнято у разі незгоди з ним, що представляє федеральний орган державної влади, Адміністрацію Президента РФ, Генеральної прокуратури РФ, до чиєї компетенції у відповідності з федеральним законодавством віднесено аналізований

питання. Таким чином члени МВК РФ можуть накласти вето на прийняте рішення.

Рішення при необхідності представляють Президенту РФ, Уряду РФ, а також (у частині, що їх стосується) до органів державної влади, органів державної влади суб'єктів РФ, органів місцевого самоврядування, на підприємства, установи та організації незалежно від їх організаційно-правових форм та форм власності. Як правило, рішення МВК РФ направляються у федеральні органи державної влади та органи державної влади суб'єктів РФ.

При необхідності за рішеннями МВК РФ можуть розроблятися проекти указів і розпоряджень Президента РФ, постанов і розпоряджень Уряду РФ, які подаються на розгляд у встановленому порядку. Наприклад, з питань ліцензування діяльності у сфері захисту ДТ, сертифікації засобів захисту інформації приймаються рішення МВК РФ, а потім розробляються і приймаються постанови Уряду.

Федеральна служба безпеки РФ (ФСБ РФ) – є федеральним органом виконавчої влади. Повноваження ФСБ РФ в області віднесення відомостей до ДТ та їх захисту відображені у Законі РФ «Про органи Федеральної служби безпеки в Російській Федерації».

Органи ФСБ являють собою єдину централізовану систему, до якої входять:

1) ФСБ РФ;

2) управління (відділи) ФСБ РФ в окремих регіонах і суб'єктах РФ (територіальні органи безпеки), наприклад, Управління ФСБ по Воронезькій області;

3) управління (відділи) ФСБ РФ в Збройних Силах РФ, військах та інших військових формуваннях, а також в їх органах управління (органи безпеки у військах) .

ФСБ РФ створює територіальні органи безпеки і органи безпеки у військах, здійснює керівництво ними і організує їх діяльність, видає у межах своїх повноважень нормативні акти і безпосередньо реалізує основні напрями діяльності органів ФСБ. Структура та організація діяльності ФСБ РФ визначаються положенням про ФСБ РФ, затверджується Президентом РФ.

Територіальні органи безпеки і органи безпеки у військах перебувають у прямому підпорядкуванні ФСБ РФ.

Органи ФСБ у своєму підпорядкуванні мають підприємства, навчальні заклади, науково-дослідні, експертні і військово-медичні установи та підрозділи, військово-будівельні підрозділи, центри спеціальної підготовки, а також підрозділи спеціального призначення.

Діяльність органів ФСБ здійснюється за такими основними напрямками:

- контррозвідувальна діяльність;

- боротьба зі злочинністю.

Розвідувальна діяльність, інші напрямки діяльності органів ФСБ визначаються законами РФ.

Контррозвідувальна діяльність – це діяльність органів ФСБ у межах своїх повноважень щодо виявлення, попередження, припинення розвідувальної та іншої діяльності спеціальних служб і організацій іноземних держав, а також окремих осіб, спрямованої на нанесення шкоди безпеці РФ.

Підставами для здійснення органами ФСБ контррозвідувальної діяльності, пов'язаної із захистом ДТ, є:

а) наявність даних про ознаки розвідувальної та іншої діяльності спеціальних служб і організацій іноземних держав, а також окремих осіб, спрямованої на нанесення шкоди безпеці РФ;

б) необхідність забезпечення захисту відомостей, що становлять ДТ.

ФСБ РФ у відповідності з федеральним законодавством здійснює такі функції із захисту ДТ:

- організовує виконання федеральних законів, інших нормативних правових актів федеральних органів державної влади в органах ФСБ;

- організує і здійснює у межах своїх повноважень контррозвідувальну діяльність, визначає порядок проведення контррозвідувальних заходів та використання негласних методів та засобів при їх здійсненні, а також встановлює порядок здійснення органами ФСБ проникнення в спеціальні служби та організації іноземних держав;

- здійснює в межах своїх повноважень отримання, обробку, аналіз і реалізацію інформації про загрози безпеки РФ, а також прогнозування цих загроз;

- бере участь у розробці та реалізації заходів щодо забезпечення інформаційної безпеки держави, захисту відомостей, що становлять ДТ, у ліцензуванні діяльності підприємств, установ і організацій, пов’язаних з використанням відомостей, що становлять ДТ, наданням послуг із захисту ДТ; визначає основні напрями діяльності органів ФСБ у цих сферах;

- здійснює контроль за забезпеченням захисту відомостей, що становлять ДТ, в державних органах, військових формуваннях, на підприємствах, в установах та організаціях;

- в установленому порядку здійснює заходи, пов’язані з допуском громадян до відомостей, що становлять ДТ, а також з прийомом на військову службу (роботу) до органів ФСБ;

- організує і здійснює шифрувальні роботи в органах ФСБ, а також контроль за дотриманням РС при поводженні з шифрованого

інформацією у шифрувальних підрозділах державних органів, військових формувань, підприємств, установ і організацій (за винятком установ РФ, що знаходяться за її межами);

- видає сертифікати якості на окремі види спеціальних технічних засобів, у тому числі – засобів захисту інформації.

З метою вирішення завдань забезпечення безпеки РФ військовослужбовці органів ФСБ можуть бути прикомандировані до державних органів, підприємств, установ та організацій незалежно від форм власності.

Міністерство оборони РФ (МО РФ) - є одним з основних власників відомостей, що становлять ДТ і виконує ряд специфічних функцій, пов'язаних із її захистом. Функції МО РФ у сфері захисту ДТ визначені Законом РФ «Про оборону», Положенням про МО РФ, низкою постанов Уряду РФ.

До таких із функцій відносяться:

- ліцензування діяльності підпорядкованих йому підприємств по допуску до проведення робіт, пов'язаних з використанням відомостей, що становлять ДТ;

- сертифікація засобів захисту інформації за вимогами безпеки інформації в інтересах міністерства в рамках системи сертифікації № РОСС RU 0001.01 ГШОО;

- міжвідомчий контроль стану захисту інформації на підприємствах, в установах і організаціях, що виконують роботи за замовленнями Міністерства оборони.

Кормі того, МО РФ, у частині забезпечення захисту інформації, що становить ДТ:

- розробляє державні довготривалі програми озброєння і розвитку військової техніки, у тому числі – засобів захисту інформації для потреб оборони, а також пропозиції щодо щорічного державного оборонного замовлення;

- координує і фінансує роботи, що виконуються з метою оборони;

- організовує наукові дослідження з метою оборони, замовляє і фінансує на договірній основі науково-дослідні і дослідно-конструкторські роботи у галузі оборони;

- замовляє і фінансує виробництво та закупівлю озброєння і військової техніки, для Збройних Сил РФ, інших військ, військових формувань і органів у межах виділених на ці цілі коштів;

- координує замовлення на озброєння та військову техніку для інших військ, військових формувань і органів з метою уніфікації озброєння і військової техніки.

Служба зовнішньої розвідки РФ (СЗР РФ) – є одним з органів зовнішньої розвідки РФ і складовою частиною сил забезпечення безпеки

РФ (відповідно до Закону РФ «Про зовнішню розвідку».

Цій службі надаються такі повноваження (у сфері захисту державної таємниці та інформації) :

- організація та забезпечення у межах своєї компетенції захисту ДТ в установах РФ, що знаходяться за межами території РФ, включаючи визначення порядку здійснення фізичного та інженерно-технічного захисту зазначених установ, заходів щодо запобігання витоку по технічних каналах відомостей, що становлять ДТ;

- забезпечення власної безпеки, тобто захист своїх сил, засобів і інформації від протиправних дій та загроз.

Для здійснення своєї діяльності СЗР може при власному ліцензуванні та сертифікації набувати, розробляти (за винятком криптографічних засобів захисту), створювати, експлуатувати інформаційні системи, системи зв'язку та системи передачі даних, а також засоби захисту інформації від витоку технічними каналами.

Державна технічна комісія при Президенті РФ (ДТК РФ) – федеральний орган виконавчої влади, що здійснює міжгалузеву координацію і функціональне регулювання діяльності щодо забезпечення захисту (не криптографічними методами) інформації, містить відомості, що становлять державну або службову таємницю:

- від її витоку технічними каналами;

- від несанкціонованого доступу до неї ,

- від спеціальних впливів на інформацію з метою її знищення, спотворення і блокування;

- і з протидії технічним засобам розвідки на території РФ (ТЗІ).

ДТК РФ організує діяльність державної системи захисту інформації в РФ від технічних розвідок і від її витоку технічними каналами.

ДТК та регіональні центри входять до складу державних органів забезпечення безпеки РФ.

Накази, розпорядження та вказівки ДТК РФ, видані в межах її компетенції, є обов'язковими для виконання апаратами федеральних органів державної влади та органів державної влади суб'єктів РФ, федеральними органами виконавчої влади, органами виконавчої влади суб'єктів РФ, органами місцевого самоврядування, підприємствами, установами та організаціями .

Членами колегії ДТК РФ за посадою є керівні працівники федеральних органів виконавчої влади, державних органів і організацій РФ відповідно до переліку, затвердженого Президентом РФ.

ДТК РФ у межах своїх повноважень є державним замовником з проведення загальносистемних наукових досліджень у галузі ТЗІ, а також з розробки та виробництва технічних засобів захисту інформації загального застосування і засобів контролю ефективності цього захисту.

Основними завданнями ДТК РФ є:

- проведення єдиної державної політики в галузі ТЗІ;
- здійснення міжгалузевої координації та функціонального регулювання діяльності щодо забезпечення ТЗІ в апаратах органів державної влади РФ органів державної влади суб'єктів РФ, федеральних органах виконавчої влади, органах виконавчої влади суб'єктів РФ, органах місцевого самоврядування, на підприємствах, в установах і організаціях;
- прогнозування розвитку сил, засобів і можливостей технічних розвідок, виявлення загроз безпеки інформації;
- протидія добування інформації технічними засобами розвідки, запобігання витоку інформації технічними каналами, несанкціонованому доступу до неї, спеціальних дій на інформацію з метою її знищення, спотворення і блокування;
- контроль у межах своїх повноважень діяльності з ТЗІ в апаратах федеральних органів державної влади та органів державної влади суб'єктів РФ, федеральних органах виконавчої влади, органах виконавчої влади суб'єктів РФ, органах місцевого самоврядування, на підприємствах, в установах та організаціях;
- здійснення організаційно-технічного забезпечення діяльності МВК із захисту ДТ центральним апаратом ДТК.

Органи державної влади, підприємства, установи та організації забезпечують захист відомостей, що становлять ДТ, відповідно до покладених на них завдань і в межах своєї компетенції.

Відповідальність за організацію захисту відомостей, що становлять ДТ, в органах державної влади, на підприємствах, установах і організаціях покладається на їх керівників. Залежно від обсягу робіт з використанням відомостей, що становлять ДТ, керівниками органів державної влади, підприємств, установ і організацій створюються структурні підрозділи з захисту ДТ, функції яких визначаються зазначеними керівниками відповідно до нормативних документів, які затверджуються Урядом РФ, і з урахуванням специфіки проведених ними робіт.

Захист ДТ є видом основної діяльності органу державної влади, підприємства, установи або організації.

Переліковий підхід до організації захисту державної таємниці

У більшості розвинених країн світу діє «переліковий» підхід до організації захисту ДТ [68]. Правовою базою для засекречування конкретних відомостей при такому підході є Переліки відомостей, що

визначають класи і категорії інформації, що відносяться до ДТ (або ЗВДТ). Такі переліки визначають – що необхідно захищати. Крім того, переліки використовуються для встановлення предмета злочинного посягання при розслідуванні випадків шпигунства, розголошення відомостей, втрати документів, що містять СІ.

На даний час в РФ існують як відкриті, так і закриті (з обмеженим доступом) переліки відомостей. Відкритими переліками є наведений у Законі РФ «Про державну таємницю» [63] *Перелік відомостей , що становлять ДТ*, а також затверджується Указом Президента РФ *Перелік відомостей, віднесених до ДТ*. Крім того, існують *відомчі переліки відомостей, що підлягають засекречуванню*, які можуть бути як відкритими, так і закритими.

Чим обумовлена необхідність розробки таких переліків?

1. Складністю процедури прийняття рішення про віднесення відомостей до ДТ.

При прийнятті такого рішення необхідно відповісти на наступні питання: Наноситься чи шкоди державній безпеці при поширенні інформації? Чи реалізовано скритність інформації про об'єкти, і яка буде надійність цієї скритності? Яка буде величина втрат у вигляді витрат на захист інформації та упущеної вигоди внаслідок її вилучення із звичайного цивільного обороту? Перевершує чи запобігає збиток при засекречування відомостей виникають при цьому витрати?

Для оцінки очікуваних наслідків засекречування або вільного поширення інформації необхідно залучати експертів найвищої кваліфікації, використовувати складні математичні моделі. Ці наслідки можуть виявлятися в різних сферах діяльності держави: військової, економічної, політичної, соціальної та інших. Необхідно також вміти зважувати, здавалося б, непорівнянні величини – якісні судження експертів до наслідків прийнятих рішень.

2. Багатократністю прийняття рішення про засекречування одних і тих же відомостей та їх носіїв у різних ситуаціях.

Відомості, віднесені до ДТ, мають певну сферу розповсюдження і використання. Вони можуть міститися в інформації, представленої на різних носіях з різним ступенем детальності розкриття відомостей. Кожен з таких носіїв повинен мати гриф, відповідний ступеню секретності міститься на ньому інформації. Таким чином, рішення про засекречування відомостей приймається багаторазово різними людьми в різних ситуаціях. При цьому важливо забезпечити однаковість прийнятого рішення з одного й того ж відома.

3. Необхідністю встановлення єдиних вимог щодо захисту відомостей в різних ситуаціях їх використання, диференційованих залежно від ступеня їх секретності. Для цього відомості повинні бути

легко ідентифіковані.

Переліковий підхід до організації захисту ДТ реалізується у вигляді *системи переліків* :

1) Переліку відомостей, що становлять ДТ.

2) Переліку відомостей, віднесених до ДТ.

3) Розгорнутих переліків відомостей, що підлягають засекречування в органі державної влади.

4) Переліків відомостей, що підлягають засекречуванню, на підприємстві, в установі та організації.

Таким чином, переліки відомостей (що становлять ДТ, віднесених до ДТ, що підлягають засекречуванню) складають правову та інформаційну основу процесу захисту цих відомостей.

Склад і взаємозв'язок використовуваних при захисті ДТ переліків відомостей представлені на рис. 3 [68].

Рис. 3. Склад і взаємозв'язки системи переліків відомостей

Перелікові системи засекречування відомостей існують також в США, ФРН, Франції, Японії та інших країнах.

У США порядок засекречування відомостей полягає в наступному:

- директивою президента США визначені відомості, які підлягають засекречування;
- встановлені персони, які можуть дозволяти іншим особам визначати СС інформації. Таких ступенів встановлено три: «ЦТ» - відповідає особливо тяжкому збитку при розкритті відомостей; «Т» - серйозному збитку; «конфіденційно» - помітному збитку;
- особа, яка має право визначати таємність одного ступеня, може визначати таємність будь нижчого ступеня. Число осіб, які мають право визначати СС інформації, обмежена і складає долі відсотка від числа осіб, допущених до СС;
- на кожному документі має бути зазначено ім'я особи, що встановила його СС;
- одне з правил, рекомендованих в США при засекречуванні (розсекреченні) полягає у тому, що будь-які сумніви у відповідності СС інформації повинні бути дозволені у бік нижчого рівня або, у разі конфіденційної інформації, вона повинна бути незасекреченою;
- якщо розкриття інформації може бути дозволено, воно повинно бути дозволено.

Раніше (до жовтня 1993р.) існувало правило: якщо вимога про розкриття інформації може бути відхилене на законних підставах, воно має бути відхилено.

Таким чином, принципова відмінність засекречування документів (відомостей) в РФ і США полягає у наступному:

в РФ СС визначає особа, яка отримала зведення (яке розробило документ), відповідно до діючого переліку відомостей, що підлягають засекречуванню;

в США СС відомостей (документів) визначають тільки особи, які мають на це право.

Критерії віднесення відомостей до державної таємниці

Змістовною основою робіт по захисту СІ є *розгорнуті переліки відомостей , що підлягають засекречуванню*. Саме в них закріплюється рішення осіб, наділених повноваженнями щодо віднесення відомостей до ДТ. На основі цих переліків Міжвідомча комісія РФ щодо захисту ДТ формує *Перелік відомостей, віднесених до ДТ*. Тому важливо розглянути критерії прийняття рішення про включення відомостей до розгорнутих переліків відомостей. Таке рішення приймається з урахуванням таких факторів.

Інформація як один з ресурсів діяльності держави, суспільства і громадян має певну тривалість свого активного періоду життєвого циклу, протягом якого вона є актуальною. На початку життєвого циклу (при виникненні нових знань) відбувається поступове зростання потреб в інформації та її вплив на діяльність держави, суспільства і громадян. Потім настає період найбільш активного використання цієї інформації і, нарешті, інформація поступово старіє і втрачає свою цінність як ресурс. Ілюстрація [68] зміна потреби в інформації та інтегрального ефекту від її використання за час життєвого циклу інформації представлена на рис. 4.

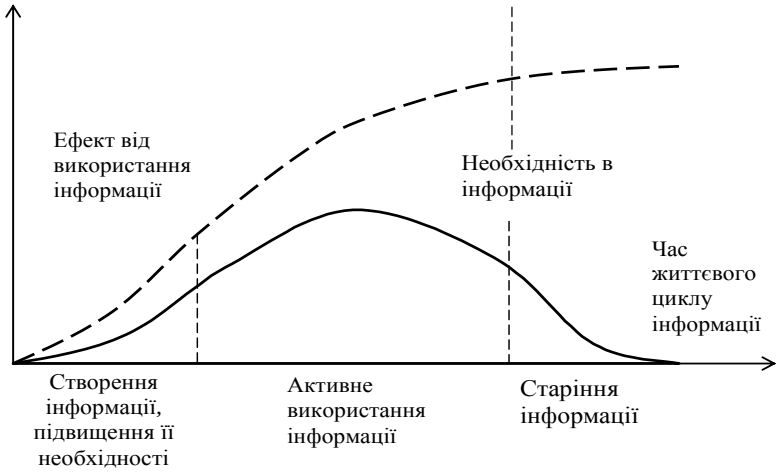


Рис. 4. Рміна потреби в інформації та інтегрального ефекту від її використання за час життєвого циклу інформації

Ефективність використання інформації як ресурсу значною мірою визначається обраним режимом її поширення. При вільному поширенні (відмову від її засекречування) повністю реалізуються переваги відкритого використання інформації у різних сферах діяльності держави, суспільства та громадян. Але при цьому національній безпеці РФ може бути завдано шкоди внаслідок того, що найбільш важливі відомості стануть передчасно відомі недружньої країні, юридичним чи фізичним особам.

Величина цієї шкоди залежить від моменту часу, коли інформація стала відома недружній стороні. Процес нанесення шкоди вимагає відповідної підготовки і займає деякий проміжок часу. Наприклад, отримавши інформацію про нову технологію, конкурент повинен цю технологію освоїти і тиражувати, що б вона стала досить ефективною. Причому, чим раніше настає етап вільного поширення інформації, тим більше можуть бути розміри можливої шкоди.

Ілюстрації зміни величини можливої шкоди в залежності від часу розкриття інформації представлені на рис. 5 [68].

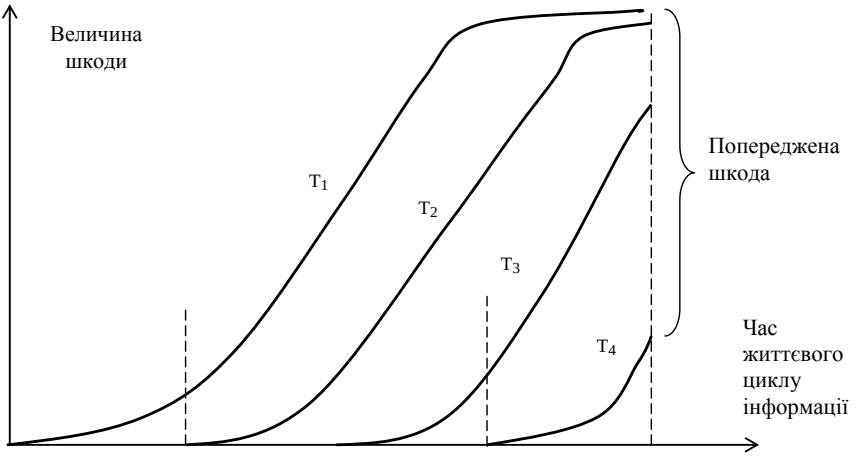


Рис. 5. Зміни величини можливої шкоди в залежності від часу (T_1, T_2, T_3, T_4) розкриття інформації

При засекречування відомостей позитивними наслідками цього акта є запобігання шкоди національній безпеці РФ. Однак при цьому знижується величина вигоди від використання інформації та необхідні додаткові витрати на захист такої інформації.

Ілюстрації зміни величини вигоди від використання інформації в залежності від часу розкриття інформації представлені на рис. 6 [68].

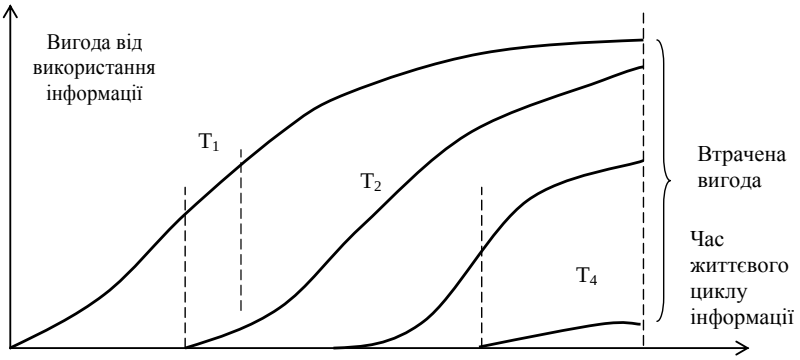


Рис. 6. Зміна величини вигоди від використання інформації в залежності від часу (T_1, T_2, T_3, T_4) розкриття інформації

Таким чином держава, суспільство і громадяни несуть витрати, що залежать від строку засекречування у вигляді витрат на захист СІ та упущеної вигоди від обмежень на вільне її поширення і використання.

З точки зору забезпечення найбільш ефективного використання інформації за час її життєвого циклу необхідно вибрати таку схему поширення інформації і таким чином змінювати її в часі, що б інтегральний ефект від використання інформації з урахуванням позитивних і негативних наслідків досягав би максимальної величини. Засекречування інформації при такому підході є способом управління національним інформаційним ресурсом з метою досягнення максимального інтегрального ефекту від його використання. Оцінка позитивних і негативних наслідків, а також інтегрального ефекту реалізації обраної схеми розповсюдження інформації являє собою значні труднощі. Необхідно мати на увазі, що збитки, вигоди та витрати, що відповідають обраній схемі поширення інформації, можуть виявлятися в різних сферах діяльності держави, оцінюватися різними шкалами і одиницями виміру. Для визначення інтегрального ефекту від використання інформації необхідно привести різні приватні оцінки до єдиної шкали, у якості якої може бути вартісна характеристика цих величин.

Також необхідно враховувати, що в силу різних важко передбачуваних обставин розміри збитків і вигод, можливості і час їх появи можуть бути точно не відомі. Також не завжди можливо отримати кінцеву оцінку витрат на захист відомостей. Тому прийняття рішення про засекречування відомостей об'єктивно здійснюється в умовах значної невизначеності.

Залежно від ступеня цієї невизначеності в теорії прийняття рішень використовуються різні критерії. При повній визначеності наших знань відносно факторів, що впливають на рішення, і відсутності випадковостей, рішення про доцільну схему поширення інформації приймається безпосередньо по максимуму величини інтегрального ефекту від використання інформації.

Вираз для оцінки цього ефекту може бути представлено наступним чином [68]:

$$E = V - U - Z, \qquad (2.1)$$

де V, U, Z – оцінки розмірів очікуваної вигоди, від вільного використання інформації (V), збитку від поширення (U) і витрат на захист (Z), за час життєвого циклу інформації, що відповідає обраної схемі поширення інформації.

При цьому необхідно мати на увазі, що якщо приватні оцінки (V, U,

Z) висловлюють відношення переваги, то не можна застосовувати звичайні операції (складати або знаходити різницю між ними).

З урахуванням визначення поняття ДТ, наведеного у Законі РФ «Про державну таємницю» [63] та виразу (2.1) критерій прийняття рішення про включення відомостей до розгорнутого переліку відомостей, що підлягають засекречуванню, формулюється таким чином.

Відомості підлягають включенню до відповідного переліку, якщо виконуються наступні умови:

а) вільне поширення цих відомостей може завдати шкоди національній безпеці РФ;

б) існують певні схеми обмеженого поширення відомості, ступінь їх секретності і тривалість (строк) засекречування, при яких ефект від використання цих відомостей перевищує ефект, що досягається при вільному їх поширенні, тобто

$$\begin{cases} U_0 \geq U_{\text{доп}}, \\ E_{\text{з}} - E_0 > 0, \end{cases} \tag{2.2}$$

де $U_{\text{доп}}$ – мінімальна величина шкоди від розповсюдження (поширення) відомостей, які вважаються суттєвими (важливими) з точки зору безпеки РФ; $E_{\text{з}}$, E_0 – оцінки інтегрального ефекту від використання відомостей при його засекречування і вільному розповсюдженні (поширенні).

Розкриваючи величини $E_{\text{з}}$ і E_0 у відповідності до (2.1) критерій прийняття рішення записується і формулюється таким чином:

$$\begin{cases} U_0 \geq U_{\text{доп}}, \\ (U_0 - U_{\text{з}}) - (V_0 - V_{\text{з}}) + Z > 0, \end{cases} \tag{2.3}$$

або

$$\begin{cases} U_0 \geq U_{\text{доп}}, \\ \Delta U_{\text{поп}} - \Delta V + Z > 0, \end{cases} \tag{2.4}$$

де U_0, $U_{\text{з}}$ – оцінки розмірів шкоди, яку може бути нанесено безпеці РФ при вільному розповсюдження (поширенні) відомостей (U_0) і при їх засекречуванні ($U_{\text{з}}$); V_0, $V_{\text{з}}$ – оцінки розмірів очікуваної вигоди при вільному поширенні відомостей (V_0) і при їх засекречуванні ($V_{\text{з}}$); $U_{\text{поп}}$ – величина попередженої шкоди при засекречуванні відомостей,

$$\Delta U_{\text{поп}} = U_0 - U_з; \qquad (2.5)$$

ΔV – величина упущеної вигоди від засекречування відомостей,

$$\Delta V = V_0 - V_з. \qquad (2.6)$$

Таким чином, відомості підлягають включенню до відповідного переліку і доцільне їх засекречування, якщо :

- поширення цих відомостей може завдати шкоди безпеці РФ;

- існують певні схеми поширення відомостей, при їх СС і терміну засекречування, від яких величина попередженої шкоди у результаті засекречування перевищує сумарну величину упущеної вигоди від їх відкритого поширення (розповсюдження) і витрат на захист .

Якщо для аналізованих схем поширення відомостей можливе настання декількох випадкових результатів і відповідно до них збитків (шкоди), вигоди та витрат, для яких відомі оцінки ймовірностей їх виникнення, то рішення про засекречування відомостей приймається в умовах ризику. Існує два підходи до прийняття такого рішення.

Перший підхід полягає у виборі альтернативи з умови максимуму очікуваного інтегрального ефекту, що розраховується шляхом усереднення оцінок шкоди, вигоди і витрат з урахуванням ймовірностей їх появи. Даний підхід відображає позицію «об'єктивіст» і забезпечує виграш у середньому при великому числі повторень процедури прийняття рішення, коли число аналізованих відомостей досить велике. У разі часткової невідомості використовуються експертні оцінки величини шкоди, вигоди та витрат, а також ймовірностей їх появи.

Другий підхід враховує, що суб'єктивна оцінка небезпечної шкоди і корисної вигоди, на відміну від першого підходу, що не лінійно залежить від ймовірностей їх появи. Існують певні криві байдужості, відповідні сполученням величини шкоди (вигоди) і ймовірностям їх появи, при яких суб'єктивна оцінка небезпечної шкоди (корисної вигоди) не змінюється. У такому випадку для встановлення інтегрального ефекту від використання інформації необхідно оцінити величину сукупної шкоди (вигоди) за новою шкалою небезпеки (корисності), що враховує ймовірність їх появи. Тому для отримання інтегральних оцінок шляхом знаходження різниці між ними ці шкали повинні бути співставні.

Недоліком другого підходу, що ускладнює його практичне застосування при засекречуванні відомостей, є необхідність проведення додаткових досліджень експертних суджень для побудови кривих байдужості і шкали суб'єктивної небезпеки (корисності).

При повній невизначеності щодо ймовірностей можливої (шкоди, вигоди, витрат) можуть використовуватися максиміний критерій корисності, мінімаксний критерій ризику або критерій, що спирається на принципи недостатніх підстав (або умов).

Згідно максимінного критерію корисності засекречування відомостей доцільне, якщо поширення цих відомостей може завдати шкоди безпеці РФ, а мінімальна з можливих величин попередженої шкоди у результаті засекречування відомостей переважає сумарну величину максимально можливої упущеної вигоди від їх відкритого використання і витрат на захист. Даний критерій гарантує мінімальний інтегральний ефект від обраного режиму використання інформації. Якщо засекречування відомостей доцільне навіть у цьому найгіршому випадку, то в інших випадках воно буде тим більш доцільне.

Використання максимінного критерію ризику при засекречуванні відомостей дає той же результат, що й мінімаксний критерій, так як у даному випадку величини корисності та ризику прямо протилежні один одному.

При використанні принципу недостатніх підстав всі результати можливої шкоди, вигоди та витрат вважаються рівноімовірними, тому при оцінці інтегрального ефекту від використання відомостей повинні розраховуватись усереднені оцінки цих фіналів за умови рівної ймовірності їх виникнення.

Необхідно підкреслити, що при використанні наведених вище критеріїв *прогнозування розмірів шкоди, вигоди і витрат має здійснюватися на момент закінчення життєвого циклу розглянутої інформації*, коли вона втрачає свою цінність як ресурс. При цьому враховуються два етапи життєвого циклу інформації, що принципово відрізняються.

Під час першого етапу (при засекречуванні відомостей) позитивний ефект від засекречування полягає у попередженні можливої шкоди безпеки РФ, але при цьому держава, суспільство, особистість несуть втрати у вигляді витрат на захист відомостей та упущеної вигоди від обмежень на вільне поширення і використання цієї інформації. Причому, чим більша тривалість цього етапу, тим більша величина попередженої шкоди і величина втрат від засекречування відомостей.

Під час другого етапу (при розсекреченні відомостей) позитивний ефект від розсекречення відомостей полягає в отриманні вигоди від вільного поширення і використання цих відомостей, але при цьому інтересам РФ може бути завдано шкоди внаслідок того, що захищені раніше відомості стануть відомі не дружній країні, юридичним та фізичним особам. Причому, чим більше була тривалість періоду засекречування, тобто, чим далі настане момент розсекречування

інформації від початку її життєвого циклу, тим менша наноситься шкода інтересам РФ при знятті обмежень на доступ до цієї інформації і, у той же час, менше залишається можливостей отримання вигоди від вільного розповсюдження і використання даної інформації.

Ілюстративні залежності часу від величин шкоди (попередженої шкоди), вигоди (упущеної вигоди), витрат на захист відомостей і інтегрального ефекту від їх використання представлені на рис. 7 [68]. Аналіз цих залежностей дозволяє зробити наступні висновки.

Рішення про засекречування відомостей, основане тільки на оцінках запобігання шкоди, упущеної вигоди і витрат на їх захист, характерних для періоду засекречування, може призвести до надмірно великого терміну засекречування. У цьому випадку не береться до уваги позитивний ефект від вільного використання інформації при її розкритті.

Так само неправомірно приймати рішення про розсекречення відомостей, ґрунтуючись тільки на співвідношенні оцінок шкоди і вигоди при їх вільному розповсюдженні. У такому випадку виникає загроза того, що відомості будуть розкриті занадто передчасно, тому такий критерій не враховує позитивний ефект, що виникає на етапі засекречування відомостей. *Тому при оцінці доцільності засекречування необхідно враховувати обидва етапи життєвого циклу інформації та оцінки позитивного ефекту і втрат, отриманих для всього життєвого циклу інформації.*

На закінчення необхідно звернути увагу на те, що різні аналізовані відомості можуть бути взаємопов'язані. У даному випадку розкриття одних відомостей, може призвести до розкриття інших відомостей, пов'язаних з ними. Тому прийняття рішення про засекречування таких відомостей, виходячи з аналізу кожних відомостей в незалежності від інших відомостей, не припустимо. Щоб уникнути помилкових рішень, у цьому випадку доцільно розглядати відомості не ізольовано, а блоками взаємозалежних відомостей, і приймати рішення про їх засекречування з використанням вищенаведених критеріїв по всьому блоку аналізованих відомостей.

Правила віднесення відомостей, що становлять ДТ, до різних СС. Вище розглянуто формалізований підхід до віднесення відомостей до ДТ. Цей підхід покликаний допомогти особі, що приймає рішення про засекречування відомостей і їх СС, обґрунтувати це рішення. Однак, у кінцевому рахунку, посадова особа, яка приймає рішення керується особистим досвідом і якісними судженнями. Для забезпечення єдності критеріїв прийняття такого рішення постановою Уряду РФ затверджено «Правила віднесення відомостей , що становлять ДТ, до різних СС».

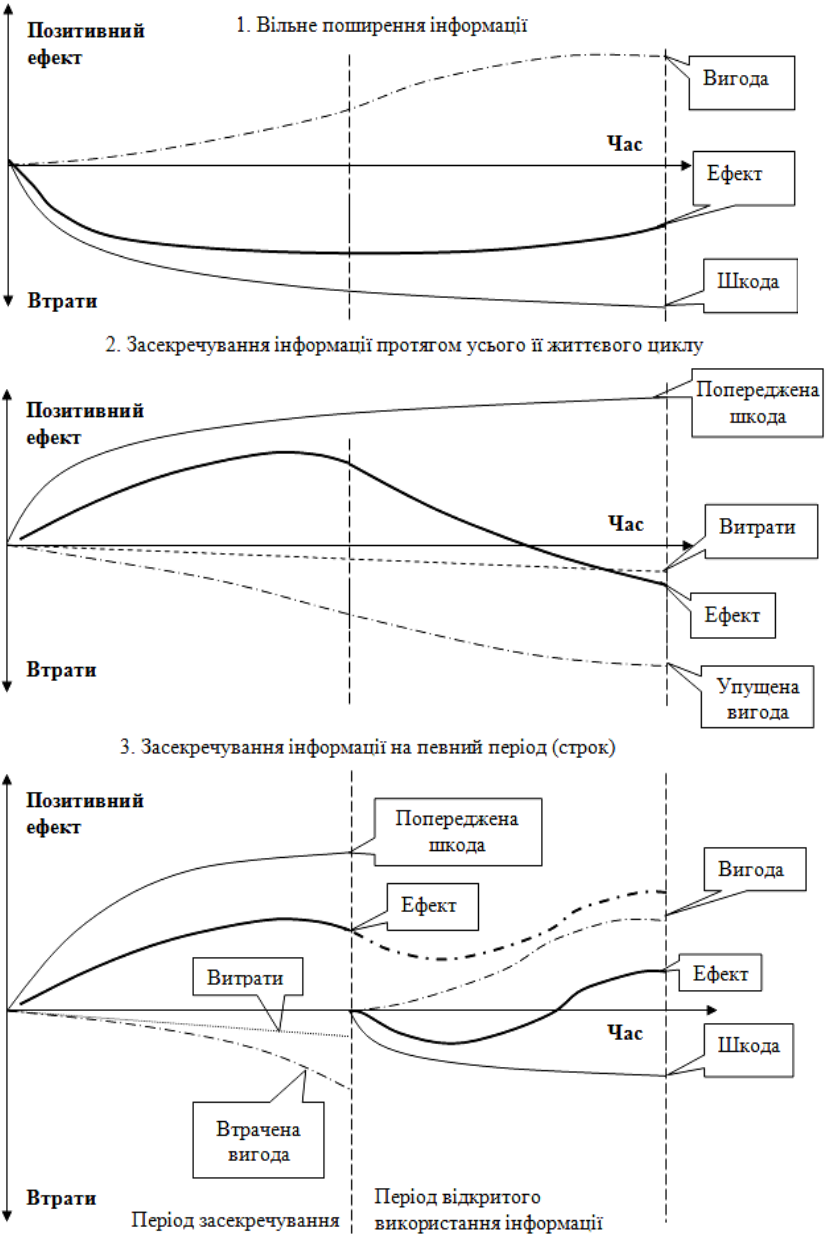


Рис. 7. Залежності часу від величини шкоди (попередженої шкоди), вигоди (упущеної вигоди), витрат на захист відомостей і інтегрального ефекту від поширення (використання) інформації

Основний зміст *Правил* ... полягає в наступному.

СС відомостей, що становлять ДТ, повинна відповідати ступеню тяжкості шкоди, що може бути нанесено безпеці РФ внаслідок поширення зазначених відомостей.

Кількісні та якісні показники шкоди безпеці РФ визначаються відповідно до нормативно-методичних документів, які затверджуються керівниками органів державної влади, які наділені повноваженнями щодо віднесення відомостей до ДТ, та погоджені з МВК із захисту ДТ.

До відомостей ОВ слід відносити відомості у військовій, зовнішньополітичній, економічній, науково-технічній, розвідувальній, контррозвідувальній та оперативно-розшуковій сфері діяльності, поширення яких може завдати шкоди інтересам РФ в одній або декількох з перерахованих сферах.

До ЦТ відомостей слід відносити відомості у військовій, зовнішньополітичній, економічній, науково-технічній, розвідувальній, контррозвідувальній та оперативно-розшуковій сфері діяльності, поширення яких може завдати шкоди інтересам міністерства (відомства) або галузі економіки РФ в одній або декількох з перерахованих сферах.

До Т відомостей слід відносити відомості з числа відомостей, що становлять ДТ. Шкодою безпеці РФ у цьому випадку вважається збиток, нанесений інтересам підприємства, установи або організації у військовій, зовнішньополітичній, економічній, науково-технічній, розвідувальній, контррозвідувальній та оперативно-розшуковій сфері діяльності.

Керівники органів державної влади, наділені повноваженнями щодо віднесення відомостей до ДТ, організують розроблення переліку і несуть персональну відповідальність за прийняті ними рішення про доцільність віднесення конкретних відомостей до ДТ.

Для розробки проекту переліку створюється ЕК, до складу якої включаються компетентні фахівці, що працюють з відомостями, що становлять ДТ.

У ході підготовки проекту переліку ЕК відповідно до принципів засекречування відомостей, встановленими Законом РФ «Про державну таємницю», проводять аналіз усіх видів діяльності відповідних органів державної влади, підприємств, установ та організацій з метою визначення відомостей, поширення яких може завдати шкоди безпеці РФ. Обґрунтування необхідності віднесення відомостей до ДТ із зазначенням відповідного СС здійснюється власниками цих відомостей і оформляється у вигляді пропозицій для включення у проект відповідного переліку.

СС відомостей, що знаходяться у розпорядженні кількох органів державної влади, встановлюється за взаємним погодженням між ними.

У перелік можуть бути включені відомості, які отримані (розроблені) іншими органами державної влади, органами місцевого самоврядування, підприємствами, установами, організаціями або громадянами, не перебувають у відношенні підпорядкованості до керівника органу державної влади, що затверджує перелік. СС таких відомостей встановлюється за погодженням між органом державної влади, які розробляють перелік, і власником відомостей.

Визначення величини шкоди від поширення інформації і збитку, що наноситься у результаті їх засекречування

Підходи до визначення величини шкоди, що може бути нанесено безпеці РФ внаслідок поширення відомостей, що становлять ДТ, залежать від багатьох факторів:

- *від галузі діяльності держави*, до якої відносяться відомості (військової, зовнішньополітичної, економічної та інших);
- *від ступеню визначеності інформації*, використовуваної при прийнятті рішення (повна інформація, знання імовірнісних характеристик, повна невизначеність);
- *від сфери прояви збитку* (у окремих сферах, наприклад, військової, зовнішньополітичної, економічної чи комплексно у декількох сферах).

Розгляд моделей для визначення величини шкоди почнемо зі випадків, коли відомості стосуються досить вузькій галузі діяльності, сфера прояву збитку обмежена та інформація для прийняття рішення цілком визначена.

Визначення величини шкоди моделлю «обізнаність – ефективність»

Даний підхід до оцінювання величини шкоди, що настає у результаті поширення відомостей, що становлять ДТ, заснований на аналізі впливу зміни обізнаності суперника, конкурента про ці відомості на ефективність функціонування об’єктів – носіїв інформації. При цьому аналізуються об’єкти, що знаходяться у найбільш гострому конфлікті з відповідними об’єктами суперника, від результату якого залежить ефективність функціонування об’єктів, їх живучість, зачіпаються життєво важливі інтереси сторін. Саме проти них суперник буде використовувати всі наявні у його розпорядженні ресурси, і, в першу чергу, прагнутиме отримати детальні відомості про них.

Основу такого підходу становить моделювання функціонування об’єкта захисту в умовах реалізації контрзаходів, розроблених з урахуванням отриманої інформації. Шкода від витоку відомостей

оцінюється за величиною зниження ефективності функціонування об'єкту і величиною економічних втрат, що виникають при цьому.

Для визначення можливої шкоди внаслідок поширення відомостей виконуються такі процедури:

1) *оцінка апріорної (вихідної) обізнаності* суперника про об'єкти, що захищаються (тобто обізнаності до поширення відомостей про об'єкти) і прогнозування її зміни протягом життєвого циклу об'єкта захисту;

2) *оцінка зміни обізнаності* суперника при поширенні відомостей про об'єкти;

3) *прогнозування можливих контрзаходів* (загроз) з боку суперника як результату його реакції на зміну обізнаності про об'єкт з урахуванням завчасної підготовки їм науково-технічного доробку для випереджаючої реакції;

4) *моделювання впливу контрзаходів* суперника на ефективність функціонування об'єкта, що захищається шляхом зміни відповідних вихідних даних і параметрів моделі для оцінки ефективності об'єкта;

5) *оцінка зниження ефективності* об'єкта в залежності від реалізованих контрзаходів;

6) *оцінка ЕШ* внаслідок зниження ефективності об'єкта.

Оцінка апріорної обізнаності суперника про об'єкт являє собою завдання прогнозування «за суперника» характеристик об'єкта і оцінка точності та достовірності такого прогнозу.

Джерелами інформації при прогнозуванні є:

- характеристики аналогічних об'єктів, опубліковані у відкритій пресі, передаються іншим державам при проведенні переговорів;
- характеристики аналогічних об'єктів інших держав;
- технічні, фізичні, економічні та інші обмеження на досяжні значення окремих характеристик об'єктів, що захищаються;
- матеріали обізнаності, які від органів розвідки.

У якості показників оцінки обізнаності суперника про об'єкти, що захищаються можуть використовуватися:

а) для відомостей кількісного характеру – середньоквадратична помилка визначення значимості відомостей (характеристики); відхилення (зміщення) математичного сподівання значимості відомостей від його істинного значення; ймовірність розкриття (визначення, вимірювання) відомостей із заданою точністю продовж заданого часу; час розкриття відомостей з точністю не гірше заданої;

б) для відомостей якісного характеру (наприклад, призначення об'єкта, наявність певної властивості) – ймовірність правильного розпізнавання (переплутування) об'єкта; ймовірність визначення відомостей впродовж заданого часу; час визначення відомостей з ймовірністю не менше заданої.

Оцінка зміни обізнаності суперника при розповсюдженні відомостей здійснюється шляхом порівняння істотної значимості відомостей зі значимістю відомостей, які можуть бути відомі супернику.

Якщо помилки визначення відомостей за результатами прогнозу несуттєві з точки зору прийнятих рішень з реалізації контрзаходів, то поширення відомостей про об'єкт практично не вплине на обізнаність суперника про нього, а отже, і на ефективність функціонування об'єкта;

Прогнозування можливих контрзаходів проти об'єкта здійснюється з використанням інформації про існуючі у суперника способи і засоби впливу на об'єкт, що захищається і їх можливий розвиток.

При цьому необхідно визначити, які з контрзаходів можуть бути швидко реалізовані у короткостроковому періоді часу, а які потребують для реалізації більш тривалого часу.

Слід зазначити, що суперник вживає додаткові контрзаходи, якщо даний об'єкт представляє для нього загрозу, наприклад, ефективність нових об'єктів значно перевищує ефективність вже існуючих.

Оцінка зниження ефективності об'єкта від можливих контрзаходів здійснюється з використанням наявних моделей функціонування об'єктів, що захищаються шляхом зміни вихідних даних і параметрів цих моделей. Для цього моделі повинні бути чутливі до змін у діях суперника, і дозволяти отримувати оцінки при значній рефлексивній зміні його вигляду в залежності від обізнаності про об'єкт.

Моделювання впливу контрзаходів суперника на ефективність функціонування об'єкта, що захищається здійснюється з використанням наступної процедури.

У процесі життєвого циклу об'єктів, як правило, відбувається поступова зміна обізнаності суперника від незнання їх характеристик до повного та достовірного їх знання. Об'єкти, що захищають, як правило, складні за складом, можуть характеризуватися значною кількістю відомостей, тому кількість можливих варіантів (станів обізнаності) суперника може бути велике.

У той же час деякі стани обізнаності можуть відрізнятися несуттєво з погляду реалізованих на їх основі контрзаходів і збитку, що завдається при цьому. Тому вибирається обмежена кількість станів обізнаності про об'єкти, що захищаються і, які принципово відрізняються один від одного. Кожен стан обізнаності характеризується певною сукупністю (комбінацією) відомостей, необхідних для реалізації хоча б одного з контрзаходів. Між різними станами обізнаності встановлюються відносини передування і слідування у часі відповідно з розширенням переліку відомостей, що характеризують ці варіанти. У результаті цього формується граф зміни обізнаності про об'єкт – див. рис. 8 а) [68].

Вершинами графа є різні стани обізнаності, а дуги – переходи з одного стану в інший. Початковий стан графа відповідає випадку відсутності у суперника достовірних відомостей; кінцевий стан – повної поінформованості.

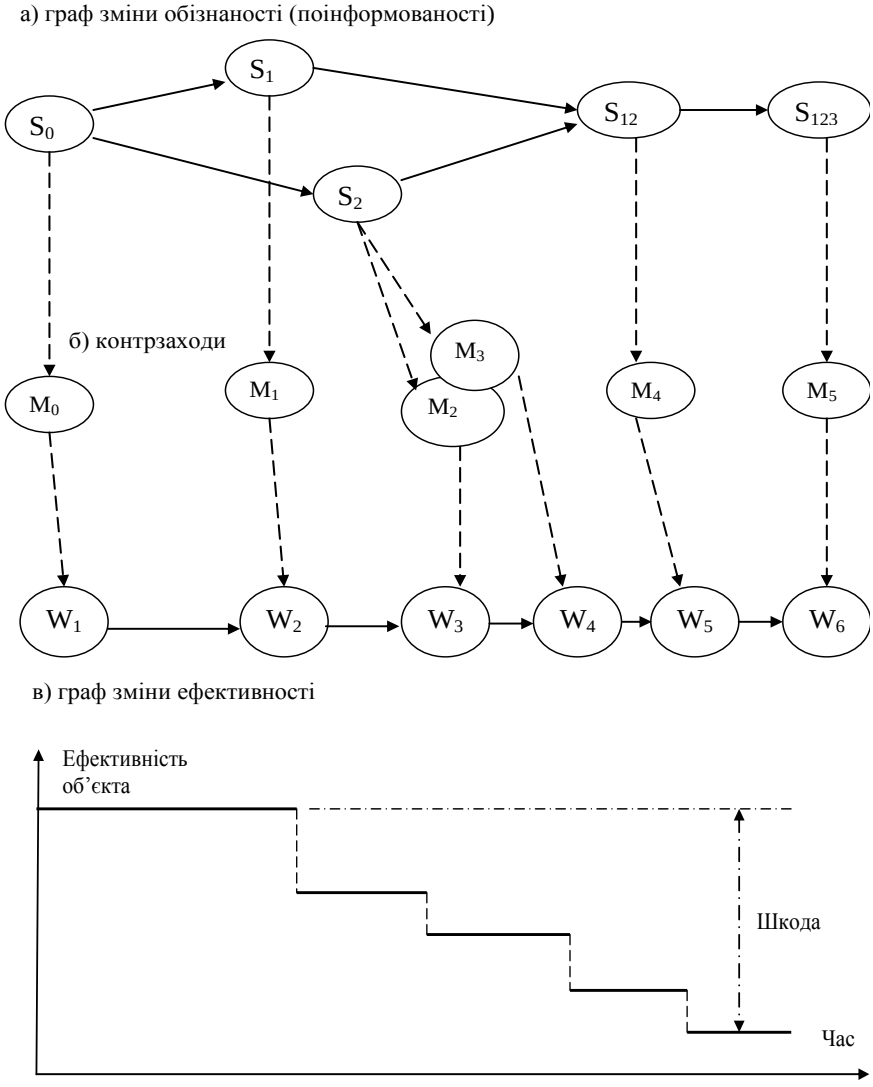


Рис. 8. Приклад графічного відображення взаємозв’язку стану обізнаності суперника про об'єкт (а), контрзаходів (б) та ефективності функціонування об’єкта (в)

Контрзаходи суперника від можливості їх одночасної реалізації поділяються на такі класи:

1) прості (для даного стану обізнаності існує тільки одна міра);

2) альтернативні (з декількох варіантів заходів одночасно може реалізуватися тільки одна);

3) узагальнені, реалізовані шляхом нарощування (при реалізації всіх заходів формується узагальнена міра).

Відносини між різними контрзаходами відображаються у вигляді графа на рис. 8 б). Вершинам графа відповідають прості і узагальнені контрзаходи, а дуги – включення даного контрзаходу до узагальнених контрзаходів.

Взаємозв'язок між варіантами обізнаності та контрзаходами відображаються у вигляді дуг, що з'єднують графи а), б) на рис. 8 [68].

Кожна з дуг може бути поставлена у відповідність оцінки часу переходу системи зі стану в стан, що пов'язуються цими дугами. Для отримання оцінок впливу обізнаності про об'єкт на ефективність його функціонування і величину виникаючої шкоди розглядаються процеси, що протікають в трьох взаємопов'язаних графах: зміни обізнаності, реалізації контрзаходів і зміни ефективності функціонування об'єкта. Зміст цих процесів полягає у наступному.

Послідовно до певного моменту часу досягається один зі станів графа поінформованості (обізнаності). При досягненні цього стану починається процес реалізації відповідного контрзаходу. При реалізації цього контрзаходу досягається один зі станів графу зміни ефективності функціонування об'єкта. Час досягнення заданого стану графу зміни ефективності функціонування об'єкта розраховується як сума часу, необхідного супернику для досягнення відповідного стану обізнаності, і часу, необхідного для реалізації пов'язаних з цим станом контрзаходів.

Результати розрахунків ефективності функціонування об'єкта при різній поінформованості (обізнаності) суперника упорядковуються за величиною ефективності та відображаються у вигляді графа на рис. 8 в).

Таким чином, представлений на рис. 8 граф наочно відображає процес зниження ефективності функціонування об'єкта при зростанні обізнаності суперника про цей об'єкт.

Оцінка ЕШ внаслідок зниження ефективності об'єкта може бути отримана за допомогою використання наступних двох способів.

Перший спосіб полягає у визначенні додаткових грошових витрат, необхідних для відновлення втраченої ефективності об'єкта (шляхом застосування додаткової кількості об'єктів, виділення додаткових ресурсів для цих об'єктів і т.д.).

Величина ЕШ при відновленні ефективності за рахунок застосування додаткової кількості об'єктів розраховується за формулою:

$$U = N_{сер} \cdot N_{дод}(C_{сер} + C_{ре} + T_{е}), \qquad (2.7)$$

де $N_{сер}$ – обсяг серійного виробництва розглянутих об'єктів; $N_{дод}$ – необхідна додаткова кількість об'єктів, що припадають на один вихідний об'єкт; $C_{сер}$ – вартість серійного виробництва об'єкта; $C_{ре}$ – вартість річної експлуатації об'єкта; $T_{е}$ – тривалість експлуатації об'єкта.

Величина $N_{дод}$ розраховується за допомогою методик (моделей) оцінки ефективності об'єктів за умови відновлення їх проектної ефективності, що знизилася внаслідок зростання обізнаності суперника про характеристики останніх.

Другий спосіб оцінки ЕШ грунтується на оцінці грошових витрат на створення об'єкта з необхідною проектною ефективністю. При зниженні цієї ефективності внаслідок зростання обізнаності суперника і прийняття ним контрзаходів вважається, що певна частка витрат на створення об'єкта, пропорційна зниженню ефективності, витрачена даремно і відображає величину шкоди.

У цьому випадку величина ЕШ орієнтовно розраховується за формулою:

$$U = N_{сер} \cdot C_{сер} \cdot \delta W, \qquad (2.8)$$

де $\delta W = \Delta W / W$ – відносне зниження ефективності об'єкта внаслідок зростання обізнаності суперника про його характеристики; W – проектна ефективність об'єкта; ΔW – очікуване зниження ефективності об'єкта внаслідок зростання обізнаності та застосування суперником контрзаходів.

Визначення величини шкоди методом експертних оцінок

Ключовим моментом у віднесенні інформації до ДТ є оцінка величини шкоди, що наноситься безпеці держави у результаті передчасного розкриття інформації.

Проблемним є випадок, коли не існує елементарних вимірювальних властивостей шкоди безпеці держави і можливості її нанесення у разі розкриття або витоку інформації. Відсутність статистичних даних і труднощі оцінки нанесеної шкоди безпеці держави у результаті розкриття інформації визначають вибір методу експертних оцінок для її вимірювання.

Для зіставлення різних відомостей з точки зору необхідності їх закриття або обмеження доступу до них, а також для визначення

відповідного цим відомостям СС, пропонується порівнювати аналізовані відомості за ступенем прояву всієї сукупності можливих загроз у разі несанкціонованого поширення відомостей, що становлять ДТ.

У даному випадку виникає завдання ранжування або визначення «ваги» (важливості) кожної загрози з тим, щоб отримати єдину міру або показник, що характеризує загрозу безпеці держави у цілому. Важливість загроз безпеці держави будемо оцінювати за величиною можливого шкоди, яку може бути нанесено безпеці держави при їх реалізації.

Під шкодою безпеці держави будемо розуміти величину зниження оборонного та економічного потенціалу країни, боєготовності та боєздатності її Збройних Сил, який може характеризуватися кількістю сил і засобів, необхідних, як для ліквідації наслідків завданої шкоди, так і для досягнення раніше наявного рівня безпеки держави.

Для розподілу загроз безпеки держави за різними рангами важливості оцінюється їх числове значення, виходячи з парних порівнянь важливості загроз, при цьому використовується надлишкова інформація, оскільки кожна загроза послідовно порівнюється з усіма іншими. Методологічною основою проведення цієї роботи доцільно вибрати наступний метод, розроблений Т.Л. Сааті [69, 70].

Використання методу парних порівнянь для оцінки відносної важливості шкоди. Перша проблема, яку необхідно вирішити при оцінці загроз і пов'язаної з ними важливості «шкоди» – це проблема вимірювання величини можливої шкоди, яка може проявитися у результаті розкриття (витоку) інформації.

Щоб уявити результат порівняння двох «шкод» у вигляді розумних цифр, потрібне глибоке розуміння порівнюваних «шкод» і особливо того, у якій мірі їх властивості впливають на інтереси підприємства (галузі, держави). Передбачається, що джерелом суджень є опитування експертів, обізнаних у цій галузі.

Групі експертів пропонується оцінити ступінь важливості кожної шкоди по їх впливу на інтереси підприємства (галузі, держави) методом парного порівняння та заповнити матрицю парних порівнянь $A = (a_{ij})$.

Кожен експерт, користуючись вербально-числовою шкалою, заповнює матрицю парних порівнянь:

$$A = \left| a_{ij} \right|, \ i = 1, Q,$$

де a_{ij} – результат порівняння відносної важливості *i*-ої і *j*-ої «шкоди».

Значення a_{ij} встановлюються відповідно до вербально-числової шкали, наведеної у табл. 1.

Основна мета застосування вербально-числової шкали полягає у тому, щоб полегшити завдання фахівцям, що залучаються до експертизи і забезпечити єдине тлумачення оцінок окремими експертами.

Таблиця 1

Шкала порівняльної оцінки важливості загроз («шкоди»)

Величина відносної важливості	*Визначення*	*Пояснення (тлумачення)*
1	Однакова важливість	Однаковий вплив двох видів «шкоди» на безпеку держави
3	Помірна перевага однієї над іншою	Досвід і судження дозволяють зробити висновок про дещо більший вплив однієї «шкоди» у порівнянні з іншою
5	Істотна або сильна перевага	Досвід і судження дозволяють зробити висновок про сильний вплив однієї «шкоди» у порівнянні з іншою
7	Значна перевага	Одному виду «шкоди» дається настільки сильна перевага, що вона стає практично значною
9	Дуже сильна перевага	Очевидність переваги, одного виду «шкоди» над іншою підтверджується найбільш сильно
2, 4, 6,8	Проміжні рішення між двома сусідніми	Застосовуються у компромісному випадку
Величини, зворотні наведеним вище	Якщо при порівнянні одного виду «шкоди» з іншим отримано одне з вищевказаних чисел (наприклад, величина 5), то при порівнянні другого виду шкоди з першим / отримуємо обернену величину (наприклад, 1/5)	

Важливості «шкоди» визначаються на основі обчислення множини власних векторів для кожної матриці. Обчислення власних векторів – не дуже складне завдання, однак, може зайняти досить багато часу. Тому використовують нескладні шляхи отримання бажаного наближення до пріоритетів – середнє геометричне. Тобто, перемножуючи елементи у кожному рядку і, вилучаючи корені *n*-го ступеня, де *n* – число елементів. Отриманий таким чином стовпець чисел нормалізується розподілом кожного числа на суму всіх чисел.

Приклад парного порівняння важливості «шкод» представлено у таблиці 2.

Таблиця 2

Матриця парних порівнянь

Шкода	*U1*	*U2*	*U3*	*Оцінка компонентів власного вектору*	*Нормалізований результат оцінки*
U1	1	6	8	3.63	0.74
U2	1/6	1	4	0.87	0.18
U3	1/8	1/4	1	0.31	0.07

Всі оцінки парних порівнянь мають похибки. Ці похибки можуть призвести до неузгоджених висновків. Ступінь узгодженості експертних суджень оцінюється індексом узгодженості (ІУ). У кожній матриці ІУ може бути обчислено наближено. Тобто, спочатку підсумовується кожен стовпець суджень, потім сума першого стовпця збільшується на величину першої компоненти нормалізованого вектора пріоритетів, сума другого стовпця – на другу компоненту тощо. Потім отримані числа додаються. Таким чином можна отримати величину, позначену λ.

Для ІУ маємо:

$$ІУ = (\lambda - n)/(n-1), \qquad (2.9)$$

де n – число порівнюваних елементів. Для оберненосиметричної матриці завжди $\lambda > n$.

Тепер порівняємо цю величину з тією, яка б вийшла при випадковому виборі кількісних суджень з шкали 1/9, 1/8, 1/7, .., 1,2, .., 9, але при утворенні оберненосиметричної матриці. Нижче наведені середні узгодженості для випадкових матриць різного порядку.

Розмір матриці	1	2	3	4	5	6	7	8	9
Випадкова узгодженість	0	0.58	0.9	1.12	1.24	1.32	1.41	1.45	1.49

Якщо розділити ІУ на число, яке відповідає випадковій узгодженості матриці того ж порядку, отримаємо різницю узгодженості (РУ). Величина РУ повинна бути 10% або менше, щоб бути прийнятною. У деяких випадках можна допустити 20%, але не більше. Якщо РУ виходить із цих меж, то учасникам потрібно досліджувати задачу і перевірити свої судження.

Для розглянутого прикладу маємо:

$\lambda = (1 + 1/6 + 1/8)\cdot 0.75 + (6 + 1 + 1/4)\cdot 0.18 + (8 + 4 + 1)\cdot 0.07 = 3.19$,

$ІУ = (3.19 - 3) / (3 - 1) = 0.095$,

$РУ = 0.095 / 0.58 = 0.16$ (тобто 16%).

Отримана величина РУ менше 20%, отже, узгодженість експертів достатня.

Ефективним способом дослідження великого числа загроз, який дозволяє істотно скоротити обсяг обчислень, є групування їх у класи. Після аналізу класів загроз безпеці держави їх елементи попарно порівнюються між собою за величиною шкоди по відносній важливості у цьому класі. Ієрархічна схема загроз безпеці держави представлена на рис. 9 [68].

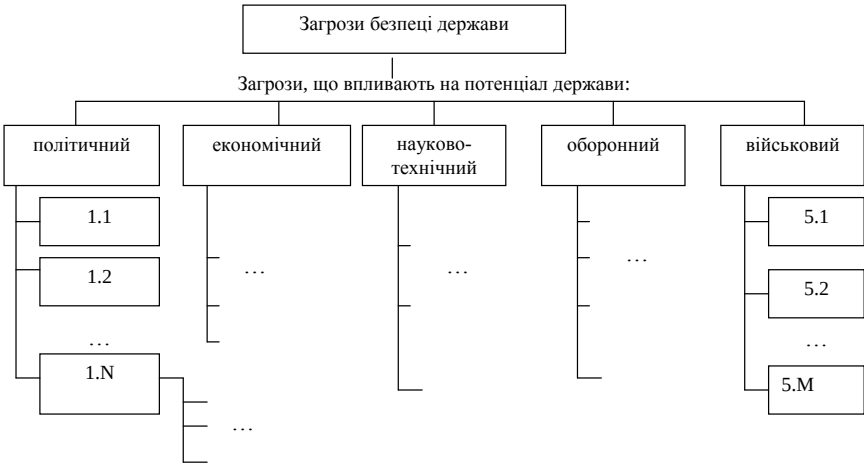


Рис. 9. Ієрархічна схема загроз безпеці держави

У загальному випадку величина шкоди від реалізації окремої загрози безпеці держави залежить від зовнішніх і внутрішніх умов розвитку держави. Тому зіставлення загроз повинно проводитися для можливих сценаріїв, наприклад, мирний і воєнний періоди, формуючи відповідному сценарію свій ряд «ваги» загроз для того, щоб надалі при визначенні СШ від поширення відомостей, що оцінюються при визначенні СС вибрати максимальну шкоду з безлічі СШ, відповідно до різних розглянутих сценаріїв розвитку держави.

Передбачається, що для оцінки кожної підмножини загроз вибирається група експертів, знайомих зі порівнюваними загрозами і їх впливом на безпеку держави. Структурна схема підходу до оцінки загроз безпеці держави представлено на рис. 10 [68].

Після визначення векторів пріоритетів всіх рівнів ієрархії загроз, розраховується вектор пріоритетів загроз нижнього рівня.

Розрахунок величин можливої шкоди у результаті прояву окремих загроз безпеці держави може бути отриманий також і з використанням наявних математичних моделей, наприклад, - «обізнаність-ефективність». Якщо в обох випадках (за допомогою експертів і на моделях) не були

допущені грубі прорахунки, то отримані оцінки не можна віднести до категорії взаємовиключних результатів. Навпаки, обидва підходи, доповнюючи один одного на незалежній основі, повинні забезпечити більш об'єктивне надання необхідних рекомендацій.

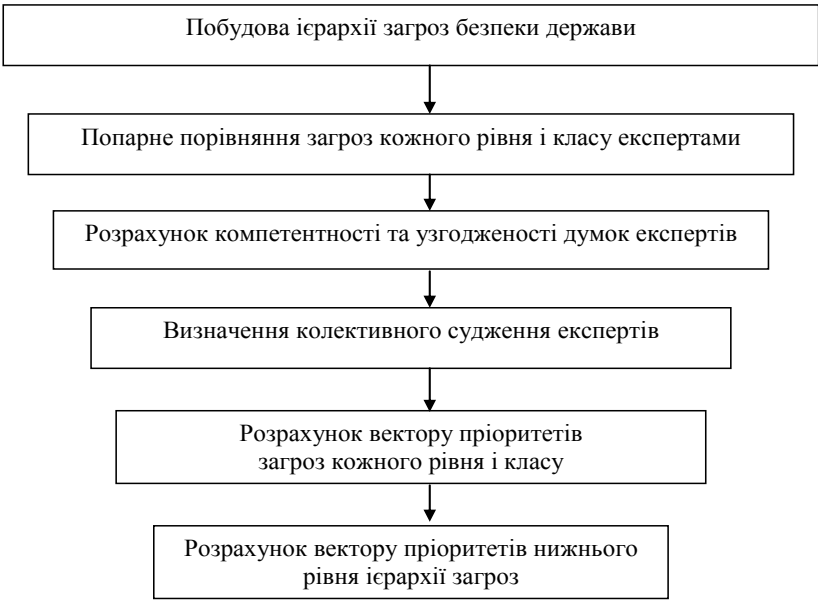


Рис. 10. Структурна схема підходу до оцінки загроз безпеці держави

Не всі з оцінених за величиною шкоди загроз безпеці держави можуть проявлятися при розкритті тих чи інших відомостей. Оцінка можливості виникнення загроз у результаті розкриття або витоку тих чи інших відомостей військово-технічного характеру може бути проведена за допомогою експертів, які добре розуміють цінність цієї інформації та їх зв'язок із загрозами безпеці держави. Для однозначного уявлення оцінок використовується спеціальна вербально-числова шкала.

Ступінь зв'язку «відомості-загроза» характеризує «ймовірність» появи оцінюваної загрози безпеці держави при розкритті (витоку) відповідних відомостей. Оцінку ступеня зв'язку «відомості-загроза» необхідно проводити для різного періоду часу. Визначення періоду часу та періоду прогнозу оцінки ступеня зв'язку «відомості-загроза» є важливим етапом при проведенні експертизи, так як можливість появи загроз при розкритті тих чи інших відомостей є випадковою величиною і залежить від багатьох факторів, у тому числі й від політичної та економічної ситуації, що складається в країні та світі.

Оцінка ступеня або можливості нанесення шкоди безпеці держави у результаті витоку окремих відомостей суб'єктивні у тому сенсі, що дві людини можуть приписати різні числа одного й того ж можливого результату. Але оскільки ці оцінки базуються на інформації, досвіді та аналізі об'єктивної дійсності, то передбачається, що за інших рівних умов відмінність між ними не є настільки істотною, щоб не можна було їх використовувати для підготовки рішень.

В результаті проведених оцінок і обробки отриманих даних формується матриця «відомості-загрози», елементи якої характеризують можливість появи загроз безпеці держави у результаті передчасного розкриття інформації.

Структурна схема підходу до оцінки ступеня появи загроз при розкритті відомостей, що становлять ДТ, показана на рис. 11 [68].

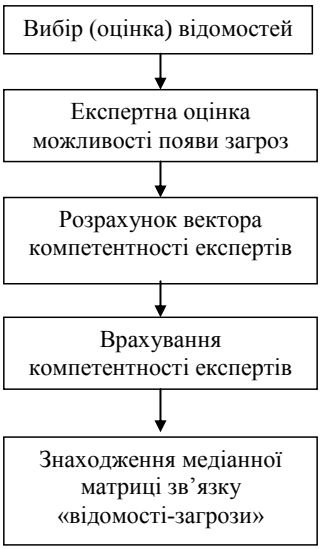


Рис. 11. Структурна схема підходу до оцінки ступеня появи загроз безпеці держави

Результатами проведених оцінок є вектор пріоритетів важливості загроз безпеки держави та результуюча матриця суджень експертів про ступінь їх прояву при передчасному розкритті оцінюваних відомостей.

Тому стоїть завдання агрегування отриманих оцінок у єдину цільову функцію, у результаті якого кожним відомостям може бути присвоєний рейтинг, який визначає не тільки ранг відомостей, але й «відстань» між ними.

Розрахунок первинного рейтингу окремих відомостей може бути проведений різними способами. Найбільш простий, який ілюструє ідею методу кількісної обробки даних, отриманих на попередньому етапі.

За цим способом отримані оцінки для окремих відомостей (категорії відомостей) визначаються за формулою:

$$r_{im}(T_j) = \sum_{m=1}^{M} k_{im}(T_j) \cdot W_m, \qquad (2.10)$$

де $k_{im}(T_j)$ – медіанне значення ступеня зв'язку S_i відомостей із загрозою y_m; W_m – значення ступеня важливості загрози y_m; $r_{im}(T_j)$ – рейтинг відомостей S_i, розрахований кількісним способом для моменту часу перегляду СС T_j; M – кількість загроз безпеці держави.

Таким чином, кожним відомостям присвоюється їх рейтинг, який відповідає розрахунку цінності цих відомостей за величиною інтегрованої шкоди (збитку).

Рейтинг відомостей є відносною характеристикою їх цінності і показує ступінь відмінності одних відомостей щодо інших за величиною шкоду, яку може бути нанесено у результаті розкриття цих відомостей.

За величиною рейтингу відомостям може бути встановлено їх СС. Для цього сукупність всіх розглянутих відомостей відображається на відповідній шкалі секретності, що дозволяє ранжувати сукупність значень рейтингів відомостей, розбитих на інтервали категорій секретності: Т, ЦТ, ОВ.

СС інформації визначається на основі попадання рейтингу відомостей у той чи інший інтервал шкали секретності, так як це показано на рис. 12 [68].

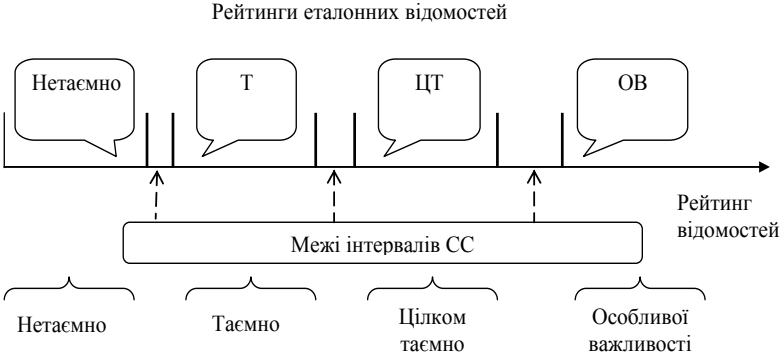


Рис. 12. Оцінка секретності відомостей за шкалою секретності з використанням рейтингів «еталонних» відомостей

Мета полягає у знаходженні глобального впорядкування відомостей за величиною їх первинного рейтингу, що характеризує величину можливого шкоди при розкритті оцінюваних відомостей.

Визначення межі переходу категорій секретності здійснюється на основі рейтингів відомостей, визначених для даної СС, як «еталонні». Для цього кожен експерт на основі якісних характеристик категорій секретності і наявного досвіду роботи вказує зі списку оцінених ним відомостей ті, в СС яких у нього немає сумнівів.

Оцінка упущеної вигоди у результаті обмежень на поширення інформації

Визначаючи негативні наслідки засекречування відомостей, необхідно оцінити фактори, які зумовлюють упущену державою вигоду.

Цінність інформації може бути визначена як різниця між результатами рішень, прийнятих з використанням даної інформації та, результатами рішень, які були отримані без її використання. Під «результатами» маються на увазі економічні та інші наслідки управлінських рішень, що вимірюються у вигляді прибутку (короткострокового або довгострокового), скорочення витрат або іншими позитивними наслідками.

Вигода від найкращого використання інформації може оцінюватися на основі оцінки:

- можливої додаткового прибутку за рахунок зниження собівартості матеріалів і виробів, що використовують нові матеріали і технології;
- можливої додаткового прибутку за рахунок продажу конкурентоспроможних матеріалів, технологій і виробів;
- скорочення витрат на розробку, виробництво та експлуатацію виробів за рахунок підвищення їх надійності, довговічності, скорочення термінів розробки і виробництва, необхідної кількості виробів у результаті застосування нових матеріалів і технологій.

Оцінка розмірів вигоди від вільного використання відомостей здійснюється експертами на основі прогнозування реалізації перерахованих вище можливостей та обліку додаткових економічних ефектів у результаті використання інформації, наприклад, в інших розроблюваних комплексах і системах.

При цьому враховується, що вигода також як і шкода може проявлятися на різних рівнях державного управління, що обумовлює необхідність оцінки інтегральної вигоди.

Реалізація прогнозованої вигоди в різні моменти часу можлива при відповідному розширенні схеми розповсюдження (поширення) інформації. Тоді для варіантів обмеженого поширення інформації дана вигода визначається як упущена.

Визначення витрат на захист відомостей, що становлять ДТ

Основними принципами оцінки витрат на захист СІ є:

- облік всіх видів витрат на заходи щодо захисту СІ, а також супутніх (побічних) ефектів, які піддаються вартісному оцінюванню;

- оцінка витрат на захист відомостей стосовно конкретного об'єкту, що захищається на розрахунковий період, який визначається тривалістю етапів життєвого циклу об'єкта.

При цьому повинні дотримуватися наступні умови:

1. Якщо яким-небудь технічним засобом (існуючим або новоствореним) завдання захисту відомостей вирішуються разом з його основним призначенням, то при оцінці витрати на такий засіб не враховуються.

2. Якщо заходи щодо захисту відомостей поширюються на декілька об'єктів захисту, то пов'язані з їх реалізацією витрати розносяться по окремих об'єктах у пайовому розрахунку.

Основними показниками витрат на захист відомостей є: річні наведені народногосподарські витрати; повні витрати на розрахунковий період.

Показник «річні наведені народногосподарські витрати» відображає всі безпосередні і побічні економічні витрати внаслідок реалізації заходів захист відомостей.

На величину безпосередніх витрат на захист відомостей впливають такі основні фактори:

- витрати на відшкодування збитку, що наноситься власникові інформації у результаті її засекречування;

- число і зміст відомостей, що захищаються;

- число носіїв відомостей (інформації);

- види і число можливих каналів витоку інформації;

- типи і кількість засобів захисту інформації, що використовуються для закриття каналів витоку інформації;

- тривалість захисту відомостей.

Побічні витрати можуть проявлятися у вигляді:

- збільшення тривалості і ускладнення роботи;

- ускладнення технічної оснащеності;

- відчуження виробничих площ під технічні засоби захисту інформації;

- впливу на навколишнє середовище (природу) і на різні сфери життя і діяльності людей;

- утруднення транспортних комунікацій і т. д.

Розрахунковий період обчислюється з того року життєвого циклу об'єкта, коли починається розробка розглянутих заходів щодо захисту відомостей. Він включає тільки ті етапи життєвого циклу (і їх тривалість) об'єкта, що захищається, на які поширюються розглянуті заходи щодо захисту відомостей.

Організація роботи з засекречування і розсекречення відомостей та їх носіїв

В основу організації роботи по засекречування відомостей покладено принцип відповідності відомостей чинному у даному органі державної влади, на підприємстві, в установі, організації переліку відомостей, що підлягають засекречуванню.

Підставою для засекречування відомостей є їх відповідність діючим переліками відомостей, що підлягають засекречування. При засекречування цих відомостей їх носіям присвоюється відповідний ГС. Засекречування носіїв відомостей здійснюють виконавці робіт. Для цього на носії наносяться відповідні реквізити:

- про СС відомостей, що містять носії з посиланням на відповідний пункт чинного переліку відомостей, що підлягають засекречуванню;
- про орган державної влади, про підприємство, про заснування, організації, що здійснили засекречування носія;
- про реєстраційний номер;
- про дату або умови розсекречення відомостей або про подію, після настання якого відомості будуть розсекречені.

При неможливості нанесення таких реквізитів на носій відомостей, що становлять ДТ, ці дані вказуються у супровідній документації на цей носій.

Якщо носії містять відомості відомостей різного СС, то гриф носія повинен відповідати найвищого СС.

При неможливості ідентифікації отриманих (розроблених) відомостей з відомостями, що містяться у діючому переліку, посадові особи зобов'язані забезпечити попереднє засекречування отриманих (розроблених) відомостей відповідно до передбачуваного СС. Потім необхідно у місячний термін направити на адресу посадової особи, яка затвердила зазначений перелік, пропозиції щодо його доповнень (змін)

Посадові особи, що ухвалили діючий перелік, зобов'язані протягом трьох місяців організувати експертну оцінку пропозицій, що надійшли і прийняти рішення по доповненню (зміні) чинного переліку або зняття попередньо присвоєного відомостям ГС.

Таким чином, реалізується принцип своєчасності засекречування.

Підставами для розсекречення відомостей є:

- взяття на себе РФ міжнародних зобов'язань з відкритого обміну відомостями, що становлять ДТ в РФ;
- зміна об'єктивних обставин, внаслідок якого подальший захист відомостей, що становлять ДТ, є недоцільною.

Відомості можуть бути розсекречені тільки шляхом періодичного, але не рідше ніж через кожні 5 років, або перегляду змісту діючих в

органах державної влади, на підприємствах, в установах і організаціях переліків відомостей, що підлягають засекречуванню, у частині обґрунтованості засекречування відомостей та їх відповідності встановленого раніше СС. При перегляді переліків відомостей застосовуються ті ж критерії віднесення відомостей до ДТ, що і при їх засекречування.

Правом зміни переліків відомостей, що підлягають засекречуванню, наділяються керівникам органів державної влади, що їх затвердили та несуть персональну відповідальність за обґрунтованість прийнятих ними рішень з розсекречення відомостей. Рішення зазначених керівників, пов'язані із зміною переліку відомостей, віднесених до ДТ, підлягають узгодженню з міжвідомчою комісією із захисту ДТ, яка має право припиняти і опротестовувати ці рішення.

Носії відомостей можуть бути розсекречені тільки за умови розсекречення відомостей, що розміщені у них. Розсекречення носія відомостей здійснюється на підставі висновку спеціальної ЕК органу державної влади, підприємства, установи чи організацій, що здійснила засекречування носія. Ухвалення рішення про розсекречення носія здійснює відповідний керівник.

Керівники наділяються повноваженнями з розсекречення носіїв відомостей, необґрунтовано засекречених підпорядкованими їм посадовими особами.

Керівники державних архівів РФ наділяються повноваженнями з розсекречення носіїв відомостей, що становлять ДТ, у разі делегування їм таких повноважень організацією-фондоутворювачем або її правонаступником. У разі ліквідації організації-фондоутворювача і відсутності її правонаступника питання про порядок розсекречення носіїв відомостей, що становлять ДТ, розглядається МВК із захисту ДТ.

Ліцензування діяльності у галузі захисту державної таємниці

Допуск підприємств, установ і організацій до проведення робіт, пов'язаних:

- з використанням відомостей , що становлять ДТ,
- створенням засобів захисту інформації, а також
- із здійсненням заходів та (або) наданням послуг із захисту ДТ,

здійснюється шляхом отримання ними у порядку, що встановлюється Урядом РФ, ліцензій на проведення робіт з відомостями відповідного СС.

Ліцензія на проведення зазначених робіт видається на підставі результатів спеціальної експертизи підприємства, установи і організації

та державної атестації їх керівників, відповідальних за захист відомостей, що становлять ДТ.

Зазначений порядок встановлено у Положенні про ліцензування діяльності підприємств, установ і організацій з проведення робіт, пов'язаних з використанням відомостей, що становлять ДТ, створенням засобів захисту інформації, а також із здійсненням заходів та (або) наданням послуг із захисту ДТ, затвердженому постановою Уряду РФ.

Органами, уповноваженими на ведення ліцензійної діяльності, є:

- по допуску підприємств до проведення робіт, пов'язаних з використанням відомостей, що становлять ДТ, ФСБ РФ та її територіальні органи (на території РФ), СЗР РФ (за кордоном);
- на право проведення робіт, пов'язаних із створенням засобів захисту інформації, – ДТК при Президенті РФ, Федеральне агентство урядового зв'язку та інформації (ФАУЗІ) при Президентові РФ, СЗР РФ, Міністерство оборони РФ (у межах їх компетенції);
- на право здійснення заходів та (або) надання послуг у галузі захисту ДТ, – ФСБ РФ та її територіальні органи, ФАУЗІ та ДТК при Президентові РФ, СЗР РФ (у межах їх компетенції).

Систему ліцензування у галузі захисту ДТ представлено у табл 3.

Таблиця 3

Система ліцензування у галузі захисту ДТ

<table>
<tr><td colspan="10">Уповноважені органи на ведення ліцензійної діяльності</td></tr>
<tr><td colspan="2">Ліцензування по допуску підприємств до проведення робіт, пов'язаних з використанням відомостей, що становлять ДТ</td><td colspan="4">Ліцензування діяльності підприємств на право проведення робіт, пов'язаних із створенням засобів захисту інформації</td><td colspan="4">Ліцензування діяльності підприємств на право здійснення заходів та (або) надання послуг у галузі захисту ДТ</td></tr>
<tr><td>ФСБ</td><td>СЗР</td><td>ДТК</td><td>ФАУЗІ</td><td>СЗР</td><td>МО</td><td>ДТК</td><td>ФСБ</td><td>ФАУЗІ</td><td>СЗР</td></tr>
<tr><td colspan="10">МВК РФ</td></tr>
</table>

На орган, уповноважений на ведення ліцензійної діяльності, покладається:

- організація ліцензування діяльності підприємств;
- організація та проведення спеціальних експертиз підприємств;
- розгляд заяв підприємств про видачу ліцензій;
- прийняття рішень про видачу або про відмову у видачі ліцензій;
- видача ліцензій;

- прийняття рішень про призупинення дії ліцензії або про її анулювання;

- розробка нормативно-методичних документів з питань ліцензування;

- залучення у разі потреби представників міністерств і відомств РФ для проведення спеціальних експертиз;

- ведення реєстру виданих, призупинених і анульованих ліцензій.

Робота органів, уповноважених на ведення ліцензійної діяльності, координується МВК із захисту ДТ.

Для отримання ліцензії заявник подає до відповідного органу уповноваженого на ведення ліцензійної діяльності заяву про видачу ліцензії та необхідні документ, що містять відомості про заявника.

Орган, уповноважений на ведення ліцензійної діяльності, приймає рішення про видачу або про відмову у видачі ліцензії протягом 30 днів з дня отримання заяви з усіма необхідними документами. Залежно від складності та обсягу підлягають спеціальній експертизі матеріалів керівник органу, уповноваженого на ведення ліцензійної діяльності, може продовжити термін прийняття рішення про видачу або про відмову у видачі ліцензії до 30 днів.

Ліцензії видаються на підставі результатів спеціальних експертиз підприємств і державної атестації їх керівників, відповідальних за захист відомостей, що становлять ДТ (далі іменуються - керівники підприємств), і при виконанні таких умов:

1) дотримання вимог законодавчих та інших нормативних актів РФ щодо забезпечення захисту відомостей, що становлять ДТ, у процесі виконання робіт, пов'язаних з використанням зазначених відомостей;

2) наявність у структурі підприємства підрозділу із захисту ДТ та необхідного числа спеціально підготовлених співробітників для роботи із захисту інформації, рівень кваліфікації яких достатній для забезпечення захисту ДТ;

3) наявність на підприємстві засобів захисту інформації, які мають сертифікат, що засвідчує їх відповідність вимогам щодо захисту відомостей відповідного СС.

Термін дії ліцензії встановлюється в залежності від специфіки виду діяльності, але не може бути менше трьох і більше п'яти років.

Підставою для відмови у видачі ліцензії є:

- наявність в документах, поданих заявником, недостовірної або перекрученої інформації;

- негативний висновок експертизи, що встановила невідповідність необхідним для здійснення заявленого виду діяльності умов;

- негативний висновок за результатами державної атестації керівника підприємства.

Спеціальна експертиза підприємства проводиться шляхом перевірки виконання вимог нормативно-методичних документів: по РС;

протидії іноземним технічним розвідкам; захисту інформації від витоку технічними каналами, а також дотримання інших умов, необхідних для отримання ліцензії .

Державними органами, відповідальними за організацію та проведення спеціальних експертиз підприємств, є: ФСБ РФ; ФАУЗІ, ДТК при Президентові РФ; СЗР РФ; МО РФ; інші міністерства та відомства РФ, керівники яких наділені повноваженнями щодо віднесення до ДТ відомостей щодо підвідомчих їм підприємств.

Для проведення спеціальних експертиз ці державні органи можуть створювати атестаційні центри, які отримують ліцензії відповідно до вимог цього Положення.

Атестаційні центри діють на госпрозрахунковій основі. Спеціальні експертизи проводяться на основі договору між підприємством і органом, що проводить спеціальну експертизу. Витрати з проведення спеціальних експертиз відносяться на рахунок підприємства.

Державна атестація керівників підприємств організується органами, уповноваженими на ведення ліцензійної діяльності, а також міністерствами і відомствами РФ, керівники яких наділені повноваженнями щодо віднесення до ДТ відомостей щодо підвідомчих їм підприємств.

Від державної атестації звільняються керівники підприємств, які мають свідоцтво про закінчення навчальних закладів, уповноважених здійснювати підготовку фахівців з питань захисту інформації, що становить ДТ.

Порядок проведення ліцензування представлений на рис. 13 [68].

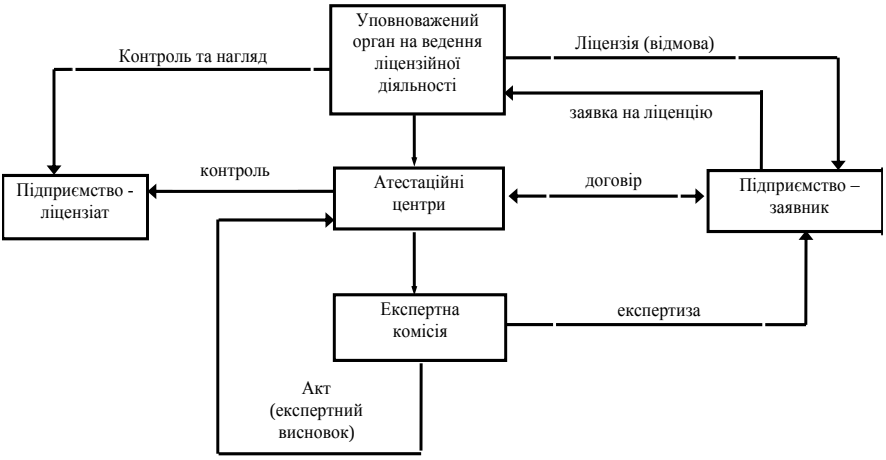


Рис. 13. Порядок проведення ліцензування

Організація захисту інформації, що становить державну таємницю, на підприємствах, в організаціях та установах

Наведені у нормативних правових документах по захисту ДТ терміни «підприємство, організація, установа» не мають однозначних несуперечливих визначень. Зазвичай зазначені вище терміни використовуються не в юридичному, а змістовному сенсах.

Під підприємством розуміється промислове підприємство незалежно від її організаційно-правової форми.

Під організаціями розуміються комерційні та некомерційні організації, що представляють собою господарські товариства і суспільства, виробничі кооперативи, благодійні та інші фонди, виробничі об'єднання, акціонерні товариства, а також інші форми об'єднання фізичних та юридичних осіб, передбачені законом.

Під установою розуміється організація, створена для здійснення управлінських, соціально-культурних чи інших функцій непромислового характеру.

Згідно ст. 20 Закону РФ «Про державну таємницю» органи державної влади, підприємства, установи та організації (далі – підприємства) забезпечують захист відомостей, що становлять ДТ, відповідно до покладених на них завдань і в межах своєї компетенції. Захист ДТ є видом основної діяльності підприємства.

Організація робіт із захисту ДТ на підприємствах здійснюється їх керівниками. Залежно від обсягу робіт керівником підприємства створюється структурний підрозділ із захисту ДТ або призначаються штатні фахівці з цих питань.

Загальні вимоги з організації та проведення робіт із захисту ДТ встановлюються в Інструкції, яка затверджується Урядом РФ. Така інструкція містить вимоги щодо забезпечення пропускного режиму, охорони території об'єкта, доступу персоналу на територію, по порядку поводження з секретними документами, захист інформації від технічних розвідок, від її витоку технічними каналами, а також інші вимоги.

Однією з важливих завдань підрозділу захисту ДТ є захист інформації, що становить цю таємницю, від технічних розвідок, витоку інформації технічними каналами, несанкціонованому доступу до інформації в системах інформатизації та зв'язку. При значному обсязі робіт з вирішення цього завдання на підприємстві може створюватися спеціальний структурний підрозділ захисту інформації.

Підрозділи захисту інформації (штатні спеціалісти) на підприємствах виконують такі функції:

- визначають (спільно з замовниками) основні напрямки робіт із захисту інформації;

- беруть участь у погодженні технічних завдань на проведення робіт із захисту інформації;

- дають висновок про можливість проведення робіт з інформацією, що містить відомості, віднесені до ДТ;

- беруть участь при виконанні заходів щодо захисту інформації;

- здійснюють контроль за виконанням та ефективністю проведених заходів.

Вони підпорядковуються безпосередньо керівнику підприємства або його заступнику і забезпечуються засобами захисту інформації та контролю відповідно до спеціалізації підприємства.

Для проведення робіт по захисту інформації можуть залучатися на договірній основі спеціалізовані підприємства та організації, які мають ліцензії на проведення робіт у сфері захисту інформації.

Правовою основою для організації захисту інформації, що становить ДТ, служать діючий на підприємстві Перелік відомостей, що підлягають засекречуванню, який розробляються на основі галузевих (відомчих, програмно-цільових) розгорнутих переліків відомостей, що підлягають засекречуванню.

Загальна технологічна схема організації захисту інформації, що становить ДТ, являє собою послідовну (при необхідності – ітераційну) процедуру, показану на рис. 14, яка включає :

- оцінку загроз безпеки інформації та стану захисту інформації на підприємстві;

- визначення цілей і завдань захисту інформації, прийняття рішення про заходи захисту інформації;

- планування заходів щодо захисту інформації;

- постановки завдань виконавцям робіт, організації їх взаємодії та всебічного забезпечення;

- виконання запланованих заходів;

- контроль за виконанням заходів та оцінка їх ефективності.

В якості вихідних даних для організації процесу захисту інформації використовуються:

- зміст інформації, що використовується, її СС, обсяги інформації;

- характеристики застосованих носіїв інформації;

- описи інформаційних процесів, що протікають;

- вимоги з питань захисту інформації, що містяться в законодавчих, організаційно-розпорядчих та нормативних документах;

- зміст програм і планів робіт установи, у тому числі з питань захисту ДТ;

- інформація, що міститься в каталогах, довідниках, посібниках та інших інформаційних документах з питань захисту інформації.

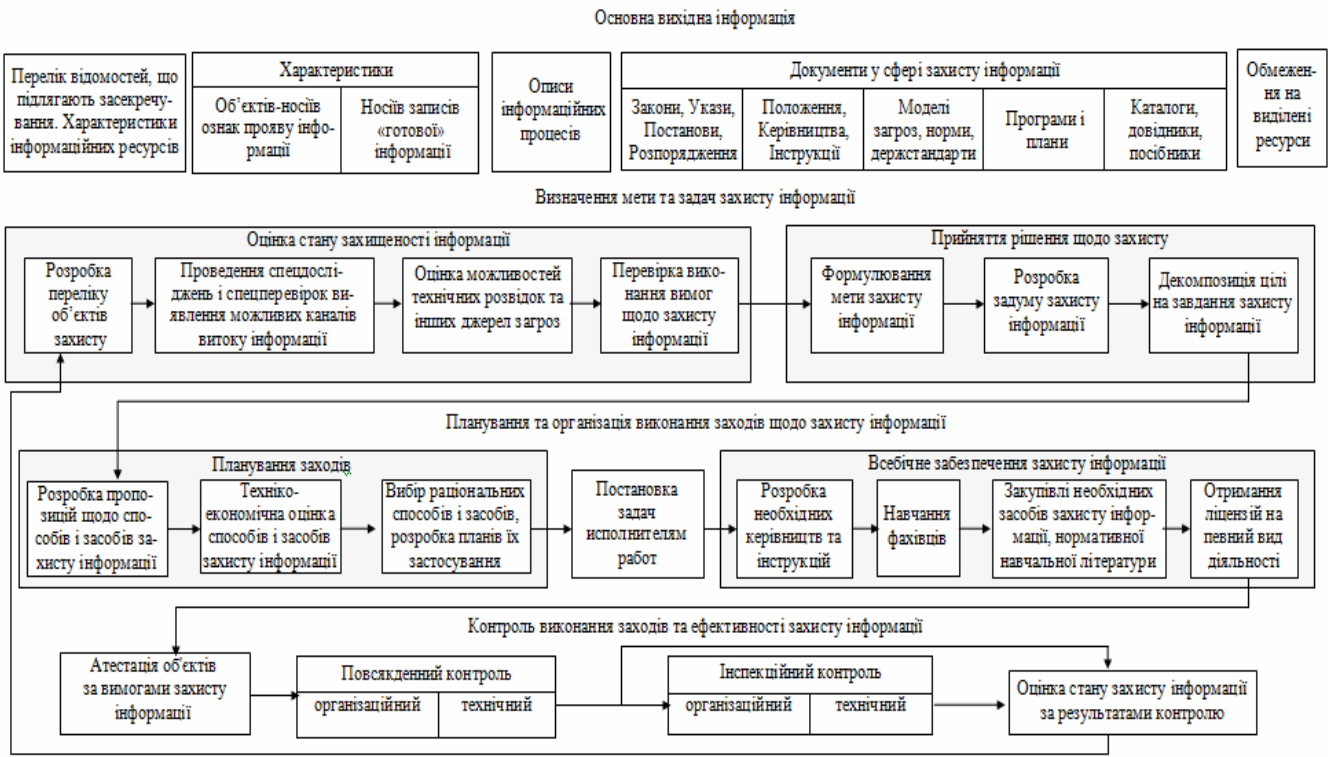


Рис.14 Технологічна схема організації захисту інформації на підприємстві (в установі, організації)

Загальна характеристика та проблемі аспекти

Складність та актуальність проблеми аналізу і оцінки шкоди в РФ підкреслює той факт, що перелік відомостей, віднесених до ДТ, формувався без наявності єдиної методики (порядку) визначення розмірів можливої шкоди, що наноситься державі розголошенням відомостей, як того вимагають норми Закону РФ «Про державну таємницю» [63], що відмічено науковою працею [64]. Відсутність такої методики обумовлена відсутністю несуперечливих (науково-обґрунтованих) критеріїв оцінювання величини можливої шкоди внаслідок розголошення відомостей, що становлять ДТ, на яких ця методика повинна ґрунтуватись.

Також у працях [65, 66] російськими вченими визнано, що зазначена методика може бути розробленою тільки на основі аналізу практики формування Переліку відомостей, віднесених до ДТ РФ, яке фактично почалося з рівня підприємств та установ, а у кращому випадку – окремих міністерств та відомств. У такому підході до формування масиву СІ нині виявилися суттєві недоліки, які створюють передумови до необґрунтованого засекречування інформації. Це було відмічено на парламентських слуханнях Комітету Державної Думи з безпеки РФ за темою «Актуальні проблеми удосконалення законодавства про державну таємницю», у рекомендаціях якого було зазначено [65]: «…віднесення інформації до «ЦТ» та «Т», що складають більшу частину відомостей, що становлять ДТ, обумовлено шкодою, яка завдається інтересам відомства чи організації, але не інтересам РФ. Це положення створює передумови для необґрунтованого засекречування, усунення яких потребує уточнення критеріїв віднесення відомостей до ДТ».

У рекомендаціях учасників зазначених слухань Уряду РФ зазначено, що законодавство РФ потребує удосконалення, зокрема необхідно [65]:

- удосконалити систему засекречування та розсекречування відомостей, що становлять ДТ (з урахуванням економічної доцільності);
- удосконалити формулювання Переліку відомостей, віднесених до ДТ, з метою однозначності розуміння, а також уточнення його окремих положень у частині відображення реалій сучасного політичного життя;
- у зв’язку з відсутністю методики оцінювання шкоди від розголошення ДТ, розглянути доцільність видання спеціальними органами висновків про завдану шкоду через порушення законодавства про ДТ та ін.

Чинний методичний апарат оцінювання показників шкоди, що завдає неправомірне розповсюдження відомостей, що становлять ДТ РФ, оснований на використанні експертних оцінок, які визначаються спеціально організованими ЕК на основі методу попарного порівняння із застосуванням методологічного підходу Т.Л. Сааті [69, 70], застосованого

також у [67]. Ця методика не враховує вартісних витрат на забезпечення заходів щодо захисту інформації, упущеної економічної вигоди у разі заборони відкритого поширення та використання цієї інформації, а також заходів з забезпечення протидії загрозам національній безпеці, що виникатимуть у разі її розповсюдження.

Однак у роботі [67] пропонуються перспективні розробки, що передбачають представлення шкоди у вигляді інтегрального показника, що складається з *кількісної* та *якісної* частин у вартісному вигляді з врахуванням вказаних чинників на результат оцінювання шкоди.

Кількісна складова шкоди є сумою витрат у вартісному (грошовому) вигляді на приховування відомостей, що становлять ДТ, втрачену економічну користь у разі їх відкритого використання, на здійснення заходів з забезпечення нейтралізації наслідків діяльності «супротивника» на основі розкритої інформації.

Якісна складова шкоди враховує зв'язок між розповсюдженням інформації та його наслідками, які неможливо формалізувати достатньою мірою для включення до кількісної складової (наприклад, зменшення рівня довіри до органів державної влади, підрив довіри до держави з боку учасників міждержавних договорів, формування негативної суспільної думки про державу, недовіра союзників та партнерів тощо).

Для відображення якісної складової на шкалі кількісної складової та наступного формування інтегральної шкоди чи *інтегрального показника шкоди* (сума кількісної та якісної складових у грошовому вигляді) пропонується використати експертне оцінювання. Інтегральний показник прямо визначає СС інформації (ступінь обмеження доступу до інформації) або його відсутність. У [64] вказується, що в РФ існують видові методики визначення кількісної складової шкоди, за допомогою яких така шкода оцінюється в міністерствах та відомствах різних сфер діяльності держави. Тому, методика зосереджується на оцінюванні *якісної* складової шкоди, що включає такий порядок оцінювання [66]:

1) визначення відомостей, що становлять ДТ;

2) визначення загроз РФ, що виникають під час неправомірного розповсюдження зазначених відомостей;

3) за допомогою визначених відомостей та загроз з використанням видових методик визначається кількісна складова шкоди в різних сферах діяльності держави (зовнішньополітичній, економічній, воєнній, розвідувальній, контррозвідувальній, оперативно-розшуковій);

4) одночасно з попередніми діями формується ЕК, яка експертними методами визначає якісну складову шкоди від неправомірного розповсюдження визначених відомостей;

5) визначається інтегральна шкода додаванням складових шкоди в грошовому вигляді;

6) на основі інтегральної шкоди корегується СС відомостей.

Методичний підхід для визначення *якісної* складової шкоди до п.4) включає розв'язання двох завдань [66]:

1) побудова на множині відомостей, що становлять ДТ, рейтингової шкали секретності;

2) експертне оцінювання ступеня проявів різноманітних загроз та формування вербальної оцінки можливої шкоди (оцінка зв'язку «загроза – шкода»).

Рейтинг, визначений експертним шляхом, являє собою кількісний внесок (у вартісному виразі) якісної складової шкоди до інтегрального показника. Шкала секретності будується відображенням рейтингів відомостей на лінійно упорядкованій множині лінгвістичної змінної «СС».

Під час розв'язання другого завдання вважається, що перелік загроз державі вже визначено і відображено у відомчих переліків відомостей, віднесених до ДТ. Для формування оцінок «загроза – шкода» необхідно використовувати такі методики як [66]:

- оцінювання значимості загроз безпеці держави;
- оцінювання ймовірності появи загроз безпеці держави;
- оцінювання відносної шкоди (рейтингів) безпеці держави від неправомірного розповсюдження відомостей.

У роботі [64] звернено увагу на те, що методика, яка пропонується у [66], передбачає корегування СС лише у бік підвищення за рахунок якісної складової. Це вказує на те, що ДТ в РФ «зароджується» на рівні міністерств та відомств з подальшим «підйомом» до загальнодержавного рівня.

2.2. Порядок засекречування класифікованої інформації в США

З 1940 року питання віднесення інформації до секретної у загальнодержавному масштабі регулюються нормативно-правовими актами Президента Сполучених Штатів Америки (США) [71, 72]. У 2009 році Президентом США був підписаний executive order (EO) (виконавчий наказ) 13526 «Classified National Security Information» [73] – «Класифікована інформація у сфері національної безпеки» – (далі – EO 13526), який встановлює сучасні правила засекречування (класифікації) інформації у США. Інтерес до системи засекречування інформації у США обумовлюється значною роллю цієї країни у світі, а також тим, що у зв'язку з опублікуванням великого масиву інформації ІзОД у мережі Інтернет (Wikileaks.org) американським установам прийшлось за

короткий строк переглянути величезний обсяг інформаційних масивів на предмет визначення необхідності їх подальшого засекречування та попередження шкоди національній безпеці, а також удосконалити власну інформаційну політику.

Для визначення СІ у США використовується термін «класифікована» (classified). Процес засекречування (віднесення до класифікованої або класифікації) інформації визначається за допомогою термінів «первинна» (original) та «похідна» (derivative) класифікація.

Первинне засекречування пов'язується зі створенням «нових» секретів і включає дві дії, аналогічні передбаченим українським законодавством щодо віднесення інформації до секретної та засекречування матеріального носія цієї інформації.

Похідне засекречування не пов'язується зі створенням «нових» секретів і включає тільки засекречування МНІ на підставі того, що він містить вже засекречену інформацію, про що зазначено на іншому носієві інформації або в окремих інструкціях із засекречування (classification guides).

У подальшому для відрізнення первинного засекречування від похідного використовуватимуться термінологічні словосполучення «засекречування інформації» та «засекречування носія інформації». Слід ще раз зазначити, що віднесення інформації до ДТ («засекречування інформації») за нормативно-правовими актами США збігається з першим засекречуванням носія цієї інформації.

У США особи, уповноважені здійснювати засекречування інформації, (original classification authorities або OCAs), яких також називають «класифікаторами» (original classifiers), призначаються Президентом і Віце-Президентом США з числа керівників агентств (центральних державних органів) та інших посадових осіб.

Президент та Віце-Президент є також особами, уповноваженими здійснювати засекречування інформації. На відміну від українського законодавства, особи, визначені класифікаторами у США у системі державної влади, можуть делегувати свої повноваження щодо засекречування інформації підпорядкованим посадовим особам.

ЕО 13526 містить норму про необхідність обмеження чисельності осіб, яким делегуються повноваження з засекречування інформації, мінімально необхідною кількістю. Також зазначається про необхідність обґрунтування таких рішень, їх централізованого обліку та уникання випадків делегування повноважень для тимчасового, разового використання права з засекречування інформації. З початку XXI сторіччя кількість осіб, яким було надано право засекречування інформації, була відносно стабільною - близько 4100 осіб. У 2008-2009 роках чисельність OCAs суттєво зменшилася (майже на 40%). Це

пов’язується саме з посиленням вимог до делегування повноважень в ЕО 13526 та зусиллями зі зменшення чисельності таких осіб, що були здійсненими насамперед у Міністерстві закордонних справ (Department of State). У 2010 році таких осіб було 2378 [71, 74].

Посадові особи з делегованими повноваженнями від інших OCAs розрізняються за своїми правами щодо класифікації інформації різних рівнів засекречування (classification levels). Якщо проводити паралель з українською термінологією сфери ОДТ, то американським рівням засекречування відповідатимуть вітчизняні СС. Найвищим (з трьох існуючих) рівнем засекречування є «Top Secret». Цьому рівню відповідає український СС «ОВ» [71, 75]. Особам, яких визначено уповноваженими засекречувати інформацію з таким рівнем засекречування, вважаються уповноваженими засекречувати інформацію з нижчими рівнями засекречування «Secret» (відповідає українському СС «ЦТ» [71, 75]) та «Confidential» (відповідає українському СС «Т» [71, 75]).

Наприклад, у 2010 році осіб, яких було визначено уповноваженими засекречувати інформацію «Top Secret», «Secret» і «Confidential», було 901 (38%), «Secret» і «Confidential» – 1463 (61,5%), «Confidential» – 14 (0,5%) [71, 74].

Для регулювання обсягу засекреченої інформації в ЕО 13526 встановлюються правила засекречування і розсекречування інформації.

До основних правил засекречування (крім того, що засекречування інформації здійснюється тільки уповноваженими на це особами) належать наступні, які повинні виконуватись разом:

1) інформація повинна мати відношення до системи державної влади США (находитись у її власності, під її контролем або створена нею чи для неї);

2) інформація повинна належати до встановлених законодавством категорій інформації;

3) особа, уповноважена засекречувати інформацію, повинна визначати, що розголошення (в ЕО 13526 використовується словосполучення «unauthorized disclosure» – несанкціоноване розкриття) цієї інформації резонно завдасть шкоди національній безпеці, у тому числі антитерористичній діяльності. При цьому така шкода повинна бути визначеною або описаною цією особою.

Інформацію слід засекречувати за рівнем «Top Secret», якщо її розголошення завдасть надзвичайно тяжкої (exceptionally grave) шкоди національній безпеці, «Secret» – серйозної (serious) шкоди, «Confidential» – шкоди національній безпеці без визначення особливих її ознак.

Під шкодою національній безпеці (damageto the national security) розуміється шкода (harm) національній обороні або міжнародним відносинам США.

З метою засекречування інформації урядів іноземних країн передбачається, що несанкціоноване поширення інформації іноземного уряду завдає шкоди національній безпеці США. Наявність суттєвих сумнівів у необхідності засекречування інформації у особи, уповноваженої на цю дію, визнається достатньою підставою для залишення інформації некласифікованою. Законодавство США визначає категорії інформації або певні сфери державної діяльності, у яких інформація може бути засекреченою, а саме:

- системи озброєння, воєнні та військові операції та плани;
- інформація іноземних урядів;
- заходи, джерела та методи розвідки або криптології;
- міжнародні відносини або закордонні заходи США, включаючи конфіденційні джерела;
- наукові, технологічні або економічні питання, пов'язані з національною безпекою;
- програми системи державної влади США для забезпечення безпеки ядерних матеріалів та устаткування;
- вразливість та можливості систем, пристроїв, інфраструктур, проектів, планів або служб захисту, пов'язаних з національною безпекою;
- розроблення, виробництво або використання зброї масового ураження.

Слід зазначити, що поняттям розвідка у ЕО 13526 охоплюється й контррозвідка. За 2010 рік у США було зареєстровано 224734 випадки засекречування інформації, з них за рівнями: «Top Secret» – 4194 (2%), «Secret» – 181045 (81%), «Confidential» – 39495 (17%) [71, 74].

Законодавство США (як і українське законодавство) визначає випадки, коли інформацію заборонено засекречувати. Рішення про необхідність засекречування чи розсекречування інформації ні в якому разі не повинні мати за мету:

- приховування порушення закону, неефективності або помилки державного управління;
- запобігання складним ситуаціям, у яких може опинитись особа, підприємство або установа;
- обмеження конкуренції;
- зупинення чи призупинення поширення інформації, для якої немає підстав для засекречування.

За загальним правилом, інформацію, що вже була розсекреченою, не слід знову засекречувати. Така дія потребує особливого обґрунтування.

Не слід також засекречувати інформацію про наукові дослідження, що не стосуються національної безпеки. Засекречування носіїв інформації (похідне засекречування), не пов'язується зі створенням «нових» секретів, а лише зі збільшенням кількості форм матеріального втілення вже існуючих, тобто кількості МНСІ.

У 2010 році у США було зафіксовано 76,6 мільйонів рішень про засекречування носіїв інформації, з них за рівнями: «Top Secret» – 21,5 млн. (28%), «Secret» – 36 млн. (47%), «Confidential» – 19,1 млн. (25%). Представляє інтерес те, що у 2009 році було зафіксовано зростання кількості таких рішень більше ніж у двічі, а у 2010 році – ще приблизно на 30%, у 2011 році також очікується їх зростання. Це явище пов'язується з виконанням керівних документів, прийнятих у 2009 році та спрямованих на підвищення пильності у фіксуванні рішень з засекречування носіїв інформації особливо у сфері електронного документообігу [71, 74].

Положення ЕО 13526 містять вимоги про обов'язкове навчання осіб, які мають право засекречувати інформацію, (раз на рік) та осіб, які засекречують носії інформації, (раз на два роки). Осіб, які не пройшли таке навчання, керівникам агентств наказується позбавляти права засекречувати інформацію чи носії інформації. Також ЕО 13526 містить деякі вимоги до змісту такого навчання, що повинне включати вивчення порядку засекречування та розсекречування інформації та її носіїв з акцентуванням уваги на попередження зайвого засекречування. Крім того навчання повинно передбачати порядок забезпечення безпеки СІ (порядок забезпечення РС) та санкції, які застосовуватимуться до порушників порядку засекречування та розсекречування інформації та її носіїв і порядку забезпечення РС. Серед таких санкцій визначено: догана, тимчасове утримання заробітної плати, звільнення з посади, обмеження у правах з засекречування, втрату чи відмову у доступі до СІ тощо.

Невід'ємною складовою системи засекречування (security classification system) визнається розсекречування. Важливими правилами розсекречування інформації є припущення про те, що ніяка інформація не може залишатись засекреченою невизначено довго, і те, що факт розголошення інформації не є підставою для її автоматичного розсекречування.

Прийнято виокремлювати чотири шляхи, за якими інформація та її носії можуть бути розсекреченими:

- внаслідок автоматичного розсекречування (Automatic Declassification),
- внаслідок систематичного перегляду для розсекречування (Systematic Declassification Review),

- внаслідок дискреційного («на власний розсуд») перегляду для розсекречування (Discretionary Declassification Review),
- внаслідок мандатного («за запитом») перегляду для розсекречування (Mandatory Declassification Review).

Автоматичне розсекречування (Automatic Declassification) є загальним правилом розсекречування інформації, за яким через 25 календарних років після засекречування інформація повинна бути розсекреченою. У зв'язку з існуванням великої кількості винятків із загального правила розсекречування ЕО 13526 передбачає необхідність здійснення систематичного перегляду інформації для розсекречування. Організація такого перегляду вимагає створення у кожному агентстві переліків СІ та її носіїв, яких виключено з автоматичного розсекречування, та відповідних планів (програм) з їх перегляду. Протягом 2010 року у США було переглянуто 45,4 млн. сторінок документів у рамках автоматичного розсекречування та 5,8 млн. сторінок документів у рамках систематичного перегляду. За результатами першого було розсекречено 24,2 млн. сторінок документів і другого – 4,6 млн. сторінок документів [71, 74]. Слід зазначити, що строк засекречування інформації може бути як менший так і більший 25 років. Найтриваліші строки (50 та 75 років) засекречування як правило встановлюються для інформації, яка може розкрити особу, яка є конфіденційним чи розвідувальним джерелом інформації, або ідеї створення зброї масового ураження.

Дискреційний перегляд («на власний розсуд») (Discretionary Declassification Review) здійснюється у випадках, коли з точки зору особи, яка засекретила інформацію, або агентства, у якому було засекречено інформацію, з'явилися підстави вважати, що ця інформація може бути розсекреченою до встановленого під час її засекречування терміну. За таким типом розсекречування протягом 2010 року у США було переглянуто 1,9 млн. сторінок документів, з яких розсекречено приблизно 181,6 тис. [71, 74].

До цього типу розсекречування законодавство США визначає відносно новий в Україні привід для розгляду доцільності обмеження доступу до інформації через «підвищений суспільний інтерес». Перевага шкоди від оприлюднення інформації над суспільним інтересом у її отриманні встановлюється сучасним українським законодавством [11] однією з необхідних умов для обмеження доступу до інформації. У США підвищений суспільний інтерес також не є достатньою підставою для розсекречування інформації. Його можна вважати обставиною, яка може виникати і яку необхідно враховувати під час прийняття рішення про необхідність залишення інформації засекреченою чи ні. Поява такої обставини становить підставу для організації позапланового розгляду

інформації, до якої такий інтерес виник, особою, яка засекретила цю інформацію, на предмет можливого її розсекречування з огляду на те, що незадоволення суспільного інтересу також може мати шкідливі наслідки для національної безпеки. Якщо така шкода перевищуватиме шкоду від розголошення СІ, то інформацію слід розсекречувати. Треба зазначити, що в ЕО 13526 рекомендується розсекречувати інформацію, до якої виник суспільний інтерес.

Мандатний перегляд класифікованої інформації «за запитом» на її можливе розсекречування (Mandatory Declassification Review) є відносно новим шляхом розсекречування інформації у США, але як визнається дуже дієвим і перспективним. Він здійснюється у відповідь на письмовий запит зовнішнього для агентства суб'єкта про розсекречування певної інформації. У 2010 році було опрацьовано 67726 запитів про розсекречування, за якими було переглянуто 331782 сторінки. У результаті такого перегляду тільки 22089 сторінок (7%) залишилися засекреченими, 213425 сторінок (64%) були розсекреченими у повному обсягу, 96268 сторінок (29%) були розсекреченими частково [71, 74].

ЕО 13526 встановлює обмеження щодо можливості невідкладного проведення перегляду інформації для її розсекречування. Ці обмеження можуть бути пов'язаними з неможливістю ідентифікації інформації у державному органі за ознаками, зазначеними у запиті, а також з тимчасовою забороною у доступі до інформації з метою невідкладного проведення її перегляду для розсекречування, у визначених законодавством випадках. Зважаючи на значущість та необхідність централізації заходів з розсекречування, в ЕО 13526 передбачається створення Національного центру з розсекречування (National Declassification Center) у структурі Адміністрації національних архівів та документації (National Archives and Records Administration) для спрямування процесів розсекречування, сприяння заходам, гарантуючим якість розсекречування, та впровадження одноманітного профільного навчання. Керівник Національного центру з розсекречування призначається керівником зазначеної адміністрації (Архівістом США) за погодженням з керівниками декількох державних органів (Міністерства закордонних справ, оборони, енергетики, внутрішньої безпеки, Генеральним прокурором, Директором Національної розвідки).

ЕО 13526 зобов'язує керівників державних органів забезпечувати директора Національного центру з розсекречування методичною документацією з розсекречування, а також за посередництвом керівництва Адміністрації національних архівів та записів визначати частину особового складу цього Центру, якому делегувалися б повноваження з перегляду, розсекречування (залишення засекреченою)

інформації, яка була створена у підпорядкованих цим керівникам державних органах.

Повноваження щодо розсекречування інформації, одержаної від інших державних органів (агентств), які у подальшому були ліквідованими, встановлюються за такими правилами:

- якщо було визначено державного органу, якому передано функції ліквідованого, то зазначені повноваження переходять до нього;

- якщо такого державного органу не було визначено, то зазначені повноваження переходять до кожного державного органу, який має секретні носії інформації, що були створеними у ліквідованому державному органі.

При цьому розсекречування таких документів слід здійснювати за погодженням з іншими державними органами, які володіють примірниками таких документів.

Річне фінансування діяльності, пов'язаної з засекречуванням інформації та забезпеченням її безпеки, у США, наприклад, у 2009 році складало близько 8,8 мільярдів доларів [15].

Висновки. Системи засекречування (розсекречування) інформації США та України у загальному є схожими: наявність класифікаторів або ДЕТ, рівнів засекречування або СС, строків засекречування, подібність загальних підходів до засекречування (розсекречування) інформації тощо. Але, звичайно, є й відмінності.

Особливістю українського законодавства у сфері ОДТ є передбачення наявності єдиного державного нормативного акта – ЗВДТ, – який об'єднує результати застосування всіх правил засекречування інформації у цілому у державі. Цей акт створює підгрунтя для централізації та уніфікації роботи всіх ДЕТ.

У США робота посадових осіб, уповноважених з засекречування інформації, має більш відокремлений та незалежний характер. Поряд з цим уряд докладає зусиль щодо підвищення ступеня уніфікації роботи зазначених посадовців, що виражається у наявності планів зі створення єдиних правил засекречування (розсекречування) інформації. Деякі методичні підходи з засекречування носіїв інформації, що застосовуються у США, можуть бути використаними і в Україні. На кожному засекреченому носії інформації (у випадку похідного засекречування) зазначаються ідентифікатори того носія інформації, використання інформації з якого стало підставою для засекречування першого. Застосуванням таких позначок можна суттєво зменшити витрати коштів на пошук і прийняття рішення про розсекречування окремого носія інформації у випадках, коли частину носіїв однієї інформації вже розсекречено. Система відміток із засекречування на носіях інформації дозволяє також завжди ідентифікувати посадову

особу, яка здійснила засекречування цієї інформації. Виокремлення спеціальними позначками місць у документах, де наведено СІ, також сприятиме зручності виконання дій з розсекречування чи перегляду документів для розсекречування. Оцінювання результатів перегляду з розсекречування інформації та документів, що містять таку інформацію, за сторінками (аркушами) документів, а не за окремими одиницями обліку – документами, справами і т.п., сприяє більш ґрунтовному аргументуванню розсекречування. До того ж такий підхід точніше відображає витрати праці на виконання такої роботи.

При організації заходів із засекречування (розсекречування) інформації у США застосовується поєднання принципів централізації та колегіальності. З одного боку при Адміністрації національних архівів та документації визначено центральний орган виконавчої влади, уповноважений за цими питаннями, а з іншого – до складу цього органу входять представники всіх державних органів, у яких створюється основна частина «секретів». Особлива увага приділяється питанню підвищення кваліфікації всіх посадових осіб, яких залучено до виконання завдань з засекречування (розсекречування) інформації, та автоматизації (комп'ютеризації) обліку засекреченої інформації та її носіїв, а також інформації, яка була розсекреченою [71-75].

2.3. Організація охорони державної таємниці країн-членів НАТО

(*Естонії, Словаччини, Болгарії, Румунії, Чехії*)

На відміну від українського законодавства, яке визначає СБУ як спеціально уповноважений орган державної влади у сфері ОДТ, законодавство більшості постсоціалістичних країн-членів НАТО не визначає єдиного спеціального органу, відповідального за організацію захисту ДТ серед спеціальних служб, а покладає такі завдання рівною мірою на служби безпеки та інші органи державної влади. При цьому встановлюються чіткі вимоги до цих органів у сфері ОДТ, їх права та обов'язки. В законодавстві країн *Естонії, Румунії, Чехії, Словаччини, Болгарії* орган державної влади, відповідальний за ОДТ, підпорядкований уряду і не належить до спецслужб. Законодавство цих країн чітко визначає відповідальний суб'єкт за організацію та координацію діяльності у сфері ОДТ. Таким суб'єктом є уряди, які в залежності від країни формують відповідальний державний орган захисту ДТ з чітким законодавчим визначенням його повноважень [76-79].

Порівняльний аналіз СОДТ свідчить, що організаційно-правові заходи як в *Естонії*, так і в *Румунії, Республік Чехії* та *Болгарії* не містять принципових відмінностей, однак мають свої особливості з більш або менш чітким визначенням меж правового регулювання

відносин у цій сфері з визначених питань. Зокрема, якщо порівнювати поняття ДТ в поданих законодавчих системах, то в цілому різниці між ними немає. Водночас в деяких країнах є суттєві моменти, які їх відрізняють. Так, в понятті ДТ вона подається як вид інформації, який встановлюється виключно законом, а також чітко зазначається, що така інформація за жодних обставин не може знаходитись поза межами уваги держави (належить, державі, знаходиться під її контролем, створена нею або для неї). Також, особливістю законодавчих систем є порядок класифікації рівнів ДТ. А саме: ДТ, визначені як «обмеженого доступу»; «конфіденційні»; «таємні»; «цілком таємні». Таким чином, вказані рівні класифікації за формою дещо відрізняються, а за змістом майже однакові. При цьому особливістю є те, що інформація яка відноситься до ДТ в іноземній державі чи міжнародній організації, що уклали міжнародну угоду, є ДТ, визначеною як «обмеженого доступу», або є міждержавними секретами [76-79].

Отже, законодавство розглянутих постсоціалістичних країн-членів НАТО містить положення, які відносять до категорії ДТ (або міждержавних секретів) відомості, передані іноземною державою чи міжнародною організацією і стосовно яких встановлюються такі ж механізми захисту як і для власних ДТ.

Характерною рисою правових механізмів даних держав є те, що ДТ усіх рівнів визначаються виключно законом, що в свою чергу не передбачає прийняття додаткових нормативних документів. В інших країнах подібний перелік «ЗВДТ» формується та затверджується урядом. Згідно з положеннями, визначеними в законах про ДТ, саме уряди мають вирішувати питання щодо передчасного розсекречування або продовження терміну секретності інформації, визначеної як ДТ. Передчасне розсекречення чи продовження терміну секретності вирішується міністром за його директивами – щодо питань стосовно певної сфери управління та відповідальності міністерства. Заяви до урядів щодо передчасного розсекречення чи продовження терміну секретності інформації, визначеної як ДТ, має бути подана через міністра, який відповідальний за сферу управління уряду, якої стосується заява.

Законодавство цих країн-членів НАТО у сфері ОДТ не містить поняття дозвільного порядку діяльності відповідних органів у сфері забезпечення ОДТ. Всі питання дозвільного порядку охоплюються наданням доступу юридичним особам до діяльності, пов’язаної з ДТ, а також наданням, відмовою, продовженням строку та відкликанням дозволу на допуск до СІ. При цьому, процедура отримання дозволу на провадження діяльності, пов’язаної з ДТ, практично ідентична у своїх основних позиційних блоках законодавству України щодо подання заявки, підготовчого етапу, перевірки готовності, прийняття рішення тощо. Особливістю законодавства розглянутих держав є те, що

законодавець чітко визначив правові підстави, які унеможливлюють надання дозволу на провадження діяльності, пов'язаної з ДТ і мають вичерпаний перелік. Законодавство країн про ДТ щодо доступу до ДТ визначає питання як дозволу на допуск до ДТ юридичних осіб, так і порядок допуску та доступу фізичних осіб, при цьому не встановлюючи чіткої різниці між поняттями дозволу, допуску та доступу. Особливістю законодавчих систем у сфері ОДТ є також питання доступу до ДТ за посадою. Зокрема, визначається право доступу згідно повноважень до ДТ, незважаючи на їх секретність, таких посадових осіб: Президент з метою виконання обов'язків, покладених на нього Конституцією і Законами [77, 78], та іншими нормативними актами, виданими на їх основі; член парламенту у випадках, передбачених законодавством про внутрішні норми його діяльності; член уряду у випадках, передбачених Законом про Уряд; суддя у випадках, передбачених у Кодексі з процедури; Командувач і Головнокомандувач Сил оборони у випадках, передбачених Законами стосовно національної оборони тощо (***Естонська Республіка***).

Отже, як випливає з визначеної нормативної системи, посадова особа згідно своїх службових повноважень може отримати доступ до всіх видів СІ згідно з законом про відповідний державний орган.

Також до особливостей окремих законодавчих систем можна віднести доступ до ДТ на основі попереднього наказу слідчого або прокурора чи на основі судового рішення учасників досудового розгляду або судового провадження на підставі порядку, прописаного в Кодексі з процедури та проведення спеціальної перевірки відповідним відомством (наприклад, в *Естонській Республіці*). Крім того, відмінністю більшості законодавчих СОДТ є те, що рішення про надання допуску на доступ до ДТ приймається відповідною службою безпеки, порядок здійснення перевірки осіб для допуску до СІ здійснюється відповідно до процедури, встановленої виключно законодавством, зокрема, Законами про нагляд та Законами про служби безпеки [77, 78]. Терміни проведення спеціальної перевірки згідно законів встановлюються доволі тривалими та можуть бути подовжені в залежності від важливості тієї інформації, до якої має намір отримати доступ зацікавлена особа, (а саме: три місяці стосовно інформації «обмеженого доступу» та «Т»; шість місяців – стосовно «ЦТ»).

Законодавство *Естонської Республіки* [77, 78] ґрунтується на базовому Законі від 26 січня 1999 року «Про державну таємницю», де зазначається, що ДТ – інформація, визначена виключно Законом, що вимагає її захисту від розголошення, в інтересах національної безпеки *Естонської Республіки* і яка належить державі, знаходиться під контролем держави, створена нею або для неї. До категорій відомостей, визначених як «Т» в основному відносяться відомості у сфері оборони, військового характеру (20 пунктів).

Також, як визначено законодавством про ДТ окремих країн особа, яка отримує доступ до ДТ в силу своїх службових повноважень, не завжди звільняється від перевірки (наприклад *Естонія, Румунія*), зокрема відповідна посадова особа отримує доступ до усіх видів СІ за посадою, якщо стосовно неї немає підстав, що унеможливлюють такий доступ. Стосовно обмеження оприлюднення, передачі або поширення іншим чином СІ, законодавство у сфері ОДТ розглянутих країн не містить конкретної чітко вираженої норми, однак включає окремі процедури, які стосуються доступу іноземців до ДТ, а також передачі відомостей, що складають ДТ та виконання відповідних зобов'язань виключно в рамках міжнародних договорів .

Щодо відповідальності за порушення законодавства у сфері ОДТ особливостей або принципових відмінностей між законодавчими системами немає, однак адміністративні аспекти у переважної більшості законодавств підсилений, при цьому позитивним профілактичним моментом є те, що вже сам факт порушення порядку визначеного законодавством про ДТ без розголошення секретних відомостей або їх втрати передбачає фінансову відповідальність шляхом встановлення штрафних санкцій (наприклад, в *Естонській Республіці* такий штраф складає 50000 естонських крон) [76-79].

Специфіка організації спеціальних служб ***Словацької Республіки*** (СР) також полягає в тому, що вони формувались у рамках щойно створеної самостійної держави після розпаду Чехословаччини і виникнення двох незалежних держав – Чехії та Словаччини. Структура спеціальних служб Словаччини з урахуванням чітко визначеного курсу керівництва країни на її інтеграцію до європейських та євроатлантичних структур зазнала суттєвих змін.

Для вирішення поставлених завдань у Словаччині було створено контррозвідувальну і розвідувальну системи спеціальних служб [80]:

− *Словацька інформаційна служба* (СІС) – цивільна розвідка і контррозвідка. СІС є основним контррозвідувальним і розвідувальним органом Словаччини, діяльність якого регламентується законом «Про Словацьку інформаційну службу» від 18.04.1995 р. №72. З моменту створення (1993р.) спецслужба безпосередньо підпорядковувалася президенту Словаччини, але внаслідок низки політичних скандалів з її участю у 1995-1996 рр. Національна Рада (парламент) СР прийняла постанову про зміни до закону «Про СІС», згідно з якою СІС була підпорядкована уряду СР. Відтоді керівника СІС призначає президент за відповідним поданням уряду Словацької Республіки. Спецслужба нараховує у своєму штаті близько 1200 співробітників.

– *Військова розвідувальна служба* (ВРС) – військова зовнішня розвідка міністерства оборони Словаччини.

– *Військова оборонна розвідка* (ВОР) – військова контррозвідка міністерства оборони Словаччини.

– *Управління національної безпеки* (УНБ СР) – основний уповноважений орган у сфері захисту відомостей, що становлять ДТ, у т. ч. таємниць НАТО, забезпечує контроль і перевірку державних службовців Словаччини, які обізнані за характером службової діяльності з відомостями, що становлять ДТ. УНБ СР виконує завдання у сфері інформаційної, фізичної, об'єктової, персональної, адміністративної безпеки та електронного підпису.

– *Міністерство внутрішніх справ* (МВС) – виконує окремі функції цивільної розвідки.

Зазначені відомства почали виконувати завдання з метою здобування розвідувальної інформації (СІС, ВРС) і забезпечення жорсткого контррозвідувального режиму в країні (СІС, ВОР та окремі підрозділи МВС). Окрім того, одним із головних завдань національної служби (СІС) стало створення в країні дієвої системи протидії розвідувальній діяльності іноземних розвідок, а також міжнародному тероризму, організованій злочинності та незаконній міграції.

Зовнішній контроль за діяльністю СР інформаційної служби здійснюють:

– *Спеціальний Комітет Національної Ради Словацької Республіки з контролю за діяльністю СІС*. Він складається з депутатів – представників коаліційних та опозиційних партій. Директор СІС щорічно звітує перед парламентом про виконання Службою поставлених завдань. Окрім того, парламент виконує і ключову контрольно-регуляційну функцію шляхом схвалення бюджету СІС. Представники згаданого вище Комітету мають право у супроводі представників Служби відвідувати об'єкти спецслужби. Засідання Комітету є закритими і відбуваються не рідше одного разу за квартал. Ініціювати позачергове засідання Комітету має право кожен з його членів. У парламенті діють також окремі комітети з контролю за роботою інших спецслужб СР. Спеціальний комітет з контролю за діяльністю військових спецслужб, Спеціальний комітет з контролю за діяльністю УНБ, Комітет з питань перевірки рішень УНБ.

– *Уряд Словацької Республіки*, який контролює ефективність функціонування систем управління та забезпечення гарантій національної безпеки. Зокрема, за ефективне виконання своїх функцій СІС є відповідальною перед Радою оборони СР, яка у письмовій формі визначає для неї ключові завдання. Крім того, на зазначеному рівні здійснюється контроль за дотриманням бюджетної дисципліни.

– *Суди і прокуратура* здійснюють контроль за можливими порушеннями службового законодавства, а також при використанні оперативно-технічних засобів, що передбачає надання дозволу суду.

Внутрішній контроль за діяльністю співробітників спецслужб здійснюють спеціалізовані контролюючі підрозділи (внутрішньої безпеки). Робота вказаних підрозділів регламентується внутрішніми наказами та інструкціями. Ефективною є система контролю за діяльністю спецслужб країни з боку *засобів масової інформації (ЗМІ) і суспільства***.**

Випадки порушення спецслужбами чинного законодавства регулярно відслідковуються і висвітлюються ЗМІ та суспільством, які ініціюють їх винесення на розгляд *профільних комітетів* Національної Ради СР. Одним із важливих інструментів контролю за діяльністю спеціальних служб СР є *Комітет Національної Ради з питань прав людини та національних меншин*. Він надає згоду або забороняє доступ до інформації, що зберігається в архівах Інституту пам'яті народу і висвітлює діяльність колишньої спеціальної служби ЧССР.

Розглядаючи питання координації роботи спецслужб у СР, слід відзначити, що державного органу, який би координував їх діяльність, не існує. Фактично керівництво ними здійснює прем'єр-міністр (особисто або через відповідальних міністрів). Поряд із цим у країні створено Раду безпеки, яка є дорадчим органом уряду та очолюється прем'єр-міністром СР. У рамках Рада безпеки СР діє *Комітет з питань координації роботи спецслужб***.** До його напрямів діяльності відносяться: координація роботи спецслужб, обговорення пропозицій із цих питань для розгляду на Раді безпеки СР, розгляд проектів нормативно-правових документів щодо координації роботи спеціальних служб та подання їх до Ради безпеки СР, підготовка професійних оцінок та базових документів з питань координації роботи спецслужб. Керівником Комітету з питань координації роботи спецслужб є керівник Ради безпеки СР (прем'єр-міністр), а заступником – заступник керівника Ради. Членами Комітету є: міністри закордонних справ, оборони, внутрішніх справ, директори СІС, ВОР міністерства оборони, президент Поліцейського корпусу МВС, директор УНБ.

Окремо слід відзначити роботу з розробки словацькими юристами норм *захисту інформації з обмеженим доступом* у внутрішньому праві своєї країни. Як відомо, кожна держава, яка вступає в НАТО, бере на себе певні зобов'язання, у т.ч. пов'язані із захистом інформації з обмеженим доступом, або у термінології НАТО – класифікованої інформації. Остання визнана такою, від якої залежить безпека НАТО і для якої визначено відповідний гриф.

У системі забезпечення реалізації національної безпеки ***Республіки Болгарії*** одне із головних місць займає питання внутрішньої та зовнішньої політики безпеки яка визначає функції органів державної безпеки та їх загальну структуру, а також участь в діяльності із забезпечення національної безпеки. Головні функції політики безпеки спрямовані на досягнення цілей системи національної безпеки,

забезпечення внутрішньої стабільності та захисту суспільства і громадян Згідно з Законом [81] Республіки Болгарія «Про Державне агентство національної безпеки» від 20 грудня 2007 року органом спеціального призначення при Раді Міністрів Республіки Болгарія є *Державне агентство національної безпеки*, яке у своїй діяльності керується принципами [81]: діє виключно в межах Конституції, законів і чинних міжнародних договорів; дотримання та забезпечення прав людини та основних свобод; захисту інформації та джерел її отримання; об'єктивності і неупередженості; співпраці з громадянами; політичного нейтралітету. До основних засад діяльності цього агентства відноситься [81]: спостереження, виявлення, припинення і запобігання порушенням у сфері національної безпеки, у тому числі із залученням інших спеціальних органів, які діють в рамках Міністерства оборони, зокрема: протидія розвідувальним спрямуванням на користь іноземних держав; визначення загроз державному суверенітету, територіальній цілісності та єдності нації; будь-яких проявів неконституційного характеру; протидія загрозам (порушенням) національній системі захисту СІ, інформаційних систем та систем зв'язку та інше.

Державне агентство національної безпеки у межах своїх повноважень у взаємодії з іншими спеціальними органами забезпечує контррозвідувальний захист стратегічних проектів, планів та напрямів діяльності держави (включаючи охорону СІ), а також відповідно до законодавства організовує і проводить оперативно-розшукову та оперативно-технічну діяльність, забезпечує криптографічний захист СІ в Болгарії, дипломатичних і консульських представництвах на придбання, систематизації та обробки інформації з іноземних джерел в інтересах національної безпеки та оперативного управління національними секторами, здійснює моніторинг діяльності у зв'язку з перебуванням іноземців в Болгарії, здійснює та забезпечує проведення заходів міжнародного співробітництва, інші види діяльності відповідно до законодавства Республіки Болгарії [81, 82].

Стосовно повноважень вищих органів влади у сфері ОДТ, то законодавство про захист СІ не містить чітких меж їх перерозподілу, однак, як випливає із Закону [83] «Про захист секретної інформації», основним органом на який покладаються питання організації захисту СІ є *Уряд Республіки Болгарія*. При цьому, Уряд встановлює і забезпечує процедуру захисту СІ шляхом прийняття відповідних рішень. З метою належної організації і координації захисту СІ Уряд Республіки Болгарія формує *Державну комісію інформаційної безпеки*. Саме на цю комісію згідно Закону покладається завдання безпосереднього захисту СІ та формування державної політики у сфері ОДТ. До її повноважень відноситься [83]: аналіз і оцінка готовності до захисту СІ у випадках загрози заподіяння шкоди інтересам, які охороняються законом в результаті несанкціонованого доступу до СІ; організація і проведення

заходів щодо запобігання і зменшення шкідливого впливу несанкціонованого доступу до СІ; розробка та подання на затвердження Ради міністрів проектів нормативних документів про захист СІ; організація і забезпечення функціонування реєстрів у галузі міжнародних відносин, пов'язаних з СІ; організація, контроль і несе відповідальності за виконання своїх зобов'язань щодо захисту СІ згідно міжнародних договорів; проведення вивчення і перевірки спільно зі службами безпеки, кандидатів для призначення на посади співробітників інформаційної безпеки; спільно з Державним агентством національної безпеки перевіряти болгарських громадян, які займають посади або залучаються для виконання спеціальних завдань, що вимагають обробки СІ в іншій країні чи міжнародній організації, після отримання письмового запиту компетентного органу з інформаційної безпеки країни або міжнародної організації; ведення єдиного реєстру виданих, анульованих або призупинених ліцензій, сертифікатів і дозволів на діяльність і роботу, пов'язану з СІ, а також реєстр матеріалів і документів, які містять відомості, що становлять державну або службову таємницю; термінове повідомлення Прем'єр-міністра про випадки несанкціонованого доступу до СІ з грифом секретності «ЦТ»; організація та координація підготовки кадрів для роботи з СІ; забезпечення технічного управління інформаційною безпекою; здійснення загального контролю за охороною СІ, яка зберігається, обробляється і передається в автоматизованих інформаційних системах і мережах; надання дозволу на проведення інспекцій відповідно до міжнародних договорів про взаємний захист СІ [82].

Водночас, болгарське законодавство передбачає організацію та проведення окремих заходів захисту СІ в межах компетенції *Служби військової інформації* (СВІ) (український аналог – Головне управління розвідки Міністерства оборони України) за своїм напрямом й сферою діяльності. При цьому встановлюються чіткі вимоги до Державного агентства національної безпеки у сфері охорони СІ, його права та обов'язки, а також виконанням контролюючих функцій [82].

Відмінністю законодавчої СОДТ Республіки Болгарія є те, що рішення про надання допуску на доступ до СІ приймається *Державним агентством національної безпеки*, який здійснює перевірку. Порядок здійснення перевірки осіб для допуску до СІ здійснюється відповідно до процедури, встановленої виключно *Урядом Республіки Болгарія* і яка передбачає три види перевірок залежно від СС інформації до якої матиме доступ відповідна особа. Тобто, залежно від СС інформації згідно Закону [83] передбачено такі види перевірок (вивчення): *звичайна перевірка*, для доступу до інформації, яка класифікується як «конфіденційна»; *розширена перевірка*, для доступу до інформації, яка класифікується як «Т»; *спеціальна перевірка*, для доступу до інформації, яка класифікується як «ЦТ» [82].

Трансформація сегмента спеціальних служб безпеки ***Румунії*** відбувалася на основі рекомендацій, що надходили від НАТО та інших міжнародних організацій. Фахівці Альянсу пропонували оптимізувати важливі складові забезпечення оборони та безпеки Румунії, зокрема чисельність армії та військово-промисловий комплекс, провести демілітаризацію та реорганізацію правоохоронних органів і спецслужб. У діяльності останніх помітне місце відводилося боротьбі з корупцією, контрабандою, тероризмом, транскордонною злочинністю тощо. На початку демократичних перетворень, зокрема у першій половині 1990-х років, у Румунії були утворені такі спеціальні служби [84]:

– *Румунська служба інформації* (РСІ) із спеціалізацією на здобуванні з позицій власної країни інформації про дії, що становлять загрозу національній безпеці;

– *Служба зовнішньої інформації* (СЗІ) із спеціалізацією на отриманні за кордоном відомостей, що стосуються питань національної безпеки;

– *Служба захисту і охорони* (СЗО) з функціями захисту високопосадових осіб (румунських громадян та іноземців).

Згідно із Законом «Про національну безпеку Румунії» від 29 липня 1991 року № 51 за значені спеціальні служби отримали відповідний правовий статус. Крім того, у рамках Міністерства оборони (МО) Румунії почали функціонувати *Головне управління інформації* (ГУІ) та *Служба спеціальних телекомунікацій* (ССТ).

У рамках приведення законодавчої бази та структури органів національної безпеки до євроатлантичних стандартів 18 листопада 2005 року на засіданні Вищої Ради з питань оборони Румунії було прийнято рішення про створення *Національної розвідувальної спільноти* (НРС). Ново створена організаційна одиниця є міжвідомчою структурою, до компетенції якої віднесено координацію дій у сфері боротьби з тероризмом, організованою злочинністю та корупцією. До складу НРС було включено РСІ, СЗІ, ГУІ МО, Генеральне управління інформації та внутрішньої безпеки Міністерства внутрішніх справ (ГУІВБ МВС). Метою її створення було бажання керівництва держави підвищити ефективність роботи національних спецслужб, усунути дублювання у роботі, розпорошення кадрових і матеріальних ресурсів. Основним завданням цієї структури, що перебуває в прямому підпорядкуванні *Президента Румунії*, є збір та обробка інформації, яка надходить від державних установ, відповідальних за забезпечення державної безпеки, та надання спеціально підготовленого інформаційного продукту для прийняття рішень у сфері безпеки та національної політики. Крім того, вона має прерогативу щодо узгодження розвідувальних, контррозвідувальних та інших безпекових операцій, що проводяться в рамках відповідних національних стратегій.

У складі НРС діють Координаційний комітет, Оперативна рада та Служба інтегрованої інформації [84]:

– *Координаційний комітет* виконує роль організатора та координатора інформаційної діяльності у сфері національної безпеки. До цього комітету входять радники президента та прем'єр-міністра з питань національної безпеки, директори РСІ та СЗІ, міністри оборони, зовнішніх справ, внутрішніх справ та юстиції. Цей комітет має відповідні права, зокрема узгоджувати заходи, передбачені Стратегією національної безпеки, різних державних і громадських інституцій з роботою розвідувальних, контррозвідувальних та інших структур.

– *Оперативна рада*, до складу якої входять радник прем'єр-міністра з питань безпеки, заступники директорів РСІ, СЗІ, ГУІ МО та ГУІВБ МВС, очолюється радником президента з питань національної безпеки і підпорядкована Координаційному комітету, забезпечує координацію та співробітництво між складовими НРС.

– *Служба інтегрованої інформації*, очолювана державним радником із Департаменту національної безпеки Адміністрації президента, забезпечує єдине планування та оцінку інформації у сфері національної політики та стратегії безпеки країни. З урахуванням складності роботи цієї служби її керівнику допомагають, за згодою Вищої ради оборони країни (ВРОК), два заступники, які визначаються директорами РСІ та СЗІ. Детальний аналіз принципів побудови НРС Румунії підтверджує, що для функціонування цієї структури обрана американська модель підлеглості головних спеціальних служб. Президенту безпосередньо підпорядковується РСІ та СЗІ, а загальна координація і контроль здійснюються через ВРОК.

Закон Румунії від 12 жовтня 2001 року № 544 «Про вільний доступ до публічної інформації» встановлює, що «вільний і необмежений доступ до інформації, яка відповідає суспільному інтересу, є правилом і обмеження в доступі повинне бути виключенням». Законом також передбачено виключення з загальних правил надання доступу до інформації, у разі якщо інформація стосується національної та суспільної безпеки й громадського порядку та належить до категорії ІзОД, інформація щодо нарад органів влади, комерційних або фінансових інтересів, особистої інформації, судочинства за кримінальними або дисциплінарними розслідуваннями, судовими процесами, а також інформації, розголошення якої може «завдати шкоди заходам щодо захисту молоді». Як зазначається Законом, ДТ – інформація, що відноситься до державної безпеки, розголошення якої може завдати шкоди національній безпеці і обороні країни. Згідно Закону до категорій СІ (ДТ) в основному відноситься інформація у сфері оборони країни (11 пунктів) [85].

Починаючи з 1 липня 2008 року почала діяти нова схема організації та функціонування РСІ, що булла затверджена ВРОК 25 березня 2008 року. Зміни цієї спецслужби були викликані необхідністю адаптування

до сучасних реалій у зв'язку зі статусом Румунії як держави-члена НАТО і ЄС та спрямовані на підвищення ефективності просування стратегічних інтересів Румунії у світі. Певних змін зазнала ССТ. Головним критерієм її реформування стало виконання програми модернізації системи шифрувального зв'язку, вивчення здатностей і можливостей реалізації власними силами європейської програми зміцнення кордонів Румунії. Досить показовою є кадрова політика румунських спецслужб. До підготовки кадрів та навчання співробітників активно залучаються спеціалісти НАТО. Керівники середньої та вищої ланок проходять обов'язкову підготовку та стажування в США, Німеччині, Великій Британії тощо [84].

Законодавство ***Чеської Республіки*** ґрунтується на базовому Законі від 11 червня 1998 року «Про захист класифікованої інформації». Цей Закон визначає інформацію, яку необхідно охороняти в інтересах Чеської Республіки а саме, СІ – це така інформація, несанкціоноване розголошення якої може завдати шкоду інтересам Чеської Республіки або тим інтересам, які Чеська Республіка зобов'язалася захищати, або які можуть зашкодити тим інтересам, які входять до реєстру СІ [85].

СІ охоплює відомості:1) у сфері оборони (23 пункти); 2) у сфері забезпечення громадської безпеки;3) наукові і технологічні процеси, виробництво, дослідження, розробка і матеріали, пов'язані із ДТ;

У порівнянні двох країн-членів НАТО – Чехії і Словаччини, їх законодавчі норми процесів і явищ у сфері регулювання захисту ІзОД вказують на наявність істотних розбіжностей. Зокрема, позначення об'єкта регулювання і збитку, пов'язаного із втратою або розголошенням класифікованої інформації, відрізняються (табл. 4) [85].

Таблиця 4

Порівняльний аналіз об'єкта регулювання Чехії і Словаччини

Визначення та норми	Чеська Республіка	Республіка Словаччина
Об'єкт регулювання	Класифікована інформація (частина 1, глава 1, секція 1)	**Класифіковані матеріали -** інформація та матеріальні об'єкти **Інформацією вважається:** - зміст документів, схем, ескізів, карт, фотографій, графічних та інших записів; - зміст усних заяв (висловлень); - зміст електричних, електромагнітних, електронних та інших фізичних носіїв. **Об'єктами вважаються:** - матеріальні носії з інформаційними записами; - вироби; - обладнання; - споруди. (стаття 2, пп. a, b, c)

Принциповим є те, що Чехія під збитком розуміє нанесення шкоди або створення загрози власним інтересам чи інтересам, які Чеська республіка зобов'язалася захищати. Це може означати, що для захисту інформації, яка належить третім країнам, потрібна наявність деяких офіційних зобов'язань з боку Чехії. У законі Словаччини така норма відсутня (табл. 5) [85].

Таблиця 5

Порівняльний аналіз збитку від втрати або розголошення класифікованої інформації Чехії і Словаччини

Визначення та норми	Чеська Республіка	Республіка Словаччина
Збиток, пов'язаний із втратою або розголошенням класифікованої інформації	Збиток або створення небезпечних умов для інтересів Чеської Республіки або інтересів, які Чеська Республіка зобов'язалася захищати, наслідки яких не можуть бути усунуті або можуть бути пом'якшені тільки певними заходами (частина 1, глава 1, секція 1 – 2)	Завдання збитків або загроза завдання збитків інтересам Словацької Республіки або інтересам, з якими пов'язаний захист Республіки Словаччина, при цьому ефект від нанесеного збитку або не може бути усунутий, або зменшення його пов'язане з необхідністю прийняття серйозних заходів (стаття 2, п. f)

Наявні розбіжності в частині нормування принципу глибини (Depth). Суттєвим є те, що Словаччина бере під захист не лише інтереси державних органів але й громадян (табл. 6) [85].

Таблиця 6

Порівняльний аналіз СС від величини нанесеної шкоди інтересам Чехії і Словаччини

Визначення та норми	Чеська Республіка	Республіка Словаччина
"Цілком таємно" TOP SECRET	у випадках, коли несанкціоноване розкриття інформації призвело б до виняткового серйозного збитку інтересам Чеської Республіки, цей ступінь класифікації позначається словами PŘÍSNĚ TAJNÉ або скорочено PT. (частина 1, глава 1, секція 1 – 2)	Цим ступенем захисту визначаються секретні матеріали, якщо у разі їх неправомочного розкриття і маніпуляції конституційність, суверенітет і територіальна цілісність держави може бути піддана небезпеці, або буде нанесена непоправна і серйозна шкода безпеці. економічним інтересам, зовнішній політиці або міжнародним відносинам Республіки Словаччини. (стаття 2, п. f)
"Для службового користування" RESTRICTED	... у випадках, коли несанкціоноване розкриття інформації призвело б до нанесення шкоди інтересам Чеської Республіки, цей ступінь класифікації позначається словами VYHRAZENÉ або скорочено V. (частина 1, глава 1, секція 1 – 2)	Цим ступенем захисту визначаються секретні матеріали, якщо у разі їх неправомочного розкриття і маніпуляції буде завдано шкоди інтересам державних органів або громадян Республіки Словаччини. (стаття 2, п. f)

Розділ 3. ТЕОРЕТИЧНІ ПОЛОЖЕННЯ ВИЗНАЧЕННЯ ЦІННОСТІ ІНФОРМАЦІЇ

3.1. Методичні основи та способи визначення цінності інформації

Поняття цінності інформації

Вище розглядався у якості критерію віднесення інформації до секретної виключно критерій величини (рівня) шкоди, заподіяної розголошенням СІ. Застосування саме цього критерію обумовлюється змістом Закону України «Про державну таємницю» [3] і тому носить імперативний характер. Однак свідоме, осмислене використання критерію шкоди, зокрема, відповіді на цілий ряд питань, пов'язаних з практичними аспектами обчислення його значень, їх шкалюванням (у тому числі визначення інтервалів шкали, відповідних певним СС інформації), інші особливості роботи ДЕТ з оцінювання рівня шкоди, вимагають підведення під цей критерій методичного базиса. Наявність теоретико-методичного обгрунтування критерію віднесення інформації до секретної дозволить відійти від жорсткого регламенту процедури віднесення (який, однак, не в змозі передбачити всі питання, що можуть виникнути за змістом цієї процедури), замінивши її гнучким механізмом експертизи, який має досить загальний характер і припускає певну об'єктивну деталізацію та уточнення з боку ДЕТ відповідно до особливостей та нюансів інформації, що експертується. При цьому дії ДЕТ мають базуватися на розумінні суті критерію, його теоретико-методичного змісту. Саме тому розуміння останнього бракує для об'єктивного, логічного застосування імперативно введеного критерію шкоди. Спробуємо знайти розв'язок цієї проблеми в близькій за своєю ідеологією до ОДТ галузі захисту інформації, зокрема, в ТЗІ.

Сфера захисту СІ набула системних ознак на рубежі XIX-XX століть [5]. Головними чинниками її формування були інтуїція та досвід професіоналів, які її опановували. Порівняно з ОДТ галузь ТЗІ системно сформувалася пізніше, у другій половині XX-го століття, а в Україні утворення системи ТЗІ (СТЗІ) фактично збіглося із становленням її незалежності. Характерною ознакою формування СТЗІ була наявність уже достатньо розвиненої науково-методичної бази, що дозволяло розв'язувати стратегічні завдання та проблемні питання становлення і розвитку ТЗІ на сучасних науково-методичних засадах. Тому доцільно ознайомитися з деякими науково-методичними наробками ТЗІ в площині питань, що досліджуються в даному розділі.

Одним з базових положень побудови систем захисту інформації (СЗІ) є принцип розумної достатності, відповідно до якого витрати на

побудову та супровід СЗІ мають зіставлятися з можливими втратами, що обумовлюються реалізаціями загроз відносно інформації, яка підлягає захисту. Це дозволяє оптимізувати витрати на створення СЗІ, забезпечивши адекватність рівня захисту рівневі цінності інформації. Тому визначення кількісного значення цінності інформації, яку треба захищати, є провідним моментом процедури оптимізації витрат на СЗІ [64, 75]. Дещо конкретніше це положення сформульоване у [64, 87]: «Захисту підлягає не будь-яка інформація, а тільки та, що має цінність. Цінною стає інформація, володіння якою дозволяє отримати який-небудь виграш: моральний, матеріальний, політичний тощо. Цінність інформації є критерієм прийняття будь-якого рішення про її захист». Зміст цього фрагменту достатньо переконливий щодо актуальності та важливості застосування поняття «*цінності інформації*» для побудови та оптимізації СЗІ, однак це поняття є фактично не визначеним.

Головним питанням практичного застосування поняття «*цінність інформації*» є знаходження (обчислення) кількісної оцінки цінності інформації. Ця проблема має давню історію, а її дослідженню присвячена значна кількість публікацій, зокрема, роботи К.Шеннона, О.О.Харкевича, Р.Л.Стратановича, М.М.Бонгарда та інших [64, 88-91]. Існуюче різноманіття підходів та методів визначення цінності інформації об’єктивно обумовлене існуванням різних видів систем (інформаційних, телекомунікаційних, автоматизованих тощо), де обробляється чи циркулює оцінювана інформація та множиною неспівпадаючих цілей щодо реалізації яких ця інформація використовується, особливостями прикладних задач до розв’язку яких вона застосовується.

Значення цінності інформації не можуть бути отримані шляхом прямого вимірювання, бо вона являє собою так звану латентну (приховану) властивість, яка є неспостережною й невимірною безпосередньо, оскільки до неї незастосовна процедура вимірювання еталонною одиницею. Для вимірювання латентної властивості необхідно виразити її через вимірювані властивості, які отримали назву *індикаторів*. Сукупність індикаторів, що заміняє латентну властивість (змінну), утворює операціональний референт [89] або операціональний конструкт. Він використовується замість латентної змінної в усіх залежностях, у які вона входить. Операціональний конструкт повинен бути достатньо валідним відносно своєї латентної змінної, тобто має достатньо точно відтворювати властивості, критичні для всіх застосувань, де задіяна латентна змінна.

У найпростішому випадку операціональним конструктом може бути окремий індикатор, зокрема, для латентної змінної «*цінність інформації*» – те, що дозволяє кількісно оцінити придатність певної

інформації до її конкретного практичного застосування у тому чи іншому виді діяльності. Очевидно, спосіб вимірювання значень обраного індикатора залежатиме від мети використання інформації у кожному окремому практичному застосуванні. Це обумовлює появу множинності підходів і методів оцінювання рівнів індикатора, про яку вже йшла мова вище. Однак, якщо у якості індикатора латентної змінної «*цінність інформації*» взяти корисність використання інформації у різних прикладних застосуваннях та, як одну з головних вимог, визначити необхідність грошової форми представлення значень цього індикатора, отримаємо достатньо універсальний операціональний конструкт, незалежний від способу вимірювання (обчислення) рівня корисності у кожному конкретному застосуванні. Зауважимо, що аналіз праць [88-91], дозволяє констатувати, що у більшості випадків оцінювання цінності інформації за умов дотримання певних додаткових вимог зводиться саме до оцінювання корисності прикладних застосувань цієї інформації. Це дозволяє сформулювати таке положення: «*Цінність інформації вимірюється рівнем максимальної корисності, отриманої від залучення оцінюваної інформації до оптимізації виконання певного завдання (виконання роботи, розв'язку задач та проблемних ситуацій, оптимізацію параметрів виробничого процесу тощо) за умови найліпшого способу використання цієї інформації*». Деякий екстремізм цього твердження, що його містять звороти «максимальна користь», «найліпший спосіб використання», отримав назву принципу (умов) екстремальності. Очевидно, якість прикладного застосування інформації може бути різною. В першу чергу, це залежить від споживача інформації, його знань, умінь, досвіду, можливостей зрозуміти, засвоїти та вдало використати отриману інформацію. Відтак корисність однієї і тієї ж інформації може змінюватися в широких межах. Дотримання принципу екстремальності гарантує найвищу якість використання інформації, відповідно найвищу (максимальну) корисність її застосування. Кількісна оцінка цієї максимальної корисності визначає цінність інформації. Тобто саме наявність принципу екстремальності у наведеному тлумаченні «*цінності інформації*» є запорукою коректного однозначного кількісного визначення цієї цінності.

Моделі цінності інформації

Формально цінність інформації можна відповідно визначити наступним чином [64, 91]:

$$V(I) = \Delta A_{extr}(I) - d(I), \qquad (3.1)$$

де A – показник, що характеризує ступінь успішності виконання певного завдання, роботи, іншого виду діяльності (цим показником може бути вартість продукції, виготовленої за певний час чи з фіксованого обсягу вихідної сировини, виграш, обумовлений вибором вдалого рішення, загальна вартість послуг, наданих споживачам у певній сфері діяльності тощо); $d(I)$ – витрати на одержання, обробку та використання інформації I у певному виді діяльності; ΔA – покращення (зростання) показника A за рахунок отриманої інформації I:

$$\Delta A(I) = A(I) - A_0, \qquad (3.2)$$

де A_0 – вихідне значення показника (за відсутністю інформації I), $A(I)$ – приріст значення показника A завдяки використанню інформації I. Зокрема, значення A може збільшитись внаслідок застосування отриманої інформації для оптимізації параметрів виробничого процесу, зменшення можливих хибних або неперспективних варіантів рішення певної проблеми, зростання іміджевої привабливості даного виду професійної діяльності тощо.

Виконання умов екстремальності обумовлює зростання показника A до його максимально можливого значення A_{extr}, а саме до:

$$\Delta A_{extr}(I) = A_{extr}(I) - A_0, \qquad (3.3)$$

У кожному конкретному застосуванні інформації I спосіб її «споживання» буде різним: разове використання інформації I у задачах прийняття рішення для вибору найкращого рішення з множини можливих, розподілене у часі поточне використання інформації для налаштування параметрів виробничих процесів тощо. Очевидно, найбільш прийнятна форма виміру значень V, A, d – грошова, хоча на практиці використовуються умовні одиниці, бали та інше. У більшості випадків величини V, A, d носять детермінований характер і їх значення можуть бути точно обчислені за існуючими нормативами та тарифами (виняток становить задача прийняття рішення на множині варіантів з відомою інформацією про розподіл ймовірностей їх реалізацій). Зазначимо, що наведений спосіб обчислення рівня корисності інформації, як і більшість традиційних методів та підходів до визначення цінності інформації, базується на парадигмі позитивності наслідків залучення інформації до оптимізації певних видів робіт (прийняття рішень, розв'язання задач, виконання завдань). Однак у задачах захисту інформації ця парадигма не спрацьовує, бо виникає

відсутня раніше потреба у чіткому визначенні суб'єкта інформаційних відносин (власника / споживача інформації чи зловмисника), для якого в цій ситуації визначається цінність інформації. Наприклад, для зловмисника несанкціонований доступ до конфіденційної інформації I, легітимне право на ознайомлення з якою у нього відсутнє, в більшості випадків стимулюється перспективою отримання певного прибутку, пов'язаного саме з використанням цієї конфіденційної інформації у своїх інтересах [92]. Тому, для зловмисника корисність цієї інформації I очевидна. Що стосується власника / споживача інформації I, то ситуація має подвійний характер: по-перше, ця інформація може бути корисна в традиційному сенсі; по-друге, компрометація інформації I здатна призвести до збитків, обсяг яких значно перевищуватиме корисність, визначену за співвідношенням (3.1). Це є достатнім мотивуванням необхідності захисту цієї інформації, отже в певному розумінні визначає цінність інформації I. Тому, питання визначення цінності інформації, яка підлягає захисту, потребує додаткового розгляду.

Як відомо з [93, 94], споживчі якості інформації у повному обсязі гарантуються за умов забезпечення трьох властивостей інформації:

– *доступності* (можливості отримання санкціонованим користувачем потрібної йому інформації не пізніше заданого (малого) проміжку часу, захищеність її від несанкціонованого блокування);

– *цілісності* (захищеності інформації від несанкціонованого знищення, модифікації);

– *конфіденційності* (неможливості отримання інформації неавторизованим користувачем, захищеності від несанкціонованого ознайомлення).

Розглянемо ситуації, що виникають у разі реалізації загроз від трьох наведених властивостей інформації. Так, у випадку разового використання інформації I в задачі прийняття рішення, знищення або блокування цієї інформації обумовлює неможливість зростання показника A, тобто $\Delta A = 0$. Це означає, що споживач інформації задарма витратив гроші $d(I)$ на підготовку та обробку вчасно невикористаної інформації I, тобто фактично зазнав збитку. Додавши сюди втрачену вигоду, максимальний обсяг якої складає $\Delta A_{extr}(I)$, отримуємо граничний обсяг збитку споживача:

$$l = \Delta A_{extr}(I) + d(I). \qquad (3.4)$$

У випадку використання поточно оновлюваної інформації, надходження якої розподілене у часі, її блокування чи знищення

призведе практично до такого самого збитку, але з деяким часовим запізненням (лагом), впродовж якого збиток зростатиме від 0 до l.

У разі модифікації інформації (при невиявленні факту модифікації) або у випадку розголошення конфіденційної інформації збитки споживача інформації можуть сягати суттєвих значень, перевищуючи як $\Delta A(I)$, так і $A(I)$. При їх оцінюванні слід зважати на існування множини можливих сценаріїв розвитку подій [95], тобто ці збитки мають принципово імовірнісний характер. Крім того, в разі виявлення факту модифікації чи компрометації конфіденційної інформації до загального обсягу збитків слід додати витрати на відновлювальні роботи, пов'язані з ліквідацією наслідків реалізації відповідних загроз інформації.

Загалом структура збитків, що їх несе власник конфіденційної інформації у разі реалізації загроз щодо цієї інформації, має чотири складові:

$$L(I) = l_1 + l_2 + l_3 + L_\Sigma(I), \qquad (3.5)$$

де l_1 – витрати на створення та обробку конфіденційної інформації I (близькі або співпадають з $d(I)$; l_2 – втрати можливого прибутку за рахунок використання конфіденційної інформації I (у ряді випадків збігаються з $\Delta A(I)$); l_3 – витрати на створення та експлуатації СЗІ; $L_\Sigma(I)$ – інтегральна оцінка збитку, що є наслідком можливих результатів розвитку ряду негативних для власника сценаріїв подій, обумовлених модифікацією, втратою чи розголошенням конфіденційної інформації.

Зазначимо, що складова l_2 у випадку, коли реалізація загрози інформації не веде до знищення чи спотворення інформації, що застосовується для оптимізації виконання певних завдань (а отже, ті виконуються в незмінних умовах), може бути відсутньою.

За своїм характером l_1-l_3 – детерміновані величини, значення яких (наприклад, для діючої виробничої системи) мають бути достеменно відомі. Складова $L_\Sigma(I)$ – імовірнісна величина, яка для обчислення вимагає знання пар $< p_j, L_j >$ – ймовірностей розвитку кожного з можливих сценаріїв та результуючих збитків за кожним з них. Зважаючи на те, що у разі недосконалості СЗІ власник конфіденційної інформації I може понести максимальний збиток в розмірі $L(I)$, саме ця величина приймається у якості цінності $V(I)$ конфіденційної інформації.

Наведені вище модельні співвідношення базуються на спрощеному підході до аналізу цінності інформації. Подальше поглиблення досліджень у цій сфері стикається з необхідністю розгляду та вивчення ряду проблемних питань. Відомо [96], що цінність інформації, у тому числі і конфіденційної, змінюється з часом. Вважається, що домінуючою тут є стала тенденція зменшення цінності, яка дістала назву *процес старіння інформації*. Вважається, що в більшості випадків адекватною моделлю процесів старіння є експоненційна функція виду:

$$L(t) = L(0)(1 - e^{-\beta t}), \tag{3.6}$$

де $L(0)$ – початкова цінність інформації, коефіцієнт β – інтенсивність старіння інформації, $1/\beta$ – середній час старіння.

Ще однією важливою особливістю інформації (як інформації взагалі, так і конфіденційної) є нелінійна залежність її цінності L від обсягу цієї інформації. Нехай повний обсяг $I_{\max}$ конфіденційної інформації є достатнім для успішної реалізації завдань певної прикладної галузі людської діяльності. Цінність цього обсягу конфіденційної інформації становить $L_{\max} = L(I_{\max})$. Якщо припустити, що певний фрагмент цієї інформації обсягом I потрапить до зловмисника, максимальний рівень збитку, який може бути нанесений власнику інформації, залежатиме від того, наскільки повно за цим фрагментом зловмисник в змозі відновити зміст всієї вихідної інформації $I_{\max}$. Якщо обсяг I близький до 0, відновити за цим фрагментом вихідну інформацію практично неможливо навіть у випадку, коли до цієї справи зловмисником залучається досвідчений і добре підготовлений аналітик. Відповідно цінність такого фрагменту дорівнює 0. Навпаки, якщо обсяг I близький до $I_{\max}$, цінність цього фрагменту фактично становить $L_{\max}$, бо дуже ймовірно, що фахівець-аналітик отримає всі необхідні для зловмисника відомості з наявного фрагменту інформації і цінність відсутньої незначної за об'ємом інформації $\Delta I = I_{\max} - I$ буде нульовою. Приймаючи це до уваги, можна припустити, що залежність $L(I)$ – монотонно зростаюча на інтервалі (0, $I_{\max}$) функція, похідна якої дорівнює чи близька 0 у початковій та прикінцевій області цього інтервалу, але інтенсивно зростає в його середній частині. Подібним вимогам задовольняє модель виду [64,91]:

$$L(I) = L_{\max}\left[1 - \frac{1}{\beta_2 + (1-\beta_2)e^{\beta_1 I}}\right], \qquad (3.7)$$

де β_1, β_2 – коефіцієнти, для значень яких виконуються умови: $\beta_1, \beta_2 > 0$, $\beta_2 \le 1$. Графічну ілюстрацію залежності (3.7) наведено на рис. 15. Слід зазначити, що інтенсивність зростання змінної L залежить від рівня підготовки та інтелекту аналітика [946]. У моделі (3.7) це відображається вибором значень коефіцієнтів β_1, β_2: зростання значень β_1 зміщує початок підйому графіка $L(I)$ вліво, до області малих значень I, а тривалість «лінійної» частини графіка регулюється підбором значень β_2, зокрема зростає із зменшенням цих значень і є короткою для значень β_2, близьких до 1.

До речі, при недостатній фаховій обізнаності аналітика можлива ситуація, коли $L(I_{\max}) < L_{\max}$, причому різниця $L_{\max} - L(I_{\max}) = \Delta L$ є достатньо суттєвою.

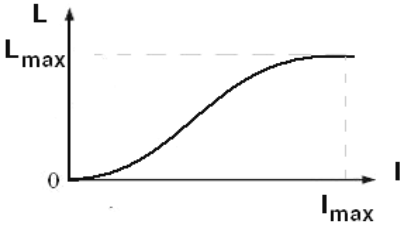


Рис. 15 Залежність цінності інформації L від її обсягу *I*

На жаль, моделі (3.6), (3.7) дають лише загальне уявлення про вплив факторів часу та обсягу інформації на її цінність. Прикладне використання цих моделей, як і ряду інших специфічних модельних механізмів впливу різних факторів на цінність інформації [88, 96], потребує деталізації й адаптації відповідних моделей до умов і особливостей конкретних застосувань. На практиці це є вкрай проблематичним через недостатню дослідженість впливу означених факторів на цінність інформації. Деякі припущення щодо походження, природи та особливостей залежності цінності інформації від її обсягу наведено у роботі [86], де аналізується наявність певних генетичних властивостей таємної інформації: якщо на базі цієї інформації утворюється нова вторинна інформація, вона наслідує особливості

вихідної інформації і також буде таємною. Також зазначається, що такий підхід є доволі спрощеним, бо якщо і відслідковується якась генетика, вона має більш складний нелінійний характер.

Наприклад, можливі ситуації, коли накопичення відкритої інформації на певній стадії цього процесу приведе до необхідності надання отриманому зібранню інформації статусу таємної. Подібне твердження наводиться в [87], де відзначається, що сукупна кількість або статистичний звід несекретних даних у підсумку можуть отримати СС, тобто матиме місце якісне перетворення сукупного масиву інформації, що суттєво виходить за межі просто генетичного наслідування. Підтвердження можливості стрибкоподібного якісного перетворення накопиченої інформації, яке змушує підвищити ступінь її секретності, знаходимо у ЗВДТ [31]. Наприклад:

Номер статті ЗВДТ	Зміст відомостей, що становлять державну таємницю	Ступінь секретності
1.9.2.	Відомості за окремими показниками про відкриття, винаходи, науково-технічні рішення, які можуть бути використані для потреб оборони держави і мають принципове значення для розробки нових видів озброєння чи військової техніки	
	- у цілому по Україні	«ОВ»
	- щодо окремого відкриття, винаходу чи науково-технічного рішення Щодо окремого відкриття, винаходу чи науково-технічного рішення: при засекречуванні ступінь секретності встановлюється і знімається за рішенням державного експерта з питань таємниць.	«ЦТ», «Т»

Як бачимо з цього витягу, сукупна інформація «у цілому по Україні» беззастережно отримує гриф «ЦТ», тоді як її фрагменти можуть мати будь-який довільний статус, хоч би й несекретний, залежно від того, що вирішить у кожному конкретному випадку ДЕТ. Таким чином, саме зібрання і спільне представлення сукупної інформації обумовлює різке зростання її сукупної важливості.

Подібний ефект достатньо просто інтерпретується з позицій теорії систем та системного аналізу [97-99]: аналітична сумісна обробка всього комплексу (блоку) інформації систематизує та впорядковує накопичені в ньому відомості і факти, дозволяє виявити і формалізувати сукупність зв’язків та співвідношень між базовими інформаційними елементами цього комплексу, тобто трансформувати вихідну неструктуровану сукупність відомостей у певним чином впорядковану систему взаємопов’язаних компонентів з більш–менш складною структурою. Як

відомо, система характеризується рядом властивостей, серед яких однією з головних є емерджентність – наявність у системи рис (властивостей), які не можуть бути безпосередньо виведені (отримані) через відомі характеристики окремих елементів, що складають систему [97-99].

Емерджентність – наслідок властивого складним системам *синергізму* [98], специфічного ефекту взаємопідсилюючих сукупних дій елементів системи, результат яких значно вищий за простий сумарний ефект від дії цих же елементів при їх взаємонезалежному функціонуванні. В нашому випадку наслідок *ефекту емерджентності* зведених у комплекс відомостей – це істотне зростання сукупної цінності СІ всього комплексу (з огляду на існуючу можливість сукупної аналітичної обробки відомостей, що утворюють інформаційний комплекс) порівняно із простим сумарним накопиченням цінностей окремих секретних складових комплексу при їх взаємонезалежному оцінюванні.

Слід ще раз підкреслити, що рівень ефективності упорядкування та систематизації початково розрізненої інформації, яка складає вихідний інформаційний комплекс, критично пов'язаний з рівнем знань та індивідуальних умінь аналітика. Останнє означає, що за кожним випадком аналізу залежно від підготовки та здібностей аналітика матимемо певну множину можливих варіантів аналітичних рішень.

Розглянемо ілюстративний приклад [86]: первинна інформація – відомості про хімічні реагенти, що ввозяться на територію підприємства, про яке відомо, що воно належить до оборонного комплексу. Ця інформація разом з певною додатковою інформацією (яким чином транспортують готову продукцію з підприємства, деталі та елементи зовнішнього вигляду транспортної тари, вид і тип транспортних засобів, інше) утворює інформаційний блок (комплекс), залежно від змісту та повноти якого шляхом аналітичного осмислення може бути запропоновано кілька варіантів висновку, різних за ступенем наближення до реального стану речей:

а) підприємство виробляє компоненти, які, можливо, застосовуються у спорядженні паливних систем військової техніки;

б) підприємство є виробником ракетного палива;

в) підприємство є виробником ракетного палива для ракет типу XXXX;

г) підприємство є виробником ракетного палива для ракет типу XXXX з приблизним обсягом виробництва YYYY тони на місяць.

Відповідно до цінності інформації, яка міститься в тому чи іншому варіанті отриманого аналітичного висновку, блоку (комплексу)

первинної СІ слід надати певний СС, який у деяких випадках (можливо, варіанти в), г)) буде вищий за СС елементів первинної інформації.

Така багатоваріантність можливого результату аналітичної обробки первинного зібрання інформації ускладнює завданн визначення сукупної цінності відомостей, що складають інформаційний комплекс. Однак при класифікації первинної інформації з точки зору її можливої належності до секретної, очевидно слід виходити з розгляду варіанту, що веде до найбільш тяжких наслідків, обумовлених втратою інформації. Зазвичай, виникнення цього варіанту можливе за умов, коли аналітик, що працює з первинною інформацією, має найвищий рівень підготовки і використовує новітні технології та механізми обробки і аналізу даних, які дозволяють йому максимально якісно трансформувати первинні дані у сукупність систематизованої та впорядкованої вторинної інформації. Фактично знов застосовується введений вище принцип екстремальності, який дозволяє уникнути багатоваріантності. Однак коли кожному варіанту з наведеної вище сукупності можна співставити ймовірність його реалізації, більш виправданим виглядає підхід, що базується на застосуванні апарату середніх ризиків [95], який дозволяє у підсумковому результаті врахувати цінність інформації за кожним з можливих варіантів через введення спеціальної системи ваг, де кожна вага пропорційна імовірності відповідного варіанту.

У підсумку сукупна цінність інформаційного комплексу може стати не співмірною із сумою цінностей окремих інформаційних одиниць, з яких утворено цей комплекс, й суттєво перевищуватиме означену суму (залежно від конкретних обставин, що виникають у кожній окремій ситуації). Це заперечує правомірність застосування достатньо поширеного на практиці підходу, за яким цінність інформаційного комплексу обчислюється як сума попередньо визначених цінностей окремих інформаційних одиниць і тим самим ігнорується існуюча залежність цінності інформаційної одиниці від обсягу та змісту вже накопиченої інформації. Таким чином, *обчислення сукупної цінності інформаційного комплексу* є нетривіальною задачею, загальна методика розв'язку якої дотепер відсутня, що обумовлює переважне використання експертних методів для розв'язку цієї задачі.

Інформація: цінність чи важливість?

Вище для можливостей кількісного оцінювання латентної змінної «цінність інформації» було введено операціональний конструкт, головну роль в якому відігравав індикатор «корисність інформації». У формальній моделі (3.1) значення цього індикатора визначалось через

показник $\Delta A_{extr}(I)$ – максимальний приріст успішності виконання певного завдання. Однак у базовому співвідношенні (3.5), яке характеризує цінність конфіденційної інформації, індикаторами, що формують операціональний конструкт, стають збитки – антипод корисності. Цими індикаторами є витрати l_1, l_3, «чисті» збитки, які інтегрально представлені змінною $L_\Sigma(I)$, та збиток l_2 – втрачений прибуток, який доречно було б назвати «негативною (втраченою)» корисністю. У зв'язку з цим асоціювання узагальненого (сумарного) збитку $L(I)$ з поняттям «цінність інформації» є, зважаючи на первинну традиційну семантику цього поняття, не зовсім коректним. Можливо, тому в деяких джерелах для узагальненої характеристики значимості інформації використовують термін «важливість інформації» [87, 66], або «значимість інформації». Цікаво, що в законі України «Про державну таємницю» [3] для порівняльної характеристики властивостей СІ застосовано термін «важливість» (його ж використано для позначення найвищого СС – «ОВ»).

Кінець кінцем, зважаючи на те, що оцінювання складової l_2 проводиться з позицій можливої (хоч і не реалізованої, тобто втраченої) цінності конфіденційної інформації, в семантичному розумінні найбільш адекватною реальній економічній ситуації, що наступає після здійснення загрози, буде структура, яка включає такі три складові:

– втрачена цінність;

– збитки, обумовлені модифікацією чи розголошенням конфіденційної інформації;

– витрати на отримання та зберігання інформації.

Відповідно до вищевикладеного, остання складова включає в себе витрати l_1, l_3. Доцільно більш детально розкрити зміст двох перших складових. Зокрема, обраховуючи втрачену цінність, зважатимемо на такі часткові показники:

а) корисність інформації як інформаційної складової забезпечення якості та ефективності певної діяльності;

б) «самостійна» корисність інформації з точки зору її необхідності для розв'язання ряду завдань означеного вище діяльності.

Обчислення збитків теж базується на двох часткових показниках:

а) величина шкоди, обумовленої модифікацією чи розголошенням конфіденційної інформації;

б) витрати на проведення робіт з ліквідації наслідків розголошення конфіденційної інформації.

3.2. Практичні аспекти визначення цінності інформації

Згідно з міжнародним стандартом ISO/IEC TR 13335-3, якому відповідає український національний стандарт ДСТУ ISO/IEC TR 13335-3: 2003, *цінність певної інформації для організації* визначається ступенем залежності ефективного функціонування організації від рівня залучення цієї інформації для забезпечення діяльності організації. Однак можливості своєчасного та повномасштабного використання відповідної інформації в організаційній, виробничій, соціальній та в інших сферах діяльності організації залежать від виконання умов цілісності, доступності та, в ряді випадків, конфіденційності необхідної інформації, відтак – від рівня захищеності цієї інформації. Стратегічним моментом керування (управління) інформаційною безпекою організації є правильний вибір прийнятного для даної організації рівня ризику. Цей вибір напряму залежить від цілей, що ставить перед собою організація при створенні СЗІ. Для того, щоб оцінити та сформулювати такі цілі, необхідно вивчити активи організації та визначити їх цінність для цієї організації ([100], розділ 7.1). Таким чином, визначення цінності активів стає одним з ключових завдань побудови системи безпеки. На жаль, деталізація процедури оцінювання активів у стандартах [100, 101] відсутня, її зміст обмежено рекомендаціями загального характеру та рядом прикладів, методичний бік проблеми оцінювання активів практично не досліджений. Проте вважаємо доцільним ознайомлення зі змістом означених стандартів та аналіз їх ключових положень з метою формування теоретико-методичних засад оцінювання активів організації та застосування отриманих результатів для розробки процедури визначення цінності інформації.

За стандартом ДСТУ ISO/IEC TR 13335–3 [100], *активи організації* – це усе, що має цінність для організації, причому цінність кожного активу визначається його важливістю щодо ділової (функціональної) складової діяльності організації. Зокрема, якщо мова йде про безпеку системи, що застосовуються в межах певної організації, оцінюванню підлягають насамперед активи цієї системи, причому при визначенні їх цінності має враховуватися те, наскільки може постраждати ця діяльність через виток, спотворення, недоступність та/або руйнування інформації, тобто внаслідок реалізації загроз по відношенню до ресурсів інформаційно-телекомунікаційної системи (ІТС) організації. Таким чином, ідентифікація та оцінювання активів, які були проведені на основі обліку ділових інтересів організації, є основним фактором у визначенні ризику.

Однак зазвичай оцінюванню активів передує кілька допоміжних етапів, один з яких – етап інвентаризації (ідентифікації) активів. За

результатами інвентаризації активів складається перелік важливих для організації активів, в якому можна виділити дві групи: активи системи ІТ та другу групу активів, куди увійшли всі інші активи організації, цінність яких залежить від стану активів першої групи.

До активів системи ІТ (інформаційних активів) звичайно відносять:

– інформаційні ресурси: бази даних, файли даних, системну документацію, настанови користувачеві, архівіровану інформацію тощо;

– активи програмного забезпечення: системне та прикладне програмне забезпечення, інструментальні засоби, утиліти;

– фізичні активи: комп'ютерне устаткування (процесори, монітори, модеми й т.п.), апаратура зв'язку (телефонні станції, маршрутизатори, телефони тощо), інше технічне обладнання, споруди та приміщення ІТС;

– персонал та співробітники ІТС.

Склад активів другої групи (інші активи організації) суттєво залежить від сфери, в якій функціонує організація, її фінансового становища, підпорядкованості тощо. Зокрема, це нематеріальні активи: репутація, імідж організації, рівень її ділової активності. Сюди ж слід віднести комунальні активи: освітлення, кондиціювання, обігрів, електроживлення. Нарешті, це можуть бути переліки робіт, замовлень, організацій-суміжників, постачальників, списки продукції, що виробляється організацією, та інше. Загалом перелік активів другої групи може бути досить об'ємним. Щоб його раціонально звузити й одночасно не втратити чогось важливого, оцінюванню активів передує ще один додатковий етап – визначення меж огляду [100]. Його задача – виділити ті аспекти ділової діяльності організації, які залежать від ІТС, що використовуються організацією. З метою виявлення цих аспектів, діяльність організації треба проаналізувати за двома групами критеріїв. Критерії першої групи дозволяють виявити межі залежності організації від ІТС й спираються на наслідки аналізу наступних положень:

– наскільки важлива частина бізнесової діяльності, яка вимагає обов'язкового залучення ІТС;

– які профільні (виробничі) завдання організації можуть бути реалізовані тільки за допомогою ІТС.

Друга група критеріїв спрямована на виявлення інформації, що потребує захисту, й на аналіз можливих наслідків реалізації загроз щодо цієї інформації:

– які важливі рішення, що приймаються в організації, залежать від точності, цілісності, доступності та конфіденційності інформації, оброблюваної в ІТС;

– яка оброблювана інформація потребує захисту;

– які наслідки можуть виникнути після інциденту, пов'язаного з порушенням безпеки критичної інформації.

Закінчивши інвентаризацію активів, можна переходити безпосередньо до встановлення цінності активів. Основою для визначення цінності може бути:

1) вартість створення та обслуговування активу;

2) вартість модернізації та відновлення активу;

3) збиток, що наноситься організації у випадку порушення конфіденційності, цілісності або доступності інформаційних активів;

4) комбінація трьох попередніх варіантів, що дає змогу отримати певну інтегральну оцінку загальної цінності активу.

Найбільш поширеним у практичних застосуваннях є *спосіб обчислення цінності активів*, в основі якого лежить третій з вищенаведених варіантів. З цього приводу в стандарті ДСТУ ISO/IEC TR 13335–3 [100] зазначається, що витрати на активи (їх вартість) – це лише мала частка їх загальної цінності. Зокрема, рекомендації з застосування оцінок збитків, обумовлених реалізацією загроз щодо інформаційних активів, для визначення їх цінності для організації наведено в обов'язкових додатках В, Е до зазначеного стандарту [100]. При аналізі цього способу обчислення цінності активів треба приймати до уваги можливі наслідки реалізації загроз безпеці інформації в ІТС, що призводять (серед іншого) до:

– зниження рівня ділової активності організації;

– втрати/погіршення репутації організації;

– фінансових втрат;

– перебоїв у виконанні ділових операцій;

– погіршення інвестиційного клімату;

– виникнення загроз особистої безпеки і т.п.

Для того, щоб визначити цінність активів, слід скласти список, який включатиме повну множину активів організації: $AS = \{as_i\}$, $i = \overline{1, n_A}$, встановити повний перелік можливих загроз інформації $T = \{t_k\}$, $k = \overline{1, n_t}$ та проаналізувати всю сукупність пар $< as_i, t_k >$, $i = \overline{1, n_A}$, $k = \overline{1, n_t}$, вирахувавши в процесі цього аналізу часткові збитки q_{ik}, обумовлені впливом реалізацій інформаційних загроз на стан (якість функціонування, забезпечення стабільності, цілісності тощо) кожного з активів. Потім за отриманими частковими збитками слід обчислити остаточні сукупні значення цінностей відповідних активів.

На жаль, в наведеній схемі знаходження цінностей активів притаманний ряд недоліків [104].

По-перше, це множинність отримуваних для кожного активу оцінок q_{ik}, кількість яких визначається кількістю тих загроз, наслідки реалізації яких ведуть до потенційних збитків, що вимагають свого обліку. Фактично кожна окрема оцінка q_{ik} відображає лише частковий збиток, що наноситься і-му активу as_i реалізацією загрози t_k. При реалізації різних загроз ураженими можуть опинитися як різні елементи, що входять до складу активу, так і такі, що частково або повністю збігаються. Очевидно, формування підсумкової цінності активу в цих випадках буде відбуватися по-різному, виходячи з інформації про механізми утворення окремих збитків, яка носить частковий характер та може бути отримана лише під час обстеження конкретної організації. Тому в стандарті ДСТУ ISO/IEC TR 13335–3 [100] відзначається наявність проблеми множинності оцінок активів, але відсутні будь-які загальні рекомендації щодо її вирішення.

По-друге, в цьому ж стандарті [100], п.9.3.3., підкреслюється необхідність обліку наявності взаємозв'язків між різними активами при визначенні рівня цінності кожного з них, що пояснюється існуванням взаємозв'язків певних вразливостей інформаційної системи організації та, відповідно, наявністю взаємозв'язків при реалізації окремих загроз інформації. Також як і у випадку множинності оцінок активів, облік взаємозв'язків активів можливий лише за наявності цілком конкретної інформації про часткові особливості та характеристики функціонування окремих підсистем організації.

По-третє, при великих значеннях n_A та n_t (порядку декількох десятків та більше) множина пар $<as_i, t_k>$, $i = \overline{1, n_A}$, $k = \overline{1, n_t}$ стає достатньо великою, а процедура оцінювання на базі цієї множини остаточних сукупних значень збитків q_i, кожне з яких визначає цінність відповідного і-ого активу as_i – надмірно громіздкою та трудомісткою. Дійсно, знаходження остаточного сукупного збитку q_i є результатом спільного аналізу версій походження часткових збитків q_{ik}, $k = \overline{1, n_t}$, максимальна кількість яких n_t у загальному випадку може значно перевищувати рекомендований граничний обсяг 7±2 (відоме число Інгве-Міллера [98], що характеризує обмеженість людських можливостей з ефективної сумісної обробки ряду інформаційних фрагментів, кожен з яких являє собою сукупність фактів та зв'язків, що сприймаються як єдине ціле). Крім того, через необхідність дослідження

й аналізу величезної кількість пар $<as_i, t_k>$ експерт навряд чи на ділі зможе свідомо виділити та визначити всі часткові збитки q_{ik}, $i = \overline{1, n_A}$, $k = \overline{1, n_t}$, тому ним відразу оцінюється сукупний збиток q_i кожного з активів, котрий і вважається цінностю цього активу. Безумовно, пряме експертне оцінювання збитку q_i, яке виключає процедуру вивчення та аналізу часткових збитків q_{ik}, значно спрощує та прискорює оцінювання активів, проте при цьому абсолютно не враховується механізм виникнення часткових збитків, внаслідок чого істотно зростає рівень суб'єктивних похибок експертизи.

Підкреслимо, що *кінцевою метою викладеної вище процедури оцінювання активів* є визначення рівня збитків, завданих активам організації реалізацією інформаційних загроз. Однак у цій процедурі фактично випала з поля зору сама інформація, відносно якої реалізуються загрози, і тому поза увагою залишається те, що збитки, нанесені активам організації, утворюються саме внаслідок ураження інформації і залежать від її важливості для організації (тобто впливу цих уражень на забезпечення ефективного функціонування організації).

Тому доцільно в процедурі оцінювання активів організації більш чітко врахувати причинно-наслідкові особливості процесу утворення часткових збитків та обчислення остаточного сукупного збитку. При цьому слід брати до уваги три наступних аспекти:

по-перше, точками введення загроз в ІТС є вразливості активів системи, тоді як наслідки реалізації цих загроз треба оцінювати на повній множині активів організації;

по-друге, на певному кроці реалізації будь-якої загрози інформації цю загрозу можна звести до однієї із трьох: конфіденційності, доступності та цілісності, що дозволяє спростити і скоротити аналіз наслідків успішної реалізації загроз, зокрема обрахунок відповідних збитків.

по-третє, наслідком реалізації будь-якої з цих загроз або їх довільної комбінації є ураження інформації організації (точніше інформаційних ресурсів організації – сукупності впорядкованої певним чином інформації, фіксованої на різних типах носіїв, пристосованих для збереження та обробки цієї інформації в ІТС). Вважатимемо, що інформаційні ресурси організації разом складають деяку підмножину активів системи: $AS^{\inf} \subset AS$.

Формально з урахуванням зазначених вище аспектів схему оцінювання збитку можна подати у вигляді триетапної процедури [104]. При її побудові будемо виходити з того факту, що в організації об'єктом

докладання загроз є елементи інформаційної інфраструктури (обладнання, програмне забезпечення, персонал), які через присутні в них вразливості роблять можливим реалізацію тих чи інших атак відносно інформаційних ресурсів. Наслідки реалізації цих атак (збитки організації) визначаються на всій множині AS активів організації.

На першому етапі процедури оцінювання збитків виконується інвентаризація активів організації, результат якої – *список активів*, що визначає повну множину активів організації: $AS = \{as_i\}$, $i = \overline{1, n_A}$. Встановлюється перелік можливих загроз інформації $T = \{t_k\}$, $k = \overline{1, n_t}$. Формується підмножина $AS^{\inf 1} \subset AS^{\inf}$, що включає лише ті інформаційні ресурси організації, до яких вірогідно можливе застосування будь-яких загроз зі складу множини T.

У ході другого етапу виконується аналіз усіх можливих пар виду $\left\langle as_l^{\inf 1}, as_i \right\rangle$, за результатами якого визначаються *групи активів*, що асоціюються з кожним елементом $as_l^{\inf 1}$ інформаційних ресурсів, стосовно якого може бути реалізована загроза. На третьому етапі, в ході аналізу всіх можливих трійок $\left\langle t_k, as_l^{\inf 1}, as_i \right\rangle$, $i = \overline{1, n_A}$, виявляються *збитки* q_{ik}, що завдаються активам as_i, $i = \overline{1, n_A}$ організації у випадку реалізації загрози t_k відносно інформаційного ресурсу $as_l^{\inf 1}$, і за сукупним значенням усіх цих збитків, обрахованим за всією множиною активів $AS = \{as_i\}$, визначають часткову цінність відповідного інформаційного ресурсу $as_l^{\inf 1}$ (так зване «надане» значення [100]).

На жаль, як це вже зазначалося вище, при великих значеннях n_A та n_t кількість аналізованих пар $\left\langle as^{\inf 1}{}_l, as_i \right\rangle$, стає достатньо великою, трійок $\left\langle t_k, as_l^{\inf 1}, as_i \right\rangle$ – ще більшою, а процедура оцінювання значень q_{ik} – вельми громіздкою. Прикладом одного з найекстремальніших варіантів, що можуть виникнути при оцінювані активів, слід вважати ситуацію, в якій організацією, чиї активи оцінюються, є ціла країна. У цьому випадку множина пар <актив-загроза>, які підлягають експертуванню, є фактично незліченною, а відтак застосування до неї наведеної вище процедури оцінювання активів – безглуздою витратою часу. Для отримання працездатної процедури оцінювання активів в цьому прикладі необхідно ввести механізми скорочення кількості

зівставлюваних експертом варіантів пар <актив-загроза> до розумно прийнятної кількості.

Одним з таких механізмів, детально розглянутим в [101], є *метод сценарного аналізу збитку*, обумовленого реалізацією загроз щодо певного інформаційного ресурсу (ІР). За цим методом експерт до кожного ймовірного випадку реалізації загрози визначає скінченну множину можливих сценаріїв розвитку подій-наслідків (3-5 варіантів). Розгортання кожного з сценаріїв асоціюється з деякою конкретною множиною активів, яка за своїм обсягом незрівнянно вужча від гіпотетичної повної групи активів. Тому експерт здатний достатньо об'єктивно оцінити наслідки розвитку кожного сценарію, які фактично становитимуть часткові інтегровані оцінки збитків (втрат), обумовлених реалізацією вихідної загрози. За остаточну оцінку збитків у разі реалізації відповідної загрози можна взяти найбільшу з часткових оцінок, отриманих за кожним зі сценаріїв, або збитки за найбільш ймовірним сценарієм, або, нарешті, середньозважений інтегрований збиток, де вагами є ймовірності реалізацій кожного з сценаріїв.

Зазначимо, що розглянута вище схема оцінювання активів достатньо універсальна з точки зору можливих галузей і діапазонів застосувань, проте в ряді випадків, які характеризуються наявністю певних обмежень у постановці задачі, ця схема стає дещо ускладненою.

Так, якщо метою оцінювання ІР є визначення їх приналежності до СІ, множина загроз T фактично звужується до єдиної – загрози витоку інформації. Через це відразу відпадає проблема множинності оцінок часткових збитків, породжуваних реалізацією численних загроз інформації. Об'єкти, відносно яких може бути реалізована загроза витоку, – це множини ІР, що звичайно мають певні типові документовані форми представлення і стало визначені галузі застосування. Останнє означає, що сукупність активів, які функціонально чи в інший спосіб пов'язані з атакованим ІР і через це можуть зазнати уражень, достатньо постійна і характерна для всіх ІР цієї галузі. Тому, якщо у множині подібних галузевих ІР є деяка сукупність вже оцінених, експерт може більш-менш вдало визначити цінність усіх інших ІР шляхом їх зіставлення і порівняння із уже оціненими. Точність отриманих при цьому оцінок залежить як від рівня компетентності експерта, так і способу (технології), що застосовується ним для порівняльного аналізу та визначення кількісного значення цінності ІР. Одну з таких технологій запропоновано в [102], однак вона не містить детального опису механізмів її реалізації. Тому нижче наведено приклад адаптації цієї технології до випадку аналізу рівня збитку, обумовленого реалізацією загрози витоку СІ.

3.3. Застосування ноніусного методу для визначення цінності інформації

Одним із базових положень побудови СЗІ є принцип розумної достатності, відповідно до якого витрати на побудову та супровід СЗІ мають співставлятися з можливими втратами, обумовленими реалізаціями загроз щодо інформації, яка підлягає захисту. Це дозволяє оптимізувати витрати на створення СЗІ, забезпечивши адекватність рівня захисту рівню цінності інформації. Тому визначення кількісного значення цінності інформації, яку треба захищати, є провідним моментом процедури оптимізації витрат на СЗІ. На методологічному рівні принцип розумної достатності реалізується в концепціях аналізу та керування інформаційними ризиками. Однак практичне втілення цих концепцій в процесі створення СЗІ вимагає вирішення ряду проблемних питань, одне з яких – оцінювання цінності інформації, зокрема ІР, які захищаються. Актуальність цього питання наглядно підтверджується тією увагою, що приділяється йому в численних нормативних та настановчих документах [100, 101], причому фактично всі означені документи у якості основного механізму оцінювання цінності ІР визначають метод експертно-аналітичних оцінок. Як приклад, можна взяти стандарт ДСТУ ISO/IEC TR 13335-3 [100], в якому даний метод експертизи цінності ІР використовується в рамках так званого «детального аналізу ризиків», що являє собою один з варіантів корпоративної стратегії аналізування ризиків. Процедура експертно-аналітичного оцінювання кожного ІР базується на системі критеріїв, за якими сукупна оцінка цінності ІР формується з витрат на його створення (придбання, обслуговування, відновлення) та можливих збитків організації, яка володіє ІР, обумовлених реалізацією загроз щодо конфіденційності, цілісності та доступності відповідного ІР.

Взагалі ефективне застосування методики «детального аналізу ризиків» вимагає від експерта глибоких знань (як в сфері інформаційних технологій, так і в сфері ділової активності організації), значного часу та зусиль. Тому експерти в своїй практичній діяльності часто віддають перевагу так званому «неформальному підходу» до аналізу ризиків [100], в якому експертиза цінності ІР спирається не на структурно-аналітичні методи аналізу витрат та прогнозування можливих збитків, а виключно на персональний досвід та рівень поінформованості експерта у відповідній предметній галузі. Тобто експерт, минаючи багатоетапну аналітичну процедуру, відразу визначає цінність ІР в цілому, не переймаючись її формуванням шляхом інтеграції певної кількості попередньо визначених фрагментарних (часткових) оцінок. Подібне пряме експертне оцінювання дає суттєву економію зусиль і часу, однак

разом з тим істотно збільшує ймовірність суб'єктивних помилок в результатах експертизи. Через це було б доцільно певним чином регламентувати проведення процедури прямого експертного оцінювання. На жаль в означених вище документах подібна інформація відсутня, зокрема, в [100] визначено лише суть «неформального підходу».

Ноніусний підхід до визначення цінності інформації

Можна припустити, що експерт, формулюючи свої висновки в ході прямої експертизи, свідомо чи підсвідомо спирається на систему певних уявлень про цінність групи добре відомих йому ІР, які він вважає базовими в сфері даної фахової діяльності. Тому, складаючи свою експертну оцінку щодо цінності представленого на експертизу нового ІР, експерт «вмонтовує» цей новий ІР до існуючої системи базових ресурсів і інтерполює його ціннісний показник за вже відомими значеннями цінності як «близьких» так і «віддалених» базових ресурсів.

На жаль отримана інтерполяційна оцінка є результатом, який формується у спосіб, що звичайно лишається поза можливістю його свідомої фіксації експертом [103].Тим не менш з літератури відомі спроби побудови евристико-емпіричних процедур, мета яких – заміщення експерта у процесі формування експертного висновку або суттєве спрощення його продукування.

Зокрема в [64, 104, 105] запропоновано так званий ноніусний підхід до визначення цінності ІР, який дозволяє поступово конкретизувати клас, групу, підгрупу ресурсів, близьких за певними характеристиками об'єкту експертизи, послідовно звужуючи до прийнятного обсягу множину базових ресурсів, призначених до порівняльного зіставлення з новим ІР.

Проілюструємо роботу ноніусної схеми. Припустимо, що оцінюється важливість ресурсу *IR*, зміст якого – дані контракту про постачання певного виду військової техніки до деякої країни (рис.15).

Загальний обсяг документів у сфері зовнішніх відносин становить:

$$N = \sum_i n_i = \sum_i \sum_k m_{ik} = \sum_i \sum_k \ldots \sum_r L_{ikr} \cdot \qquad (3.8)$$

Відповідно до суті ноніусного підходу, деталізуючи характер та особливості ресурсу *IR*, поступово спускаємося щаблями ієрархії рис.16, редукуючи початкову множину з *N* аналізуємих документів до вмісту певної «атомарної» комірки з обмеженою кількістю базових ІР $\{IR_l\}, l = \overline{1, L}$.

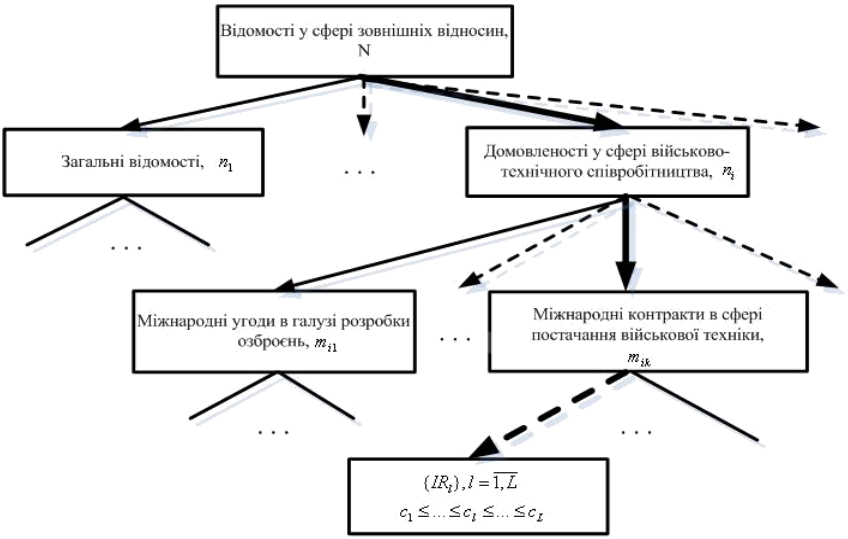


Рис. 16. Приклад схеми класифікації ІР у певній предметній сфері

Вважаємо, що цінність c_l кожного з цих ресурсів вже відома і разом вони утворюють скінчену лінійно впорядковану множину $\{c_1, c_2, ..., c_L\}$. Для вироблення рішення щодо цінності c_{IR} ресурсу *IR* експерту потрібно «втиснути» цей ресурс у множину $\{IR_l\}$, та, орієнтуючись за ціновими показниками елементів цієї множини, визначити цінність c_{IR}. Можливою формою оцінки може бути зважена сума [64, 104, 105]:

$$c_{IR} = \sum_l w_l c_l, \tag{3.9}$$

де w_l – система ваг, що задаються експертом за результатами співставлення ресурсу IR з іншими елементами множини $\{IR_l\}$ із застосуванням методу попарних порівнянь Сааті [70] чи у інший спосіб. Надалі оцінений ресурс IR можна ввести до множини базових ресурсів.

Слід зазначити, що умовою реалізації ноніусного підходу є існування ієрархії взаємопов'язаних понять, які охоплюють певну предметну (фахову) галузь. Саме наявність такої ієрархії дозволяє здійснити віднесення об'єкту експертизи до певної підгрупи базових ІР.

Ще одним прикладом прямого експертного оцінювання, близьким за своєю суттю до ноніусного підходу, є процедура надання ГС МНСІ.

ГС має відповідати СС інформації, розміщеної на МНСІ, який визначається шляхом зіставлення змісту цієї інформації зі змістом статей ЗВДТ [31, 106] та виявленням конкретної статті, під зміст якої підпадає інформація, розміщена на МНСІ. Реалізація цієї пошукової процедури забезпечується ієрархічною структурою ЗВДТ [31, 106], яка дозволяє достатньо просто віднайти відповідну статтю.

Онтологічна ієрархія

В обох наведених вище прикладах прийняття рішень базується на використанні специфічних ієрархічних структур – онтологій, вивченню, розробленню та застосуванню яких останнім часом приділяється значна увага [107, 108].

Онтологія – це спроба всеосяжної та детальної формалізації деякої області знань за допомогою концептуальної схеми. Зазвичай така схема складається зі структури даних, які містить усі релевантні класи об'єктів, їх точні специфікації для певної предметної області, зв'язки і правила (теореми, обмеження), прийняті в цій області.

Вперше поняття онтології, як формального опису термінів, зустрічається в області вивчення штучного інтелекту. Проте, останнього часу дане поняття поширюється і на інші предметні області.

Потреба в розробці онтологій виникає в разі необхідності виконання структуризації знань у певній предметній області для багаторазового повторного використати цих знань або для спільного розуміння широким загалом користувачів структури інформації у різних сферах діяльності.

В найпростішому випадку побудова онтології зводиться до виділення базових понять предметної області та встановлення співвідношень між ними. Однією з проблем розробника онтології є необхідність виявлення усіх елементів, які входять до складу предметних областей. Проте онтологічна структура має бути динамічною щодо змін. Онтології зазвичай будуються на аналізі функціональних властивостей та зв'язків елементів певної предметної області або на аналізі змісту термінів відповідної сфери, їх співпідрядності.

Одним з прикладів вдалого застосування та використання онтологічного аналізу можна вважати ЗВДТ. В ЗВДТ всі сфери діяльності розподілено на чотири: сфера оборони, сфера економіки, науки і техніки, сфера зовнішніх відносин та сфера державної безпеки і охорони правопорядку [31]. Відповідно, сфера оборони містить основні специфікації понять щодо даних про вид збройних сил, округ, полки, окремі військові частини, тощо. Сфера економіки охоплює специфікації питань мобілізаційної потужності, створення державних матеріальних

резервів, формування, фінансування та виконання оборонного замовлення й т.п. Те саме стосується і інших сфер діяльності. Всі вони містять в собі певні специфіковані поняття, які в свою чергу розкриваються через ще більш деталізовані та конкретизовані категорії. Фактично кожна із зазначених сфер являє собою часткову онтологічну ієрархію, що поглинається ще більш загальною онтологічною ієрархією, кореневим поняттям якої є вся множина відомостей, які становлять ДТ. З іншого боку будь який елемент цієї онтологічної ієрархії припускає своє розвинення у відповідну часткову ієрархічну структуру. Зразком такого розвинення є онтологічна ієрархія, що утворилася з поняття **Відомості у сфері зовнішніх відносин** (розділ ЗВДТ) (рис.16) і являє собою часткову онтологію загальної ієрархічної онтології ЗВДТ. Менша за обсягом часткова ієрархічна структура підпорядкована ІР **Домовленості у сфері військово-технічного співробітництва**, ще більш обмежена – ресурсу **Міжнародні контракти в сфері постачання військової техніки**. Підлеглі ієрархічні структури відсутні лише для елементів найнижчого «атомарного» рівня онтології ресурсів СІ сфери зовнішніх відносин.

Такий же підхід можна використовувати при побудові онтологій і в інших випадках, зокрема для організацій, в тому числі і комерційних: всю сукупність даних, понять, термінів чи об’єктів, які утворюють предметну область у сфері функціонування відповідної організації, треба категоріювати, дати докладні специфікації цих категорій та вказати їх зв’язки, можливі підпорядкованості, залежності. Для ЗВДТ ці категорії розроблено ДЕТ в процесі багаторічної роботи, а ефективність отриманої структуризації СІ підтверджена часом. Однак чи можна забезпечити належну якість проведення онтологічного аналізу у більш стислий час, при залученні до цієї справи спеціалістів різних рівнів компетентності, які не є фаховими експертами або навіть зовсім не мають досвіду проведення експертиз? Як формалізувати цей процес?

Методика побудови онтологічної ієрархії визначення цінності інформації

Припустимо, що об’єктом онтологічного аналізу є представлена у різних формах (в тому числі і у вигляді сукупності ІР) інформація, існування якої є необхідною умовою сталого та якісного функціонування деякої виробничої організації, мета діяльності якої – створення (виготовлення) певного матеріального продукту (товарів).

Як відомо, *виробництво* – це сукупність взаємопов’язаних процесів: основних, допоміжних і обслуговуючих [109]. Основними процесами є технологічні процеси (ТП) виробництва, завдяки яким саме

і утворюється матеріальний продукт – основний результат виробництва. В зв'язку з цим процес формування онтологічної інформаційної ієрархії виробничої організації треба починати з аналізу найнижчих щаблів виробництва, тобто з визначення інформації, задіяної у основних виробничих процесах (або бізнес – процесах, якщо виробництво не є матеріальним, наприклад, якщо мета діяльності організації – надання послуг). Зокрема, якщо мова йде про певне матеріальне виробництво, починати треба з аналізу його основних ТП.

На рис.17 наведено фрагмент схеми ТП, представленого на рівні виконання окремих операцій (кружечки на схемі – виконання відповідних операцій) [105]:

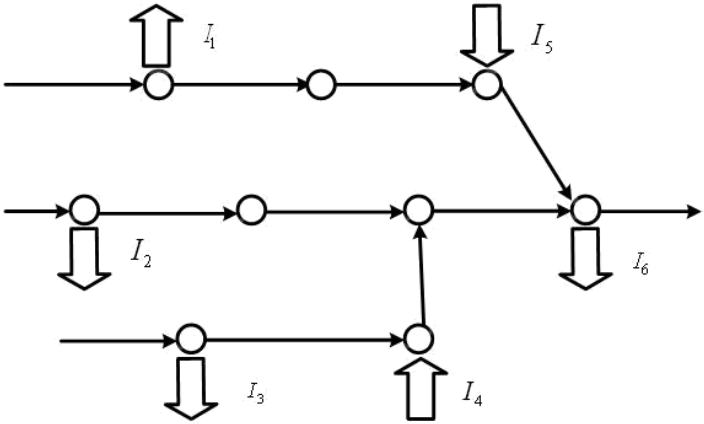


Рис. 17. Фрагмент схеми технологічного процесу

Потовщені стрілки на схемі вказують на потоки інформації (I_1, I_2, I_3, I_6), відбір якої забезпечує контроль параметрів вихідної сировини і матеріалів, задіяних у процесі виробництва, та характеристик стану ТП. Ця так звана параметрична інформація (дані зворотнього зв'язку), яка передається від об'єкта до системи управління ТП. За результатами оброблення отриманих даних система управління видає інформацію, яка передається каналом прямого зв'язку (інформаційні потоки I_4, I_5) до об'єкту управління. Ця інформація, змінюючи режими роботи сервісних пристроїв та устаткування, безпосередньо пов'язаних з регулюванням стану ТП, забезпечує оптимізацію виконання окремих операцій ТП та технологічного циклу виробництва в цілому. Загалом усю перелічену вище інформацію можна узагальнити єдиним поняттям «технологічна інформація».

Аналогічним чином можна проаналізувати інші ТП, що входять до виробничого циклу організації. Крім різних фрагментів технологічної інформації основне виробництво буде характеризуватися інформацією про випуск кінцевого продукту, постачання та споживання сировини, енергоресурсів, кількісними та якісними показниками виробництв в цілому і т.ін. Слід також зазначити, що в межах управління даним ТП реалізуються зв'язки із суміжними ТП, забезпечується ремонт устаткування та обладнання, постачання інструментів.

Крім того, до складу організації мають входити забезпечуючи підрозділи, в яких циркулює фінансово-економічна інформація, статистично-звітна інформація, відомості кадрової служби (включно з відповідними персональними даними), інформація, пов'язана з розробкою, проектуванням, технологічною підготовкою та плануванням випуску нових видів продукції тощо. Представлена у документованому вигляді, уся ця інформація становить внутрішні ІР організації. Циркуляцію цих документів в організації забезпечує система документообігу та архівний підрозділ.

Окремий ІР формується з інформаційних потоків, орієнтованих назовні організації (зовнішня інформація). Це відомості про продаж та маркетинг, логістику та постачання, податковий облік та виплату податків, зовнішнє інвестування, портфель замовлень, інше.

Загалом уся інформація, перелічена вище, являє собою **Сукупну інформацію організації**, яку можна представити у вигляді багаторівневої ієрархії.

На першому рівні виокремлемо:

1.Внутрішня інформація / 2.Зовнішня інформація.

Деталізуючи їх, отримуємо елементи другого рівня ієрархії:

1.1. Виробнича інформація / 1.2.Інформація забезпечуючих підрозділів

2.1. Відомості про продаж та маркетінг / 2.2. Статистично-звітна інформація / 2.3. Рекламно-довідкова інформація / 2.4. Розрахунки з постачальниками та отримувачами продукції / ...

Третій рівень ієрархії:

1.1.1. Технологічна інформація / 1.1.2. Документація з технологічної підготовки виробництва;

1.2.1. Дані про бухгалтерський облік / Відомості про облік та керування кадрами / Планово-фінансова інформація / Адміністративно-керівна інформація / Аналітико-маркетингова інформація / ...

. . . . . .

2.1.1. Відомості про постачальників, обсяги закупівель та специфікації сировини, матеріалів / 2.1.2. Договори з покупцями

товарів, специфікації до них / 2.1.3. Ведення цінових структур, формування прайс-листів / ...

. . . . . .

В тих випадках коли це є необхідним або доцільним, можливо введення додаткових рівнів ієрархії. Наприклад:

1.1.1.1. Параметрична інформація: I_1, I_2, I_3, / 1.1.1.2. Інформація прямого каналу керування ТП: I_4, I_5.

Ступінь деталізації за напрямами онтологічної ієрархії індивідуальна для кожного з них і тісно пов'язана з можливістю підрахунку цінності інформації відповідного найнижчого рівня ієрархії. Так, якщо найнижчі «атомарні» комірки ієрархії за напрямом **1.1. Виробнича інформація** утворюють елементи параметричної інформації та інформації прямого каналу керування ТП, їх цінність обраховується за втратами від блокування чи перекручування (модифікації) цієї інформації, що призводить до погіршення якості продукту ТП, збільшенню відсотку браку або зупинці ТП.

Загалом цінність технологічної інформації будь-якого ТП (бізнес-процесу) визначається через оцінку впливу негативних наслідків реалізації загроз відносно цілісності чи доступності цієї інформації на характеристики стану ТП (бізнес-процесу), його сталість. При такій оцінці враховується опосередкований вплив атак на інформаційні ресурси через зміни у вартості кінцевих продуктів ТП (на окремих стадіях бізнес-процесу) та продукції виробництва в цілому. Зокрема для «атомарних» елементів інформації I_1 - I_6 отримуємо часткові оцінки корисності (важливості) кожного типу цієї інформації для забезпечення виробничого процесу. Узагальнення (об'єднання) інформації I_1 - I_6 в категорію **1.1.1.Технологічна інформація** має супроводжуватися обрахуванням відповідної сукупної оцінки втрат від реалізації загроз щодо цієї категорії. Загалом мають бути отримані сукупні оцінки впливу кожної із загроз за кожним узагальненим ІР (типізованою інформаційною категорією) по всім підрозділам організації.

Доречно зауважити, що особливістю подібної процедури визначення цінності інформації або ІР є те, що вона відбувається на початковому етапі аналізу ризиків, коли ще відсутня деталізація можливих для даної організації інформаційних загроз та способів їх реалізації. Тому відповідно до вже сталого розуміння змісту поняття «цінність інформації» реальна цінність інформації (або ІР) визначається винятково за впливом порушень доступності, цілісності та конфіденційності конкретної інформації (або ІР) на діяльність (стан функціонування) організації, точніше за можливими втратами організації через ці порушення.

Для зовнішньої інформації організації (як і для деяких видів внутрішньої) часто характерні підвищені вимоги до її конфіденційності. Розрахунок можливих втрат в цьому випадку носить ймовірнісний характер й виконується із залучення ситуаційно-сценарних методів прогнозування [64, 95].

Підкреслимо, що наведена вище методика побудови інформаційної онтології базована на виділенні основних інформаційних елементів онтології та встановленню співвідношень між ними шляхом аналізу функціонально-виробничої структури організації. Очевидно, що це є не єдино можливий підхід до формування онтології. Зокрема можна сподіватися на ефективне застосування для побудови онтології так званої інформаційної піраміди, яка характеризує особливості та властивості інформації, задіяної на різних рівнях управління організацією [110]: стратегічному, тактичному, оперативному. Цей підхід дозволяє ввести до структури онтології достатню кількість інформаційних елементів, що зможуть більш-менш повно представити предметну сферу, однак структура їх взаємозв'язків буде відрізнятися від відповідної структури, отриманої при побудові онтології за функціонально-виробничим принципом.

Висновок. Спрощення процедури експертного визначення цінності інформації (ІР) за умов збереження достатньо високого рівня якості експертних оцінок можна отримати при використання так званого ноніусного підходу. Однак можливість його застосування вимагає попередньої структуризації інформації у певній предметній сфері (галузі діяльності). Вдалою формою такої структуризації є побудова онтологічної ієрархії інформаційних елементів відповідної сфери (галузі) діяльності. Аналіз існуючих застосувань інформаційних онтологічних ієрархій, їх основних властивостей та особливостей структури обумовлює доцільність використання у формування інформаційної онтологічної ієрархії підходу, який базується на вивчені та досліджені комплексу реалізованих в організації функціонально-виробничих процесів. Метою цих досліджень є визначення складу, змісту та взаємозв'язків інформації, чия наявність забезпечує ефективне та стале функціонування організації. Саме на базі цієї інформації формується інформаційна онтологія.

Крім того, дослідження цих зв'язків з позицій забезпечення сталості виробничих процесів та якості кінцевої продукції дозволяє достатньо прозоро обчислити цінність певних інформаційних блоків, що утворюють різні рівні інформаційної онтології.

3.4. Застосування системи комбінованих шкал для оцінки інформаційних втрат

Узагальнена задача вимірювання й типологія комбінованих шкал для визначення цінності (значущості) інформації

Процедури вимірювання супроводжують будь-яку людину впродовж всього її життя і в більшості випадків виконуються підсвідомо (цей чоловік вищий, той – нижчий; сьогодні він в доброму настрої/не в гуморі; веселий/радісний/сумний/пригнічений й т.п.), її результати здебільшого не фіксуються, залишаючись звичайно поза нашою увагою. Саме тому, коли мова заходить про вимірюваня, його асоціюють із технікою, природничими науками та іншими видами діяльності, де *суттю вимірювання* є зіставлення вимірюваної якості (часто це геометричні, фізичні властивості досліджуваного об'єкта) з відповідним еталоном (мірою), причому в процедурі вимірювання широко застосовуються спеціальні вимірювальні технічні засоби і отримані результати вимірювання мають цілком об'єктивний характер. Однак у багатьох галузях людської діяльності (економіка, соціологія, психологія, інші соціальні науки) єдиним вимірювальним засобом, що застосовується в процесі вимірювання, є сама людина, а у процедуру вимірювання, окрім чисто технічних дій, вводяться елементи інтелектуальної діяльності. Наприклад, вивчаючи складний соціальний об'єкт, дослідник може ввести певну змінну, яка, за його думкою, відображає головні властивості цього об'єкту та може виступати у якості інтегральної характеристики об'єкту в цілому. Часто ця зміна не може бути виміряна безпосередньо, її значення оцінюються дослідником, експертами або визначаються в якийсь інший непрямий спосіб, маючи, очевидно, суб'єктивний характер. У цій ситуації виникає потреба в розробці загальної теорії вимірювання, яка розв'язала б проблему уніфікації вимірювань на об'єктах різного походження, відтворивши загальну формальну схему як об'єктивних, так і суб'єктивних вимірювань. Одна з перших робіт, в якій було зроблено спробу побудови загальної теорії вимірювань в основу якої покладений теоретико-множинний апарат відношень, належить П.Суппесу [111].

Розглянемо сукупність досліджуваних об'єктів, належних до одного класу, інтегральна характеристика яких відображається змінною x. Природно, що для кожного *r*-ого об'єкту відповідно до його стану ця змінна має різний ступень інтенсивності x_r, тобто за всією сукупністю об'єктів отримаємо множину інтенсивностей $X = \{x_r, r = \overline{1,m}\}$. Зафіксуємо структуру цієї множини шляхом визначення парних

(бінарних) відношень між її елементами, позначаючи ці відношення виразом $q_{rk}(x_r, x_k)$ або ж просто q_{rk}. Сукупність усіх можливих відношень зручно представити квадратною матрицею $Q = \|q_{rk}\|_{m,m}$. Назвемо кортеж (двійку) $S = \langle X, Q \rangle$ *емпіричною системою з відношенням* (ЕСВ). Припустимо, що можливе однозначне відображення

$$\gamma : X \to R, \tag{3.10}$$

де R – множина всіх дійсних чисел, зокрема кожен елемент x_r можна зіставити з числом $z_r = \gamma(x_r) \in R$.

Тоді всю множину елементів X можна зіставити з множиною $Z = \{z_r, r = \overline{1,m}\}$, елементами якої є дійсні числа. Структуру множини Z визначимо через систему парних відношень d_{rk} аналогічно тому, як це було зроблено для множини X, представивши сукупність цих відношень квадратною матрицею $D = \|d_{rk}\|_{m,m}$. Пару $C = \langle Z, D \rangle$ назвемо *числовою системою з відношеннями* (ЧСВ). Якщо сукупність числових значень ЧСВ, які утворилися внаслідок відображення (3.10), має таку структуру, що для неї задовольняється умова $Q = D$, то система C являє собою гомоморфний образ (гомоморфізм) системи S, а відображення

$$\gamma^* : S \to C, \tag{3.11}$$

називається *гомоморфним*.

Якщо відображення S є взаємооднозначним, маємо випадок ізоморфного відображення (*ізоморфізм*). Тобто ізоморфізм гарантує однаковість структур систем, а гомоморфізм – їх подібність. Кортеж (трійка) $\langle S, C, \gamma^* \rangle$ зветься *шкалою вимірювання*.

У більш вузькому сенсі *шкала* – це сукупність правил, за якими виконується зіставлення множини станів емпіричної властивості досліджуваного об'єкта множині дійсних чисел. Сам процес зіставлення складає процедуру вимірювання, визначальною особливістю якої є забезпечення (відтворення) між елементами числової системи характеру відношень між відповідними станами емпіричної властивості.

Зазаначимо, що одну і ту ж ЕСВ S можна відобразити у числову систему різними способами. Зокрема, якщо результатами таких відображень γ_1 і γ_2 є ЧСВ C_1 та C_2, до складу яких входять відповідні множини $Z_1 = \{z_{1r}, r = \overline{1,m}\}$, $Z_2 = \{z_{2r}, r = \overline{1,m}\}$ і існує функціональне

перетворення *f*, за допомогою якого відображення γ_1 можна взаємно однозначно перевести у відображення γ_2 ($\gamma_2 = \gamma_1 f$, $\gamma_1 = \gamma_2 f^{-1}$), то шкали $\langle S, C_1, \gamma_1 \rangle$ і $\langle S, C_2, \gamma_2 \rangle$ вважаються *приналежними до одного типу*, а перетворення *f* зветься *припустимим перетворенням*.

Введення поняття припустимих перетворень дещо трансформує прийняте в рамках класичного підходу [111] визначення поняття шкали як трійки $\langle S, C, \gamma \rangle$. Відповідно до сучасних уявлень, найбільш повною і змістовною характеристикою шкали є множина *Ф* припустимих перетворень значень емпіричної властивості, виміряних у даній шкалі. Залежно від складу множини *Ф*, характерного для певних типів шкал, можливе проведення структуризації множини довільних шкал, результатом якої має бути побудова типології шкал. Загальноприйнятий варіант такої типології наведений у табл. 7. При аналізі введеної типології, зокрема, порівнянні різних типів шкал звичайно використовуються поняття сильних (потужних) шкал й, відповідно, слабких. Назвемо одну з двох шкал більш сильною (потужною), якщо множина її припустимих перетворень серед інших включає усі припустимі перетворення, притаманні другій шкалі.

Таблиця 7

Типологія множини довільних шкал

Тип шкали	Припустимі перетворення для даного типу шкали
Номінативна	Взаємнооднозначне: $(x_1 = x_2) \equiv (f(x_1) = f(x_2))$
Порядкова	Монотонно зростаючі: $(x_1 < x_2) \equiv (f(x_1) < f(x_2))$
Інтервальна	Додатні лінійні: $f(x) = ax + b; a, b$ – довільні дійсні числа, $a > 0$
Шкала відношень	Перетворення подібності: $f(x) = ax, \quad a > 0$
Абсолютна	Тотожність: $f(x) = x$

Найбільш слабким типом шкали вважається *номінативна* (інакше – шкала найменувань). У ній числа є лише умовними найменуваннями класів, на які поділено вихідну множину об‘єктів, тобто виконання математичних операцій з цими числами є некоректним, числа відіграють ролі власних імен. Наприклад: надання множині жінок умовного числового позначення «α», множині чоловіків – «β», зокрема α=1, β=2, або будь-які інші числові позначення.

Більш сильною є *шкала порядку* (порядкова, ординальна), в якій усі об‘єкти шикуються за певною ознакою (властивістю) за принципом її зростання (збільшення) або навпаки, тобто для об‘єктів, що

порівнюються за емпіричною властивістю X, має встановлюватися відношення порядку: $x_1 < x_2 \le x_3 < ... < x_n$. Суттєво є те, що принцип пропорційності в цій шкалі не виконується, тобто не можна вказати, наскільки x_2 краще за x_1 (у загальному випадку – x_i краще, ніж x_j, якщо $j < i$).

Шкала інтервалів є частково метричною, дозволяє застосовувати лінійні перетворення, але не має встановленої точки нульового відліку, точніше, ця точка може встановлюватися довільним чином.

Ще більш сильною є *шкала відношень* (пропорційна). Це метрична шкала, в якій є припустимою зміна масштабу і яка має «природну» нульову точку. Це типова шкала для вимірювання більшості технічних чи фізичних величин (швидкості, ваги, ємності, грошових статків тощо).

Абсолютна шкала є найбільш потужною (сильною) шкалою. Для неї множина припустимих перетворень містить тотожне перетворення $f(x) = x$, тобто фактично отриманий результат вимірювань є єдино можливим і відносно нього неприпустимі будь-які додаткові перетворення. Абсолютна шкала *метрична*, має природну нульову точку відліку та природну одиницю вимірювання – одиницю лічби. Ця шкала застосовується для вимірювання кількості елементів у скінченій множині, тобто є шкалою натуральних чисел. Фізичний приклад абсолютної шкали – шкала температур за Кельвіном.

Наведені в табл. 7 типи шкал утворюють своєрідну ієрархію, в якій кожна наступна шкала включає в себе попередню і тому є більш потужною порівняно з усіма попередніми. Таким чином, абсолютна шкала матиме властивості усіх інших, тобто з даних, отриманих в абсолютній шкалі, можна визначити все, що може дати вимірювання в інших шкалах.

Наприклад, якщо відомо, що в групі А – 20 студентів, а в групі В – 10 студентів, то маємо наступні висновки: в групі В студентів удвічі менше (шкала відношень), їх менш на 10 (шкала інтервалів), група А кількісно більша за групу В (порядкова шкала), кількість студентів в групах неоднакова (номінативна шкала).

Слід зазначити, що в типізації виділяються лише основні типи шкал. Тому треба взяти до уваги, що кожний окремий тип шкали може мати численні модифікації, а будь-яка пара основних типів здатна породити множину проміжних, змішаних (або комбінованих) шкал. Крім того, для сучасного розуміння шкали зовсім не обов'язково відображати ЕСВ у ЧСВ – замість останньої може бути інша формальні знакова система, за допомогою якої можна адекватно змоделювати ЕСВ.

Експертно-аналітична процедура оцінювання значущості інформаційних ресурсів в загальному випадку

Розглянемо наступну ситуацію. Існує узагальнений (множинний) ІР J_{Σ}, що містить інформацію про найрізноманітніші галузі людської діяльності, який постійно поповнюється, розширюється, але при цьому припускає свою фрагментацію на часткові ІР. Рівень цієї фрагментації може бути довільним, залежно від потрібного ступеня деталізації описів об'єктів (елементів) у тій чи іншій предметно-прикладній галузі діяльності. Ступінь деталізації може змінюватися з часом, тому фрагментація вихідного ресурсу J_{Σ} на часткові носить динамічний характер. Потрібно побудувати процедуру оцінювання цінності (значущості) виділених часткових ІР.

Очевидно, з плином часу обсяг узагальненого ресурсу J_{Σ} буде збільшуватися, що є природним наслідком цивілізаційного процесу. Сукупна значущість ресурсу J_{Σ} буде, напевно, зростати. Закономірності зміни цінності (значущості) часткових ІР, які залежать від впливу множини найрізноманітніших та, як правило, лише частково врахованих факторів, практично не піддаються прогнозу та можуть проявлятися найнесподіванішим чином. Тому *єдиним способом визначення значущості часткових ІР є* <u>*експертне оцінювання*</u>, помилки якого мають суб'єктивний характер і залежать лише від рівня компетентності експертів та складності поставленого перед ними певного завдання. Підбір компетентних експертів є організаційним моментом підготовки експертизи і розглядається окремо. У зв'язку з цим зупинимося лише на мінімізації помилки, зумовленої складністю об'єкта експертизи. Один з варіантів розв'язку цього завдання полягає у відмові від проведення традиційної одноетапної експертизи із знаходженням прямих оцінок значущості ІР та переході до експертно-аналітичної процедури формування оцінок, яка, на відміну від звичайно експертизи, використовує поетапне структурування процесу експертизи та певну логічну регламентацію змісту його окремих етапів.

При формування експертно-аналітичної процедури оцінювання цінності (значущості) ІР враховується *два принципових аспекти*, а саме:

– звуження предметної області об'єктів експертизи, утвореної сукупністю ІР, відносно цінності яких повинен визначитися експерт, що дозволяє спростити підбір експертів з високим рівнем компетентності;

– врахування можливої наявності до моменту проведення експертизи ІР певної кількості вже оцінених ресурсів, що істотно спрощує прийняття рішення стосовно нового, ще не експертованого ІР, і

робить доцільним виокремлення двох відмінних не співпадаючих типових задач визначення цінності ІР:

1) задачі первинної експертизи ІР, де оцінюванню підлягає вся вихідна сукупність ІР, що складають узагальнений (множинний) інформаційний ресурс J_{Σ} (по аналогії до [32] – *оцінка*);

2) задачі вторинної експертизи, де частина часткових ІР вже пройшла первинну експертизу (по аналогії до [32] – *експертиза*).

Можливими є різні способи побудови експертно-аналітичної процедури, які залежать від об'єктів експертизи та сформованих у відповідних предметних галузях традиційних підходів до проведення експертизи.

Зокрема, спираючись на наведені в [102] матеріали, для виконання *первинного експертно-аналітичного оцінювання* значущості ІР можна запропонувати наступну послідовність дій.

1. Увесь представлений на експертизу узагальнений ресурс J_{Σ} подається у вигляді *об'єднання ресурсних областей* J_i, що не перетинаються, кожна з яких відповідає певній предметно-прикладній сфері:

$$J_{\Sigma} = \bigcup_{i=1}^{n} J_i \,,\ i = \overline{1,n} \,,\ J_i \cap J_j = \varnothing \text{ при } i \neq j. \qquad (3.12)$$

2. У кожній окремій ресурсній області J_i *виділяються групи ресурсів*, які допускають за своїми характеристиками та рівнями значущості взаємне зіставлення. Задаються наближені (грубі) межі діапазонів оцінок відповідних ресурсних груп, серед яких вибираються найбільша верхня $C_{max\ i}$ і найменша нижня $C_{min\ i}$ межі, які визначають верхню та нижню границі шкали оцінок для відповідної предметно-прикладної сфери. Отримані пари ($C_{max\ i}$, $C_{min\ i}$), $i = \overline{1,n}$ оцінюються в умовних одиницях (балах), які не прив'язані до будь-якої конкретної грошової одиниці. Зіставлення цих пар, які визначені для різних предметно-прикладних галузей, дозволяє здійснити погодження та ув'язування рівнів значущості інформації по всій множині ІР, які входять в узагальнений ресурс J_{Σ}, а також вносить необхідні поточні корекції у випадку природної зміни значущості ІР окремих предметно-прикладних галузей. При цьому стає очевидною певна конвенціональність отриманих оцінок значущості інформації, які залежать, зокрема, від повноти та репрезентативності системи часткових ІР, що складають узагальнений ІР J_{Σ}.

3. Для множини часткових ІР $\{I_{kl}\}$, $l=\overline{1,L_k}$, які утворюють *k*-у ресурсну групу I_k, експертним шляхом за допомогою методу попарних порівнянь виконується впорядкування вихідної сукупності відповідних часткових ІР.

У рамках цієї класифікаційної операції для елементів, що зіставляються в ресурсній групі I_k, шляхом введення бінарного відношення $\leq$ на множині часткових ІР $\{I_{kl}\}$, $l=\overline{1,L_k}$ формується *решітка (гратка) цінностей ІР* цієї ресурсної групи.

4. Для впорядкованої сукупності часткових ІР визначається множина оцінок значущості $\{c_{kl}\}$.

Застосовуючи метод експертних оцінок, кожному елементу сформованої решітки приписується кількісне значення його цінності, сукупність яких утворює шукану множину оцінок значущості $\{c_{kl}\}$ відповідних часткових ІР. При оцінюванні значущості із застосуванням векторних критеріїв, тобто коли значущість ІР визначається рядом споживчо важливих ознак, для знаходження результуючих оцінок значущості доцільно застосовувати відомі методи багатокритеріального аналізу, зокрема *метод аналізу ієрархій* (MAI) [70, 98].

Після знаходження множин оцінок значущості часткових ІР для окремих ресурсних груп отримаємо множину сукупності ІР всієї ресурсної області J_i, а потім – всього узагальненого ресурсу J_Σ. У разі необхідності можливе проведення додаткових експертиз з метою перевірки якості отриманих оцінок цінності через попарне зіставлення базових елементів окремих ресурсних груп та областей й приписаних їм кількісних оцінок цінності. Після цього завдання первинної експертизи ІР можна вважати виконаним.

Якщо виконання робіт здійснюється групою експертів по етапам пп. 1-4, для обробки отриманих у цьому випадку результатів доцільно використовувати *методи теорії нечітких множин* [112].

Задачу вторинної експертизи розглянемо на прикладі експертизи нового одиничного часткового ІР (очевидно, вторинна експертиза групи нових часткових ІР може бути просто зведена до цього прикладу). При появі нового часткового ІР перш за все визначається конкретна предметно-прикладна сфера, до якої належить цей новий ІР, тобто відповідна цьому ІР ресурсна область та ресурсна група. Далі експерт, компетентний у цій сфері, спочатку виявляє місце розташування нового ІР в лінійно впорядкованій множині часткових ІР, які утворюють решітку цінностей (наприклад, застосувавши метод парних порівнянь), а

потім, завершаючи експертизу, кількісно оцінює цінність (значущість) нового часткового ІР, використовуючи, якщо в тому є потреба, МАІ. При цьому кількість елементів решітки збільшується на одиницю, а класифікація чергового нового ІР відбувається в більш деталізованій решітці.

Якщо поява нового часткового ІР є результатом перефрагментації раніш існуючих, необхідно зіставити його з близькими інформаційними комплексами, отриманими на більш ранніх фрагментаціях узагальненого ресурсу J_{Σ}, порівняти їх об'єми та зміст, перевірити можливість наявності включень одного ресурсу в інші. Це дозволить певною мірою спростити процедуру визначення цінності (значущості) нового ІР та ввести в неї елементи контролю.

При збільшенні обсягу ІР за рахунок об'єднання деяких часткових ресурсів слід враховувати можливість стрибкоподібного зростання рівня цінності нового інтегрованого ІР внаслідок можливого прояву в ньому ефекту емерджентності [113].

Загалом процедуру визначення цінності (значущості) деякого часткового ІР можна інтерпретувати як вимірювання цінності цього ресурсу в складній комбінованій шкалі**,** формування якої виконано у відповідності з пп. 1-3.

Розглянемо склад та структуру цієї шкали. Розподіл узагальненого ресурсу J_{Σ} по предметно-прикладних сферах фактично являє собою побудову номінативної шкали, яка забезпечує грубу попередню класифікацію множини можливих часткових ІР. Всередині кожної номінації (класу тієї шкали, якому відповідає ресурсна область J_i, $i=\overline{1,n}$) здійснюється більш детальна класифікація часткових ІР за ресурсними групами. Як наслідок отримуємо набір локалізованих номінативних шкал, по одній на кожну ресурсну область. Загалом ця структура являє собою подвійну ієрархічну номінативну шкалу. Якщо кількість часткових ІР, які входять до деяких номінацій другого рівня ієрархії, велика, для цих номінацій доцільно сформувати ще один, третій рівень номінативної шкали. Очевидно, що при необхідності можливо нарощувати ще більш високі рівні шкали. В номінаціях останнього рівня, в нашому випадку, згідно з п.3 – другого рівня номінативної ієрархії, множина часткових ресурсів у межах кожної ресурсної групи I_k впорядковується за своєю значущістю, утворюючи порядкову шкалу виду: $I_{k(1)} \le I_{k(2)} \le ... \le I_{k(l)} \le ... I_{k(L)}$, яка є шкалою третього рівня ієрархії.

Враховуючи те, що кожній ресурсній групі I_k ставиться у відповідність деякий діапазон оцінок в балах ($c_{k\ max}$, $c_{k\ min}$], отримуємо комбіновану порядково-інтервальну шкалу. Приписуючи кожному елементу I_{kl} експертну оцінку в балах c_{kl}, $k=\overline{1,L}$, посилюємо порядкову шкалу до інтервальної. Це посилювання носить штучний характер, правильність отриманих результатів визначається винятково точністю відповідних експертних оцінок c_{kl}. Слід зазначити, що неявна спроба посилення шкали присутня і на етапі побудови подвійної ієрархічної номінативної шкали, при введенні бальних значень меж діапазонів оцінок ($c_{k\ max}$, $c_{k\ min}$], $k=\overline{1,L}$ ресурсних меж, що робить можливим метризацію порядкових шкал для ресурсних груп.

Введення подібної комбінованої вимірювальної шкали дозволяє відносно легко реалізувати оцінювання рівня значущості деякого ІР I', інтерпретувавши процедуру оцінювання як рішення узагальненої задачі вимірювання в цій шкалі. Зокрема, використовуючи подвійну ієрархічну номінативну шкалу, достатньо просто знайти ресурсну групу, до якої відноситься ресурс I', а потім експертним або експертно-аналітичним шляхом визначити положення ресурсу I' у відповідній локальній порядковій шкалі та кількісну оцінку c' рівня значущості цього ІР.

Можливість застосування сучасної теорії вимірювань до задач оцінювання рівня втрат, обумовлених витоком СІ, спирається на застосування двох базових *методів прикладного аналізу інформації*: методу парних порівнянь та ноніусного підходу до класифікації інформації.

Класичний *метод парних порівнянь* дозволяє розташувати елементи, що складають певну множину, у порядку збільшення або зменшення ознаки, спільної для всіх елементів даної множини. Відома також методика, коли подібна класифікація (ранжування) відбувається за кількома ознаками (комплексом або вектором ознак), – *метод аналізу ієрархій* (MAI) [98]. На жаль, парні порівняння добре працюють за умов, коли кількість елементів множини, що аналізується, незначна. Із збільшенням обсягу цієї множини трудомісткість та складність застосування методу парних порівнянь різко зростає, що робить його непридатним для практичного використання.

Виходом в цьому випадку може бути своєрідний гіпертекстовий варіант порівняльного аналізу, в якому вихідна сукупність елементів поділяється на певні підмножини, що утворюють так звану *ноніусну лінійку шкал*. Ця лінійка є своєрідною ієрархією шкал, де кожна з них, починаючи з другої, є більш точною допоміжною шкалою, яка деталізує,

уточнює окремі елементи (фрагменти) попередньої грубішої шкали вищого рівня ноніусної ієрархії.

Наприклад, перша – груба шкала (найвищий рівень ієрархії) утворюється четвіркою інформаційних блоків, що містять інформацію в сферах:

1) оборони;

2) економіки, науки, техніки;

3) зовнішніх відносин;

4) державної безпеки та охорони правопорядку.

Кожен з перелічених блоків грубої номінативної шкали може бути представлений більш деталізовано підмножиною конкретизуючих його зміст допоміжних інформаційних елементів, наприклад:

3.1) загальні відомості про дипломатичні відносини з іншими державами;

3.2) відомості про домовленості у сфері військово-технічного співробітництва з іноземними державами;

3.3) ..... .

Ці інформаційні елементи припускають ранжування за рівнем втрат, обумовлених витоком відповідної інформації, тобто утворюють ноніусну ранжовану шкалу другого рівня. При необхідності можлива конкретизація окремих (чи всіх) елементів цієї шкали введенням додаткових множин деталізуючих інформаційних елементів. Приміром, за п. 3.2) можемо отримати:

3.2.1) інформація про міжнародні угоди в галузі розробки озброєнь та військової техніки;

3.2.2) інформація про міжнародні контракти в сфері постачання озброєнь та військової техніки;

3.2.3) ..... .

Додатково введені інформаційні елементи після їх ранжування за рівнем можливих втрат внаслідок витоку відповідної інформації утворюють ноніусну ранжовану шкалу третього рівня. Продовжуючи процедуру деталізації (якщо це є доцільним) інформаційних елементів шкали третього рівня, отримаємо ноніусні ранжовані шкали ще більш високих рівнів.

Певною мірою прикладом подібного ноніусного підходу до класифікації інформації є структура представлення інформації в ЗВДТ.

Упорядкована таким чином множина інформаційних елементів утворює систему номінативно-рангових шкал, до якої експерт має змогу «вмонтувати» будь-який новий елемент, що підлягає оцінюванню щодо визначення рівня можливих втрат через розголошення змісту даного елемента. Для цього експерт визначає на ноніусній лінійці шкалу, найближчу за змістом і рівнем деталізації до об’єкту оцінювання та

виконує низку парних порівнянь об'єкту з вузлами (елементами) обраної шкали. Місце, яке зайняв об'єкт оцінювання в системі рангових шкал, можна надалі сприймати як новий вузол шкали, що в подальшому буде використаний у процедурі наступних парних порівнянь при оцінюванні нових інформаційних елементів.

Для визначення належності оцінюваної інформації до секретної необхідним є отримання кількісних оцінок можливих втрат, обумовлених розголошенням цієї інформації, які в порядковій (ранжованій) шкалі обрахувати немає змоги. Тому слід виконати метризацію ноніусної системи шкал, присвоївши її вузлам-елементам кількісні оцінки рівнів втрат.

Для цього розглядається все, що має певну цінність (іміджеву, економічну, політичну тощо) і у той чи інший спосіб може бути асоційоване з відповідним інформаційним елементом. В ДСТУ ISO/IEC 13335 [100] це «все» визначається терміном «активи», пов'язані з інформаційним елементом, а збитки, обумовлені зменшенням цінності активів внаслідок витоку інформації, виступають в якості кількісної оцінки рівня відповідних втрат. У Методичних рекомендаціях ці активи (у дуже скороченому обсязі) наведено у Додатку 1 [38] (див. *Додаток 5*), де їх цінність визначається терміном «питома вага» об'єкту тієї чи іншої сфери діяльності (оборони, економіки, державної безпеки тощо). Очевидно, що ефективне застосування подібної методики оцінювання втрат можливе лише за умов існування дуже докладних переліків активів у кожній сфері діяльності, пов'язаної з використанням СІ, зокрема, при складанні таких переліків до кожної шкали ноніусної лінійки шкал.

Крім того, слід мати на увазі, що втрати інформації лише за змістом одного інформаційного елемента можуть обумовити збитки щодо різних активів, тобто слід аналізувати та розглядати різні варіанти подій, поштовхом до яких стала втрата відповідної інформації.

У розгорнутій постановці задача шкалювання та вимірювання цінності інформації, включаючи деякі відомості з теорії узагальненого вимірювання, побудови та інтерпретації систем ноніусних (комбінованих) шкал (у тому числі і в «Рекомендаціях..» [38]), наведено в статті [102]. Матеріали з методики парних порівнянь, МАІ та апарату нечітких множин, який може ефективно використовуватися у задачі експертного оцінювання рівня збитків, обумовлених витоком СІ.

3.5. Проблеми методики обробки оціночних суджень членів групової експертизи

Експертне оцінювання, загальні відомості

Експертне оцінювання – здавна одна з найбільш поширених інформаційних технологій, яка і в наш час приваблює широке коло фахівців – як практиків, так і теоретиків. Пояснюється це рядом особливостей, притаманних *методу експертних оцінок.*

По-перше, даний метод – найбільш доступний, універсальний, а іноді просто єдиний можливий для отримання та аналізу інформації, що використовується для вирішення широкого спектра задач управління, прогнозування, планування в соціології, техніці.

По-друге, сфера застосування експертного оцінювання постійно розширюється – визначення параметрів і структури складних систем, особливо тих, що не мають достатньої передісторії функціонування і характеризуються високим рівнем структурно-параметричної невизначеності: складних соціально-економічних систем, систем проектного менеджменту, СЗІ і т.д. Загальною, досить привабливою стороною експертних методів є оперативність і простота отримання потрібних відомостей.

При використанні методу експертних оцінок основним джерелом інформації є експерт – його судження, якісні та кількісні оцінки. Тобто експертні методи ґрунтуються виключно на оцінках експертів, зроблених щодо проблеми, яку вони вичерпно знають. При цьому механізм продукування цих оцінок лишається невизначеним. Як правило, він невідомий навіть самому експертові, має виключно індивідуальний, особистий характер і не може бути повторений чи відтворений кимсь іншим. Це обумовлює особливі вимоги щодо вибору складу експертів, зокрема рівня їх компетентності, адже недостатній рівень компетентності експерта може призвести до появи грубих (аномальних) помилок у даних експертизи чи просто зумовити високий рівень неоднорідності цих даних. В обох випадках можливі суттєві втрати інформації, що призведуть до неправильно прийнятих за результатами експертизи рішень, помилкового завдання параметрів, оцінок й т.п., негативні наслідки яких можуть бути відчутні і на всіх наступних етапах застосування результатів, отриманих за даними експертизи.

Тому ефективна, якісна обробка експертних даних значною мірою визначає коректність й правильність виконання всієї експертизи в цілому. У цій ситуації особливу важливість і актуальність набуває

проблема аналізу та обробки експертної інформації, так як виконання тільки цих заходів дозволяє забезпечити якість рішень, що приймаються.

Відсутність загальновизнаних формально-теоретичних і методичних положень, що пояснюють механізм формування експертних даних (і в тому числі похибок у цих даних), обумовлює той факт, що загальні рекомендації по обробці експертних даних, тим більш реалізовані в формі програмного продукту, на сьогодні відсутні. Оброблювач, що використовує експертні дані, найчастіше сам вирішує, як з ними працювати. Математичні методи обробки, що застосовуються, як правило, дуже прості, бо використання більш складних методик обробки потребує залучення додаткової інформації, зазвичай відсутньої. Все сказане вище обумовлює актуальність досліджень, пов'язаних з вивченням і розробкою методів або методик обробки експертних даних. Особливо актуальна проблема обробки даних експертизи в нових сферах людської діяльності, в яких ще недостатньо сформувався формально-теоретичний базис, не структурована різноманітність властивостей і особливостей об'єктів, що вивчаються, не сформувалась достатня кількість спеціалістів, за якістю своєї підготовки адекватним вимогам, що пред'являються рівню експерта.

Чим «молодша» предметна галузь та динамічніший її розвиток, тим загалом, частіше доводиться застосовувати експертні методи вирішення задач в цій галузі і тим складніше сформувати групу експертів, які мають однаково високий рівень компетентності. На жаль, організатори експертизи часто усвідомлюють цю проблему лише після ознайомлення з отриманими експертними даними, коли ці дані виявляються єдиною «сировиною», з якої можна дістати потрібні відомості про рівень компетентності кожного експерта.

Методи, що основані на використанні експертних оцінок, діляться на дві групи: індивідуальні (персональні) експертні оцінки; групові (колективні) експертні оцінки.

Методи індивідуальних експертних оцінок, у свою чергу, діляться на аналітичні експертні оцінки, інтерв'ю, парні порівняння та інші.

Методи колективної оцінки – відповідно метод комісії, метод Дельфі, Паттерн тощо.

Поділ на методи індивідуальних та колективних експертних оцінок проводиться в залежності від того, як визначається кінцевий результат експертизи: на основі висновків одного експерта чи за наслідками роботи групи експертів, причому результат групової експертизи може обчислюватися шляхом інтеграції індивідуальних оцінок експертів.

Головною проблемою будь-якої експертизи є вибір способу формування суджень експертів. Саме це питання має першочерговий пріоритет в аналізі, дослідженні та розробці різних аспектів експертизи,

пов’язаних з її організацією і проведенням. Частково ці проблеми вже розглядалися вище, коли йшлося про критерії віднесення інформації до секретної, формування структури та вибір складових елементів відповідного критеріального показника, способи визначення його кількісних оцінок експертами (МАІ, ноніусний підхід, технології розмитих множин). Дещо менше уваги приділяється засобам та методам зменшення похибок у сукупності вже отриманих індивідуальних оцінок, зокрема при їх інтеграції у кінцевий результат групової експертизи.

У роботі [114] наведено опис ряду поширених методів експертного оцінювання з елементами їх аналізу з точки зору можливості забезпечення інформативності та точності результатів експертизи. За матеріалами цієї оглядової розвідки можна зробити висновок, що, незважаючи на відмінності наведених методів, їм властивий ряд спільних заходів (прийомів, процедур), спрямованих на підвищення інформативності та точності експертних даних. Серед цих заходів та прийомів можна виділити і класифікувати такі напрями:

– визначення необхідних і достатніх умов для оцінки спеціаліста як експерта;

– оцінка характеристик експерта;

– організація проведення експертизи;

– вибір методів стимулювання експертів;

– вибір методів обробки експертної інформації та інші.

Узагальнення наведених у роботі [114] матеріалів дозволяє виділити три основні групи методів зменшення похибки в експертних оцінках:

– *організаційні методи* – вони базуються на запровадженні спеціальних організаційних засобів з отримання та використання додаткової інформації, яка безпосередньо використовується експертами для продукування суджень високого рівня достовірності (насамперед, це так звані «складні експертизи», зокрема «дельфійська», в яких безпосередньо застосовуються такі організаційні форми проведення експертування, що гарантовано забезпечують високу кінцеву точність результатів експертизи, а також різні способи відбору експертів, що гарантують їх високу компетентність);

– *організаційно-розрахункові методи* – суть їх полягає в запровадженні спеціальних організаційних засобів з отримання додаткової інформації про рівень компетентності експертів та використанні цієї інформації у процесі подальшої спеціальної обробки результатів експертизи;

– *математичні методи обробки даних експертизи*, що базуються виключно на видобуванні та наступному використанні допоміжної інформації безпосередньо із результатів експертизи, без застосування

спеціальних організаційних засобів на етапах підготовки та проведення експертування.

Аналізуючи найбільш поширені методи експертного оцінювання, варто зосередити увагу на часовому і вартісному аспекті застосування цих методів. Складні експертизи (наприклад, метод Дельфі) вимагають проведення достатньо копіткої організаційної роботи, яка й дозволяє отримати і якість, і надійність вихідних результатів експертизи. Сама процедура складної експертизи займає доволі багато часу (наприклад, знов-таки, дельфійська процедура). У сукупності і часовий фактор, і організаційний обумовлюють високу вартість експертизи. Однак вище вже зазначалося, що до експертних оцінок звертаються саме через можливість зекономити і час, і кошти. Тому використання складних експертиз часто суперечить самій логіці спонукальних мотивів, які обумовлюють звернення до цих процедур. Значно частіше звертаються до простих експертиз, швидких, оперативних, при цьому необхідна якість їх результатів забезпечується проведенням апостеріорної математичної обробки вихідних оцінок, отриманих у простій експертизі. Зважаючи на те, що в багатьох застосуваннях ця обробка має типовий характер, доцільно реалізовувати її за допомогою системи підтримки прийняття рішень, яка виконувала б функції підкажчика для користувача, що є непрофесіоналом у галузі обробки даних [114].

Отримання та обробка оціночних суджень членів експертних комісій при державних експертах з питань таємниць

Відповідно до Закону України «Про державну таємницю» [3], *віднесення інформації до ДТ* – це процедура прийняття (ДЕТ) рішення про віднесення категорії відомостей або окремих відомостей до ДТ з установленням ступеня їх секретності шляхом обґрунтування та визначення можливої шкоди національній безпеці України у разі розголошення цих відомостей, включенням цієї інформації до ЗВДТ, та з опублікуванням цього Зводу, змін до нього [3].

Для виконання поставлених перед ними завдань ДЕТ мають, зокрема, право створювати ЕК з фахівців і науковців, які мають допуск до ДТ, для підготовки проектів рішень про віднесення інформації до ДТ, зниження ступеня її секретності та скасування зазначених рішень. Крім названих завдань, до компетенції цих комісій, відповідно до «Положення про експертні комісії з питань державної таємниці» (далі – Положення [30]), віднесено визначення та зміну СС інформації, віднесеної до ДТ.

Положенням [30] закріплено лише цільові настанови, повноваження та загальні організаційні засади роботи ЕК із питань ДТ. Документом, яким встановлено порядок віднесення відомостей до ДТ та ступеня їх

секретності в Україні, є «Рекомендації…» [38]. Виходячи із цих документів, до сьогодні залишається на жаль не вирішеною низка проблем, існування яких прямо впливає на ефективність діяльності ДЕТ. Перш за все, це відсутність будь-яких регламентацій із способу визначення експертами кількісних оцінок об'єкту експертизи та порядку узагальнення оціночних суджень членів ЕК [54].

Нині у працях вітчизняних та зарубіжних науковців досліджуються методичні проблеми діяльності експертних груп та застосування експертного оцінювання для розв'язання широкого кола завдань, зокрема прогнозування соціальних явищ [115-117]. Аналіз цих наукових здобутків дозволяє зробити висновок щодо можливості їх використання після відповідної адаптації в заповненні прогалин методичного забезпечення діяльності ЕК при ДЕТ.

Зазначимо, що застосування методу опитування експертів для прогнозування можливих наслідків розголошення інформації, в тому числі їх тяжкості, цілком відповідає традиційній сфері використання цього наукового інструменту, бо він переважно використовується для аналізу й оцінювання об'єктів високої складності за умов недостатньо сформованого формалізованого інструментарію опису та дослідження цих об'єктів, що не дозволяє охопити єдиною логіко-математичною структурою багатоманітність властивостей досліджуваного об'єкта [70].

Відповідно до «Рекомендацій…» [38] для визначення належності відомостей до ДТ при ДЕТ спеціально створеними із цією метою ЕК розраховується рівень потенційної СШ державі у визначених законодавством сферах шляхом врахування низки показників, які визначаються членами ЕК і заносяться ними до індивідуальних листів опитування, що включають наступні питання (див. *Додаток 7*):

1) відомості, що підлягають експертизі;

2) сфера чи сфери діяльності, до якої відносяться відомості;

3) об'єкт, який містить відомості, що підлягають експертизі, їх питома вага (у балах);

4) прогнозні дії сторони, що оволоділа відомостями;

5) складова частина (елемент) об'єкта, яка безпосередньо підпадає під дію сторони, що оволоділа відомостями, її відносна вартість від вартості об'єкта (у відсотках);

6) зниження ефективності використання СЧО або об'єкта в цілому внаслідок дії сторони, що оволоділа відомостями (у відсотках);

7) величина ЕШ (у балах);

8) ІТН від втрати відомостей, рівень завданої ними шкоди (у балах);

9) СШ (у балах).

Згідно з розділом 5.1 «Рекомендації…» [38], пункти 2-5 листа опитування визначаються членами ЕК спільно. Це обумовлює

можливість об'єктивізації суб'єктивних оцінок експертів за цими пунктами у ході їх обговорення. Проте кожен член ЕК робить незалежно один від одного висновки за пунктами 6-9. Таким чином, за характерними особливостями роботи комісії, виконувану нею експертизу слід вважати груповою (колективною, колегіальною), остаточний кількісний експертний висновок якої визначається на базі обробки попередньо отриманих індивідуальних експертних оцінок. Процедуру цієї обробки у «Рекомендаціях…» [38] зведено до обчислення середньоарифметичного значення відповідних індивідуальних оцінок.

На жаль, середньоарифметичне є оцінкою, дуже чутливою до так званих аномальних даних, тобто даних, які за своїми значеннями «випадають» із загальної сукупності експертних оцінок (від англомовного outstanding date). Зокрема, якщо хоча б один з експертів, що входять до складу ЕК (за 5-им розділом «Рекомендацій…» [38] чисельність ЕК – 5-7 осіб або більше) дасть кількісну оцінку, суттєво відмінну від інших, це призведе до істотного зміщення середньоарифметичного, особливо відчутного за мінімальної кількості експертів. Наприклад, у разі формального виконання настанов «Рекомендацій…» [38], за отриманою сукупністю бальних оцінок {85, 90, 90, 95, 160} об'єкт експертизи, згідно з шкалою, введеною в п. 3.3 цих «Рекомендацій…» [38], має отримати СС «ОВ» (середньоарифметична оцінка дорівнює 104 і потрапляє у межі «від 100 і більше», що відповідає ступеню «ОВ»), тоді як перші чотири експерти одностайно визначили доцільність ступеня «ЦТ» (середньоарифметична оцінка перших чотирьох експертів дорівнює 95 балів і потрапляє в межі «від 10 до 100 балів», що відповідає СС «ЦТ») [38].

Спираючись на наведений приклад, можна констатувати, що настанова «Рекомендацій…» [38] з обробки індивідуальних оцінок експертів не розрахована на можливість наявності оцінки з суттєвим відхиленням від рівня інших оцінок і її формальне виконання гарантує прийнятні результати лише у випадку, коли індивідуальні оцінки експертів утворюють більш-менш однорідну сукупність. Очевидно, в реальності виникнення ситуації, подібної до наведеного прикладу, стає причиною додаткового позаформального обговорення експертами об'єкта експертизи, тобто фактично відбувається другий тур експертизи, в якому найшвидше за все відбудеться виявлення суперечних особливостей об'єкта, спроба порозуміння і, як наслідок, можливе зближення індивідуальних експертних оцінок.

Недосконаліть середньоарифметичного як інтегрального показника, що обчислюється на сукупності індивідуальних оцінок експертів, є достатньо відомим фактом [38]. В якості альтернативи середньоарифметичному частіше за все застосовується медіанне середнє

або спеціальна двоетапна методика обробки сукупності індивідуальних оцінок, за якою спочатку на множині індивідуальних експертних оцінок виявляються і вилучаються з подальшої обробки аномальні дані, що дозволяє на другому етапі застосувати середньоарифметичне для формування інтегральної оцінки групової експертизи.

Подальшим розвитком цієї методології можна вважати так зване зважене середнє. В цьому підході система спеціально обрахованих ваг, в яких зафіксовано рівень довіри до індивідуальних оцінок експертів, дозволяє диференціювати внесок кожної окремої експертної оцінки в сукупну групову (інтегральну). При цьому максимальний внесок припадає на індивідуальні оцінки, отримані від найбільш досвідчених та компетентних експертів, мінімальний – на оцінки, отримані від експертів з найнижчим рівнем компетентності. Якщо певному експерту відповідає нульова чи близька до нульової вага, це фактично означає, що його дані вилучаються з обробки, що і відбувається у випадку, коли індивідуальна експертна оцінка являє собою аномальні дані.

Проблемним аспектом зваженого середнього є об'єктивізація визначення ваг експертів, успішність якої в свою чергу обумовлена ступенем ефективності процедури оцінювання рівнів компетентності експертів. Нижче розглянуто деякі підходи та способи розв'язання цих двох завдань, що важко формалізуються [118-122].

Способи формування групових експертних оцінок

Одним з ключових питань обробки експертних даних є визначення рівня показника компетентності експертів й урахування цього рівня при остаточній обробці висновків експертизи. Особлива вага показника компетентності зумовлена тим фактом, що одностайність висновків експертів з проблеми, яка аналізується, – це ймовірне свідоцтво або тривіальності означеної проблеми, або відсутність можливості вільного висловлення кожним з експертів своєї особистої думки. Принциповою особливістю процедури експертизи є можливість отримання істотно відмінних чи навіть несумісних оцінок за темою експертування, і як наслідок цього – проблема коректного синтезу остаточного експертного висновку, розв'язання якої можливе тільки з урахуванням об'єктивно визначеного рівня компетентності експертів.

Конкретизуємо завдання [119]. Припустимо, що мета експертизи – визначення рівня важливості призначених до експертизи кількох інформаційних продуктів (інформаційних блоків, одиниць, об'єктів тощо), наприклад, трьох: $П_1$, $П_2$, $П_3$. Кожен з них експерти $E_1,\ldots, E_n$ оцінюють у кількісній шкалі *0–L* балів. Важливішому присуджується

більша кількість балів. За результатами групової експертизи кожний з об'єктів експертизи отримує певну суму балів:

$$Q_t = \sum_{i=1}^{n} q_{it}, \tag{3.13}$$

або відповідний середній бал:

$$\overline{q}_t = \frac{1}{n}\sum_{i=1}^{n} q_{it} = \frac{1}{n} Q_t, \tag{3.14}$$

де q_{it} – оцінка, яку дав експерт $E_i, i = \overline{1,n}$ інформаційному продукту $П_t$, $t = \overline{1,3}.$ Якщо до уваги не приймати рівні компетенції експертів, найбільш важливим буде об'єкт експертизи з найбільшою сумою балів Q, або з найвищим середнім балом $\overline{q}.$

Врахування компетентності експертів у подібній ситуації найчастіше реалізується шляхом введення спеціальних вагових коефіцієнтів ω_i, значення яких залежать від рівня компетенції C_i відповідного експерта. Звичайно, на сукупність вагових коефіцієнтів накладається так звана вимога незміщеності:

$$\sum_{i=1}^{n} \omega_i = 1, \tag{3.15}$$

сенс якої полягає в тому, що у разі, коли всі експерти дали об'єкту оцінювання однакову оцінку q, зважений середній бал збігається з цією ж оцінкою:

$$\overline{q}_t = \sum_{i=1}^{n} \omega_i q_{it} = q\sum_{i=1}^{n} \omega_i = q. \tag{3.16}$$

Щоб вага ω_i залежала від C_i й одночасно виконувалася вимога незміщеності (3.15), значення ω_i розраховуються за формулою:

$$\omega_i = \frac{C_i}{\sum_{j=1}^{n} C_j}. \tag{3.17}$$

Зазначимо, що середньозважений бал $\overline{q}_t$ можна знайти за формулою:

$$\overline{q}_t = \frac{\sum_{i=1}^{n} C_i q_{it}}{\sum_{i=1}^{n} C_i} = \frac{1}{\sum_{i=1}^{n} C_i} Q_t^{(k)}, \qquad (3.18)$$

де $Q_t^{(k)}$ – сумарний бал, отриманий t-им об'єктом із врахуванням рівня компетентності $C_i, i = \overline{1,n}$.

Як визначити рівні компетентності? Найбільш просто й оперативно це можна зробити методом взаємо- та самооцінювання експертів (метод взаємо- та самоаналізу), у якому кожен з експертів $E_1, E_2, \ldots, E_n$ визначає рівень компетентності свій та інших експертів у певній кількісній шкалі. Усереднення оцінок рівня компетентності, отриманих кожним з експертів, дає осереднену компетентність кожного з експертів:

$$\overline{Z}_i = \frac{1}{n} \sum_{j=1}^{n} z_i(E_i), i = \overline{1,n}, \qquad (3.19)$$

де $z_i(E_j)$ – оцінка рівня компетентності *i*-го експерта, визначена *j*-м експертом, у разі $i = j$ маємо самооцінку $z_i(E_i)$.

Недоліком цього методу є ймовірне суб'єктивне забарвлення отриманої середньої компетентності, обумовлене, наприклад, приналежністю експертів до протилежних наукових шкіл або напрямків, особиста неприязнь, вікові розбіжності й т.п.

З цього боку більш прийнятним можна вважати так званий документаційний метод оцінки рівня компетентності, який базується на можливому зв'язку компетентності експерта з такими його особистими документованими даними, як число публікацій за тематикою експертизи, кількість посилань на його публікації, галузь спеціалізації експерта, рівень його обізнаності з станом справ у галузі експертування, досвід практичної роботи у цій галузі у ранзі виконавця, керівника та інші дані, що об'єктивно характеризують особистість експерта. Вважається, що наведені вище фактори (визначимо їх ідентифікаторами $f_1, f_2, \ldots$) впливають на формування рівня компетентності C_i експерта E_i, і це може бути відображено певною лінійною формою:

$$C = a_1 x_1 + a_2 x_2 + ... + a_k x_k , \qquad (3.20)$$

де коефіцієнти впливу a_k фіксують рівень впливу факторів $f_1 = x_1$, $f_2 = x_2,...,$ або залежних від цих факторів змінних $x_l = \varphi_l(f_1, f_2,...)$, $..., x_k = \varphi_k(f_1, f_2,...)$ на рівень компетенції експерта.

На жаль, у цій ситуації знову ж таки вельми вагомим є суб'єктивний фактор, що на цей раз наявний при виборі значень коефіцієнтів впливу a_j, $j = \overline{1,k},$ причому ступінь суб'єктивізму у даному випадку ще вищий, ніж у першому випадку.

Можливе позитивне вирішення проблеми визначення рівнів компетентності експертів полягає у суміщенні обох наведених вище методів шляхом побудови моделі компетентності експертів, яка пов'язує оцінки усередненої компетентності $\overline{Z}_i$ з об'єктивними документованими даними про експертів. При цьому вважаємо, що

$$\overline{Z} = C + \xi , \qquad (3.21)$$

де ξ – суб'єктивна похибка в оцінці рівня компетентності експерта.

Після підстановки

$$C = \overline{Z} - \xi \qquad (3.22)$$

у рівняння останнє набуває форми лінійної регресії:

$$\overline{Z} = a_1 x_1 + a_2 x_2 + ... + a_k x_k + \xi , \qquad (3.23)$$

єдиною відмінністю якої від раніше розглянутих є гетероскедастичність залежної змінної $\overline{Z}$, тобто несталість її дисперсії оцінок $D\{\overline{Z}\}$. У цьому легко пересвідчитись, підрахувавши дисперсії оцінок Z_i, $i = \overline{1,n},$ отриманих кожним з експертів:

$$D\{\overline{Z}_i\} = \sigma_z^{\,2} \approx \frac{1}{n-1} \sum_{j=1}^{n} [Z(E_j) - \overline{Z}]^2 , \qquad (3.24)$$

які можуть мати вельми суттєві розбіжності.

Відповідні дисперсії середніх будуть у n разів менші, однак відносний рівень розбіжності їх значень залишиться без змін. Вектор регресійних коефіцієнтів у цьому випадку оцінюється за формулою:

$$\widetilde{A} = (X^T W X)^{-1} X^T W Z, \tag{3.25}$$

де W – вагова матриця, $W = D^{-1}$,

$$D = \begin{vmatrix} D\{\overline{Z}_1\} & 0 & ... & 0 \\ 0 & D\{\overline{Z}_2\} & ... & 0 \\ ... & ... & ... & ... \\ 0 & 0 & ... & D\{\overline{Z}_n\} \end{vmatrix}. \tag{3.26}$$

Дещо іншим способом розрахунку вектору $\widetilde{A}$ є перехід до так званої зваженої регресії:

$$V = a_1 u_1 + a_2 u_2 + ... + a_k u_k + v, \tag{3.27}$$

коефіцієнти якої обчислюються звичайним методом найменших квадратів з перевизначеної системи зважених рівнянь:

$$\begin{cases} \dfrac{\overline{Z}_1}{\sqrt{D\{\overline{Z}_1\}}} = a_1 \dfrac{x_{11}}{\sqrt{D\{\overline{Z}_1\}}} + ... + a_k \dfrac{x_{1k}}{\sqrt{D\{\overline{Z}_1\}}} + \dfrac{\xi_1}{\sqrt{D\{\overline{Z}_1\}}} \\ \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \\ \dfrac{\overline{Z}}{\sqrt{D\{\overline{Z}_n\}}} = a_1 \dfrac{x_{n1}}{\sqrt{D\{\overline{Z}_n\}}} + ... + a_k \dfrac{x_{nk}}{\sqrt{D\{\overline{Z}_n\}}} + \dfrac{\xi_n}{\sqrt{D\{\overline{Z}_n\}}} \end{cases}, \tag{3.28}$$

Приймаючи до уваги, що $\sqrt{D\{\overline{z}_i\}} = \sqrt{\dfrac{1}{n} D\{z_i\}} = \dfrac{1}{\sqrt{n}} \sigma_{Z_i}$, й множник $\dfrac{1}{n}$ можна винести з-під радикалу в знаменниках системи (3.28) й скорочено, процедуру зважування вихідних даних у векторно-матричній формі можна подати співвідношеннями:

$$V = T^{-1} \overline{Z} = \begin{vmatrix} \overline{Z}_1 / \sigma_{Z_1} \\ ... \\ \overline{Z}_n / \sigma_{Z_n} \end{vmatrix}, \tag{3.29}$$

$$U = T^{-1}X = \begin{vmatrix} x_{11}/\sigma_{Z_1} & \dots & x_{1k}/\sigma_{Z_1} \\ \dots & \dots & \dots \\ x_{n1}/\sigma_{Zn} & \dots & x_{nk}/\sigma_{Z_n} \end{vmatrix}, \qquad (3.30)$$

де $TT^T = nD,$

$$T = T^T = \begin{vmatrix} \sigma_{Z_1} & 0\dots & 0 \\ 0 & \sigma_{Z_2}\dots & 0 \\ 0 & 0\dots & \sigma_{Z_n} \end{vmatrix}, \qquad (3.31)$$

$$T^{-1} = \begin{vmatrix} 1/\sigma_{Z_1} & 0 & \dots & 0 \\ 0 & 1/\sigma_{Z_2} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1/\sigma_{Z_n} \end{vmatrix}. \qquad (3.32)$$

Після зважування елементи вектора $V^T = [v_1, v_2, \dots, v_n]$ будуть мати однакову дисперсію, тобто це буде гомоскедастична змінна й коефіцієнти регресії (3.27) визначаться як традиційні оцінки методу найменших квадратів:

$$\tilde{A} = (U^T U)^{-1} U^T V. \qquad (3.33)$$

Коли буде знайдено модель (3.20) залежності рівня компетентності експертів від їх особових документованих даних, можна буде, підставивши до неї відповідні набори значень регресорів $X_i = [x_{i1}, x_{i2}, \dots x_{ik}]$, знайти оцінки компетентності $\tilde{C}_i = X_i \tilde{A}$ експертів E_i, $i = \overline{1,n}$ й далі, використавши формули (3.16)-(3.18), обчислити результати експертизи, тобто q_t або $Q_t^{(k)}$, $t = \overline{1,3,}$ й визначити важливості кожного з об'єктів експертизи.

Оцінювання якості роботи експертів за даними багатооб'єктної експертизи

Серед множини експертних технологій, що залучаються для вирішення різноманітних завдань, можна виділити досить розповсюджений вид колективної експертизи, яка називається багатооб'єктною експертизою (БОЕ). У БОЕ бере участь група з N експертів, кожен з яких здійснює індивідуальну експертизу M об'єктів, які складають сукупність, що експертується. Отримані в ході індивідуальних експертиз підмножини з M експертних оцінок зводяться в загальну матрицю даних, що підлягають наступній спільній обробці:

$$Z = [z_{ij}] = \begin{bmatrix} z_{11} & z_{12} & \dots & z_{1N} \\ z_{21} & z_{22} & \dots & z_{2N} \\ \dots & \dots & \dots & \dots \\ z_{M1} & z_{M2} & \dots & z_{MN} \end{bmatrix} = [Z_1, Z_2, \dots, Z_N]. \qquad (3.34)$$

Особливістю БОЕ є достатньо великі обсяги M об'єктів, що підлягають експертизі, у якості яких можуть виступати зразки певних типів продукції, виробів, інформаційні продукти (зокрема, програмне забезпечення), художні або літературні твори, списки питань (опитувальники) у соціологічних або психологічних дослідженнях, прислані на конкурс проекти і т.п. Зокрема, робота постійно діючих груп (комісій) експертів, що діють у певній фаховій сфері, реалізуючи експертизу більш-менш усталеного класу (чи класів) інформаційних продуктів, є типовим зразком БОЕ. Отримані в цьому випадку відносно великі об'єми індивідуальних експертних оцінок серед іншого містять певну інформацію про особисті якості експертів, зокрема, про рівні їхньої компетентності, знання яких досить актуальні для організації ефективної обробки результатів експертизи. Звичайно, для оцінювання рівнів компетентності експертів виконується ряд спеціальних додаткових заходів організаційно-аналітичного характеру [119, 123, 124], частково вже розглянутих вище (метод само- та взаємоаналізу, документаційний, інші), результати яких мають або досить суб'єктивний характер, або потребують виконання достатньо значного обсягу додаткових обчислень. Тому перспектива оцінювання компетентності експерта безпосередньо за результатами виконаної ним експертизи, з урахуванням у тому числі і стану експерта на момент проведення експертизи, є досить привабливою.

Результати індивідуальної експертизи, здійсненої *j*-м експертом, являють собою випадкову послідовність $Z_j = [z_{1j}, z_{2j}, ..., z_{Mj}]^T$, кожен елемент якої містить інформативну складову x_{i0}, спільну для всіх експертних оцінок z_{ij} і випадкову похибку e_{ij}, характеристики якої індивідуальні у кожного конкретного експерта:

$$z_{ij} = x_{i0} + e_{ij},\ i = \overline{1, M},\ j = \overline{1, N}. \qquad (3.35)$$

Поставивши у відповідність елементам послідовності Z_j цілочислові моменти часу $t_i = 1,2,...,M$, отримаємо певний аналог часового ряду $\{z_{ij}\}$, у загальному випадку нестаціонарного. Однак якщо припустити, що характеристики експерта як деякої інформаційно-аналітичної оцінюючої системи залишаються незмінними впродовж процедури експертування, а всі похибки, помилки та неточності в експертних оцінках визначаються винятково властивостями і станом експерта на момент проведення експертизи, то справедливим уявляється припущення щодо стаціонарності та ергодичності випадкових послідовностей $E_j = \{e_{1j}, e_{2j}, ..., e_{Mj}\}$, $j = \overline{1, N}$. В останньому випадку для більших значень *M* виявляється можливим оцінювання емпіричних моментних характеристик і емпіричних функцій розподілу відповідних похибок E_j, й наступне зіставлення цих оцінок, знайдених для різних експертів [120-122]. Можна припустити, що результати порівняльного аналізу будуть містити певну інформацію про рівні компетентності експертів. Актуальною є проблема виділення цієї інформації та її представлення у вигляді сталих показників компетентності, що легко інтерпретуються. Спроба часткового вирішення цієї проблеми розглянута в [116, 117], де за даними порівняльного аналізу експертних оцінок виявлялися так звані «аномальні» експерти. Оцінки, отримані від «аномальних» експертів, істотно відрізняються від оцінок, отриманих від інших експертів. Зокрема, це стосується форми розподілу похибок оцінок експертизи і відповідних моментних характеристик. У цілому характер рішень, представлених в [116, 117], ближче до методів класифікації й не містить прямих підходів до оцінювання компетентності експертів.

Матеріали, більш адекватні змісту задач, що розглядаються в рамках сформульованої вище проблеми, представлені в [117]. Однак запропонований у них рівень опису й формалізації задач не дозволив отримати достатньо загального методу рішення, інваріантного до варіації умов початкової постановки проблеми.

За аналогією з відомими положеннями кластерного аналізу [116, 117] введемо поняття образу експерта як деякої точки $Z_j = [z_{1j}, z_{2j}, ..., z_{Mj}]^T$, $j = \overline{1, N}$ у *M*-вимірному просторі результатів БОЕ. При повному збігові думок експертів їхні образи однакові, тобто всі результати експертизи будуть представлені єдиною точкою в просторі результатів БОЕ. Наявність помилок експертів приводить до розщеплення точки в хмару (кластер), щільність якої (якого) неоднорідна і зазвичай максимальна в області, що прилягає до центру кластера з координатами $Z_0 = [z_{10}, z_{20}, ..., z_{M0}]^T$, визначеними співвідношенням [116, 117]:

$$Z_0 = \underset{Z_j, Z_0 \in R^M}{\operatorname{argmin}} \sum_{j=1}^{N} r_j(Z_j, Z_0), \tag{3.36}$$

де $r_j(Z_j, Z_0)$ – відстань між образом *j*-ого експерта і центром Z_0 кластера в *M*-вимірному просторі R^M результатів БОЕ. При використанні для знаходження $r_j(Z_j, Z_0)$ евклідової метрики:

$$r_j = r_j(Z_j, Z_0) = [\sum_{i=1}^{M} (z_{ij} - z_{i0})^2]^{\frac{1}{2}}, \ j = \overline{1, N}, \tag{3.37}$$

мінімізація співвідношення (3.36) досягається при:

$$z_{i0} = \frac{1}{N} \sum_{j=1}^{N} z_{ij} \ . \tag{3.38}$$

Наявність аномальних даних у рядках матриці *Z* спричиняє зміщення оцінок (3.38), у зв'язку із чим більш надійний результат (при ймовірній наявності «аномальних» експертів) дає застосування робасних медіанних оцінок виду:

$$z_{i0} = med(Z_i) = med(z_{i1}, z_{i2}, ..., z_{iN}) . \tag{3.39}$$

При відсутності аномальних експертів справедливе припущення про рівність нулю математичних очікувань помилок експертизи: $\mu\{E_j\} = 0$, $j = \overline{1, N}$, що приводить до виконання рівності $\mu\{Z_0\} = X_0 = [x_{10}, x_{20}, ..., x_{M0}]^T$ і дозволяє обґрунтувати гіпотезу незміщеності середньогрупових експертних оцінок:

$$\mu\{\overline{Z}_i\} = \mu\{\frac{1}{N} \sum_{j=1}^{N} Z_{ij}\} = \frac{1}{N} \mu\{\sum_{j=1}^{N} x_{i0} + e_{ij})\} = \frac{1}{N} (N x_{i0}) = x_{i0} \ . \tag{3.40}$$

Метризація віддаленості образів експертів від центра Z_0 дозволяє представити в інтегрованій формі інформацію про помилки кожного з експертів і допускає можливість існування шкального перетворення $c_j = f(r_j)$, що забезпечує взаємооднозначне відображення елементів множини R ($r_j \in R$, $j = \overline{1,N}$) у відповідні оцінки компетентності експертів $f : R \to C$; $c_j \in C$.

Вибір структури й параметрів відображення f представляє нетривіальну задачу, що вимагає окремого розгляду.

При формуванні вимог до шкального перетворення $c = f(r)$ будемо виходити з наступних міркувань. По-перше, очевидно, що із ростом компетентності *C* значення *r* зменшуються, тобто похідна $dc/dr < 0$. Із цього виходить також твердження про монотонний характер залежності $c = f(r)$. По-друге, при побудові шкали виміру компетентності *C*, множину можливих значень *r*, визначену на напіввідкритому інтервалі $R = [0,\infty)$, зручно відображати в замкнутий інтервал *C* = [1,0], що відповідає типовій шкалі компетентності. При цьому значенням $r \to \infty$ відповідає права гранична відмітка *c* = 0 шкали компетентності, а значенню *r* = 0 – ліва, *c* = 1. Для малих значень оцінок *r*, враховуючи, що величина похибки оцінювання в цьому випадку може бути зіставимою або навіть істотно перевищувати невідоме істинне значення відстані *r*, з метою зменшення впливу похибки на точність значень компетентності *C*, доцільно ввести умову:

$$dc/dr \approx 0. \qquad (3.41)$$

При цьому для області малих значень *r* буде справедливе співвідношення $f(r) = c \approx 1$. Умову, аналогічну (3.41), варто ввести і для області великих значень r, яка прилягає до правого кінця інтервалу $R = [0,\infty]$. Тоді точки цієї досить протяжної області великих значень *r* (що відповідають суттєво віддаленим образам малокомпетентних експертів від центра Z_0) будуть відображатися в значеннях компетентності *C*, рівні або близькі 0. У підсумку, якщо припустити, що значення похідної dc/dr максимальні (за модулем) у центральній частині шкали й зменшуються, прагнучи до 0, з наближенням до периферії шкали, справедливе співвідношення:

$$dc/dr = -c(b_0 - b_1 c),\ b_0, b_1 > 0,\ b_0 \geq b_1. \qquad (3.42)$$

Квадратичний зсув b_1c^2 у правій частині (3.42) дозволяє реалізувати виконання умови (3.41) в області великих значень *r*. У цілому співвідношення (3.42) являє собою диференціальне рівняння з відокремлюваними змінними, яке розв'язавши матимемо:

$$\ln \frac{c}{b_0 - b_1 c} = -b_0 r + \ln A, \qquad (3.43)$$

де *A* – постійна інтегрування. З урахуванням граничної умови $c(0) = 1$, після потенціювання і ряду перетворень, вводячи сталу $B = b_1 / b_0$, отримаємо:

$$c = f(r) = \frac{1}{(1 - \frac{b_1}{b_0})e^{b_o r} + \frac{b_1}{b_0}} = \frac{1}{(1 - B)e^{b_o r} + B}. \qquad (3.45)$$

Графік залежності *c*(*r*), наведений на рис. 18, за своїм характером – «перевернута» логістична крива.

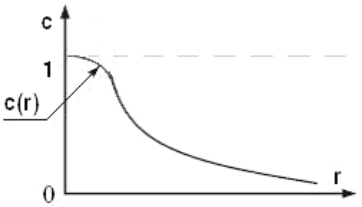


Рис. 18. Графік залежності *c*(*r*)

Отримані вище результати, на жаль, носять суто прикладний характер. Розраховані за формулою (3.37) оцінки *r* дозволяють зіставляти рівні помилок експертів тільки в рамках конкретної задачі через те, що ці оцінки залежать від числа об'єктів експертизи *M* та кількісних характеристик прийнятої шкали оцінок *r*. Отримана на базі достатньо загальних і об'єктивних передумов структура шкального перетворення $c = f(r)$ для своєї конкретизації й прикладного застосування вимагає завдання кількісних значень параметрів b_0, *B*, що стає можливим лише при визначенні конкретного типу експертизи.

Тому далі трохи звузимо клас досліджуваних процедур експертизи для одержання можливості більш деталізованого врахування особливостей і характеру БОЕ, що проводяться. Розглянемо досить розповсюджену на практиці процедуру БОЕ, у якій використовується бальне оцінювання.

Якщо процедура БОЕ полягає в оцінюванні кожного з об'єктів експертизи в бальній шкалі 0,1,2,..., $l_{\max}$, тобто $z_{ij} \in \{0,1,...,l_{\max}\} = L$, то теоретично можливими мінімальними й максимальними значеннями *r* будуть $r_{\min} = 0$ і $r_{\max} = l_{\max}\sqrt{M}$. Вводячи у вираз (3.37) нормуючі множники $1/l_{\max}$ та $1/\sqrt{M}$, отримаємо формулу для обчислення нормованої відстані образу *j*-ого експерта від центру кластера Z_0:

$$r_{нj} = r_j /(l_{\max}\sqrt{M}). \qquad (3.46)$$

Нормована відстань не залежить від числа *M* об'єктів, що підлягають експертизі, і кількості відліків бальної шкали, тобто від $l_{\max}$, будучи індивідуалізованою оцінкою експерта, що враховує тільки величину і характеристики розподілу помилок експерта. Досвід практичної роботи з даними БОЕ свідчить, що значення $r_н \le 0{,}2$ характерні для експертів досить високої кваліфікації, значення $r_н \ge 0{,}3 \div 0{,}35$ свідчать про присутність аномальних даних в оцінках експерта, область значень $0{,}2 < r_н < 0{,}3 \div 0{,}35$ відповідає образам експертів, що мають відносно невисокий рівень професійної підготовки, нерівно проводять експертизу і допускають у своїх оцінках помилки досить значної величини. Типовий розподіл сукупності значень $r_н$ для групи експертів представлений на рис. 19.

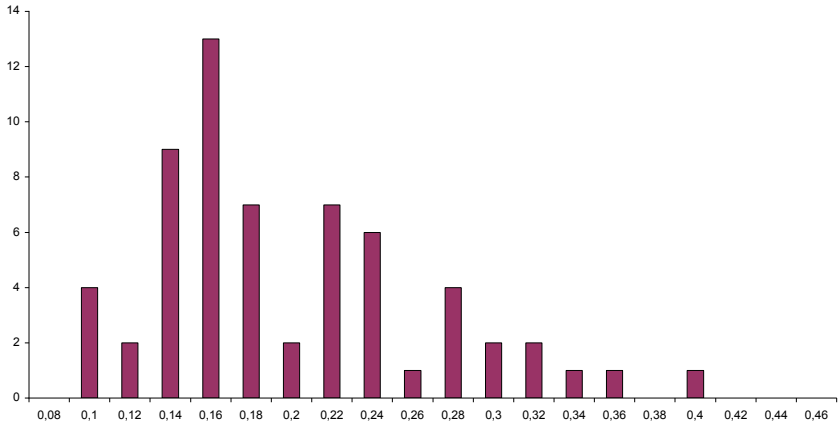


Рис. 19. Типовий розподіл сукупності значень $r_н$ для групи експертів

Зокрема, подібну характеристику шкальному перетворенню забезпечують наступні значення параметрів: b_0=15, B=0,967 (рис. 20). У цьому випадку безпосереднє виявлення й виключення з обробки даних «аномальних» експертів відсутнє, однак при здійсненні обробки із введенням ваг, пропорційних компетентності експертів, фактично обнуляються дані, отримані від експертів, для яких $r_н$ >0,4.

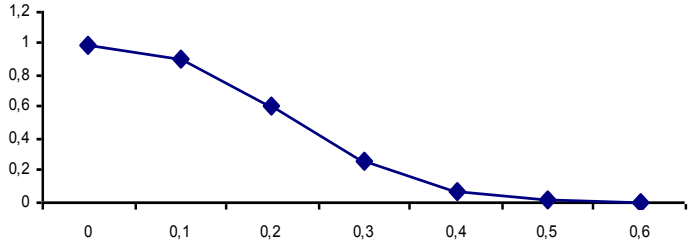


Рис. 20. Графік характеристики шкального перетворення (3.47) з параметрами: b_0=15, B=0,967

Очевидно, завдання параметрів шкального перетворення містить істотний суб'єктивний момент і визначається цілями перетворення, особливостями прийнятої моделі розподілу похибок оцінок експертизи, застосовуваним способом кількісного оцінювання рівня компетентності (бальна шкала, шкала з однобічним обмеженням, шкала із двостороннім обмеженням і т.п.).

Теза про те, що величина і характер помилок, які допускаються експертом у ході експертизи, визначаються винятково рівнем його компетентності, робить правомірним припущення, відповідно до якого оцінка компетентності j-ого експерта може бути знайдена безпосередньо з відомостей про характеристики його помилок, зокрема, з вибіркових моментних характеристик послідовності $E_j = \{e_{1j}, e_{2j}, ..., e_{Mj}\}$. Розрахунки, виконані для реальних даних, показали обґрунтованість даного припущення. Оцінки компетентності, знайдені для сукупності експертів шляхом перерахування оцінок $r_{нj}$ за формулою:

$$c = f(r_н) = (0{,}033e^{15r_н} + 0{,}967)^{-1}, \qquad (3.47)$$

одержаної із загального співвідношення (3.42) після підстановки в нього параметрів b_0=15, B=0,967, практично збігаються з оцінками компетентності для цих же експертів, обчисленими за апроксимативною моделлю виду:

$$c(x_1, x_2, x_3) = 1 - 11{,}6x_3 + 50x_1x_3 + 40x_2^2, \qquad (3.48)$$

або

$$c(x_1, x_2, x_3) = 1 - 0{,}01x_2x_4 - 0{,}81x_1^{-2} - 0{,}056x_1, \qquad (3.49)$$

де x_1, x_2, x_3 – відповідно вибіркові оцінки моментних характеристик послідовності E_j: середнього $\bar{e}$, дисперсії σ^2, ентропії H та другого початкового моменту ν_2, розраховані за даними експертизи, виконаної кожним експертом.

Вираз (3.48) дає можливість кількісно оцінити рівні компетентності кожного з експертів, що брали участь у БОЕ, не вдаючись до попереднього обчислення нормованої відстані $r_н$. Для цього по відповідному *j*-му експерту вектору оцінок погрішностей експертизи $E_j, j = \overline{1, N}$ спочатку обчислюються вибіркові значення моментних характеристик $\bar{e}$, σ^2, H, ν_2 (змінних x_1, x_2, x_3, x_4), після чого за формулою (3.48) розраховуються відповідні рівні компетентності. Розрахунок елементів вектора E_j проводиться за формулою:

$$e_{ij} = (z_{ij} - med_i)/l_{\max}, \qquad (3.50)$$

де med_i – медіана *i*-того рядка матриці *Z* (формула (3.34)).

Модель (3.48) – звичайна лінійна (по параметрах) регресія, побудована за даними, отриманими у ході обробки результатів експертизи (матриця *Z*, формула (3.34)).

Методика побудови цієї моделі наступна: моментні характеристики похибок в оцінках експертів утворюють матрицю $X = [X_1, X_2, X_3, X_4]$ незалежних змінних,

$$X_t = [x_{t1}, x_{t2}, ..., x_{tN}]^T, \ t=1,2,3, \qquad (3.51)$$

де $[.]^T$ – символ транспонування.

Зокрема, моментні характеристики $x_{1j}, x_{2j}, x_{3j}, x_{4j}$ *j*-ого експерта утворюють *j*-ий рядок матриці *X*. Розраховані за тими ж вихідним даним (матриця *Z*) за допомогою формул (3.37), (3.47) значення компетентностей c_j, $j = \overline{1, N}$ утворюють вектор *C* значень залежної змінної. На базі сформованої у такий спосіб розширеної матриці даних $[C, X_1, X_2, X_3, X_4]$, застосовуючи методи та прийоми регресійного

аналізу (зокрема, крокову регресію для підбору структури регресії і метод найменших квадратів для обчислення регресійних коефіцієнтів), будується моделі виду (3.48), (3.49).

У табл. 8 наведений фрагмент матриці вихідних даних, а також значення нормованої відстані $r_{нj}$ та модельні значення компетентностей $C(x_{1j}, x_{2j}, x_{3j})$, знайдені за формулою (3.48).

Таблиця 8

Фрагмент матриці вихідних даних

№	$r_{нj}$	$c_j = f(r_{нj})$	$c(x_{1j}, x_{2j}, x_{3j})$	x_{1j}	x_{2j}	x_{3j}
1	0,402	0,07	0,05	-0,296	0,0741	0,1616
2	0,300	0,25	0,24	-0,197	0,0510	0,0899
3	0,291	0,28	0,27	-0,137	0,0657	0,0845
4	0,256	0,40	0,41	-0,049	0,0633	0,0656
5	0,246	0,44	0,45	0,217	0,0136	0,0605
6	0,206	0,59	0,57	0,166	0,0152	0,0426
7	0,184	0,67	0,65	-0,032	0,0330	0,0340
8	0,137	0,81	0,80	0,031	0,0177	0,0186
9	0,110	0,88	0,87	-0,009	0,0120	0,0121
10	0,097	0,90	0,90	0,008	0,0093	0,0093

Ймовірність суттєвих суб'єктивних помилок в індивідуальних (персональних) експертних оцінках вимагає в разі використання цих оцінок для прийняття важливих рішень спиратися на результати групових (колективних) експертиз, що, в свою чергу, обумовлює необхідність розроблення спеціальних методик обробки даних групових експертиз. Переважна більшість цих методик базується на використанні додаткової інформації про індивідуальні рівні компетентності експертів, задіяних у експертизах, в зв'язку з чим виникає потреба в проведенні допоміжних організаційних заходів для отримання даних щодо рівнів компетентності експертів.

Однак у випадку так званої багатооб'єктної експертизи, вимогам якої відповідають форми роботи експертних комісій, що створюються при державних експертах з питань таємниць, необхідні відомості щодо компетентностей експертів стає можливим отримати безпосередньо з даних групової експертизи. Це суттєво спрощує і прискорює проведення організаційних процедур групової експертизи.

Розділ 4. ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ СИСТЕМИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ В УКРАЇНІ

Задача оцінювання ефективності СОДТ має кілька аспектів. Перш за все це методичний аспект, пов'язаний з відсутністю єдиної базової методики оцінювання ефективності СОДТ. Залежно від того, що розуміємо під об'єктом, де циркулює СІ, можливе застосування різних підходів до визначення ефективності відповідної СОДТ, створеної на цьому об'єкті.

Так, для оцінювання ступеня ефективності СОДТ окремого підрозділу, підприємства, установи, адекватним є підхід, що базується на співставленні переліку загроз СІ, що циркулює на цьому локальному об'єкті, із комплексом заходів та засобів, які застосовано для нейтралізації визначених загроз. Надійність функціонування цього комплексу, який власне і реалізує СОДТ на окремому об'єкті, рівень нейтралізації сукупності загроз та, можливо, вартість СОДТ визначають ефективність ОДТ. Фактично цей підхід орієнтовано на оцінювання ефективності СОДТ на окремих об'єктах, тобто елементів нижнього рівня національної СОДТ.

Якщо досліджується СОДТ країни в цілому, наведений вище підхід до оцінювання ефективності СОДТ не спрацьовує через невідповідність деталізації загроз меті дослідження – оцінюванню ефективності національної СОДТ. Перелік загроз для цього випадку буде занадто довгим, можливість дослідити або хоча б відстежити вплив кожної окремої загрози на стан ОДТ в країні – завданням вкрай проблематичним. В зв'язку з цим слід використати інший підхід, що базується не на поелементному дослідженні нейтралізації кожної окремої загрози з сукупності загроз, а на побудові моделі ефективності функціонування національної СОДТ, яка пов'язує ступінь ефективності з певним нечисленним набором діагностичних показників. Останні є опосередковано залежними від комплексу захисних функцій, притаманних національній СОДТ, припускають ту чи іншу змістовну інтерпретацію і можуть бути кількісно обраховані через певні об'єктивні дані, що характеризують функціонування національної СОДТ (наприклад, становлять результати моніторингу стану СОДТ).

Припустимо існування деякого «перехідного» ступеня узагальнення (централізації) інформаційної діяльності, на якому можна одночасно застосувати обидва підходи й, склавши розширений перелік загроз СІ, співставити їх із комплексом діагностичних показників. Якщо при цьому застосувати математико-статистичні методи скорочення розмірності набору вхідних даних (факторний, дисперсійний аналіз, інші), реально отримати прозору інтерпретацію властивостей діагностичних показників, встановити їх зв'язок з функціями захисту інформації.

Другим проблемним аспектом оцінювання СОДТ є достатньо поширена думка про неможливість (або недоречність з етичних міркувань) використання грошового виміру для визначення збитків (шкоди), що виникли внаслідок втрати СІ. Ця проблема знімається після ознайомлення із змістом «Рекомендацій…» [38], де наведено критерії та процедуру визначення СС відомостей, що містять ДТ. В цій процедурі використано умовні бальні оцінки (розрахункові або експертні) шкоди, заподіяної повною чи частковою втратою СІ. Зворотна процедура визначення за відомим СС певної інформації й умовно-бальної вартості дозволяє розрахувати можливу шкоду від втрати цієї інформації внаслідок реалізації тієї чи іншої загрози (частково або у повному обсязі). У ряді випадків наведена в [38] допоміжна інформація дозволяє уточнити отримані бальні оцінки вартості.

Наявність відомостей про сукупність актуальних для конкретного об'єкту загроз в купі із співставленою цим загрозам інформацією про можливу шкоду від їх реалізації роблять очевидним застосування першого з означених вище підходів до оцінювання ефективності СОДТ.

Слід зазначити, що практичне застосування даного підходу пов'язане з необхідністю складання повного переліку загроз, специфічних для кожного конкретного об'єкту інформаційної діяльності (ОІД). Це само по собі є достатньо складною задачею, яка становить ще один важливий аспект оцінювання ефективності СОДТ. Особливої гостроти цей аспект набуває в умовах комп'ютеризації та автоматизації робіт з обробки СІ. Полегшити розв'язок задачі аналізу загроз можна шляхом розробки спеціальних базових переліків загроз для певних типових ситуацій.

В даній роботі зроблено спробу формування типової методики для практичної реалізації першого підходу.

Застосування другого підходу, орієнтованого на ОІД із широким спектром функціональних задач, принципово не може бути зведено до типової процедури і в кожному випадку потребує проведення спеціальної наукової розробки.

Однак, виходячи із існуючої структуризації СІ, зокрема її розподілу за окремими сферами (оборони, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку) [3], з перспективою подальшої деталізації в межах кожної із сфер і отриманням багаторівневої ієрархічної структури, видається можливим адаптувати запропоновану методику для оцінювання ефективності СОДТ більш високих рівнів за результатами оцінювання стану захисту СІ на нижчих рівнях, наприклад, ефективності иаціональної СОДТ через захищеність СІ в окремих сферах. Це реалізується шляхом введення спеціальних коефіцієнтів захищеності СІ в цих сферах.

4.1. Загрози інформації, обумовлені використанням засобів обчислювальної техніки для обробки секретної інформації

Дедалі зростаюче використання сучасної обчислювальної та комунікаційної техніки в найрізноманітніших галузях людської діяльності створило умови для практично необмеженого використання в усіх сферах життя суспільства інформаційних технологій і спричинило виникнення феномену, що отримав назву інформатизація [125].

Глобальний характер інформатизації, стрімкі темпи її розвитку обумовлені суто об'єктивними причинами: ефективність вирішення задач виробничої, господарської, фінансово-економічної, політичної і будь-якої іншої сфери суспільної діяльності напряму пов'язана з обсягами інформації, застосованої на етапах аналізу й, відповідно, розв'язання цих задач.

В свою чергу, результативність та якість аналізу і обробки зростаючих обсягів інформації можливі лише за умов застосування сучасних ІТС, що саме й пояснює об'єктивність та невідворотність розвитку процесу інформатизації.

На жаль, неупереджене ставлення до інформатизації черговий раз підтверджує давно відому особливість соціально-технічного прогресу: розв'язок одних проблем породжує нові, іноді ще навіть складніші за попередні. Зокрема це стосується проблеми безпеки інформації, яка надзвичайно загострилась у процесі бурхливого розвитку і становлення нових інформаційних технологій. Як не дивно, особливої ваги ця проблема набула для структур, в котрих вона існувала і до їх інформатизації. Справа в тому, що до впровадження сучасних ІТС в державних органах, на підприємствах, установах і організаціях (далі – організаціях), для яких безпека інформації становила певне значення, існував усталений порядок роботи з інформацією (наприклад, з секретними документами), який визначав структуру інформаційних потоків в межах організації, обмін інформацією із зовнішнім середовищем, тобто цей порядок визначав правила керування цими інформаційними потоками, та правила доступу до інформації, що транспортувалася ними, включно із заходами з контролю доступу.

З комп'ютеризацією процесів обробки інформації, зокрема секретної, змінюється вихідна схема інформаційних потоків та можливих доступів до інформації. Це пояснюється тим, що будь-яка інформація після введення її до автоматизованої системи (АС) набуває специфічного представлення: чи то у вигляді послідовності електричних сигналів, що циркулюють між блоками та компонентами АС, чи то у вигляді певної статичної форми, якій відповідає сукупність фіксованих у

часі станів електронних елементів АС (зокрема, елементів пам'яті). Ці електронні форми представлення інформації, динамічні або статичні, фактично являють собою віртуальні документи, що циркулюють в АС і можуть бути виведені з нього за допомогою програмних чи апаратних засобів у вигляді, придатному для безпосереднього сприйняття людиною або на певному фізичному носії для наступного зберігання та транспортування цієї інформації. При цьому слушно зауважити, що зазначене виведення інформації може бути результатом застосування як штатних можливостей програмного забезпечення (ПЗ) (тобто ці можливості передбачені специфікацією програмних продуктів, що використовуються у АС), так і наслідком певного несанкціонованого втручання у програмні коди, через що стає можливою поява нових не задекларованих можливостей модифікованого ПЗ, які відомі тільки особі, що реалізувала втручання.

Для ілюстрації викладеного розглянемо роботу інформаційно-аналітичної системи (ІАС), яка реалізує певні операції з обробки СІ у випадку застосування «паперових» та «без паперових» технологій [125].

Інформаційну модель, що відображає процеси обміну та утворення вторинної інформації I_2 під час роботи такої ІАС, зокрема процеси підготовки і виконання вторинного документу $Д_2$, розробка якого ініційована отриманням секретного первинного документу $Д_1$, зображено на рис. 21.

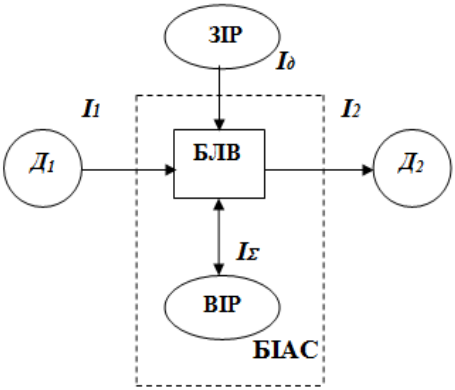


Рис. 21. Інформаційна модель процесів обміну і утворення вторинної інформації за «паперової» технології обробки інформації

За цією моделлю вихідна інформація ІАС – це інформація I_2, що у документованому вигляді являє собою документ $Д_2$. Вторинний документ $Д_2$ є результатом сукупної аналітико-синтетичної переробки вхідної інформації I_1, що міститься у документі $Д_1$, та залученої додаткової інформації $I_Д$, отриманої від зовнішнього ІР (ЗІР). Остання може мати процедурний чи декларативний характер [126], залежно від конкретних задач, що виникають у процесі відпрацювання документу $Д_2$.

У разі «паперової» (або ручної) технології аналітико-синтетичної переробки інформації функції ІАС виконує фахівець, що має необхідний рівень знань та досвіду для формування вторинного документу $Д_2$, тобто, додержуючись прийнятої термінології, це біологічна ІАС (БІАС). В БІАС виділимо блок логічного виводу (БЛВ), яким відобразимо функцію інтелектуальної діяльності фахівця у процесі обробки інформації, та внутрішній інтелектуальний ресурс (ВІР) – знання фахівця, зокрема, накопичені в його пам'ять різні відомості, факти, дані й т.д., що у сукупності дозволяє йому успішно працювати, розв'язуючи різноманітні завдання у відповідній предметній сфері. Ці знання, на відміну від інформації I_1, I_2, $I_Д$, мають недокументований характер, непідконтрольні будь-кому із зовнішнього оточення фахівця. Більш того, певна частина цих знань (так звані знання другого роду [127]) уособлюють інтуїтивні емпіричні уявлення фахівця в предметній сфері, які навіть він сам достеменно не усвідомлює, не в змозі висловити їх у формалізованому вигляді, опублікувати, оприлюднити в формі, прийнятній для загального сприйняття. Проте саме ці знання дозволяють фахівцеві прийняти рішення в умовах невизначеності, недостатньої чи суперечливої інформації, забезпечуючи ефективну роботу БЛВ.

Інформаційний потік між БЛВ та ВІР має двосторонній характер, в напрямі від БЛВ до ВІР передається весь обсяг інформації, що аналізувався в БЛВ, тобто $I_1 \cup I_Д$, та інформація, синтезована за результатами цього аналізу, тобто I_2. Таким чином, сукупна інформація I_Σ, що поступає до ВІР, поєднує в собі всі види інформації: I_1, I_2, $I_Д$. Інформаційні потоки містять (I_1), або можуть містити ($I_Д, I_2, I_\Sigma$) СІ, однак можливості контролю за доступом до цієї інформації істотно відмінні для документованої (I_1, I_2) та недокументованої ($I_Д$, I_Σ)

інформації. Остання через фахівця, що полишив межі контрольованої території, як через канал передачі транспортної системи, може бути перенаправлена будь-куди. Ця ситуація віддзеркалює чи не найбільш серйозну потенційну загрозу витоку СІ, тому запобігання та профілактика подібного «переадресування» інформації є головною складовою організаційно-правових заходів із захисту інформації. Ефективним в цьому випадку є наслідування двом фундаментальним організаційним принципам захисту інформації [128-130]:

- розподіл обов'язків (separation of duties), суть якого в цілеспрямованому подрібненні вихідного завдання на окремі фрагменти та розподілі їх між кількома виконавцями, так, щоб жоден з них не мав повної уяви про задачу в цілому;
- мінімізація привілеїв (least privelegies) – виділення кожному виконавцеві мінімального доступу до СІ в обсязі, мінімально необхідному для виконання дорученого.

Додержання цих принципів дає надію на те, що жоден з виконавців не матиме доступу до СІ: в обсязі, достатньому для нанесення серйозної шкоди у випадку витоку цього обсягу інформації.

Розглянемо загрози, що виникають у зв'язку з введенням комп'ютеризації підготовки документа $Д_2$, тобто при включенні до процедури підготовки документа засобів обчислювальної техніки (ЗОТ). Під час обробки інформації в АС до роботи з інформацією залучаються ті чи інші засоби та елементи АС, які далі будемо називати об'єктами O_1, O_2, ... , O_k – елементами процесора, пам'яті, периферії (принтери, дисплеї, сканери тощо). Безпосереднє включення об'єкта O_i до процедури обробки назвемо активацією цього об'єкта, а сам процес обробки представимо схемою на рис. 22.

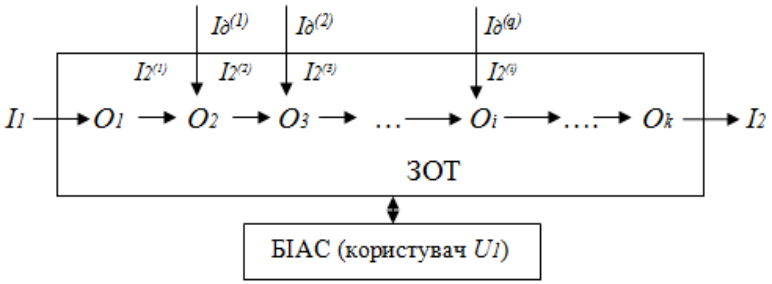


Рис. 22. Інформаційна модель процесів обміну і утворення вторинної інформації при «без паперовій» технології обробки інформації

Відповідно до рис. 22 процедура підготовки документа $Д_2$ є багатостадійною, у ході якої інформація передається від об'єкта до об'єкту із залученням елементів допоміжної інформації $I_Д$, утворюючи певний інформаційний потік, який на виході кінцевого об'єкту O_k містить інформацію I_2. Після завершення роботи з документом $Д_2$ активовані об'єкти O_1, O_2, ... , O_k, багато з яких можуть мати у своєму складі елементи пам'яті, зберігають набутий під час останньої активації стан, який є фіксацією відповідної часткової інформації I_2. Тому звертання до цих об'єктів користувача U_2, що почав працювати в системі після користувача U_1 (фахівця, котрий виконував документ $Д_2$), робить можливим несанкціоноване отримання користувачем U_2 інформації про документ $Д_2$. Назвемо цей випадок «прямим» несанкціонованим доступом (НСД) на відміну від випадку отримання інформації I_2 без безпосереднього входження користувача U_2 до системи. Останнє має місце при використанні для отримання інформації так званих технічних каналів витоку інформації. Прикладом утворення такого каналу можуть бути наслідки впливу електромагнітного випромінювання об'єкту O_i на роботу (стан) елементів чи пристроїв іншої, безпосередньо не задіяної у підготовці документу $Д_2$ системи, розташованої у приміщенні АС. Прикладом такої «іншої» системи можуть слугувати системи зв'язку, електроживлення, в кабельних елементах яких електромагнітне поле, створюване активованим об'єктом O_i, наводить електрорушійні сили (так званий небезпечний сигнал), у разі контролю вимірювання яких можливе повне відновлення відповідної інформації I_2 [131, 132].

В узагальненому випадку ситуацію опосередкованого НСД ілюструє рис. 23 [125], де об'ємною стрілкою схематично зображено вплив фізичних полів або сигналів (S (I_2)), що утворюється у процесі обробки інформації на об'єкті O_i, на певні інформаційні параметри допоміжних технічних засобів і систем (ДТЗС). Фактично маємо модуляцію небезпечним інформаційним сигналом (S (I_2(i))) певного параметра (групи параметрів) ДТЗС, зміни якого у часі описуються функцією (процесом) ϕ(I_2 (i)). Зворотна процедура демодуляції, яка

реалізується системою відновлення інформації (СВІ), дозволяє отримати практично всю вихідну інформацію, тобто $I^*_2{}^{(i)} \approx I_2{}^{(i)}$.

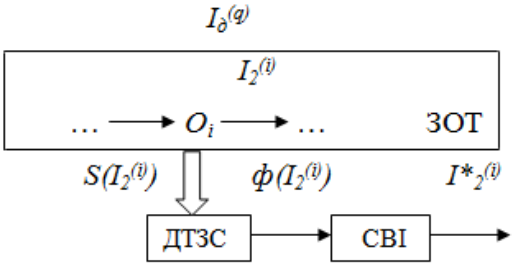


Рис. 23. Утворення технічного каналу витоку інформації через ДТЗС

Наприкінці зазначимо, що можливий прямий НСД без входження до автоматизованої системи обробки даних. Прикладом цього може бути застосування сучасних апаратів мобільного телефонного зв'язку із вбудованими фотокамерами, які здатні робити якісні знімки текстових документів та передавати їх на відстань радіоканалом, тобто ці засоби мобільного зв'язку використовуються у якості технічного засобу розвідки, яким, зокрема, можливе зробити знімок з екрану дисплея варіанту документу $Д_2$ у процесі відпрацювання цього документу [133].

Ще одне джерело загроз, пов'язане з застосуванням ЗОТ, - деструктивні силові впливи, що є результатом якихось природних явищ (наприклад, блискавка) або утворилися внаслідок певних техногенних процесів, ненавмисно (випадкові імпульсні високовольтні завади промислового походження) або навмисно згенерованих (електромагнітний тероризм), які можуть передаватися як через кабельні мережі (силові, зв'язку) так і бездротовим шляхом у формі потужних електромагнітних імпульсів [134, 135]. Таким чином, комп'ютеризація обробки будь-якої ІзОД із застосуванням сучасних ЗОТ призводить до виникнення ряду нових загроз, обумовлених тим, що носіями інформації у цьому випадку є фізичні поля та сигнали, які утворюються у процесі функціонування ЗОТ.

Характеристики цих загроз суттєво залежать від видів та типів ЗОТ, наявних у приміщенні АС ДТЗС, їх просторового розміщення відносно ЗОТ, ступеню взаємної сумісності. Всі ці обставини ускладнюють процедуру визначення переліку реально існуючих загроз, ускладнюють формалізацію цієї процедури, можливості використання шаблонів чи каталогів типових загроз, вимагаючи проведення індивідуального поглибленого аналізу інформаційного середовища та факторів, що впливають на функціонування АС.

Наявність носіїв інформації у недокументованій формі представлення, застосування нових інформаційних технологій, пов'язаних з інтенсивною експлуатацією ЗОТ, призводить до зменшення ефективності застосування традиційних методів контролю документопотоків, що використовувалися для «паперових» технологій й вимагає розробки нової системи правил та рекомендацій із захисту ІзОД, тобто формування нової політики безпеки інформації.

4.2. Системні аспекти захисту інформації

Слід зазначити, що вперше наведені вище проблеми, пов'язані з застосуванням ЗОТ для обробки СІ окреслилися наприкінці 60-х на початку 70-х років двадцятого століття, а особливої актуальності набули в останні десять років через масоване впровадження в різних сферах діяльності сучасних інформаційних технологій.

За цей час техніка та методологія захисту інформації пройшли довгий шлях розвитку від окремих розрізнених нескладних механізмів захисту до системної концепції захисту, втіленням якої є цілеспрямоване використання комплексу організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів захисту інформації [135, 136]. Суть системної концепції – поєднання у найбільш раціональний спосіб усіх наведених вище заходів в певній організаційній формі – СЗІ. Наскільки вдалим є це поєднання, як визначити рівень успішності функціонування СЗІ? Ці цілком природні в загальному випадку питання набувають особливої актуальності в разі, коли об'єктом захисту є ДТ, рівень важливості й, відповідно, потрібний ступінь захисту якої є найвищим порівняно з іншими видами ІзОД.

Відповідь на поставлені вище питання стає можливою після введення системи певних формальних критеріїв якості (рівня) захисту, що його реалізує СЗІ, причому найбільш бажаною, універсальною й зручною формою цього критерію є кількісна, бо вона максимально спрощує аналіз та порівняння різних варіантів захисту, а в деяких випадках дозволяє оптимізувати вибір найкращого варіанту.

Побудова СЗІ в загальному випадку являє послідовний розвязок трьох задач: аналізу, синтезу та управління.

Зміст задачі аналізу – об'єктивне оцінювання загроз інформації й можливої шкоди від їх реалізації, *задачі синтезу* – визначення та використання найбільш ефективних механізмів захисту від загроз, що їх визнано значущими. *Задача управління* – забезпечення ефективного захисту інформації у часі і просторі на всіх етапах обробки та існування ІзОД в умовах змін, що відбуваються в оточуючому інформаційному середовищі.

Втілення системної концепції захисту інформації на практиці стикається з рядом труднощів, головними з яких є потреба загальновизнаної єдиної базової методології узгодженого розв'язку задач аналізу, синтезу і управління, яка б забезпечила застосування для всіх цих задач єдиної системи критеріїв (показників), підпорядкованих спільній меті – досягненню потрібного рівня захисту ІзОД. Тут знов виникає проблема введення зазначених у вступі формалізованих критеріїв якості СЗІ, універсальний характер яких має забезпечити пророблення, співставлення, аналіз різних варіантів СЗІ та оптимізацію вибору кращого за умов визначеного рівня захисту.

Аналіз публікацій з питань захисту інформації, матеріалів науково-дослідних робіт та практичних розробок СЗІ, вивчення змісту міжнародних, регіональних, національних галузевих нормативних документів та стандартів [138] дозволяє стверджувати, що в якості подібної системної методології може бути використано підхід, відомий як оцінювання та керування інформаційними ризиками [138-141]. Спираючись на цей підхід, можна визначити, що входить до складу ІзОД, яка потребує захисту, оцінити необхідний ступінь захисту ІзОД, обрати стратегію розвитку інформаційної структури організації й підтримувати на відповідному рівні її безпеку. Розглянемо можливість та перспективи застосування методології оцінювання та керування інформаційними ризиками для аналізу ефективності СОДТ.

Суть методології оцінювання ризиків полягає в співставленні вихідного та залишкового ризиків для ІзОД, які розраховуються через оцінки можливих збитків, що можуть виникнути внаслідок ймовірної реалізації загроз ІзОД до (вихідний ризик R) або після (залишковий ризик r) впровадження СЗІ. За результатами співставлення робиться висновок щодо доцільності використання тих чи інших механізмів захисту ІзОД, їх ефективності та ефективності функціонування СЗІ в цілому.

В формальному представленні маємо:

$$R_i = P_i \cdot Q_i, \tag{4.1}$$

$$r_i = p_i \cdot P_i \cdot Q_i, \tag{4.2}$$

де P_i - ймовірність реалізації i-ої загрози, Q_i - втрати (в грошових одиницях або балах), обумовлені реалізацією i-тої загрози щодо ІзОД, p_i - ймовірність реалізації i-тої загрози після впровадження СЗІ через наявність вразливості в системі захисту щодо цієї загрози.

Маючи ризики R_i, r_i, можна оцінити ефективність захисту ІзОД від *i*-тої загрози:

$$E_i = (R_i - r_i) / R_i = 1 - p_i, \qquad (4.3)$$

де показник E_i може змінюватися від 1 (випадок «абсолютної» захищеності від *i*-тої загрози, r_i = 0) до 0 (нульову ефективність захисту маємо у випадку $R_i = r_i$, тобто при абсолютній, стовідсотковій вразливості СЗІ щодо *i*-тої загрози).

Інша форма функціоналу ефективності захисту має вираз:

$$e_i = R_i / r_i = 1 / p_i, \qquad (4.4)$$

Діапазон змін e_i – від 1 (абсолютна неефективність) до нескінченності ∞ (абсолютно ефективний захист). Показник ефективності захисту, який також дозволяє оцінити доцільність введення механізму захисту, задається співвідношенням [125]:

$$e_i = (R_i - r_i) / q_i = (1 - p_i) \cdot P_i \cdot Q_i / q_i, \qquad (4.5)$$

де q_i - оцінка вартості витрат на створення та впровадження механізму (механізмів) захисту проти *i*-тої загрози.

Наведені вище вирази дають змогу оцінити ефективність фрагментарного захисту від окремої часткової загрози. Однак інформація, що захищається, може зазнавати впливу ряду потенційних загроз, тому окрім аналізу часткових ризиків R_i, принциповим є визначення сукупної ймовірності *P* існуючої щодо ІзОД небезпеки й сукупного ризику *R* (відповідно значень *p, r*). Якщо ІзОД складається з кількох окремих інформаційних ресурсів (IP_1, ..., IP_m), то об'єднання ризиків за всіма *m* складовими та розрахунок відповідного об'єднаного залишкового ризику дає змогу оцінити ефективність СЗІ по всьому комплексу ІзОД. Визначивши загальносистемний ризик ідентифікаторами R_Σ, r_Σ, можна розраховувати за вже вживаними раніше формулами (4.4), (4.5) показники $E_{\Sigma 1}$, $E_{\Sigma 2}$, що безпосередньо характеризують ефективність СЗІ. На жаль, проблему «згортання» часткових ризиків до загальносистемного на сьогодні математично строго не розв'язано.

Для аналізу сукупних втрат від реалізації всієї множини загроз часто використовують функціонал виду (так званий сумарний ризик):

$$R_{\Sigma} = \sum_{i=1}^{m} P_i \cdot Q_i \ . \qquad (4.6)$$

Через те, що множина загроз може не складати повної групи подій (загрози можуть реалізовуватися по одинці, сумісно або ж не реалізовуватися зовсім), застосування сумарного ризику не має прийнятної ймовірносної інтерпретації й відповідного математичного обґрунтування, обумовлюючи часто отримання занадто завищених оцінок загальносистемного (інтегрального) ризику (більш детально в [137] та див. п.5.2 «*Сценарний метод оцінювання шкоди, заподіяної витоком секретної інформації*»).

В практиці захисту ІзОД популярні системні показники ефективності СЗІ, наприклад, показник повернення інвестицій (*ROI* – return on investment) [140]:

$$ROI = (R_{\Sigma} - r_{\Sigma} - q_{\Sigma}) / q_{\Sigma}, \qquad (4.7)$$

де q_{Σ} - загальні витрати на створення та обслуговування СЗІ,

Або так звана сукупна вартість володіння (*TCO* – total cost of ownership) [140]:

$$V_{\Sigma} = (R_{\Sigma} - r_{\Sigma}) / Q, \qquad (4.8)$$

де знаменник *Q* може бути різним за змістом. Це, зокрема, загальна вартість певного ОІД, де циркулює ІзОД, її вартість та інформаційних послуг з її обробки, загальна вартість ІР, що їх задіяно в ІАС, яку захищає СЗІ тощо.

Системні показники на зразок V_{Σ} дають змогу співставити витрати на створення СЗІ на ОІД, яка забезпечує певні вимоги до рівня захисту ІзОД, із загальноекономічними характеристиками ОІД чи показниками інформаційної діяльності, що ним забезпечується (наприклад, швидкість передачі інформації в захищеній системі зв'язку суттєво залежить від складності алгоритму криптозахисту, яка в свою чергу напряму пов'язана з вимогами щодо потрібного рівня захисту інформації в каналі зв'язку).

Можливість врахування аспекту економічної доцільності в задачі синтезу СЗІ є вельми привабливою й разом з тим актуальною особливістю аналізу та керування інформаційними ризиками, зокрема в умовах сучасної ринкової економіки. Тому цей підхід починають широко застосовувати як методологію побудови СЗІ різні бюджетні структури (в АС, ІТС, ІАС тощо), а також структури, орієнтовані у своїй діяльності на міжнародні стандарти у сфері інформаційної безпеки,

наприклад, заклади банківської галузі. Однак застосування методології інформаційних ризиків для СОДТ суттєво обмежено.

Можливою причиною цього є існуюче уявлення про некоректність введення поняття залишкового ризику для СЗІ у сфері ДТ. Так в ДСТУ 3396.1-96. «Захист інформації. Технічний захист інформації. Порядок проведення робіт» в розділі 3.2. постановка задачі захисту ІзОД, що складає ДТ, формулюється наступним чином: «досягнення максимального рівня захисту ІзОД за необхідних затрат і мінімального рівня обмежень видів інформаційної діяльності», що можна трактувати як гарантування $p_i = 0$ за будь-яку вартість q_Σ. Очевидно, така декларативна постановка задачі аж ніяк не відповідає сьогоднішній реальності і стимулює ситуацію, коли особа, відповідальна за захист інформації, може небезпідставно стверджувати, що ретельно відслідковуючи вимоги чинних нормативів та керівних документів, в яких закумульовано набутий досвід захисту інформації, стовідсотково гарантує ОДТ.

Однак такий підхід до забезпечення захисту інформації є принципово невірним. СЗІ, що будується виключно на аналізі порушень, котрі мали місце в минулому, за своєю суттю не може бути ефективною, як неефективна будь-яка пасивна СЗІ, бо вона адаптується до змін в інформаційному середовищі, зокрема до змін його агресивних складових, лише за відомостями про інформаційні атаки. Однак виявлення такої атаки у пасивній СЗІ можливо лише за наслідками атаки, тобто коли вона почалася, отримала розвиток і призвела до певних втрат, за якими саме й була зафіксована.

Тому ефективними можуть бути лише активні СЗІ, що мають прогностичні якості й забезпечують успішний випереджальний захист щодо можливих атак, маючи таким чином практично нульові втрати. Однак така активна СЗІ принципово не може будуватися за єдиним шаблоном й повинна мати індивідуальні властивості, залежні від напрямку діяльності конкретного об’єкту захисту, його інформаційної структури, рівня й особливостей ІР, кадрового забезпечення й т.п. Крім того, активний прогностичний захист будується на засадах постійного пошуку та аналізу інформацій про наміри і можливості потенційного порушника, моніторингу загроз в умовах постійних змін інформаційного середовища. Звичайно, що при цьому мають бути враховані і певні загальні тенденції й рекомендації, які відпрацьовуються на більш високому системному рівні, перш за все на державному.

Окреслені вище задачі є і багатоаспектними, і достатньо фінансово ємними, тому наявність економічного співставлення витрат на СЗІ, її окремі складові з можливими наслідками від втрат ІзОД є необхідною

умовою створення ефективної СЗІ, обов'язковим зворотнім зв'язком, який дозволяє оцінити доцільність і достатність реалізації того чи іншого елементу СЗІ, дієвість функціонування СЗІ в цілому, й адекватність існуючим зовнішнім та внутрішнім загрозам.

Наразі реальну ситуацію із рівнем ОДТ можна, хоча, певно, дуже приблизно оцінити, спираючись на наведені в чисельних літературних джерелах аналітичні відомості про залежність ефективності СЗІ від сумарних витрат на її функціонування. Так в [138] зазначається, що для досягнення ефективності захисту ІзОД в 50% витрати на захист повинні досягати 10% вартості інформаційної системи, а ефективність в 90% - 15-20% вартості. В [141] наведено фактично аналогічні відомості: за твердженням експертів-практиків, оптимум в питанні захисту ІзОД, який дозволяє почувати себе в цьому аспекті достатньо впевнено, досягається при витратах на СЗІ в 10-20% від загальної вартості інформаційної системи. Дещо іншу залежність наведено в [142]: витрати на захист ІР в більшості випадків не повинні перевищувати 10% від їх вартості.

Крім того, у вже цитованому вище джерелі [141] йдеться про додаткові асигнування на безпеку інформації в розмірі 5-15% від суми коштів, що витрачаються на підтримку роботи інформаційної системи. Очевидно, що в наведених вище двох групах джерел мова йде про різні речі: в [141, 143] загальна сума, від якої нараховуються відсотки на СЗІ – це вартість основних засобів таких підприємств як АС, ІТС та їм подібних, які за своїм базовим, головним призначенням орієнтовані на обробку, передачу, накопичення та зберігання даних з ІзОД, а в [141, 142] нарахування відсотків йде на сумарний обсяг фінансування робіт, що проводяться на підприємстві, в науковому закладі (наприклад, науково-дослідних розробок, результатом яких буде створення певного ІР або продукту).

В наведених джерелах мова йде про захист конфіденційної інформації, тому цитовані оцінки слід вважати нижньою межею витрат q_Σ на ОДТ. Отже приблизна оцінка мінімально потрібних асигнувань на СЗІ для відомостей, що становлять ДТ, дорівнює $q_\Sigma = 20\%Q$.

Прикладом невідповідності практики ОДТ принципам системного аналізу є традиційне обмеження аналізу загроз ДТ тільки загрозами витоку СІ або загрозами несанкціонованого доступу до неї, тоді як загрози знищення, модифікації та немотивованого обмеження доступу фактично не оцінюються. Остання із зазначених загроз – це за своєю суттю загроза необгрунтованого віднесення інформації до ДТ. За оцінками, наведеними в [62], втрати через необгрунтоване закриття

інформації в 70-80 рр. в колишньому СРСР доходили до кількох десятків мільярдів рублів. Ці збитки виникли через втрату вигоди від:

- нереалізованих впроваджень та нереалізованого продажу радянських технологій за кордон;
- заборони продажу промислових виробів, військової техніки та озброєння, а також через відсутність, внаслідок необгрунтованого віднесення відповідної інформації до ДТ, взаємодії та координації між організаціями, що проводили розробку нових технологій.

Таким чином несистемне, звужене сприйняття загроз щодо ДТ призводить до однобічної, необ'єктивної оцінки відповідних інформаційних ризиків і далі трансформується у цілком реальні економічні збитки. Слід зауважити, що в Законі України «Про державну таємницю» [3] одним з завдань ДЕТ є «визначення доцільності віднесення до ДТ інформації про винаходи (корисні моделі), що мають подвійне застосування, на підставі порівняльного аналізу ефективності цільового використання та за згодою автора; ...». Однак в «Рекомендаціях…» [38] для ДЕТ відсутні будь-які згадки про необхідність проведення порівняльного аналізу зокрема та аналізу збитків (інформаційних ризиків) через втрату вигод від відкритого використання інформації, що є предметом експертизи, а також внаслідок обмеження доступу до цієї інформації зацікавлених осіб або продажу відповідних інформаційних продуктів. Тобто в в «Рекомендаціях…» [38] маємо редукцію системного аналізу інформаційного об'єкту, що експертується, до аналізу лише інформаційних ризиків внаслідок розголошення інформації про об'єкт експертизи.

Загалом, аналізуючи поточну ситуацію, можна констатувати, що в середині 90-х років XX сторіччя серед множини питань, пов'язаних із забезпеченням захисту ІзОД, найбільш проробленим та впорядкованим в плані нормативно-правового, організаційного та технічного забезпечення було питання ОДТ. На жаль, нині, на фоні загального динамічного розвитку СЗІ, інтенсивної гармонізації національної нормативної бази із світовими та європейськими стандартами у галузі інформаційної безпеки, ситуація у сфері ОДТ виглядає стабільно консервативною, відстороненою щодо сприйняття і використания нових напрямів, технологій та ідей в галузі захисту ІзОД. Зокрема це стосується системного підходу до оцінювання ефективності функціонування СОДТ і в першу чергу питання введення формалізованих критеріїв та показників ефективності, відсутність яких виключає можливість об'єктивної оцінки рівня стану ОДТ, достатність ресурсів, залучених до ОДТ.

4.3. Дослідження і оцінка стану охорони державної таємниці

Визначення критерію стану охорони державної таємниці

Як показав аналіз підходів до оцінювання впливу стану ОДТ на національну безпеку, цей вплив практично не враховується через відсутність кількісних показників захищеності СІ, які могли б бути враховані у моделі ефективності системи національної безпеки держави.

Сьогодні немає методики, яку можна було б використовувати для оцінки стану ОДТ у всьому її комплексі. Тому актуальним є питання розробки такої методики як у загальному випадку (національна безпека держави), так і для більш вузьких застосувань.

Нижче наводиться методика, призначена для оцінювання стану ОДТ на окремому об'єкті [125]. На наш погляд, можливо адаптувати цю методику для оцінювання ефективності ОДТ у більш загальному випадку, в тому числі для оцінки стану ОДТ у державі в цілому.

Підходи до розробки методики, а також основні поняття (сфери, до яких відносяться відомості, що становлять ДТ; можлива шкода національній безпеці України; ОДТ, як комплекс заходів та інші), які використовуються при цьому, базуються на положеннях Закону України «Про державну таємницю» [3], ЗВДТ [31] та інших нормативних документах.

Виходячи з положень законодавства, можна зазначити, що стан ОДТ визначається ступенем захищеності СІ, тобто критерієм стану ОДТ є захищеність СІ. Однак, для того, щоб використовувати цей критерій в моделях інформаційної або національної безпеки держави, бажано виразити його в кількісному вимірі.

Для забезпечення ОДТ у державі створена відповідна система, основною метою якої є запобігання розголошенню СІ, недопущення втрат її матеріальних носіїв і використання цієї інформації на шкоду безпеці держави –СОДТ.

Для того, щоб визначити, як існуюча система відповідає вимогам щодо досягнення зазначеної вище мети і виконання свого основного завдання, необхідно обрахувати кількісну оцінку рівня реалізації системою своїх функцій, іншими словами – оцінити її ефективність.

Ефективність СОДТ можна визначити через ефективність комплексу заходів з ОДТ і оцінити ступенем захищеності СІ.

Показники кількісної оцінки захищеності державної таємниці

Припустимо, що Всі заходи по забезпеченню ОДТ на об'єкті проведено з найвищою ефективністю, її розголошення або/і втрати МНСІ не сталося. Вважаємо, що зміст СІ повністю прихований від окремих осіб чи групи осіб, які зацікавлені в її отриманні.

Оцінюючи стан ОДТ, у даному випадку можна очікувати, що він буде найвищим, забезпечить необхідну реалізацію можливостей СОДТ і безпеку в інформаційній сфері.

Якщо комплекс заходів з ОДТ проведено з низькою ефективністю і не досягнуто бажаного результату, вважаємо, що можливості СОДТ реалізовані не повною мірою або не реалізовані взагалі, безпека держави в інформаційній сфері буде знижена або не забезпечена.

Стан ОДТ у цьому випадку можна оцінити відповідним показником, порівнявши ефективність заходів з її охорони в конкретному стані (який оцінюється) з ефективністю комплексу заходів при умові забезпечення повної захищеності СІ.

Це можна відобразити таким чином:

$$K^{СОДТ} = E_p^{СОДТ} / E^{СОДТ}, \qquad (4.9)$$

де $K^{СОДТ}$ – коефіцієнт ефективності СОДТ, характеризує ступінь реалізації можливостей СОДТ та ефективність засобів і способів ОДТ в заданих умовах; $E_p^{СОДТ}$ – ефективність СОДТ з урахуванням реального стану захищеності СІ в заданих умовах; $E^{СОДТ}$ – ефективність СОДТ при повній захищеності СІ (відсутності розголошення СІ або втрати МНСІ).

Виходячи з призначення СОДТ, її ефективність у загальному вигляді можна визначити співвідношенням:

$$E = W_{\text{пш}} / W, \qquad (4.10)$$

де E – ефективність СОДТ; $W_{\text{пш}}$ – можливості СОДТ по зниженню шкоди безпеці держави (попереджена шкода), тобто можливих втрат, які обумовлені розголошенням СІ або/і втратами МНСІ; W – потенційна шкода безпеці держави, тобто можливі втрати, які обумовлені розголошенням СІ або/і втратами МНСІ (у нашому випадку визначається згідно «Рекомендацій…» [38], якими користуються ДЕТ під час визначення підстав для віднесення відомостей до ДТ та ступеня її секретності).

Можливості СОДТ зі зниження шкоди безпеці держави з врахуванням реального стану ОДТ позначимо $W_p^{СОДТ}$, а можливості СОДТ зі зниження шкоди безпеці з врахуванням повної захищеності СІ – $W^{СОДТ}$. Ефективність СОДТ в реальних умовах E_p визначається співвідношенням [125]:

$$E_p^{СОДТ} = W_p^{СОДТ} / W, \tag{4.11}$$

а ефективність СОДТ $E^{СОДТ}$ з урахуванням повної захищеності СІ як:

$$E^{СОДТ} = W^{СОДТ} / W. \tag{4.12}$$

У відповідності до співвідношення (4.9) [125]:

$$K^{СОДТ} = W_p^{СОДТ} / W^{СОДТ}. \tag{4.13}$$

Згідно ст. 8 Закону України «Про державну таємницю» [3] вся СІ, яка належить державі розподіляється за окремими сферами (позначимо їх символом "*N*"): оборони; економіки, науки і техніки; зовнішніх відносин; державної безпеки та охорони правопорядку. Така структуризація СІ дозволяє визначити ефективність СОДТ через стан захисту СІ в окремих сферах.

Тоді:

$$W_p^{СОДТ} = \sum (W_N \cdot K_{зі\,N}),\ N = 1...4. \tag{4.14}$$

де W_N – потенційна СШ державі у окремій сфері *N*; $K_{зі\,N}$ – коефіцієнт захищеності СІ, яка належить до окремої сфери (*N*), в реальних умовах.

У свою чергу:

$$W^{СОДТ} = \sum W_N. \tag{4.15}$$

Тоді, у відповідності до співвідношення (13) [125]:

$$K^{СОДТ} = \sum (W_N \cdot K_{зі\,N}) / \sum W_N. \tag{4.16}$$

Обраний критерій кількісної оцінки стану ОДТ $K^{СОДТ}$ має виразний зміст – ступінь реалізації можливостей СОДТ, яка визначається відношенням розміру попередженої шкоди в умовах реального стану ОДТ до розміру попередженої шкоди при повній захищеності СІ. Він може бути розрахований за допомогою існуючих

методик, які використовують ДЕТ, та наведеної у цьому виданні методики кількісного оцінювання стану ОДТ. У подальшому цей критерій може бути застосований для визначення впливу стану ОДТ на інформаційну та національну безпеку держави шляхом використання його у відповідних аналітичних моделях.

В якості часткових показників оцінки стану ОДТ використовуються коефіцієнти захищеності СІ у відповідних сферах $K_{зі\,N}$. Це коефіцієнти характеризують ступінь захищеності сукупності відомостей, що відносяться до відповідних сфер, при умові виконання комплексу заходів з охорони цих відомостей, або ступінь зниження можливих втрат (потенційної шкоди), які обумовлені розголошенням СІ або/і втратами МНСІ.

Деталізація задач інформаційної діяльності в окремих сферах дозволяє визначити шкоду від втрат СІ при будь-якому ступеню узагальнення (або локалізації) СОДТ, що є об'єктом аналізу.

Методика кількісної оцінки стану охорони державної таємниці

Кількісна оцінка стану ОДТ обраховується у чотири етапи (див. рис. 24.):

- на *першому* етапі визначаються вихідні дані для розрахунку коефіцієнтів захищеності відомостей $K_{зі\,N}$, які відносяться до відповідних сфер *N*, що визначені у Закону України «Про державну таємницю» [3], ЗВДТ [31] та критерієм визначення СС [38, 125]: «Т» ($1 \le x_T < 10$), «ЦТ» ($10 \le x_{ЦТ} < 100$), «ОВ» ($100 \le x_{ОВ} \le 300$), які визначені середнім інтервальним значенням: $x_T = 5$, $x_{ЦТ} = 55$, $x_{ОВ} = 200$;

- на *другому* етапі здійснюється розрахунок коефіцієнтів захищеності СІ $K_{зі\,N}$ у відповідних *N* сферах;

- на *третьому* етапі розраховується коефіцієнт ефективності СОДТ $K^{СОДТ}$;

- на *четвертому* етапі кількісне значення $K^{СОДТ}$, яке розраховано, порівнюється з тим, яке потрібне, аналізується ефективність комплексу заходів з ОДТ.

При необхідності, з метою підвищення рівня ОДТ і забезпечення її необхідного стану, перелік заходів коригується (див. табл. 9). При цьому можливий розглял кількох варіантів посилення захисту, їх аналіз, співставлення та вибір найбільш прийнятного.

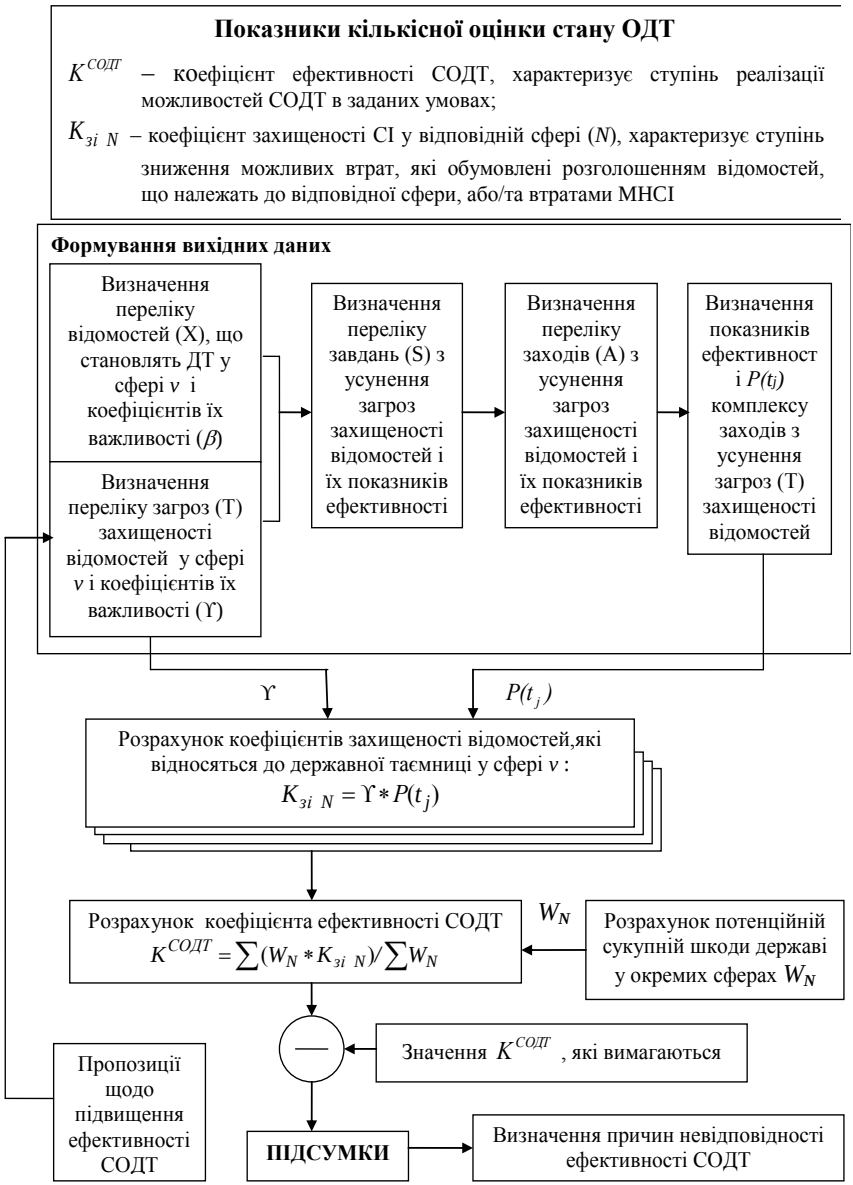


Рис. 24. Схема кількісного оцінювання стану СОДТ

В якості вихідних даних для розрахунку $K_{зі\,N}$ обрані наступні [125]:

а) перелік відомостей ***X****, що становлять ДТ у сфері N:*

$$X = \{x_1, x_2, ..., x_i, ..., x_m\}, i = \overline{1,m}, \quad (4.17)$$

де x_i – відомості, що становлять ДТ у сфері *N*; *m* – кількість відомостей, що становлять ДТ у сфері *v*;

б) перелік коефіцієнтів важливості $\boldsymbol{\beta}$ *відомостей, що становлять ДТ у сфері N:*

$$\beta = \{\beta_1, \beta_2, ..., \beta_i, ..., \beta_m\}, i = \overline{1,m}, \quad (4.18)$$

де β_i – коефіцієнт важливості *i*-х відомостей x_i, що становлять ДТ у сфері *N*.

Коефіцієнт важливості β_i окремих відомостей x_i обраховуються у відповідності зі шкодою, обумовленою розголошенням цих відомостей.

в) перелік загроз ***T*** *захищеності відомостей, що становлять ДТ у сфері N:*

$$T = \{t_1, t_2, ..., t_j, ..., t_n\}, \; j = \overline{1,n}, \quad (4.19)$$

де t_j – *j*-а загроза захищеності відомості x_i, що належить до ДТ у сфері *N*, *n* – кількість загроз захищеності *m* відомостей сфери *N*. У загальному випадку $m \neq n$.

Перелік загроз захищеності відомостей, що становлять ДТ у сфер *N*, визначається за допомогою матриці загроз, яка складається за експертними оцінками. Такими загрозами, наприклад, можуть бути: несанкціоноване одержання СІ з використанням спеціальної апаратури; втрата МНСІ; неусвідомлюване розголошення СІ персоналом тощо.

г) перелік узагальнюючих коефіцієнтів важливості $\boldsymbol{\Upsilon}$ *загроз захищеності відомостей, що становлять ДТ у сфері N:*

$$\Upsilon = \{\Upsilon_j\}, \; j = \overline{1,n}, \quad (4.20)$$

де Υ_j – узагальнюючий коефіцієнт важливості *j*-ої загрози захищеності відомостей сфери *N*.

Для розрахунку коефіцієнтів важливості Υ_j, використовується матриця *R* взаємозв'язку СІ x_i з загрозами *t*:

$$R = \left\| r_{ij} \right\|_{m,n}. \quad (4.21)$$

Кожний елемент матриці визначається згідно з виразом:

$$r_{ij} = \begin{cases} 0, \text{якщо } t_j \bar{\in} T_i \\ £_{ij}, \text{якщо } t_j \in T_i \end{cases}, \tag{4.22}$$

де T_i – множина загроз ($T_i \in T$) захищеності відомостям x_i відповідної сфери; $£_{ij}$ – значення коефіцієнта важливості загрози t_j захищеності відомостей x_i, що належать до сфери *N*.

При обчисленні $£_{ij}$ враховуються коефіцієнти важливості β_i таким чином, щоб виконувалась умова:

$$\sum_{t_j \in T_i} £_{ij} = \beta_i, \tag{4.23}$$

$£_{ij}$ визначається виходячи із виразу:

$$£_{ij} = \beta_i / |T_i|, i = \overline{1,m}, \tag{4.24}$$

де $|T_i|$ – кількість загроз у множині T_i.

Виходячи з умов, що визначені виразами (4.20)-(4.24), коефіцієнти важливості загроз захищеності відомостей відповідної сфери, можуть бути представлені у вигляді:

$$\Upsilon = J_m \cdot R, \tag{4.25}$$

де $\Upsilon = \|\Upsilon_1, \Upsilon_2, ..., \Upsilon_j, ..., \Upsilon_n\|$ – вектор-рядок коефіцієнтів важливості загроз захищеності відомостей, що становлять ДТ у певній сфері; Υ_j – узагальнюючий (сумарний) коефіцієнт важливості загрози t_j. Характеризує важливість усунення (нейтралізації) загрози t_j з урахуванням сумарної кількості і важливості відомостей окремої *N* сфери, для яких існує ця загроза; J_m – вектор-рядок, який складається з *m* елементів, кожен з яких рівен 1; *R* – матриця взаємозв'язку *X* з *T*, яка має вигляд:

$$R = \left\| \begin{array}{l} r_{11} r_{12} \dots r_{j1} \dots r_{n1} \\ r_{11} r_{12} \dots r_{j1} \dots r_{n1} \\ \dots\dots\dots\dots\dots\dots \\ r_{1i} \; r_{2i} \dots r_{ji} \dots r_{ni} \\ \dots\dots\dots\dots\dots\dots \\ r_{1m} \; r_{2m} \dots r_{jm} \dots r_{nm} \end{array} \right\|, \tag{4.26}$$

Остаточно з виразу (4.22) отримаємо:

$$\begin{aligned}
&\Upsilon_1 = r_{11} + r_{12} + ... + r_{1i} + ... + r_{1m} \\
&\Upsilon_2 = r_{21} + r_{12} + ... + r_{2i} + ... + r_{2m} \\
&... = \ ... \ ... \ ... \ ... \ ... \ ... \ ... \ ... \\
&\Upsilon_j = r_{j1} + r_{j2} + ... + r_{ji} + ... + r_{jm} \\
&... = \ ... \ ... \ ... \ ... \ ... \ ... \ ... \ ... \\
&\Upsilon_n = r_{n1} + r_{n2} + ... + r_{ni} + ... + r_{nm}
\end{aligned} . \qquad (4.27)$$

д) перелік завдань ***S*** *з усунення (нейтралізації) загроз захищеності відомостей, що становлять ДТ у сфері N:*

$$S = \{s_g\}, g = \overline{1, l}, \qquad (4.28)$$

де s_g – *g-е* завдання щодо усунення (нейтралізації) загроз захищеності відомостей сфери *N*; l – кількість завдань з усунення (нейтралізації) загрози захищеності відомостей сфери *N*. Формування переліку завдань щодо усунення (нейтралізації) загроз захищеності відомостей відповідної сфери здійснюється експертним методом.

Завдання s_g впорядковуються за місцем і часом їх вирішення, якщо це потрібно. В завданнях s_g формулюються такі позиції: спосіб усунення (нейтралізації) загрози (обмеження допуску до ДТ, регламентування порядку робіт з ДТ, проведення технічних заходів захисту СІ і таке інше); сама загроза, що підлягає усуненню (нейтралізації); період часу (діяльності), на протязі якого загрозу захищеності СІ необхідно усунути (нейтралізувати).

Множина завдань *S* у варіанті задуму усунення (нейтралізації) загрози захищеності відомостей, що становлять ДТ у сфері *N*, повинна бути достатньою для захисту кожного елементу відомостей $x_i \in X$ від кожної загрози $t_j \in T$, але, за можливістю, мінімальною.

е) перелік заходів ***M*** *з усунення (нейтралізації) загроз захищеності відомостей, що становлять ДТ у сфері N:*

$$M = \{m_k\}, k = \overline{1, l}, \qquad (4.29)$$

де m_k – захід (засіб чи спосіб), який забезпечує виконання *g*-го завдання s_g з усунення (нейтралізації) загрози захищеності окремих x_i відомостей.

Заходи (засоби і способи) обираються у відповідності з переліком організаційно-правових, технічних, криптографічних та оперативно-розшукових заходів, які визначені у [3, 14] та іншими законодавчими і регламентуючими документами у сфері діяльності, пов'язаної з ДТ.

Захід (засіб чи спосіб) m_k усунення (нейтралізації) загрози захищеності окремих відомостей визначається для кожного завдання s_k. Порівнянням можливих засобів і способів розв'язання завдання захисту відомостей обираються найбільш ефективні з них.

ж) перелік $\boldsymbol{P_k}$ *показників ефективності окремих заходів (засобів і способів) з усунення (нейтралізації) загроз захищеності відомостей, що становлять ДТ у сфері N:*

$$P_k = \{P(t_j/m_k)\}, k = \overline{1,l,}, \qquad (4.30)$$

де $P(t_j/m_k)$ – показник ефективності *k*-го заходу (засобу чи способу) з усунення (нейтралізації) *j*-ї загрози захищеності окремої відомості, що становить ДТ.

Показник $P(t_j/m_k)$ розраховується для кожного заходу (засобу чи способу) з використанням існуючих методик або обирається за допомогою експертів [112-122, 144]. Цей показник характеризує ефективність *k*-го заходу (засобу чи способу) при умові виконання відповідного завдання з усунення (нейтралізації) загрози захищеності окремих відомостей сфери *N* і має імовірнісний характер.

з) показники ефективності комплексу заходів (засобів і способів) з усунення (нейтралізації) загрози захищеності окремих відомостей, що становлять ДТ у сфері N.

Усунення (нейтралізація) однієї загрози t_j в загальному випадку забезпечується за умов реалізації декількох завдань захисту відомостей, що становлять ДТ.

Нехай сукупність заходів з нейтралізації певної *j*-ої загрози може виконуватись одночасно. Визначимо ці заходи як $m_g,...,m_q$ ймовірність усунення кожним із них загрози t_j, через $P(t_j/m_g),...,P(t_j/m_q)$. Ймовірність того, що загроза t_j не буде нейтралізована окремо кожним з цих заходів обчислюється за виразами:

$$\overline{P}(t_j/m_k) = 1 - P(t_j/m_k), k = g,...,q. \qquad (4.31)$$

Ймовірність того, що загроза t_j існуватиме попри реалізацію всієї сукупності заходів, тобто остатня ймовірність існування загрози після введення системи заходів із захисту інформації, визначається як:

$$\overline{P}(t_j/m_g,...,m_q) = \prod_{k=g,...,q}(1-P(t_j/m_k)). \qquad (4.32)$$

Ймовірність нейтралізації загрози t_j сукупною дією усіх заходів $m_g,...,m_q$ обчислюється за виразом:

$$P(t_j/m_g,...,m_q) = 1-\overline{P}(t_j/m_g,...,m_q) = 1-\prod_{k=g,...,q}(1-P(t_j/m_k)). \qquad (4.33)$$

За результатами обчислень складається вектор-рядок *P* значень $P(t_j)$ показників ефективності усунення (нейтралізації) відповідних загроз t_j:

$$P = \left\| P_1,P_2,...,P_j,...,P_n \right\|. \qquad (4.34)$$

де ймовірність нейтралізації *j*-ої загрози скорочено позначаємо через P_j, j=1,n.

На цьому етап формування вихідних даних закінчується. Всі вихідні дані заносяться у відповідні таблиці (див. табл.15-16).

і) розрахунок коефіцієнта захищеності $K_{зі\,N}$.

З урахуванням ступеня усунення (нейтралізації) загроз захищеності СІ сфери *N*, їх взаємозв'язку із відомостями, що підлягають захисту, а також коефіцієнтів важливості згаданих загроз, визначається коефіцієнт захищеності відомостей, які відносяться до ДТ у сфері *N*:

$$K_{зі\ N} = \Upsilon \cdot P^T. \qquad (4.35)$$

де Υ – вектор-рядок значень коефіцієнтів важливості загроз захищеності СІ сфері *N*; *P* – вектор-рядок значень показників ефективності усунення (нейтралізації) відповідних загроз t_j; $(.)^T$ – символ операції транспонування.

Слід зазначити, що при визначенні ефективності СОДТ на окремому конкретному ОІД необхідність в обрахуванні сукупності коефіцієнтів $K_{зі\,N}$ відпадає.

В цьому випадку множина β (вираз (4.18)) буде складатися з коефіцієнтів важливості усіх відомостей, що циркулюють на ОІД, без їх поділу на сфери приналежності. Для цих відомостей визначається загальний перелік загроз й певна сукупність заходів з їх нейтралізації, відповідно до чого розраховуються вектори Υ і P, безпосередньо за якими обчислюється коефіцієнт ефективності СОДТ для ОІД:

$$K^{СОДТ} = \Upsilon \cdot P^T, \tag{4.36}$$

В даній ситуації немає потреби в оцінці потенційної СШ, заподіяної втратами СІ. Це витікає з виразу (4.13): через відсутність поділу СІ за окремими сферами значення $N = 1$, тобто

$$K^{СОДТ} = W_i \cdot K_{зі1} / W_i = K_{зі1}, \tag{4.37}$$

де $K_{зі1}$ обчислюється за формулою (4.35).

к) розрахунок показника ефективності СОДТ $K^{СОДТ}$.

Обчисливши сукупність значень потенційної шкоди державі в окремих сферах, за формулою (4.15) розрахуємо можливості СОДТ у разі повної захищеності СІ, за формулою (4.14) – за умов реального стану ОДТ й згідно виразу (4.16) отримаємо кількісну оцінку показника ефективності СОДТ.

л) оцінка стану ОДТ. Оцінка стану ОДТ проводиться за рівнем достатності шляхом порівняння розрахованих значень $K^{СОДТ}$ з тими, що потрібні. При цьому широко використовують експертні методи, методи нечітких множин тощо [112-122, 144]. Проведені дослідження оцінки ефективності інших систем дають підстави визначити класифікацію критерію $K^{СОДТ}$, яка наведена у таблиці 9.

Далі проводиться аналіз ефективності і оптимізація комплексу заходів з ОДТ. При необхідності готуються пропозиції із вдосконалення ОДТ шляхом проведення додаткових чи більш ефективних заходів.

Таблиця 9

Класифікація критерію $K^{СОДТ}$ ***для оцінки стану ОДТ***

Класифікація критеріїв оцінки стану ОДТ	*Значення* $K^{СОДТ}$
Не відповідає вимогам (ОДТ не забезпечена)	$K^{СОДТ} \le 0{,}37$
Відповідає вимогам у цілому (ОДТ забезпечена у цілому, але є можливість розголошення СІ або/та втрати МНСІ)	$0{,}81 > K^{СОДТ} > 0{,}37$
Відповідає вимогам (ОДТ забезпечена повністю, можливості розголошення СІ або/та втрати МНСІ практично не існує)	$K^{СОДТ} \ge 0{,}81$

4.4. Практичні аспекти реалізації оцінювання впливу стану охорони державної таємниці на національну безпеку

Як зазначалося вище, при оцінюванні ефективності СОДТ проблемним моментом є визначення шкоди, заподіяної витоком певної СІ. Нижче пропонується методика оцінювання шкоди у цьому випадку. Методика базується на аналізі наведених в ЗВДТ даних про структуру інформації, що становить ДТ, з наступним присвоєнням їм кількісних значень, формування яких проводиться з урхуванням відомостей, залучених з «Рекомендацій…» для ДЕТ [38].

ЗВТД формується СБУ за результатами роботи постійно функціонуючого в державі інституту ДЕТ, в складі якого найбільш досвідчені фахівці із галузей оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, яким надано право віднесення відомостей до ДТ, незалежність яких забезпечує держава і які несуть персональну відповідальність за прийняті рішення [3,43].

ЗВДТ – це документ, змістовне наповнення якого, завдяки постійно функціонуючому інституту ДЕТ, забезпечує врахування сучасного рівня розвитку науки і техніки, результатів новітніх досліджень у різних сферах науки, за найбільш перспективними технологічними напрямами, : оптимізуючись під сучасні вимоги життєво важливих інтересів особи, суспільства та держави, що в свою чергу сприяє зосередженню зусиль з впровадження заходів з ОДТ на найбільш актуальних напрямках [43]. На практиці це реалізується відповідно до діючих положень і рекомендацій [38] шляхом перегляду та корекції статей чинної редакції ЗВДТ, виключенню з нього матеріалів, що вже не становлять ДТ (розсекречування відомостей), внесення нових, які містять ознаки ДТ. Наразі, слід зазначити, що рівень відомостей, вміщених у ЗВДТ, має достатньо загальну, інтегровану форму (відомості з більшим рівнем конкретизації і деталізації складають галузеві або відомчі РПВДТ або відповідні міжгалузеві чи міжвідомчі розгорнуті переліки [3]).

Саме пункти ЗВДТ утворюють ту сукупність вихідних даних, структура яких, ступінь повноти та загальнодержавний рівень узагальнення відповідає задачі формування переліку елементів державних ІР, що містять ДТ.

Як вже зазначалося, формування змісту ЗВДТ відбувається із застосуванням експертних оцінок, побудова яких спирається на рекомендовану в [38] експертно-аналітичну методику обчислення СШ від розголошення ДТ, що визначається в бальному вимірі, тобто у шкалі інтервалів, інформативність котрої вище, ніж для шкали порядку, і більш придатна для порівняльного аналізу втрат, спричинених витоком

інформації на різних ОІД. Звісно, що зазначена експертно-аналітична методика [38] в цілому не вільна від недоліків, зокрема має суттєві вади в стадії прийняття рішення за результатами обробки експертиз групи експертів [54], однак в даному випадку нас цікавить можливість використання отриманих за нею бальних оцінок втрат від розголошення ДТ для окремих елементів державних ІР, наведених у ЗВДТ. Використання цих оцінок дозволить уникнути складної і значної за обсягом роботи з аналізу розмірів можливих втрат, вже проведеної ДЕТ при складанні ЗВДТ.

На жаль, безпосередньо бальні оцінки в ЗВДТ відсутні, замість них наведено СС відомостей, внесених до ЗВДТ, визначені на базі відповідних бальних оцінок. Перехід до СС за своєю суттю є переходом до порядкової шкали з трьома градаціями: «Т», «ЦТ», «ОВ», який супроводжується неминучою втратою інформації через те, що відстань в один ранг у шкалі порядку залежить від того, між якими рангами шкали вона розрахована. Однак, завдяки наведеним в [38] даним можливе зворотне перетворення ранжованих оцінок в бальні.

До цих даних належить:

1) співставлення СС відомостей, що містять ДТ, діапазону можливих бальних оцінок втрат від розголошення ДТ: «Т» - від 1 до 10 балів, «ЦТ» - від 10 до 100 балів,, «ОВ» - 100 балів і більше;

2) категорований перелік ІТН від розголошення ДТ, упорядкований за ступенем їх тяжкості в балах з коротким описом наслідків:

Наслідки І категорії (перелік можливих наслідків) - більше 200 балів;

Наслідки ІІ категорії (перелік можливих наслідків) - 100-200 балів;

Наслідки ІІІ категорії (перелік можливих иаслідків) - 70-100 балів;

Наслідки IV категорії (перелік можливих наслідків) - 30-70 балів;

Наслідки V категорії (перелік можливих наслідків) - 10-50 балів;

3) «питома вага» в балах окремих важливих об’єктів різних сфер діяльності (оборона, економіка, державна безпека), ефективність функціонування яких у відповідній сфері в значній мірі залежить від стану ОДТ, діапазон значень «питомої ваги» (Q) - від 5 до 500 балів.

Зазначимо, що кожна позиція ЗВДТ – це елемент державних ІР, що поєднує в собі певну сукупність відомостей, зібраних разом за фаховою, галузевою, організаційною ознакою, за принципом ієрархічної підпорядкованості й т.п. і які містять ДТ. Рівень втрат від розголошення ДТ окремо для кожних з цих відомостей згідно наведених вище даних може коливатися в досить широких межах. Тому, співставивши кожному СС бальну оцінку, наприклад, середнє цілочисельне значення відповідного бального інтервалу, можемо приблизно «реставрувати» вихідні бальні експертні оцінки за кожною позицією ЗВДТ.

Для цього спершу визначимо праву межу бального інтервалу для СС «ОВ». Зважаючи на те, що найвище значення «питомої ваги» в 500 балів відповідає єдиному випадку – компрометації державних шифрів, що є дуже малоймовірною подією, доцільно проаналізувати найближчу меншу оцінку - в 300 балів. Сфера застосування цієї оцінки згідно [38] значно ширше, ніж у попередньої (оборона, економіка), тому використаємо її для визначення правої межі. Остаточно для трьох СС встановимо такі інтервали їх бальних оцінок x: «Т» ($1 \leq x_T < 10$), «ЦТ» ($10 \leq x_{ЦТ} < 100$), «ОВ» ($100 \leq x_{OB} \leq 300$), а для відповідних середніх інтервальних значень матимемо: $x_T = 5$, $x_{ЦТ} = 55$, $x_{OB} = 200$.

Вище вже зазначалося, що на базі ЗВДТ можна скласти структурно повний перелік елементів державних ІР, що містять ДТ (далі Перелік), однак в ньому будуть відсутні кількісно-об'ємні характеристики структурних елементів. Щоб пояснити, про що йде мова, наведемо зміст статті 4.11.13 редакції ЗВДТ, чинної на серпень 2006 року: "*Відомості за окремими показниками про зміст наукових відкриттів, винаходів, науково-дослідних (дослідно-конструкторських) робіт, спрямованих на підвищення рівня технічного захисту секретної інформації (протидії технічним розвідкам), володіння якими дає змогу зацікавленній стороні впливати на їх результати, що створює загрозу національним інтересам і безпеці*".

Відповідно до змісту цієї статті весь масив державних ІР, що містить відомості про зміст наукових відкриттів, винаходів, науково-дослідних (дослідно-конструкторських) робіт, пов’язані з ЗОДТ, входить елементом до структури ЗВДТ. Однак, при цьому не деталізується обсяг цих відомостей, наприклад, кількість науково-дослідних (дослідно-конструкторських) робіт, їх характеристики інше. Зважаючи на те, що кількість цих робіт може змінюватися рік від року залежно від реальних потреб держави, бюджетних ресурсів, інших умов, подібна виключно структурна форма фіксації елементів державних ІР зручна і, можливо, доцільна, бо не потребує щорічної або навіть поточної корекції. Однак, відсутність кількісно-об’ємних характеристик окремих елементів ЗВДТ не дає змоги дістати повне уявлення про вплив втрат від розголошення ДТ в цих ресурсах на рівень національної безпеки.

Внаслідок чисто механічної заміни СС «Т» цієї статті ЗВДТ на відповідний середній бал $x_T = 5$ шкоді від розголошення ДТ, що міститься в усьому означеному масиві ІР, буде співставлена оцінка саме в 5 балів, хоча реально ці 5 балів – це узагальнені втрати від розголошення секретної інформації за кожною з науково-дослідних (дослідно-конструкторських) робіт цього масиву.

Найпростіше, що можна отримати із складеного на базі ЗВДТ Переліку державних ІР, що містять ДТ, це обрахувати структуру можливих максимальних втрат, обумовлених розголошенням ДТ у сферах: (А) оборони, (Б) економіки, науки і техніки, (В) зовнішніх відносин, (Г) державної безпеки та охорони правопорядку.

Заміна СС відомостей, що входять до кожної з перелічених сфер, на відповідні середні бальні оцінки x_T = 5, $x_{ЦТ}$ = 55, $x_{ОВ}$=200 та наступне підсумовування бальних оцінок у кожній з означених сфер дає результати, наведені на рис. 25 (для цього рисунку, як і в наведеному далі розрахунковому прикладі, використано вихідні дані з [125], тому на поточний час отримані результати мають виключно ілюстративний характер).

В абсолютному вимірі, тобто в умовних балах, структура питомої шкоди від втрат СІ, що належать сферам (А), (Б), (В), (Г), має наступний вигляд: (А) - 4395 балів, (Б) - 1572 балів, (В) - 70 балів, (Г) - 8210 балів.

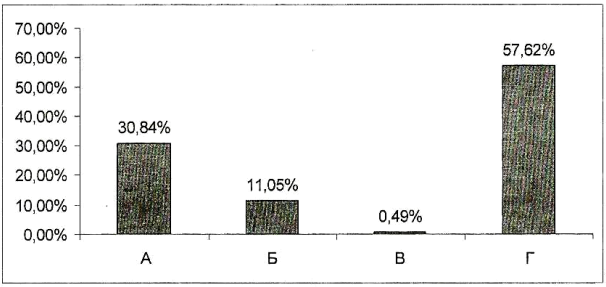


Рис. 25. Структура можливих максимальних втрат, обумовлених розголошенням відомостей, що містять ДТ в (А) - оборони, (Б) - економіці, науці і техніці, (В) - зовнішніх відносинах, (Г) - державній безпеці та охороні правопорядку

Фактично в «силових» сферах повністю зосереджені всі секретні відомості стосовно ТЗІ та КЗІ. Шкода від втрати цих відомостей становить 11,3% від максимально можливого обсягу втрат, пов'язаних з розголошенням ДТ, або 14% від максимальних втрат внаслідок розголошення ДТ в «силових» сферах.

Шкода від розголошення ДТ в відомостях, що належать до сфери інформаційних технологій (КЗІ, ТЗІ, зв'язок та телекомунікації, голографічні засоби захисту, інформаційно-аналітичні технології) сягає 20,6% від максимального обсягу втрат (1910 умовних балів), «вклад» наукових досліджень та розробок становить 11,6% (1070 умовних балів).

Зазначимо, що інформація, акумульована у ЗВДТ, достатня для деталізації структури втрат за кожною сферою. Так для сфери (Г) маємо наступні відомості:

Таблиця 10

Рубрикацію сфери (Г) за дев'ятьма складовими (Г1), (Г2), ..., (Г9), які несуть найбільшу шкоду національній безпеці

Відомості	**Оцінки втрат (бали/%)**
(Г1) про особовий склад органів, що здійснюють оперативно-розшукову, контррозвідувальну та розвідувальну діяльність	695/8,47
(Г2) про засоби, зміст, плани, організацію, фінансування та матеріально-технічне забезпечення, форми, методи та результати оперативно-розшукової, контррозвідувальної та розвідувальної діяльності; про осіб, які співпрацюють або раніше співпрацювали на конфіденційній основі з органами, що проводять таку діяльність, про склад і конкретних осіб, що є негласними штатними працівниками органів, які здійснюють таку діяльність	3785/46,1
(Г3) про організацію та порядок здійснення охорони адміністративних будинків та інших державних об'єктів, посадових та інших осіб	510/6,21
(Г4) про систему урядового та спеціального зв'язку	900/10,96
(Г5) про організацію, зміст, стан і плани розвитку криптографічного захисту СІ, зміст і результати досліджень у сфері криптографії, системи та засоби криптографічного захисту, державні шифри, їх розроблення, виробництво, технології вироблення та використання	1090/13,28
(Г6) про організацію РС в органах державної влади, місцевого самоврядування, на підприємствах, в установах; державні програми, плани та інші заходи у сфері ОДТ	515/6,27
(Г7) про організацію, зміст і результати науково-дослідних і дослідно-конструкторських робіт з розробки, створення, вдоскопалення заходів і засобів оперативно-розшукової, контрррозвідувальної та розвідувальної діяльності, методики та тактики їх застосування, відомості про їх характеристики	195/2,38
(Г8) про результати перевірок, здійснених згідно з законом прокурором, зміст матеріалів дізнання, досудового слідства та судочинства з питань державної безпеки та охорони правопорядку	330/4,02
(Г9) про інші засоби, форми і методи забезпечення державної безпеки й охорону правопорядку	190/2,31

Рубрикацію сфери (Г) за дев'ятьма складовими (Г1), (Г2), ..., (Г8), використану в табл. 10, сформовано в значній мірі відповідно до змісту пункту 4 ст. 8 Закону України «Про державну таємницю» [3].

З даних, наведених у табл. 10, очевидно, що найбільшу шкоду національній безпеці несе розголошення ДТ, що присутня у відомостях про засоби, зміст, плани, організацію, результати та певні специфічні особливості здійснення оперативно-розшукової, контррозвідувальної та розвідувальної діяльності (складова (Г2). Другим за розміром нанесеної шкоди є розголошення СІ в сфері КЗІ (складова (Г5). Порівнюючи ці складові, зазначимо, що складової (Г2) стосується 35 елементів державних ІР, що містять ДТ (або 35 статей ЗВДТ), (Г5) - лише 10 елементів, тобто питома вага шкоди, заподіяної на один елемент держресурсу, становить для (Г2) 108,1 бали, для (Г5) - 132,8 бали. Ймовірно, що елемент державних ІР, що входять до складової (Г5), є найбільш «важким» з точки зору можливих негативних наслідків втрати СІ порівняно з усіма іншими елементами державних ІР.

Об'єднання складових (Г4), (Г5) дає інформаційну складову сфери (Г), СШ від розголошення ДТ в котрій становить 24,24% від максимально можливої шкоди, заподіяною розголошенням всієї СІ в сфері (Г). Загалом, якщо порівнювати питому вагу одного елементу державного ІР в сферах (А) і (Г), то відповідно маємо: 55,6 і 76,7 умовних бали, тобто наслідки розголошення ДТ в «середньому» елементі сфери державної безпеки і охорони правопорядку більш вагомі.

Виходячи із змісту проведеного вище аналізу структури втрат, обумовлених розголошенням ДТ у сфері (Г), можна визначити умовно-бальні втрати W(Г1), W (Г2),..., W (Г9), за кожною складовою цієї сфери, кількісні значення котрих подані у табл. 10 й становлять відповідно 695, 3785, ..., 190, надалі використати їх для визначення потенційної СШ W_{Γ} у цій сфері, а також обрахувати значення коефіцієнтів важливості відповідних складових:

$$\beta_i = W(\Gamma_i) / \sum_{j=1}^{9} W(\Gamma_j),\ j = \overline{1,9}, \qquad (4.38)$$

які становитимуть: β_1=0,0847; β_2=0,461;...; β_9=0,0231.

Аналогічним чином можна виконати необхідні для аналізу ефективності СОДТ підрахунки у інших сферах і, знаючи обсяги секретних відомостей за кожною складовою, отримати всі дані, потрібні для оцінювання ефективності національної СОДТ за чотирма сферами (А), (Б), (В), (Г).

4.5. Приклад використання методики розрахунку ефективності системи охорони державної таємниці

В якості прикладу використания вищенаведеної методики проведемо розрахунок коефіцієнту ефективності СОДТ деякого об'єкту, на якому знаходяться секретені відомості у сферах оборони (А), а також безпеки та охорони правопорядку (Г).

З урахуванням Закону України «Про державну таємницю» [3], ЗВДТ [31], і умов установи визначаємо перелік відомостей *X*, що становлять ДТ у сфері безпеки та охорони правопорядку (Г). За допомогою «Рекомендацій…» [38] робимо розрахунок коефіцієнтів важливості β відомостей, що становлять ДТ у даній сфері. За результатами розрахунків формуємо таблицю 11.

Таблиця 11

Перелік відомостей, що відносяться до ДТ у сфері безпеки та охорони правопорядку, та їх коефіцієнти важливості (варіант)

x_i	**Найменування відомостей, що відносяться до державної таємниці у сфері безпеки та охорони правопорядку:**	**Коефіцієнт важливості β_i**
x_1	про особовий склад органів, що здійснюють оперативно-розшукову, розвідувальну та контррозвідувальну діяльність	0,0847
x_2	про засоби, зміст, плани, організацію, фінансування та матеріально-технічне забезпечення, форми, методи та результати оперативно-розшукової, контррозвідувальної та розвідувальної діяльності; про осіб, які співпрацюють або раніше співпрацювали на конфіденційній основі з органами, що проводять таку діяльність, про склад і конкретних осіб, що є негласними штатними працівниками органів, які здійснюють таку діяльність	0,461
x_3	про організацію та порядок здійснення охорони адміністративних будинків та інших державних об'єктів, посадових та інших осіб	0,0621
x_4	про систему урядового та спеціального зв'язку	0,1096
x_5	про організацію, зміст, стан і плани розвитку криптографічного захисту СІ, зміст і результати досліджень у сфері криптографії, системи та засоби криптографічного захисту, державні шифри, їх розроблення, виробництво, технології вироблення та використання	0,1328
x_6	про організацію РС в органах державної влади, місцевого самоврядування, на підприємствах, в установах; державні програми, плани та інші заходи у сфері ОДТ	0,0627
x_7	про організацію, зміст і результати науково-дослідних і дослідно-конструкторських робіт з розробки, створення, вдосконалення заходів і засобів оперативно-розшукової, контррозвідувальної та розвідувальної діяльності, методики та тактики їх застосування, відомості про їх характеристики	0,0238
x_8	про результати перевірок, здійснених згідно з законом прокурором, зміст матеріалів дізнання, досудового слідства та судочинства з питань державної безпеки та охорони правопорядку	0,0402
x_9	про інші засоби, форми і методи забезпечення державної безпеки й охорони правопорядку	0,0231

За допомогою експертів та з використанням результатів досліджень визначимо перелік типових загроз захищеності секретних відомостей сфери безпеки та охорони правопорядку і з використанням формул (4.20)-(4.27) розрахуємо коефіцієнти важливості ϒ загроз захищеності цих відомостей. Результати аналізу і розрахунків показані у табл. 12, 13.

Таблиця 12

Результати розрахунку коефіцієнтів важливості загроз секретних відомостей, яка відносяться до сфери безпеки та охорони правопорядку

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	Υ
β	0,0847	0,461	0,0621	0,1096	0,1328	0,0627	0,0238	0,0402	0,0231	
t_1	0.0141	0.0922		0.0219	0.0221	0.0209	0.0048	0.0101	0.0039	0.19
t_2	0.0141	0.0922	0.0207	0.0219	0.0221		0.0048		0.0039	0.18
t_3	0.0141	0.0922	0.0207	0.0219	0.0221	0.0209	0.0048	0.0101	0.0039	0.21
t_4	0.0141	0.0922		0.0219	0.0221	0.0209	0.0048	0.0101	0.0039	0.19
t_5	0.0141	0.0922	0.0207	0.0219	0.0221		0.0048	0.0101	0.0039	0.19
t_6	0.0141				0.0221				0.0039	0.04

Таблиця 13

Перелік типових загроз захищеності відомостей, що становлять ДТ у сфері безпеки та охорони правопорядку, та їх коефіцієнти важливості

tj	**Найменування типових загроз**	**Коефіцієнт важливості Υ_1**
t_1	Несанкціоноване отримання СІ зацікавленими особами у результаті порушення правил секретного діловодства і порядку допуску та доступу до МНСІ	0,2206
t_2	Отримання СІ іноземними спецслужбами у результаті агентурного проникнення	0.1896
t_3	Розголошення СІ співробітниками підприємства, установи, організації	0,2206
t_4	Втрата МНСІ співробітниками підприємства, установи, організації	0.1896
t_5	Перехоплення СІ, яка передається за допомогою засобів телекомунікації, а також через технічні канали витоку інформації, в тому числі канали побічного електромагнітного випромінювання і наводок (ПЕМВН), зокрема в мережах електроживлення технічних засобів обробки і збереження інформації	0.1896
t_6	Знищення або модифікація СІ деструктивними силовими впливами	0.1186

Використовуючи дані, що наведені у [125, 128, 145-147], визначаємо перелік завдань s_g, а також заходи (засоби і способи) m_k з усунення (нейтралізації) загроз t_j захищеності відомостей, що становлять ДТ. Результати відображаємо у таблиці 14.

Таблиця 14

Перелік типових завдань і заходів (способів) з усунення (нейтралізації) загроз захищеності відомостей,що становлять ДТ у сфері безпеки та охорони правопорядку

s_k	Найменування завдань	Перелік заходів(способів)
s_1	Унеможливлення несанкціонованого отримання СІ	m_1,m_2,m_3,m_6,m_7,m_9,m_{12},m_{13}, m_{20},m_{21},m_{23}, m_{30},m_{32},m_{47}
s_2	Попередження розголошення СІ	m_1,m_3,m_4,m_5,m_8,m_{14},m_{15}, m_{17},m_{18},m_{19},m_{20},m_{32}
s_3	Запобігання втратам МНСІ	m_1,m_2,m_5,m_6,m_7,m_8,m_{14}, m_{15},m_{17},m_{18},m_{19},m_{20},m_{32}
s_4	Запобігання агентурому проникненню до СІ збоку іноземних спецслужб	m_{22},m_{23},m_{24},m_{25},m_{26},m_{28}, m_{29},m_{30},m_{31},m_{32}
s_5	Виключення можливостей перехоплення СІ, яка передається за допомогою засобів телекомунікації, а також існує у ПЕМВН в межах електроживлення технічних засобів обробки і зберігання СІ	m_{33},m_{34},m_{35},m_{36},m_{37},m_{38}, m_{39},m_{40},m_{41},m_{42},m_{43},m_{44}, m_{45},m_{46}
s_6	Запобігання знищення або модифікація СІ деструктивними силовими впливами	m_1,m_2,m_3,m_4,m_5,m_6,m_7,m_8, m_9,m_{18},m_{21},m_{23},m_{30},m_{38},m_{42},m_{47}

Експертним методом визначаємо ефективність $P(t_j/m_k)$ заходів (засобів і способів) виконання завдань з усунення (нейтралізації) загроз захищеності ДТ. Деякі результати наведені у таблиці 15.

При цьому слід зазначити, що частина вміщених у табл. 15 даних, зокрема ті, що стосуються застосування засобів захисту інформації, мають умовний характер, бо вони наведені беззастережно до конкретних умов та мети застосування відповідних засобів і мають вельми загальне значення. Так, використання спеціальних пристроїв і фільтрів (m_{43}), залежно від того, де та з якою метою їх встановлено (наприклад, в лінії зв'язку або в лінії енергопостачання (в останньому випадку, у свою чергу, для захисту від витоку інформації або як елемент захисту від деструктивного силового впливу)), характеризується різними показниками ефективності $P(t_j/a_k)$.

Таблиця 15

Перелік можливих заходів щодо усунення (нейтралізації) загроз захищеності відомостей, що становлять ДТ у сфері ОДТ, і показників їх ефективності

m_k	**Найменування заходів (засобів і способів) щодо усунення (нейтралізації) загроз захищеності відомостей, що становлять ДТ**	**Показники ефективності $P(t_j/a_k)$**
	Організаційно-правові заходи	
m_1	Обладнання приміщень для проведення робіт,пов'язаних з ДТ, у відповідності з вимогами НД	0,95
m_2	Зберігання секретних документів та інших МНСІ у спеціальних сховищах	0,95
m_3	Недопущення необґрунтованого доступу та допуску осіб до СІ	0,85
m_4	Обізнаність персоналу з законодавством про ДТ	0,8
m_5	Своєчасне планування та реалізація заходів, що забезпечують ОДТ	0,9
m_6	Своєчасне виявлення та закриття каналів витоку СІ	0,99
m_7	Організація секретного діловодства у відповідності з вимогами НД	0,8
m_8	Здійснення контролю стану РС,своєчасне проведення комплексних,тематичних та контрольних перевірок	0,8
m_9	Обмеження доступу до ДТ іноземцям та особам без громадянства	0,75
m_{10}	Обмеження у праві виїзду за кордон громадян,яким було надано допуск та доступ до ДТ	0,6
m_{11}	Обмеження на оприлюднення СІ у пресі та інших засобах масової інформації	0,5
m_{12}	Обмеження щодо передачі СІ іноземним державам чи міжнародним організаціям	0,75
m_{13}	Обмеження щодо перебування і діяльності іноземців, осіб без громадянства та іноземних юридичних осіб, а також розташування та переміщення об'єктів і технічних засобів,що їм належить на територіях підприємств, установ і організацій, діяльності яких пов'язана з ДТ	0,75
	Контрозвідувальні та оперативно-розшукові заходи	
m_{14}	Планування та проведення інформаційно-аналітичної роботи в інтересах ОДТ	0,7
m_{15}	Проведення заходів оперативного контролю за станом РС і оцінка його ефективності	0,8
m_{16}	Проведення оперативних перевірок поінформованості громадян у ДТ	0,75
m_{17}	Оголошення офіційних зосереджень відносно розголошення СІ і втрати МНСІ	0,75

Продовження табл.15

m_{18}	Застосування відкритих заходів з попередження і припинення правопорушень у сфері ОДТ	0,75
m_{19}	Отримання фактичних даних про правопорушення у сфері ОДТ шляхом опитування осіб	0,75
m_{20}	Вчинення негласного попереджувально-профілактичного впливу на секретоносіїв	0,9
m_{21}	Затримання і утримання осіб,підозрілих у шпигунської діяльності	0,9
m_{22}	Здійснення агентурно-оперативного захисту секретоносіїв від підривних акцій спецслужб іноземних держав під час виїзду за кордон	0,9
m_{23}	Проведення режимних і агентурно-оперативних заходів на імовірних шляхах проникнення до ДТ, в оперативно-вигідних ситуаціях, на каналах зв'язку	0,85
m_{24}	Отримання інформації про спрямування,факти та ознаки розвідувальної діяльності спецслужб іноземних держав, а також про їх поінформованість про ДТ	0,85
m_{25}	Отримання первинної інформації про РПД і про осіб, підозрюваних у причетності до агентури іноземних спецслужб	0,75
m_{26}	Виявлення секретоносіїв, які мають підрозділи контакти з іноземцями або мають намір встановити зв'язок з іноземними спецслужбами	0,9
m_{27}	Отримання компрометуючих документів та даних про осіб, підозрюваних у підготовці або вчинення злочинів у сфері ОДТ	0,65
m_{28}	Оперативна розробка осіб,причетних до державної зради та шпигунства	0,5
m_{29}	Агентурне проникнення у спецслужби іноземних держав і їх агентурну мережу	0,8
m_{30}	Оперативне попередження і припинення виявленої шпигунської діяльності	0,9
m_{31}	Проведення контррозвідувальних операцій на виявлених каналах зв'язку	0,85
m_{32}	Проведення оперативних перевірок ефективності заходів з ОДТ	0,75
Заходи з технічного захисту інформації від витоку каналами ПЕМВН у лініях зв'язку, у засобах обчислювальної техніки і в автоматизованих системах		
m_{33}	Проведення заходів з блокування технічних каналів витоку СІ (ТКВІ) або встановлення схем захисту	0,99
m_{34}	Проведення заходів з блокування каналів можливого витоку СІ у системах телефонного зв'язку або встановлення найпростіших схем захисту	0,9
m_{35}	Проведення заходів з запобігання витоку СІ через діючи системи гучномовного зв'язку через радіотрансляційну мережу, що виходить за межи виділеного приміщення	0,9

Продовження табл.15

m_{36}	Проведення заході з запобігання витоку СІ через радіотрансляційну мережу, що виходить за межи виділеного приміщення	0,9
m_{37}	Відключення електронного обладнання, незахищеного технічними засобами, на період проведення заходів,що характеризуються наявністю СІ	0,99
m_{38}	Проведення заходів з блокування витоку СІ через системи електронної оргтехніки та кондиціонування на період проведення закритих заходів	0,75
m_{39}	Проведення заходів щодо захисту СІ від витоку через кола електроосвітлення та електроживлення побутової техніки на період проведення закритих заходів	0,99
m_{40}	Розміщення ОТЗ на контрольованої території в одному приміщенні або у суміжних приміщеннях	0,85
m_{41}	Встановлення ОТЗ, прокладання проводів і кабелів в екранованому приміщенні (камері)	0,95
m_{42}	Заміна незахищених ОТЗ на захищені	0,95
m_{43}	Встановлення у незахищених каналах зв'язку, лініях, проводах і кабелях спеціальних фільтрів і пристроїв	0,85
m_{44}	Виконання заходів щодо захисту СІ від витоку колами заземлення та електроживлення	0,75
m_{45}	Встановлення генераторів лінійного і просторового зашумлення	0,75
m_{46}	Заземлення всіх металевих конструкцій ОТЗ	0,75
m_{47}	Вживання заходів криптографічного захисту	0,95

Подготовлені вихідні дані концентруємо в таблиці 16 і здійснюємо розрахунок коефіцієнту захищеності відомостей, які відносяться до ДТ у сфері безпеки та охорони правопорядку.

Талиця 16

До розрахунку коефіцієнта захищеності відомостей, що належить до ДТ у сфері безпеки та охорони правопорядку

t	1	2	3	4	5	6
m_k	$m_1,m_2,m_3,m_6,$ $m_7,m_9,m_{12},$ $m_{13},m_{20},m_{21},$ $m_{23},m_{30},m_{32},$ m_{47}	$m_1,m_3,m_4,m_5,m_8,$ $m_{10},m_{11},m_{12},m_{14},$ $m_{15},m_{16},m_{17},m_{18},$ $m_{19},m_{20},m_{22},m_{27},$ m_{32}	$m_1,m_2,m_5,$ $m_6,m_7,m_8,$ $m_{14},m_{15},m_{17},$ $m_{18},m_{19},$ m_{20},m_{32}	$m_{22},m_{23},m_{24},$ $m_{25},m_{26},m_{28},$ $m_{29},m_{30},m_{31},$ m_{32}	$m_{33},m_{34},m_{35},$ $m_{36},m_{37},m_{38},$ $m_{39},m_{40},m_{41},$ $m_{42},m_{43},m_{44},$ m_{45},m_{46},m_{47}	$m_{41},$ $m_{42},$ $m_{43},$ m_{46}
P	0,9	0,98	0,91	0,84	0,85	0,9
Υ	0,19	0,18	0,21	0,19	0,19	0,04
$K_{зі\ Г}$	**0,88**					

У кожній комірці першого рядка табл. 16 наведено сукупності заходів та засобів, що можуть бути застосовані для нейтралізації відповідної загрози t_j (номер комірки співпадає з індексом загрози). З кожної комірки вибирається конкретна сукупність заходів, що мають бути застосовані для нейтралізації *j*-тої загрози захищеності відомостей, у відповідність кожному з яких ставиться згідно із переліком (4.30) сукупність показників ефективності їх застосування. Далі за цими показниками, згідно формули (4.31), розраховуються (вираз (4.32)) елементи вектора *P*.

Наприклад, обравши з повного переліку заходів, що забезпечують усунення (нейтралізацію) загрози t_6, сукупність заходів m_{43}, m_{46} за формулою (4.31) отримаємо: $P(t_6 / m_{43}, m_{46}) = 0{,}9625$. В разі застосування сукупності заходів m_{41}, m_{43} маємо $P(t_6 / m_{41}, m_{43}) = 0{,}9925$; а в разі m_{41}, m_{42}, m_{43} – $P(t_6 / m_{41}, m_{42}, m_{43}) = 0{,}999625$. Розраховані таким чином складові вектора *P* заносяться до відповідної комірки. Якщо припустити, що складові вектора *P*, обчислені аналогічним чином, набули значень наведених у табл. 16, маємо за результатами розрахунків $K_{зі\ Г} = 0{,}88$. За аналогічними розрахунками у сфері оборони $K_{3i\ A} = 0{,}812$.

З використанням «Рекомендацій…» [38] і ЗВДТ [31] розрахуємо розмір можливих максимальних втрат W_N, обумовлених розголошенням СІ у сфері оборони (А) і у сфері безпеки та охорони правопорядку (Г). Якщо припустити, що обсяги СІ за всіма складовими цих сфер однакові і дорівнюють *q*, за результатами розрахунків $W_A = q4395$ балів, $W_Г = q8210$ балів.

З використанням формули (4.16) розрахуємо коефіцієнт ефективності СОДТ у сферах оборони і безпеки та охорони правопорядку. За результатами розрахунків $K^{СОДТ} = 0{,}856$.

Здійснюємо порівняння розрахованого значення $K^{СОДТ}$ з тими, що наведені у табл. 9. Аналіз отриманих результатів показує, що у нашому випадку стан ОДТ у сферах оборони і безпеки та охорони правопорядку відповідає вимогам (охорона забезпечена повністю, можливості розголошення СІ або/та втрати МНСІ практично не існує). Якщо у результаті розрахунків $K^{СОДТ} \le 0{,}81$, тобто стан ОДТ відповідає вимогам у цілому (охорона забезпечена у цілому, але є можливість розголошення СІ або/та втрати МНСІ), то для досягнення стану ОДТ, який вимагається, необхідно додатково провести заходи, що мають більшу ефективність ніж ті, для яких проведено дані розрахунки. Після чого розрахунки треба повторити знову, доки показник стану ОДТ $K^{СОДТ}$ не буде задовольняти встановленим вимогам.

Розділ 5. МОДЕЛІ ТА МЕТОДИ ОЦІНЮВАННЯ ШКОДИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ У РАЗІ ВИТОКУ ДЕРЖАВНОЇ ТАЄМНИЦІ

5.1. Моделі оцінювання шкоди національній безпеці України у разі витоку державної таємниці

Класифікація інформації з обмеженим доступом

Для ефективного управління важливе значення має режим доступу до інформації. Це передбачений правовими нормами порядок одержання, використання, поширення, зберігання, використання, поширення, охорона та захист інформації. Слід мати на увазі, що держава здійснює контроль за режимом доступу до інформації. Завданням його є забезпечення дотримання вимог законодавства про інформацію всіма державними органами, підприємствами, установами та організаціями, недопущення необґрунтованого віднесення відомостей до категорії ІзОД, адже захист цієї інформації є одним з першочергових завдань забезпечення інформаційної безпеки.

Як відомо, обмеження доступу до інформації здійснюється відповідно до закону при дотриманні сукупності таких вимог [11]:

- виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоровя населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;
- розголошення інформації може завдати істотної шкоди цим інтересам;
- шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

За [3, 9, 12, 13, 148-162] виділимо множину причинно-наслідкових і просторово-часових характеристик та ознак інформації (***F***), що стали основною для побудови ***схеми узагальненої класифікації інформації*** за визначеним порядком та ступенем обмеження доступу до видів ІзОД, зокрема, таємної (рис. 26): за порядком доступу (f_1); за правовим режимом (f_2); за правом доступу (f_3); за видом таємниці (f_4); за грифом обмеження доступу МНІ (f_5); за ступенем секретності (f_6); за видом діяльності (f_7).

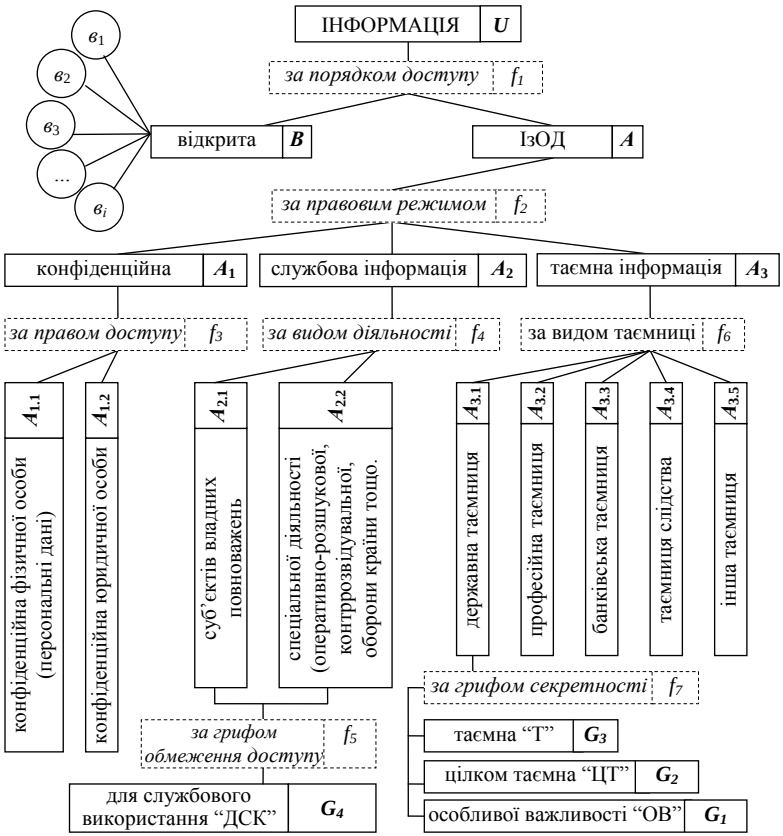


Рис. 26. Схема логіко-правової класифікації інформації за визначеним порядком та режимом обмеження доступу

Інформація (***U***) за f_1 поділяється на відкриту (***B***) та ІзОД (***A***) [161, 162]:

$$U = f_1(B, A),$$

де ***B*** (*відкрита інформація*) – вся інформація, крім тієї, що віднесена до ІзОД; ***A*** (*ІзОД*) – є такою, що шкода від її оприлюдненні переважає суспільний інтерес в її отриманні і становить загрозу національній безпеці, обороні, запобігання злочину тощо.

A_1 за f_3 поділяється на інформацію фізичної особи (персональні дані) ($A_{1.1}$) та юридичної особи ($A_{1.2}$), що виражається як [161, 162]:

$$A_1 = f_3(A_{1.1}, A_{1.2}),$$

де $A_{1.1}$ (*персональні дані*) – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована; $A_{1.2}$ (*конфіденційна юридичної особи*) – інформація, яка міститься в договорах, контрактах, листах, звітах, аналітичних матеріалах, виписках з бухгалтерських рахунків, схемах, графіках, специфікаціях і інших документах, що фігурують в діяльності юридичної особи і, у разі їх розголошення, може бути використано конкурентами для завдання економічної та іншої шкоди.

До A_2 за f_4 може належати інформація $A_{2.1}$ та $A_{2.2}$, що наведено виразом [161, 162]:

$$A_2 = f_4(A_{2.1}, A_{2.2}),$$

$$A_2 = \bigcup_{\beta=2} \bigcup_{\rho=1}^{m} A_{\beta.\rho}, \ \rho = \overline{1, m}.$$

A_3 визнається інформація, яка за f_6 містить державну ($A_{3.1}$), професійну ($A_{3.2}$), банківську таємницю ($A_{3.3}$), таємницю слідства ($A_{3.4}$) та іншу передбачену законом таємницю ($A_{3.5}$) [161, 162]:

$$A_3 = f_6(A_{3.1}, A_{3.2}, A_{3.3}, A_{3.4}, A_{3.5}),$$

$$A_3 = \bigcup_{\beta=3} \bigcup_{\rho=1}^{m} A_{\beta.\rho}, \ \rho = \overline{1, m},$$

де $A_{3.1}$ (*ДТ*) – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у встановленому порядку ДТ і підлягають охороні державою. Тлумачення інших видів таємної інформації наводиться законодавством.

Сегментом обмеженої класифікації інформації є відомості, що не можуть бути віднесені до $A_{3.1}$ та A, тобто відносяться до множини B = {*відкрита*} інформація. До них належать відомості [3, 9, 12, 13, 148-162]: про стан довкілля, якість харчових продуктів і предметів побуту ($в_1$); про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей ($в_2$); про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення ($в_3$); про факти

порушення прав і свобод людини і громадянина (***в₄***); про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб (***в₅***); інші відомості (***в₆***), доступ до яких не може бути обмежено відповідно до законів та міжнародних договорів України, згода на обов'язковість яких надана ВРУ; про розміри, види благодійної та іншої допомоги, що надається фізичним та юридичним особам чи одержується від них особами, що є суб'єктами відповідальності за корупційні правопорушення (***в₇***); розміри, види оплати праці зазначених осіб, а також одержані цими особами за правочинами, які підлягають обов'язковій державній реєстрації, дарунки (пожертви) (***в₈***); про розпорядження бюджетними коштами (***в₉***), володіння, користування чи розпорядження державним, комунальним майном (***в₁₀***), у тому числі до копій відповідних документів, умови отримання цих коштів чи майна, прізвища, імена, по батькові фізичних осіб та найменування юридичних осіб, які отримали ці кошти або майно; декларації про доходи осіб та членів їхніх сімей, які: претендують на зайняття чи займають виборну посаду в органах влади (***в₁₁***); обіймають посаду державного службовця, службовця органу місцевого самоврядування першої або другої категорії (***в₁₂***) та інші (***вᵢ***). Такі відомості можна об'єднати у наступний вираз [161, 162]:

$$B = \bigcup_{\alpha=1}^{i} в_{\alpha},\ \alpha = \overline{1, i},\ \ в \notin A.$$

Результатом проведення даної класифікації інформації є можливість визначення із універсальної множини ***U*** окремих видів інформації, що за нормативною складовою наносять шкоду особі ***A₁***, суспільству ***A₂*** та державі ***A₃*** у разі їх втрати, і тому їх віднесено до ІзОД ***A*** [161, 162]:

$$A = \bigcup_{\beta=1}^{h} \bigcup_{\rho=1}^{m} A_{\beta,\rho},\ \beta = \overline{1,3},\ \rho = \overline{1, m},\ A \notin B.$$

За основними видами ІзОД як реальної та потенційної загрози в інформаційній сфері для національної безпеки держави і тієї, що може міститися на матеріальних носіях і стати об'єктом для протиправних посягань (зокрема, і кібератак), є такі види як: *службова* A_2 (***A₂.₁, A₂.₂***) та *таємна* A_3 (***A₃.₁***) інформація.

Документам та іншим МНІ, що містять інформацію ***A₂*** за f_5 присвоюється гриф обмеження доступу ДСК (G_4) [161, 162]:

$$G_4(ДСК) = f_5(A_2).$$

Зокрема, МНСІ, у яких розміщена $\boldsymbol{A_{3.1}}$, за f_7 бувають «Т» (G_3), «ЦТ» (G_2) і «ОВ» (G_1) [161, 162]:

$$\underset{g=1}{\overset{3}{G}}(ОВ, ЦТ, Т) = f_7(A_{3.1}).$$

Законодавчо визначено, що A_2 і $A_{3.1}$ повинні мати встановлені щодо їх МНІ реквізити обмеження доступу, а саме G_4 для A_2 та G_3, G_2, G_1 для $A_{3.1}$. І навпаки, наявність реквізиту обмеження доступу на МНІ чи на його супровідному листі, дає змогу ідентифікувати вид ІзОД.

Тобто, має місце ***твердження***: МНІ без реквізиту обмеження доступу ($G_i = 0$) містять відкриту $\boldsymbol{B}$ інформацію, інакше ($G_i = 1$) – ІзОД $\boldsymbol{A}$, що можна виразити наступною закономірністю [161, 162]:

$$f_1(U) = A \text{ якщо } f_2(A) = A_2 \text{ при } f_5(G_4) = 1,$$

або

$$f_1(U) = A \text{ якщо } f_2(A) = A_3, \text{ яка за } f_6(A_3) = A_{3.1} \text{ при } f_7(G_i) = 1, i = \overline{1, 3},$$

інакше

$$f(U) = B \text{ при } f(G_i) = 0, i = \overline{1, 4}.$$

Далі проводиться подальша сегментна обмежена класифікація множин $\boldsymbol{A_2}$ та $\boldsymbol{A_{3.1}}$ відносно окремих переліків СлІ чи ЗВДТ.

Тому, обмеження доступу до них є своєчасним і адекватним заходом захисту національних інтересів держави збоку СРСД.

Модель складної орієнтованої інформаційної мережі Зводу відомостей, що становлять державну таємницю

Звід відомостей, що становлять державну таємницю (далі- ЗВДТ) – акт, в якому зведено переліки відомостей, що згідно з рішеннями ДЕТ становлять ДТ у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку [3] та є єдиною формою реєстрації цих відомостей в Україні [31].

З моменту опублікування ЗВДТ держава забезпечує захист і правову охорону відомостей, які зареєстровані в ньому. Реєстрація відомостей у ЗВДТ є підставою для надання документу, виробу чи іншому МНІ, що містить ці відомості, ГС, який відповідає СС, установленому для них у ЗВДТ [31].

У зв'язку з цим постає важливе завдання, яке полягає в оцінюванні відповідності змісту відомостей на МНСІ до змісту статей ЗВДТ. З

огляду на те, що сучасні наукові публікації [42-50] дуже обмежено висвітлюють методику використання ЗВДТ, актуальним виявляється питання розгляду цього акту у якості моделі засобу забезпечення сфери ОДТ. Такий вибір пояснюється наступними обставинами: відомості вважається ДТ з часу опублікування ЗВДТ, до якого вона включена; ЗВДТ наводить зміст відомостей, що становлять ДТ, їх СС, термін засекречування та реєстраційний номер і дата рішення ДЕТ (як відомо, СС відомостей, що становлять ДТ, визначає інтервал можливих бальних значень прогнозованої величини СШ національній безпеці відповідно до критеріїв її визначення за виразами (1.4)-(1.6)); після опублікування ЗВДТ дотримання вимог ОДТ за цим переліком стає обов'язковим.

Застосувавши основи теорії складних мереж та теорії графів [163-166], проведено моделювання ЗВДТ у якості складної орієнтованої інформаційної мережі (далі – СОІМ).

Розроблена ***модель СОІМ ЗВДТ*** за принципом онтологічної ієрархії цінності структури [102-107], яка зводиться до поступової конкретизації класу, групи, підгрупи відомостей, близьких за певними характеристиками до об'єкта ДТ, послідовно звужуючи до прийнятного обсягу множину базових (встановлених) відомостей, призначених до порівняльного зіставлення з новими, розміщеними на МНІ. Зазвичай така схема складається зі структури даних, які містить усі релевантні класи об'єктів, їх точні специфікації для певної предметної області, зв'язки і правила (теореми, обмеження), прийняті в цій області, тобто все те, що визначає її орієнтацію.

Онтологічна цінність структури СОІМ ЗВДТ визначається наступними рівнями ієрархії [106]:

– *перший рівень* (предметна область) – зведений перелік усіх відомостей (***PV***), що становлять ДТ (***A*** $_{3.1}$) (див. рис. 26);

– *другий рівень* (класи) – сфери (***N***) відомостей, що становлять ДТ, а саме: 1 – оборони; 2 – економіки, науки і техніки, 3 – зовнішніх відносин; 4 – державної безпеки і охорони правопорядку;

– *третій рівень* (групи) – сукупності відомостей (***N.i***), споріднених за певною темою чи близьких за певними характеристиками до об'єкта ДТ у межах однієї сфери *N*;

– *четвертий рівень* (стаття) – відомості, що становлять ДТ (***N.i.j***), які входять до складу певної *i*-ї групи у межах окремої сфери *N*. Позначаються як $PV_{N.i.j}$ і визначаються за номером у ЗВДТ, наприклад, 1.9.9, зміст якої приведено у табл. 17;

– *n'ятий рівень* – наявна *n* кількість об'єктів ($O_{N.i.j}$) відомостей $PV_{N.i.j}$;

– *шостий рівень* – належність *m* показників ($I_{N.i.j}$) до об'єктів $O_{N.i.j}$ відомостей $PV_{N.i.j}$; *сьомий рівень* – встановлена **СС** (Т, ЦТ, ОВ) цих відомостей $PV_{N.i.j}$ та термін (***T***) їх необхідного зберігання і охорони.

Таблиця 17

***Звід відомостей, що становлять ДТ* (*уривок* [31])**

Номер статті ЗВДТ	Зміст відомостей, що становлять державну таємницю	Ступінь секретності	Строк дії рішення про віднесення інформації до ДТ (у роках)	Суб'єкти режимно-секретної діяльності, держаними експертами яких прийняті рішення про віднесення інформації до ДТ
1	2	3	4	5
	1. Сфера оборони (*N=1*)			
1.9.9	Відомості про бойові можливості, основні тактико-технічні характеристики, результати випробувань зразків (систем, комплексів або складових цих зразків) озброєння чи військової техніки або боєприпасів, які перебувають (плануються) в експлуатації (зберіганні) у військах. При засекречуванні ССвстановлюється і змінюється за рішенням ДЕТ – (*N=1, i=9*)			МО
	за сукупністю всіх показників щодо окремого зразка (системи, комплексу або складових цих зразків) озброєння чи військової техніки, або боєприпаси – *(N=1, i=9, j=9 (1)).*	ЦТ Т	10 5	
	за окремими показниками щодо окремого зразка (системи, комплексу або складових цих зразків) озброєння чи військової техніки, або боєприпаси – *(N=1, i=9, j=9 (2)).*	Т	5	

Інтерес становить можливість врахування у моделі СОІМ ЗВДТ так званих у ЗВДТ «допоміжних слів» (за окремими показниками, за сукупністю всіх показників та ін. [31]), за допомогою яких висуваються умови (*if, then*) до показників $I_{N.i.j}$, які ідентифікують об'єкт $O_{N.i.j}$ або

СЧО, що впливає на визначення СС за цими відомостями $PV_{N.i.j}$, тобто виникає *додатковий рівень* ієрархії онтологічної структури цінності.

Отже, онтологічної цінності структури СОІМ ЗВДТ визначається за упорядкованістю (підпорядкованістю) основних, допоміжних та деталізуючих інформаційних рівнів (вузлів) ієрархії, що показано на рис. 27 відповідними стрілками, а саме як [106]:

$$\boldsymbol{PV}\,(A_{3.1}) \rightarrow \boldsymbol{N} \rightarrow \boldsymbol{N.i} \rightarrow \boldsymbol{N.i.j} \rightarrow \boldsymbol{O}_{N.i.j} \rightarrow \boldsymbol{I}_{N.i.j}(\textit{if, then}) \rightarrow \boldsymbol{CC}\ (\text{Т, ЦТ, ОВ}).$$

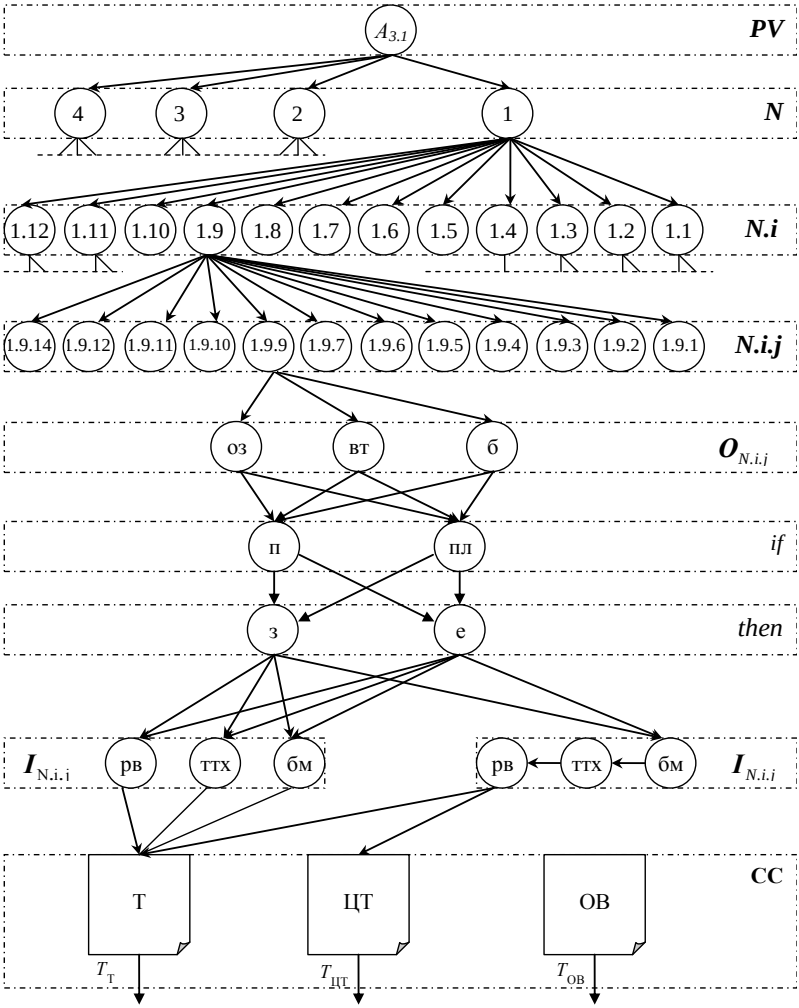


Рис. 27. Модель СОІМ статті 1.9.9 ЗВДТ

Для дослідження змісту, основних характеристик, умов та наявності використання «допоміжних слів», на прикладі використано статтю 1.9.9. ЗВДТ (див. табл. 17), яка має наступну орієнтацію онтологічної ієрархії цінності своєї структури (див. рис. 27), а саме як [106]: *PV* ($A_{3.1}$) → *N*=1 (сфера оборони)→ *N.i* = 1.9 (9-та група статей у сфері оборони) → *N.i.j* = 1.9.9 (стаття) → $O_{1.9.9.n}$ (об'єкти) при *n* = 3 наступні: $O_{1.9.9.1}$ – озброєння (оз) (системи, комплексу або складових цих зразків); $O_{1.9.9.2}$ – військова техніка (вт); $O_{1.9.9.3}$ – боєприпаси (б) → $I_{1.9.9.m}$ (показники) при *m* = 3 слідуючи: $I_{1.9.9.1}$ – бойові можливості (бм), $I_{1.9.9.2}$ – тактико-технічні характеристики (ттх), $I_{1.9.9.3}$ – результати випробувань (рв) → умови (*if, then*), а саме: if_1 – перебувають (п), if_2 – плануються (пл), $then_1$ – в експлуатації (е), $then_2$ – в зберіганні (з) → СС (Т, ЦТ).

Така ієрархія СОІМ $PV_{1.9.9}$ дозволяє визначати множину об'єктів $O_{1.9.9.n} \in \{O_{1.9.9.1}, O_{1.9.9.2}, O_{1.9.9.2}\}$ та їх показників $I_{1.9.9.m} \in \{I_{1.9.9.1}, I_{1.9.9.2}, I_{1.9.9.3}\}$ відомостей, що віднесені до ДТ за статтею 1.9.9 ЗВДТ. Тому, вживання у статтях так званих «допоміжних слів» встановлюють умови до повної або часткової ідентифікації сукупності множини об'єктів $O_{N.i.j}$, їх показників $I_{N.i.j}$ або СЧО відомостей $PV_{N.i.j}$. Це дає можливість створити їх бази даних і, використовуючи операції $\bigcup$(АБО) і $\bigcap$(ТА), отримати систему логічних висловів та сформувати набір можливих правил для побудови апарату логіки блоку виводу попереднього результату експертизи МНІ за [112-114].

Отже, ***СОІМ ЗВДТ*** ($\boldsymbol{PV}_{N.i.j}$) – це зосереджений у складну мережу за визначеними *N* сферами ІР *PV*, що складається з окремих тематичних *N.i* груп (кліків мережі) шляхом упорядкування за визначеною орієнтацією окремих її елементів *N.i.j* з врахуванням певних умов (*if, then*) до об'єктів $O_{N.i.j}$ та їх показників $I_{N.i.j}$, які виникли у результаті наявності «допоміжних слів».

Модель складної орієнтованої інформаційної мережі Переліку відомостей, що становить службову інформацію

Перелік відомостей, що становлять службову інформацію (ПСлІ) – це акт, в якому зведено у категорії відомості, що становлять СлІ,

складений окремим органом державної влади, органами місцевого самоврядування, іншими суб'єктами владних повноважень за певними сферами їхньої діяльності. Документам, що містять інформацію, яка становить СлІ, присвоюється гриф ДСК на підставі ПСлІ, який складається органами державної влади, органами місцевого самоврядування, іншими суб'єктами владних повноважень, у тому числі на виконання делегованих повноважень, не може бути обмеженим у доступі [11, 148].

Обмеження доступу до інформації, що включається до ПСлІ, відбувається при дотриманні сукупності *вимог* [11]: виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя; розголошення інформації може завдати істотної шкоди цим інтересам; *шкода* від оприлюднення такої інформації *переважає суспільний інтерес* в її отриманні.

Розглянемо на прикладі СлІ (***A*****2.2**), що зібрана в процесі спеціальної діяльності у сфері оборони, яку не віднесено до ДТ (A_3), але включено до ПСлІ Збройних Сил України (далі – ЗСУ) [167, 168].

Розроблено ***модель ПСлІ ЗСУ*** за принципом створення СОІМ ЗВДТ, де онтологічна цінність структури СОІМ ПСлІ ЗСУ визначена наступними рівнями ієрархії [168]:

– *перший рівень* – узагальнений перелік відомостей (***SI***), що становлять СлІ ($A_{2.2}$) у сфері оборони (*N*=1) (див. рис. 26);

– *другий рівень* – тематичні розділи (***R***), як класи у структурі ранжованої шкали деталізації предметної множини *SI*;

– *третій рівень* – статті (***R.l***) *R*-го розділу відомостей, що становлять СлІ, позначаються як $SI_{R.l}$ і визначені номером у ПСлІ ЗСУ, наприклад, стаття 1.1.;

– *четвертий рівень* – визначена *n* кількість об'єктів ($O_{R.l.n}$) відомостей, що становлять $SI_{R.l}$;

– *n'ятий рівень* – визначена *m* кількість показників ($I_{R.l.m}$) об'єктів $O_{R.l.n}$ відомостей $SI_{R.l}$, а також наявність умови (*if, then*) їх належності як «за окремими показниками» та/або «за сукупністю всіх показників» тощо;

– *шостий рівень* – ступінь обмеження доступу (СОД) «ДСК».

Наприклад, проведемо дослідження змісту розділу 16 статті 16.1 на упорядкованість інформаційних елементів для формування онтологічної цінності структури та моделювання СОІМ ПСлІ, що показано на рис. 28 [168]:

16. Охорона ІзОД [167] – $R=16$:

$$SI_R=\sum_1^l SI_{R.l}, R=16, l=\overline{1,7}.$$

16.1. Відомості *за окремими показниками* про планування ($I_{16.1.1}$), організацію запровадження заходів ($I_{16.1.2}$), фактичний стан ($I_{16.1.3}$), наявність недоліків ($I_{16.1.4}$) щодо ОДТ ($O_{16.1.1}$) [167] – $R=16, l=1$:

$$SI_{R.l}=O_{R.l.n}\bigcap_1^m I_{R.l.m}, R=16, l=1, n=1,\ m=\overline{1,4}.$$

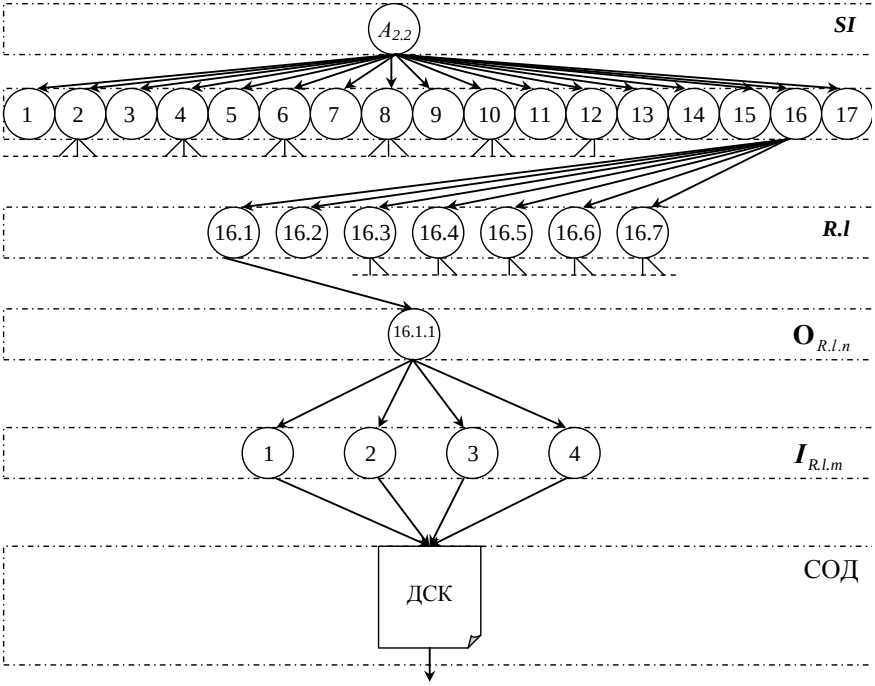


Рис. 28. Модель СОІМ статті 16.1 ПСлІ ЗСУ

Принцип створення моделі СОІМ ПСлІ ЗСУ
та ідентифікація її елементів

Модель СОІМ ПСлІ формує клас {*SI*} досліджуваних *n* об'єктів $O_{R.l.n}$ сукупності *m* морфологічних класифікаційних ознак (показників $I_{R.l.m}$), що характеризують найбільш суттєві структурні особливості представників досліджуваного класу об'єктів («за окремими показниками», «за сукупністю показників») та завдання для кожного з цих параметрів на множині його можливих значень – відомості розділу (*R*) та статті (*l*).

Перелік або множина (***SI***) являє собою сукупність роділів (***R***), кожний з яких – це кортеж з *l* статей, по одному з відповідному вихідного морфологічного простору: з $SI_{1.1.}$, з $SI_{1.2.}$, …, з $SI_{1.l}$. Даний ПСлІ включає кортежі, які обіймають комбінації значень класифікаційних ознак (показників $I_{R.l.m}$), утворюючи морфологічну скриню – спільний морфологічний простір $\{SI_{R.l}\}$ для всього класу обєктів $O_{R.l.n}$ як [168]:

$$\{SI_{R.l}\} = \{SI_{1.l}, SI_{2.l}, SI_{3.l} ..., SI_{17.q}\}, R = \overline{1,17}, \; l = \overline{1,q},$$

де $\{SI_{R.l}\}$ – морфологічний простір *R*-го розділу *l*-х статей *SI*.

Далі для формування ПСлІ ЗСУ визначається декартів або прямий добуток морфологічних просторів усіх ознак [168]:

$$\boldsymbol{SI} = \{SI_{1.l}\} \times \{SI_{2.l}\} \times \{SI_{3.l}\} \times ... \times \{SI_{17.q}\}, \; l = \overline{1,q}.$$

Отже, ***модель СОІМ ПСлІ ЗСУ*** ($\boldsymbol{SI}_{R.l}$) – це зосереджений у складну мережу у сфері оборони інформаційний ресурс *SI*, що складається з окремих тематичних *R* груп (кліків мережі) шляхом упорядкування за визначеною орієнтацією окремих її елементів *R.l* з врахуванням певних умов (*if, then*) до об'єктів $O_{R.l.n}$ та їх показників $I_{R.l.m}$, які виникли у результаті наявності «допоміжних слів».

Модель оцінювання шкоди національній безпеці
як складова експертизи матеріальних носіїв інформації

Для запобігання виникнення реальної та потенційної загрози національній безпеці в інформаційній сфері, а саме розголошення ІзОД [1], проводяться експертизи МНІ на предмет наявності або відсутності у них відомостей, що становлять ДТ, що є одним із завдань суб'єкта режимно-секретної діяльності (СРСД) під час провадження діяльності, пов'язаної з ОДТ [32].

Експертиза – організоване ДЕТ комплексне вивчення МНІ на предмет наявності чи відсутності у них відомостей, що становлять ДТ, їх достовірності, актуальності та повноти, визначення ступеня обмеження доступу до цих відомостей, встановлення та обґрунтування шкоди, яка може бути завдана державним інтересам внаслідок їх витоку [32].

Проводиться за ініціативою ДЕТ, звернення СРСД у випадках [32]: втрати МНСІ; розголошення відомостей, що становлять ДТ; надання МНІ іноземній державі, міжнародній організації чи її представникам.

За результатами її проведення у експертному висновку окрім даних про ДЕТ, ініціатора, пропозицій ЕК, також зазначаються [32]: 1) повні ідентифікаційні ознаки матеріалів експертизи (назва, дата, реєстраційний номер, ГС, номер примірника носія інформації); 2) назви та вид МНІ, їх реєстраційні номери, сторінка, пункт, абзац та інші дані, які містять відомості, що становлять ДТ; 3) до якої сфери забезпечення життєдіяльності належить інформація, яку віднесено до ДТ; 4) стаття ЗВДТ, під дію якої підпадає інформація, що становить ДТ; 5) СС інформації; 6) коротке описання інформації, розголошення якої може завдати шкоди національній безпеці; 7) обставини розголошення інформації, за яких може бути завдано шкоди національній безпеці; 8) *обґрунтування шкоди національній безпеці* України, яку може завдати (чи вже завдав) витік інформації, що міститься у матеріалах експертизи (наслідки витоку цієї інформації).

Проведемо аналіз можливості отримання зазначених у п. 1-8) даних для формування експертного висноку. Зокрема за п.1-2) наводиться вичерпний перелік відомостей, який слід зазначити і особливих труднощів в їх отриманні не виникає. Отримання необхідної інформації за п.3-6) зводяться до прямого використання Закону України «Про державну таємницю» [3] та ЗВДТ [31] як основних нормативно-правових документів, де визначено, що у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку може належати інформація, яку віднесено до ДТ. Також у ЗВДТ наведено перелік та номери статей за якими зареєстровані відомості, що становлять ДТ, їх СС та короткий опис (зміст статей).

Що ж стосується обставин за п.7), то вони визначаються за наявністю реальних та потенційних загроз в інформаційній сфері [1], переліком можливих подій-загроз [125], що приводять до порушень у порядку організації та забезпечення РС СРСД і ефективності діяльності СОДТ. У цілому виникають питання до п.8) в обґрунтуванні можливої шкоди національній безпеці, що потребує більш детального аналізу.

З метою узагальнення отриманих ідентифікуючих і оціночних параметрів СОІМ ЗВДТ та СОІМ ПСлІ розроблено ***модель оцінювання шкоди національній безпеці як складова експертизи МНІ***, яку приведено на рис. 29.

Модель представляє собою сукупність моделей, методів та методик, лінгвістичних регуляторів та лінгвістичних регуляторів вибору, баз даних та знань, взаємопов'язаних і взаємодіючих із ЕК при ДЕТ під час підготовки, прийнятті і контролі виконання управлінських рішень щодо необхідності вжиття додаткових заходів, спрямованих на охорону МНІ, у разі наявності у них відомостей, що становлять ДТ. Дана процедура здійснюється на основі ЗВДТ або РПВДТ [3]. Якщо відомості не становлять ДТ відповідно до прийнятого ДЕТ рішення, то вони вивчаються на предмет їх віднесеності до СлІ з наданням СОД «ДСК» за визначеним ПСлІ на підставі постанов Уряду [19, 26-29, 36, 37].

До складу моделі входять (рис. 29) [168]:

– *методики* (**МК**) оцінювання інформації (***U***): МК 1 – відкритої (***B***) та ІзОД (***A***), МК 2 – конфіденційної (A_1), МК 3 – таємної (A_3), МК 4 – службової (A_2) (див. рис. 26);

– *лінгвістичні регулятори* (**ЛР**) (закони України): ЛР 1 – «Про інформацію» [9], ЛР 2 – «Про захист персональних даних» [13], ЛР 3 – «Про державну таємницю» [3], ЛР 4 – «Про доступ до публічної інформації» [11] тощо;

– *лінгвістичний регулятор вибору* (**ЛРВ 1**) СлІ ($A_{2.2}$) спеціальної діяльності (оборони країни, контррозвідувальної, оперативно-розшукової) чи ДТ ($A_{3.1}$) – накази СБ України (наприклад, [32]);

– *бази знань* (**БЗ**): БЗ 1 – ЗВДТ (РПВДТ); БЗ 2 – ПСлІ;

– *моделі* (**МЛ**) засобів оцінювання: МЛ 1 – СОІМ ЗВДТ, МЛ 2 – СОІМ ПСлІ;

– *бази даних* (**БД**): БД 1.1 – об'єктів ($O_{N.i.j}$) відомостей ЗВДТ ($PV_{N.i.j}$), БД 1.2 – показників ($I_{N.i.j}$) об'єктів відомостей ЗВДТ, БД 2.1 – об'єктів ($O_{R.l}$) відомостей ПСлІ ($SI_{R.l}$), БД 2.2 – показників ($I_{R.l}$) об'єктів відомостей ПСлІ;

– *методи* (**МД**) оцінювання шкоди національній безпеці: МД 1 – у

разі розголошення ДТ чи втрати МНСІ ($W_{PV_{N.i.j}}$), МД 2 – у разі розголошення СлІ або втрати матеріальних носіїв СлІ ($W_{SI_{R.l}}$).

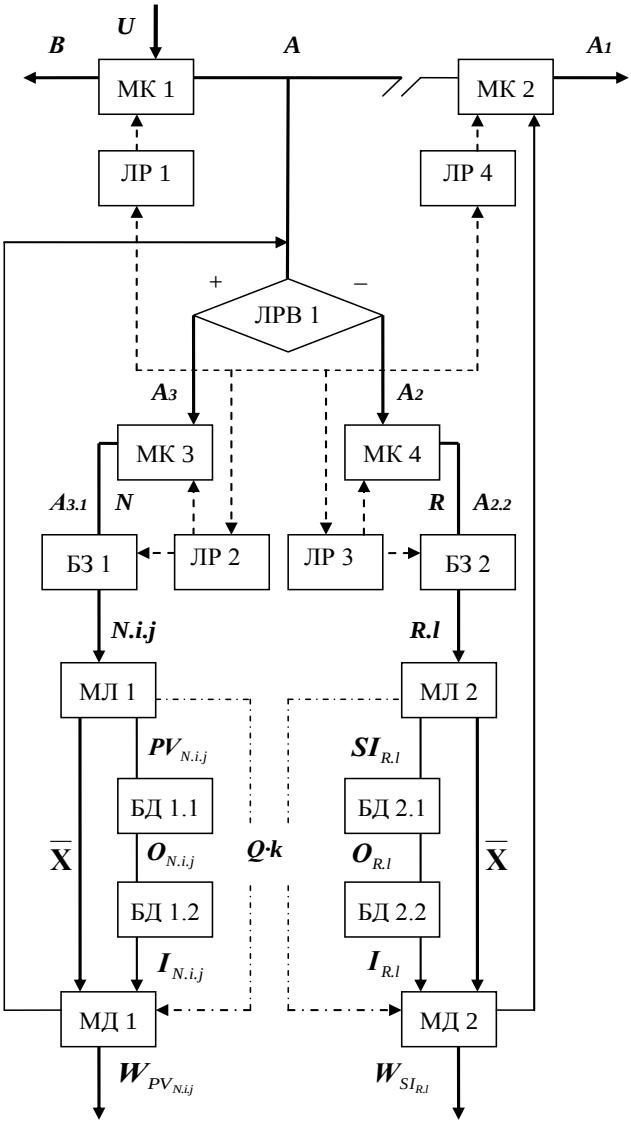


Рис. 29. Модель оцінювання шкоди національній безпеці як сладова експертизи МНІ

Основними задачами *методики оцінювання відкритої* ***B*** та ІзОД ***A*** (МК 1) є [168]: визначення відомостей до яких обмеження у доступі забороняється вимогами чинного законодавства; визначення інших відомостей, що потенційно можуть становити *A*.

Дані за даною МК 1 використовуються для визначення із загальної сукупності відомостей *U*, які розміщені на МНІ тих, що визначені законодавством як *B* або *A*.

До основних задач методики оцінювання конфіденційної $\boldsymbol{A_1}$ інформації (МК 2) відносяться [168]:

- виявлення конфіденційної A_1 інформації фізичної особи – персональні дані $A_{1.1}$;
- виявлення конфіденційної A_1 інформації юридичної особи $A_{1.2}$: 1) конфіденційної інформації, що є власністю держави $A_{1.2.1}$; 2) інша конфіденційна інформація, що є приватною власністю $A_{1.2.2}$ юридичної особи.

До основних задач *методики оцінювання таємної* $\boldsymbol{A_3}$ інформації (МК 3) слід віднести [168]: виявлення відомостей, що становлять ДТ $A_{3.1}$; виявлення іншої передбаченої законодавством таємниць (професійна таємниця $A_{3.2}$, банківська таємниця $A_{3.3}$, таємниця слідства $A_{3.4}$, інша таємниця $A_{3.5}$); визначення сфери життєдіяльності (*N*) відомостей, що становлять ДТ $A_{3.1}$;

Основними задачами *методики оцінювання СлІ* $\boldsymbol{A_2}$ (МК 4) є [168]:

- виявлення СлІ $A_{2.1}$, що зібрана у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до ДТ $A_{3.1}$;
- виявлення СлІ $A_{2.2}$, що міститься в документах суб'єктів владних повноважень, яка становить внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень.

Зміст МК 1-4 визначається і формується за наявними постановами та розпорядженнями КМУ, порядками, наказами і інструкціями в інформаційній сфері для СРСД.

За результатами створених моделей засобів забезпечення сфери ОДТ (СОІМ ЗВДТ, СОІМ ПСлІ та моделі оцінювання шкоди як сладова експертизи МНІ) необхідно об'єднати у єдиний кортеж ідентифіковані та оціночні параметри для побудови базової моделі інтегрованого представлення параметрів шкоди національній безпеці цій сфері.

Базова модель інтегрованого представлення параметрів шкоди національній безпеці у сфері охорони державної таємниці

На сьогоднішній день є нешироким спектр засобів аналізу та оцінки шкоди національній безпеці в інформаційній сфері, особливо це стосується сфери ОДТ, при виборі яких експерт стикається з безліччю питань, що стосуються вибору параметрів і математичного апарату для здійснення оцінювання на основі використання кількісних статистичних даних і якісних, отриманих в умовах невизначеного слабоформалізованого середовища тощо. Ці та інші фактори створюють ряд труднощів при виборі відповідних засобів оцінювання. З урахуванням цього здійснено аналіз моделі оцінювання шкоди як складової експертизи МНІ (див. п. 2.4), яка використовуючи моделі засобів СОІМ ЗВДТ та СОІМ ПСлІ, узагальнює ідентифікуючі й оціночні компоненти у ***базову модель інтегрованого представлення параметрів шкоди*** (ІППШ) для їх використання при оцінюванні шкоди національній безпеці у сфері ОДТ.

Запропонований підхід, дає можливість відносно ІППШ уніфікувати процес аналізу інструментальних засобів оцінювання шкоди і підвищити ефективність здійснення їх вибору.

Модель ІППШ національній безпеці у сфері ОДТ розроблено у вигляді десятикомпонентного кортежу [169]:

$$<E, A, x_i, CC, S, K_{зі}, \rho, ВВСЧО, K_c, W>,$$

де E – подія (порушення), як обставина для оцінювання шкоди;

A – атака (подія-загрози), що призвела до появи E;

x_i – відомості, що становлять ДТ;

CC – ступінь секретності відомостей x_i (ГС для МНСІ);

S – завдання ОДТ (як комплекс m заходів (способів));

$K_{зі}$ – коефіцієнт захищеності інформації;

ρ – рівень зниження ефективності СЧО;

$ВВСЧО$ – відносна вартість СЧО;

K_c – коефіцієнт морального старіння інформації;

W – показник СШ.

Отже, запропоновано базову модель ІППШ, яка за рахунок узагальнення ідентифікуючих та оціночних параметрів, відображених десятикомпонентним кортежем, дозволяє використовувати необхідну множину наборів параметрів (бази даних) існуючих засобів (ЗВДТ (РПВДТ) та ПСлІ) забезпечення сфери ОДТ для оцінювання величини можливої шкоди національній безпеці України.

5.2. Методи оцінювання шкоди національній безпеці України у разі витоку державної таємниці

Метод аналізу і оцінки величини можливої шкоди національній безпеці у сфері охорони державної таємниці

Розроблено ***метод аналізу і оцінки величини можливої шкоди національній безпеці у сфері ОДТ***, який за рахунок базової моделі ІППШ і логіко-лінгвістичного підходу до динамічно змінюваних наборів ідентифікуючих та оціночних параметрів існуючих засобів, розраховує умовну (бальну) і вартісну величину ЕШ та ІТН, що дозволило визначити величину можливої СШ (збиток) національній безпеці держави у разі розголошення ДТ чи втрати МНСІ. Метод складає систематизовану сукупність десяти кроків, які потрібно здійснити для виконання оцінювання шкоди національній безпеці:

Крок 1. Ідентифікація події та атак. За нормативно-правовими документами організація РС і стану забезпечення ОДТ відбувається на основі організаційно-правових, технічних, криптографічних та оперативно-розшукових заходів захисту, які направлені на запобігання реалізації основних ***загроз* (*T*)** (від англ. *threat*) порушення властивостей захищеності відомостей, що становлять ДТ, а саме при j=3: t_1 = «конфіденційності»; t_2 = «цілісності»; t_3 = «доступності». Множина загроз T приймає вигляд: $T = \{t_j\},\ j = \overline{1,l}.$

На основі проведеного аналізу ефективності СОДТ (див. розділ 4), визначено перелік подій-загроз T, пов'язаних з описом певних способів реалізації загроз спільно з характеристиками ймовірних наслідків кожної з реалізацій. Так як кожна подія-загроза t_j реалізується за допомогою ***атак* (*A*)** (від англ. *attack*), що призводять до появи наслідків (інцидентів, порушень, подій тощо), то до таких атак $A \in \{a_1,...,a_j\}$ при j=6 відносяться: a_1 = «несанкціоноване отримання СІ зацікавленими особами у результаті порушення правил секретного діловодства і порядку допуску та доступу до МНСІ» (НСД); a_2 = «отримання СІ іноземними спецслужбами у результаті агентурного проникнення (шпигунство)» (Ш); a_3 = «розголошення відомостей, що становлять ДТ» (Р); a_4 = «втрата МНСІ» (В); a_5 = «перехоплення СІ, яка передається за допомогою засобів телекомунікації (ІТС, АС тощо), а також через технічні канали витоку інформації, в тому числі канали побічного електромагнітного випромінювання і наводок, зокрема в мережах електроживлення технічних засобів обробки і збереження інформації» (П); a_6 = «знищення або модифікація СІ деструктивними силовими

впливами» (С). Узагальнено множина можливих атак A приймає наступний вигляд: $A = \{a_j\},\ j = \overline{1,l}.$

Внаслідок реалізації атак A у сфері ОДТ виникають ***порушення*** або ***події*** **(*E*)** (від англ. *events*), які за [29] при j=2 ідентифікуються як: E_1= «Розголошення» (Р); E_2= «Втрата» (В). Множина можливих подій E_j до інформаційних ресурсів держави у сфері ОДТ за табл. 18 наступна $E = \{E_1, E_2\}$.

Таблиця 18

Зразок розділу 6 звіту про стан забезпечення ОДТ

№ п/п	Повна назва установи	Кваліфікація порушення (розголошення або втрата, позначається "Р" або "В")	Назва МНСІ, ким виготовлений	Реєстраційний номер МНСІ, номер примірника, дата реєстрації	Гриф секретності МНСІ, стаття ЗВДТ, дата засекречування	Дата виявлення втрати, розголошення	Номер, дата інформування органу СБУ	№ і дата експертного висновку державного експерта з питань таємниць про СС відомостей
1	2	3	4	5	6	7	8	9
29	Державна установа …	"В"	Каталог координат геодезичних пунктів "Укрінж-геодезія"	Інв. № 43, прим. № 12	Таємно/ 1.11.5 ЗВДТ 2005 р.	20.05. 2008	№ 13/4 від 21.05. 2008	№ 128 від 28.05. 2007

У якості засобу для практичної ідентифікації подій E_j використаємо *звіт про стан забезпечення сфери ОДТ* [29], а саме зразок розділу 6 «Відомостей про виявлені факти втрати МНСІ або розголошення відомостей, що становлять ДТ», які у колонці 3 табл. 18 кваліфікуються як порушення. Відповідно до п. 2.6 [29] відомості надаються лише за ті СРСД, в яких мали місце E_1 або E_2.

Крок 2. Ідентифікація відомостей, що становлять ДТ. За цією ж табл. 18 у колонці 6 конкретизуються (або ідентифікуються) ***відомості*** **(x_i)**, що становлять ДТ у вигляді номера статті ЗВДТ та їх СС щодо яких відбулися події E_1 чи E_2 (наприклад, 1.11.5 / Таємно (див. табл. 18)) як $x_i \in \boldsymbol{PV}_{\boldsymbol{N.i.j}}$, де PV – короткий зміст цих відомостей, N – сфера ДТ, що

виражена у вигляді символьної змінної як $N \in \{N_1, N_2, ..., N_v\}$ (v – кількість ідентифікаторів сфер), при v=4 наступні: N_1= «оборони»; N_2= «економіки, науки і техніки»; N_3= «зовнішніх відносин»; N_4= «державної безпеки і охорони правопорядку», а $i.j$ – ідентифікатори статті ЗВДТ за сферою N_v.

Крок 3. Визначення прогнозованої (бальної) величини шкоди за СС відомостей. Компонент кортежу – ***ступінь секретності*** **(СС)**, можна відобразити його двокомпонентною множиною $CC \in \{Wcc_в, Wcc_н\}$, де $Wcc_в$ – визначена ДЕТ прогнозована величина СШ:

$$\text{«Т»},\ 1 \le W_{CC_T} < 10,\ \overline{W_{CC_T}} = 5;$$

$$\text{«ЦТ»},\ 10 \le W_{CC_{ЦТ}} < 100,\ \overline{W_{CC_{ЦТ}}} = 55;$$

$$\text{«ОВ»},\ 100 \le W_{CC_{ОВ}} \le 300,\ \overline{W_{CC_{ОВ}}} = 200,$$

а $Wcc_н$ – як нечітка величина шкоди. Слід зазначити, що коли виникають труднощі з отриманням статистичних даних, а також для простоти інтерпретації величин, експерти використовують логіко-лінгвістичний підхід і відображають цей компонент через ЛЗ «СТУПІНЬ СЕКРЕТНОСТІ» (СС) з базовою терм-множиною $CC = \bigcup_{i=1}^{c} CC_i$ (c – кількість термів), для членів якого справедливе відношення порядку $CC_1 < CC_2 < ... < CC_c$. Наприклад, при c = 3 для зазначеної ЛЗ можна сформувати множину термів $CC = \bigcup_{i=1}^{3} CC_i = \{\text{«Т»}, \text{«ЦТ»}, \text{«ОВ»}\}$, яка відображається нечіткими числами $\underset{\sim}{\text{Т}}$, $\underset{\sim}{\text{ЦТ}}$, $\underset{\sim}{\text{ОВ}}$, для яких визначаються відповідні функції належності (рис. 30) за виразом [170]:

$$\mu(x_i) = \begin{cases} L\left(\dfrac{b_{1j} - \overline{W}_{cc}}{b_{1j} - a_j}\right), & W_{cc} \in [a_j, b_{1j}]; \\ 1, & W_{cc} \in [b_{1j}, b_{2j}]; \\ 0{,}5, & W_{cc} \in [W_i, W_j]; \\ R\left(\dfrac{\overline{W}_{cc} - b_{2j}}{c_j - b_{2j}}\right), & W_{cc} \in [b_{2j}, c_j]. \end{cases} \qquad (5.1)$$

Для компактного опису трапециевидних функцій належності $\mu(x_i)$ ЛЗ «СС» застосуємо трапециевидні нечіткі числа виду $F_f = (a_j, b_{1j}, b_{2j}, c_j)_{LR}$, де a_j і c_j – абсциси нижньої основи, а b_{1j} і b_{2j} – абсциси верхньої основи трапеції, що показано на рис. 30, де $a_j < b_{1j} \le b_{2j} < c_j$, при, $j = \overline{1,m}$ $\{a_1, c_m\} = \{\varnothing\}$, а $L(W_{cc})$, $R(W_{cc})$ – функції, які задовольняють властивостям: $L(-W_{cc}) = L(W_{cc})$, $R(-W_{cc}) = R(W_{cc})$, $L(0) = R(0) = 1$.

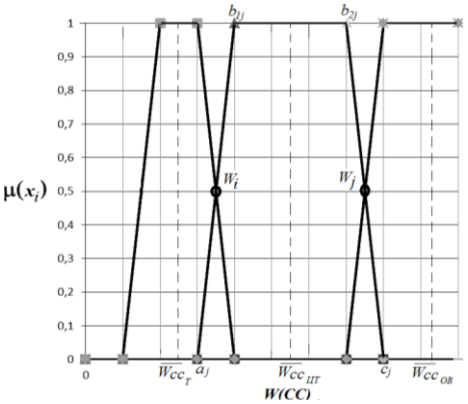


Рис. 30. Функція належності $\mu(x_i)$ ЛЗ “СС”

Значення функції належності $\mu(x_i)$ показує впевненості ДЕТ ($[b_{1_j}, b_{2_j}]$ - *max*, $[a_j, b_{1_j}]$ і $[b_{2_j}, c_j]$ - *min*, $[W_i, W_j]$ - *normative*) у встановленні СС відомостям, що становлять ДТ.

Крок 4. Розрахунок коефіцієнта захищеності відомостей. Наступний компонент кортежу – ***завдання*** **(S)**, що складаються із комплексу *m* заходів (способів) ОДТ нейтралізації визначеного переліку можливих атак *A*. Параметр *S* можна виразити у вигляді символьної змінної $S \in \{S_1, S_2, ..., S_g\}$ (g – кількість ідентифікаторів завдань), що також приймає одне із можливих значень кінцевої множини ідентифікаторів. Кількість ідентифікаторів завдань $S = \{S_g\}, g = \overline{1,l}$ визначаються за кількістю потенційних атак *A* і при *g*=6 можуть бути як: S_1= «Унеможливлення НСД»; S_2= «Попередження Р»; S_3= «Запобігання В»; S_4= «Виявлення Ш»; S_5= «Усунення П»; S_6= «Недопущення С».

Сукупність заходів (способів) ОДТ *m* обирається за показниками їх ефективності (*P*) забезпечення завдання S_g (див.табл. 14) з усунення атак A_a [125, 170]:

$$P = \sum_{g=1}^{l} P(A_a/S_g), g = \overline{1,l}. \qquad (5.2)$$

Коефіцієнт захищеності відомостей залежить від ефективності усунення (нейтралізації) атак a_j за допомогою типових завдань S_g та коефіцієнту важливості відомостей. Для цього проведемо розрахунок коефіцієнтів захищеності $\Upsilon = \{\Upsilon_j\},\ j = \overline{1, n},$ відомостей $PV_{N.i.j}$ до атак a_j:

$$\Upsilon = \beta_x / \left| A_j \right|,\ j = \overline{1, l}, \tag{5.3}$$

де $|A_j|$ – кількість можливих атак у множині A. Коефіцієнт Υ характеризує захищеність відомостей $PV_{N.i.j}$, що циркулюють на окремому СРСД як відношення коефіцієнта їх важливості β_x до кількості можливих щодо них атак a_j певних існуючий загроз T.

Для окремого СРСД коефіцієнт захищеності $K_{зі\,N}$ характеризує рівень збереження властивостей захищеності відомостей $PV_{N.i.j}$ як ефективність (результативність) виконання типових *завдань* S, що складаються із сукупності заходів (способів) нейтралізації визначеного переліку загроз T.

Проведено розрахунок узагальнюючого компоненту кортежу моделі ІППШ – ***коефіцієнту захищеності*** **($K_{зі\,N}$)** відомостей $PV_{N.i.j}$ [125, 169, 170]:

$$K_{зі\,N} = \Upsilon \cdot P^T, \tag{5.4}$$

де Υ – вектор-рядок значень коефіцієнтів захищеності СІ у сфері N від атак (загроз); P – вектор-рядок значень показників ефективності усунення (нейтралізації) можливих атак a_j, $(.)^T$ – символ операції транспонування.

Завдання S_g впорядковуються за місцем і часом їх вирішення і формулюються з таких позицій: ***захід (спосіб)*** **(*M*)** (від англ. *measures*) ОДТ попередження можливих атак (наприклад, обмеження допуску до ДТ, регламентування порядку робіт з ДТ, проведення технічних заходів захисту СІ і таке інше); атака a_j, що підлягає усуненню (нейтралізації); період часу на усунення (нейтралізації) загрози захищеності СІ. Кожне g-е завдання S має певну M множину заходів ОДТ $S_g \in \{m_1, m_2, ..., m_l\}$ з усунення (нейтралізації) загроз t_j захищеності окремих відомостей x_i, що становлять ДТ. Множина заходів (способів) $M \in \{m_l\}, l = \overline{1, i}$, кожного завдання S_g повинна бути достатньою для захисту кожного елементу відомостей $x_j \in X$ від кожної атаки $a_j \in A$, але, за можливістю, мінімальною (див. табл. 14):

S_1={m_1,m_2,m_3,m_6,m_7,m_9,m_{12},m_{13}, m_{20},m_{21},m_{23},m_{30},m_{32},m_{47}};
S_2={m_1,m_3,m_4,m_5,m_8,m_{14},m_{15},m_{17},m_{18},m_{19},m_{20},m_{32}};
S_3={m_1,m_2,m_5,m_6,m_7,m_8,m_{14},m_{15},m_{17},m_{18},m_{19},m_{20},m_{32}};
S_4={m_{22},m_{23},m_{24},m_{25},m_{26},m_{28},m_{29},m_{30},m_{31},m_{32}};
S_5={m_{33},m_{34},m_{35},m_{36},m_{37},m_{38},m_{39},m_{40},m_{41},m_{42},m_{43},m_{44},m_{45},m_{46}};
S_6= {m_1,m_2,m_3,m_4,m_5, m_6,m_7,m_8,m_9,m_{18},m_{21},m_{23},m_{30},m_{38},m_{42},m_{47}}.

Тобто, їх перелік обирається за показниками ***ефективності*** **(*P*)** забезпечення виконання g-го завдання з усунення атак a_j, який розраховується за формулою (5.2). У табл. 15 наведено узагальнений перелік заходів (способів) ОДТ $M \in \{m_1, m_2, ..., m_i, ..., m_j\}$. У загальному випадку усунення реалізації атак a_j існуючих загроз *T* забезпечується за умови виконання декількох завдань *S* захисту відомостей, що становлять ДТ. Нехай сукупність заходів m_l з нейтралізації певних атак a_j деякої загрози t_j може виконуватись одночасно. Визначимо ці заходи як m_i, ..., m_l, а ймовірність усунення кожним із них атаки a_j через $P(a_j/m_i)$, ..., $P(a_j/m_l)$. Ймовірність того, що атака a_j не буде нейтралізована окремо кожним з цих заходів обчислюється за виразом [125, 169, 170]:

$$\overline{P}(a_j/m_i) = 1 - P(a_j/m_i). \qquad (5.5)$$

Ймовірність того, що атака a_j існуватиме, незважаючи на виконання усієї сукупності заходів *M*, тобто як загрози після введення системи заходів із захисту інформації, визначається як [125, 169, 170]:

$$\overline{P}(a_j/m_i,..,m_l) = \prod_{l=j,...,i}(1 - P(a_j/m_i)). \qquad (5.6)$$

Цей перелік можна розглядати як сукупність сценаріїв типових інцидентів з відповідними можливими наслідками. Однак слід мати на увазі, що ці сценарії можуть мати місце як поодинці, так і у певних сполученнях, що знайшло своє відображення у табл. 19. У повному обсязі множина структур подій E_j та вирази для обчислення ймовірностей їх настання $P(E_j)$ відносно реалізації комбінацій (*d*) можливих сценаріїв атак *A* наведено у табл. 19.

Загальна кількість елементів множини можливих атак $\{a_j\}$ визначається формулою [169, 170]:

$$m = \sum_{d=0}^{j} c_j^d = 2^j, \qquad (5.7)$$

де c_j^d – число сполучень з *j* по *d* елементів, при *j* = 6 отримаємо *m* = 64.

Крок 5. *Розрахунок рівня зниження ефективності СЧО*. Виконання типових завдань S_g є обов'язковим для кожного РСО окремого СРСД і направлені на попередження прогнозованих дій (як атак) сторони, яка заволоділа відомостями з метою повного забезпечення захищеності відомостей, що становлять ДТ ($K_{зі\,N}=1$).

Таблиця 19

Сценарій можливих атак та ймовірність їх реалізації

Можливі атаки a_j	d	Зміст події E	Ймовірність P
НСД	1	$a_1 \cap \overline{a_2} \cap \overline{a_3} \cap \overline{a_4} \cap \overline{a_5} \cap \overline{a_6}$	$p_1(1-p_2)(1-p_3)(1-p_4)(1-p_5)(1-p_6)$
Ш		$\overline{a_1} \cap a_2 \cap \overline{a_3} \cap \overline{a_4} \cap \overline{a_5} \cap \overline{a_6}$	$(1-p_1)p_2(1-p_3)(1-p_4)(1-p_5)(1-p_6)$
…..		……	……
С		$\overline{a_1} \cap \overline{a_2} \cap \overline{a_3} \cap \overline{a_4} \cap \overline{a_5} \cap a_6$	$(1-p_1)(1-p_2)(1-p_3)(1-p_4)(1-p_5)p_6$
НСД, Ш	2	$a_1 \cap a_2 \cap \overline{a_3} \cap \overline{a_4} \cap \overline{a_5} \cap \overline{a_6}$	$p_1p_2(1-p_3)(1-p_4)(1-p_5)(1-p_6)$
Ш, В		$\overline{a_1} \cap a_2 \cap \overline{a_3} \cap a_4 \cap \overline{a_5} \cap \overline{a_6}$	$p_2p_4(1-p_1)(1-p_3)(1-p_5)(1-p_6)$
…..		……	……
П, С		$\overline{a_1} \cap \overline{a_2} \cap \overline{a_3} \cap \overline{a_4} \cap a_5 \cap a_6$	$p_5p_6(1-p_1)(1-p_2)(1-p_3)(1-p_4)$
НСД, Ш, В	3	$a_1 \cap a_2 \cap a_3 \cap \overline{a_4} \cap \overline{a_5} \cap \overline{a_6}$	$p_1p_2p_3(1-p_4)(1-p_5)(1-p_6)$
….		……	……
В, П, С		$\overline{a_1} \cap \overline{a_2} \cap \overline{a_3} \cap a_4 \cap a_5 \cap a_6$	$p_4p_5p_6(1-p_1)(1-p_2)(1-p_3)$
НСД, Ш, Р, В	4	$a_1 \cap a_2 \cap a_3 \cap a_4 \cap \overline{a_5} \cap \overline{a_6}$	$p_1p_2p_3p_4(1-p_5)(1-p_6)$
……		……	……
Р, В, П, С		$\overline{a_1} \cap \overline{a_2} \cap a_3 \cap a_4 \cap a_5 \cap a_6$	$p_3p_4p_5p_6(1-p_1)(1-p_2)$
НСД, Ш, В, Р, П	5	$a_1 \cap a_2 \cap a_3 \cap a_4 \cap a_5 \cap \overline{a_6}$	$p_1p_2p_3p_4p_5(1-p_6)$
…..		……	……
НСД, Ш, В, Р, П, С	6	$a_1 \cap a_2 \cap a_3 \cap a_4 \cap a_5 \cap a_6$	$p_1p_2p_3p_4p_5p_6$

У такому разі розраховується коефіцієнт захищеності відомостей $PV_{N.i.j}$ відносно можливих атак a_j, який, у випадку їх відсутності, рівний коефіцієнту ефективності СОДТ ($K_{зі\,N}=K^{СОДТ}$), тобто при відсутності подій E_j і розраховується за формулою [169, 170]:

$$K^{СОДТ}=W(X)\cdot K_{зі\,N}/W(X)=K_{зі\,N}. \qquad (5.8)$$

У разі настання подій E_1 або E_2 коефіцієнт ефективності СОДТ приймає своє значення у межах ($0{,}37 < K^{СОДТ} < 0{,}81$) (див. табл. 9), тобто має місце наступний вираз [169, 170]:

$$K^{СОДТ} = 1 - \rho, \tag{5.9}$$

де ρ приймає своє значення у межах від «0» до «1».

Для забезпечення повної ефективності ($K_{зі\,N} = 1,\ \rho = 0$) використання об'єкта $O_{N.i.j}$ відомостей, що становлять ДТ використовується перелік $X = \{PV_{1.i.j}(O_{N.i.j}),....,PV_{N.i.j}(O_{N.i.j})\}$ та значення його «питомої ваги» $W(X)$, які циркулюють в РСО окремого СРСД і містять відомості про цей об'єкт. При виникненні подій E_1 або E_2 значення «питомої ваги» даного переліку $W(X)$ зменшиться на величину «питомої ваги» тих відомостей $w(x_i)$ щодо яких відбулася подія E_j, тобто відбудеться часткова ($\rho < 1$) втрата ефективності використання об'єкта на величину його СЧО. Дану закономірність визначено формулою [169, 170]:

$$(W(X) - w(x_i)) / W(X) = K_{зі\,N} - \rho / K_{зі\,N}, \tag{5.10}$$

при повній захищеності відомостей про об'єкт ($\rho = 0$):

$$(W(X) - w(x_i)) / W(X) = 1, \tag{5.11}$$

при E_1 або E_2, тобто частковій втраті відомостей ($\rho < 1$) про об'єкт $O_{N.i.j}$:

$$(W(X) - w(x_i)) / W(X) = K_{зі\,N}(1 - \rho) / K_{зі\,N}, \tag{5.12}$$

$$\rho = 1 - (W(X) - w(x_i)) / W(X). \tag{5.13}$$

Крок 6. Визначення відносної вартості СЧО. Наявність вживання у статтях ЗВДТ так званих «допоміжних слів» пропонується використати у якості номінативної шкали *відносної вартості СЧО* від значення "питомої ваги" (Q) об'єкта $O_{N.i.j}$ у цілому як ЛЗ **«*відносна вартість СЧО*» (*ВВСЧО*)**, яка задається кортежем $\left\langle ВВСЧО, k_{ВВСЧО}, X_{ВВСЧО}, \overline{k_{ВВСЧО}} \right\rangle$, де базові терм-множини задаються i термами $k_{ВВСЧО} = \bigcup_{1}^{i} k_{ВВСЧО_i}$

(наприклад, для ЗВДТ 2013 року $i=5$ – $\bigcup_{i=1}^{5} k_{ВВСЧО_i} =$ {«за окремими складовими показниками» (ОСП), «за сукупністю всіх складових показників» (ССП), «за окремими показниками» (ОП), «за сукупністю всіх показників» (СП), «об'єкт у цілому» (О)}), які можуть бути відображені на універсальну множину $\overline{k_{ВВСЧО}} \in \{0, max_{ВВСЧО}\}$. Кожному з термів $k_{ВВСЧО_1},...,k_{ВВСЧО_i},...,k_{ВВСЧО_k}$ задається інтервал значень $[k_{min}; k_1[,..,[k_i; k_{i+1}[,..,[k_k; k_{max}]$ за шкалою Харрингтона і середнє значення інтервалу $\overline{k_{ВВСЧО_1}},...,\overline{k_{ВВСЧО_i}},...,\overline{k_{ВВСЧО_k}}$ як кортеж [169, 170]:

$$
\begin{aligned}
\text{ОСП} &= \left\langle ОСП,\, k_{ОСП},\, [0;0{,}2],\, \overline{k_{ОСП}} = 0{,}1 \right\rangle,\\
\text{ССП} &= \left\langle ССП,\, k_{ССП},\, [0{,}2;0{,}4],\, \overline{k_{ССП}} = 0{,}3 \right\rangle,\\
\text{ОП} &= \left\langle ОП,\, k_{ОСП},\, [0{,}4;0{,}6],\, \overline{k_{ОП}} = 0{,}5 \right\rangle,\\
\text{СП} &= \left\langle СП,\, k_{СП},\, [0{,}6;0{,}8],\, \overline{k_{СП}} = 0{,}7 \right\rangle,\\
\text{О} &= \left\langle О,\, k_{О},\, [0{,}8;1],\, \overline{k_{О}} = 0{,}9 \right\rangle.
\end{aligned}
\qquad (5.14)
$$

Значення функції належності $\mu(k_k)$ ЛЗ «ВВСЧО» розраховується за виразом (5.1), що показує на рис. 31 скільки можливо ідентифікувати об'єкт чи СЧО у статтях ЗВДТ.

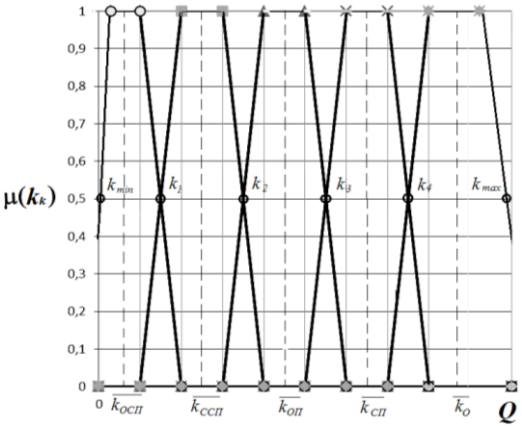


Рис. 31. Функція належності $\mu(k_k)$ ЛЗ "ВВСЧО"

Практичним рішенням для знаходженні показника k є розроблена модель СОІМ ЗВДТ (див. п. 5.1).

Крок 7. Розрахунок показника ІТН. Цим кроком на основі отриманих значень показників ЕШ – ρ, ВВСЧО та «питомої ваги» (Q) об'єкта $O_{N.i.j}$ відомостей за наявним переліком (див. *Додаток 5*) і, використовуючи максимальне значення інтервалу величини прогнозованої СШ за *критерієм СС*, розраховується компонент кортежу – ***величина ІТН*** **($W_{ін}$)** як [169, 170]:

$$W_{ін} = W - Q \cdot k \cdot \rho = W_{cc_{max}} - Q \cdot k \cdot \rho . \qquad (5.15)$$

Отримане значення порівнюється за *переліком ІТН*, що визначає категорію та тяжкий наслідок для інтересів національної безпеки держави від подій *Е*.

Крок 8. Розрахунок коефіцієнта морального старіння відомостей. Строк дії рішення протягом якого інформація є секретною ($T_н$) встановлюється з урахуванням її СС, а саме для «ОВ» – 30, «ЦТ» – 10, «Т» – 5 років. Після закінчення дії цього строку ДЕТ приймає рішення щодо скасування раніше прийнятого рішення про віднесення цих відомостей до ДТ або продовження строку його дії у визначених межах. Пропонується, у випадку скасування рішення ДЕТ або на його розсуд, проводити розрахунок наступного коефіцієнта кортежу – ***коефіцієнта морального старіння*** **(K_c)** відомостей, що становлять ДТ.

Для цього використаємо колонки 7-9 розділу 6 (див. табл. 18) та розрахуємо його наступним чином [169, 170]:

$$K_c = 1 - T_ф / T_н \text{ при } T_н \neq 0 , \qquad (5.16)$$

де $T_ф$ – термін дії охоронного документа в розрахунковому році *t* (наприклад, дата виявлення E_3 чи E_4 або дата інформування органу СБУ (колонка 7, 8) (див. табл. 18)); $T_н$ – номінальний термін дії охоронного документа (дата експертного висновку ДЕТ про СС відомостей (колонка 9) (див. табл. 18)).

Крок 9. Розрахунок показників ЕШ. На даному кроці проводиться аналіз звіту про стан забезпечення ОДТ, а саме розділу 2 «Відомості про РСО, фінансування заходів на ОДТ» [29], де з метою забезпечення повної захищеності відомостей, що становлять ДТ для кожного СРСД передбачено фінансування (витрати) W_1 заходів (способів) *А* виконання типових завдань *S*.

У табл. 20 наведено розділ 2 звіту [29], де обсяг витрат зазначається у колонках 8-14 і у загальному може розраховуватися як:

$$Ц_{S_1} + Ц_{S_2} + Ц_{S_3} + ... + Ц_{S_g} = \sum_{i=1}^{g} Ц_{S_g},\ g = \overline{1, l}, \qquad (5.17)$$

де $Ц_{S_1}$ – витрати на утримання штатних працівників РСО; $Ц_{S_2}$ – витрати на розмір виплаченої компенсації громадянам у зв'язку з виконанням секретних робіт (без урахування працівників РСО); $Ц_{S_3}$ – витрати на матеріально-технічне забезпечення, а також на перевезення та пересилання МНСІ, їх фізичну охорону; $Ц_{S_4}$ – витрати на виплату грошових надбавок ДЕТ та членам експертних комісій; $Ц_{S_5}$ – витрати на технічний захист СІ; $Ц_{S_6}$ – витрати на криптографічний захист СІ.

Таблиця 20

Зразок розділу 2 звіту про стан забезпечення ОДТ

№ п/п	Повна назва установи	Штатна кількість працівників РСО або кількість відповідальних працівників	усього РСО	У звітному періоді РСО			Фінансування заходів на ОДТ (у тис. грн.) у звітному періоді						
				створено	реорганізовано	ліквідовано	усього	у тому числі:					
								на утримання штатних працівників РСО	на розмір виплаченої компенсації громадянам у зв'язку з виконанням секретних робіт (без урахування працівників РСО)	на матеріально-технічне забезпечення, а також на перевезення та пересилання МНСІ, їх фізичну охорону	на виплату грошових надбавок ДЕТ та членам експертних комісій	на технічний захист СІ	на криптографічний захист СІ
1	2	3	4	5	6	7	8	9	10	11	12	13	14
29	Державна установа …	1	1		1		125,6	53,07	55,07	0,5		16,96	29

Для розрахунку ***вартісної величини показників ЕШ*** $Ц_{W_1}$ та $Ц_{W_2}$, мають місце наступні вирази при умові $K_{зі\ N} = 1$ [169, 170]:

$$Ц_{W_1} = \sum_{i=1}^{g} Ц_{S_g} \cdot K_{зі\ N}, \tag{5.18}$$

$$Ц_{W_2} = Ц_{W_1} \cdot K^{СОДТ}. \tag{5.19}$$

Загальна вартісна ***оцінка величини ЕШ*** $Ц_{W_{ек}}$ і ***величини ІТН*** $Ц_{W_{ін}}$ визначається як [169, 170]:

$$Ц_{W_{ек}} = Ц_{W_1} - Ц_{W_2}, \tag{5.20}$$

$$Ц_{W_{ін}} = Ц_{W_{ек}} \cdot W_{ін} / W_{ек} = Ц_{W_{ек}} \cdot W_{ін} / Q \cdot \rho \cdot k. \tag{5.21}$$

Крок 10. Розрахунок грошової величини СШ. На цьому останньому кроці проводиться розрахунок вартісної величини компоненту кортежу – ***показника СШ*** ($Ц_W$), який за рішенням ДЕТ, з урахуванням можливого до цих відомостей закону старіння інформації, виражається наступною узагальненою формулою [169, 170]:

$$Ц_W = \sum_{t_n=1}^{t_{к\text{-}1}} (Ц_{W_{ек}} + Ц_{W_{ін}}) + \sum_{t_n=t_{к\text{-}1}}^{t_к} (Ц_{W_{ек}} + Ц_{W_{ін}}) \cdot K_c, \tag{5.22}$$

а у разі відсутності старіння цих відомостей як [169, 170]:

$$Ц_W = \sum_{t_n=1}^{t_к} (Ц_{W_{ек}} + Ц_{W_{ін}}). \tag{5.23}$$

де t_n – початковий рік розрахункового періоду; $t_к$ – кінцевий рік розрахункового періоду.

Отримане кінцеве значення показника СШ показує *вартісну* (*грошову*) величину можливої шкоди національній безпеці України у сфері ОДТ у разі настання існуючих подій *E*.

Метод оцінювання важливості відомостей за визначеними сферами державної таємниці

Проведений аналіз *методики визначення підстав для віднесення відомостей до ДТ та визначення їх СС* (див. п. 1.3), яка реалізована за принципом експертних оцінок дозволяє визначити в однакових бальних одиницях величину ЕШ та ІТН, що можуть бути завдані життєво важливим інтересам України внаслідок розголошення відомостей, як віднесених так і тих, що повинні бути віднесені до ДТ, надавши їм відповідного СС. Розглянуто аспекти реалізації цієї методичної процедури віднесення інформації до СІ, зокрема, виконано її формалізацію з представленням чотириетапної схеми обробки вихідної інформації (див. рис. 1). Також наведена *методика для оцінювання ефективності системи ОДТ* (див. розділ 4) більш високих рівнів за результатами оцінювання стану захисту СІ на нижчих рівнях, наприклад, ефективності національної СОДТ через захищеність СІ в окремих її сферах. Це реалізується шляхом введення та розрахунку спеціальних коефіцієнтів важливості відомостей, що становить ДТ за визначеними її сферах, які також використовуються у кроці 4 «*Методу аналізу і оцінки величини можливої шкоди національній безпеці у сфері ОДТ*» (див. п. 5.2) при визначенні коефіцієнтів захищеності інформації в РСО СРСД. Порядок проведення та розрахунок таких коефіцієнтів наведено у розробленому ***методі оцінювання важливості відомостей за визначеними сферами ДТ*** [169, 176].

Реалізація *методу* потребує виконання трьох кроків, які проводять оцінювання важливості відомостей за визначеними сферами ДТ [169]:

Крок 1. Визначення «ваги» відомостей, що становлять ДТ за їх СС.

Даний крок потребує ідентифікацію ***відомостей*** **(x_i)**, що становлять ДТ та визначення сфери N цих відомостей, що можливо виконати за допомогою як і моделі СОІМ ЗВДТ (див. п. 5.1) так і за кроком 2 *методу аналізу і оцінки величини можливої шкоди національній безпеці у сфері ОДТ* як: $\boldsymbol{x_i} \in PV_{N.i.j}$, де PV – короткий зміст цих відомостей, N – сфера ДТ, а $i.j$ – ідентифікатори статті ЗВДТ за сферою N_v. Далі, використовуючи *критерії визначення СС* (див. п. 1.3) відомостей $PV_{N.i.j}$, за формулами (1.4)-(1.6) отримуємо значення СШ у межах інтервалу їх бальних оцінок від їх розголошення чи втрати і внаслідок механічної заміни приведеної у ЗВДТ СС цих відомостей $PV_{N.i.j}$ на відповідні середні значення цих інтервалів $\overline{W_T}; \overline{W_{ЦТ}}; \overline{W_{ОВ}}$ визначається

їх «вага» $w(PV_{N.i.j})$ як і серед інших відомостей так і у межах окремої тематичної групи *N.i* чи сфери *N*, до якої вони належать.

Розрахункові дані «ваги» окремих відомостей $PV_{N.i.j}$, наприклад, у сфері оборони приведено у табл. 21, які визначені наступним виразом:

$$w(PV_{N.i.j}) = (\overline{W_T} + \overline{W_{ЦТ}} + \overline{W_{OB}})_{i.j},\ N = \overline{1,v},\ i = \overline{1,y},\ j = \overline{1,c}. \quad (5.24)$$

Крок 2. Визначення «ваги» переліку X відомостей, що містять СІ у сфері N.

На цьому кроці формується ***перелік* (*X*)** із сукупності відомостей $PV_{N.i.j}$ у межах окремої тематичної групи *N.i* певної сфери або у цілому сфери *N*, а також у межах сукупності відомостей РСО окремого СРСД.

Далі визначається узагальнена «вага» $W(X)$ сформованого переліку *X* відомостей шляхом простого сумування кожної «ваги» $w(PV_{N.i.j})$ окремих відомостей, що увійшли до цього переліку, а саме як [169, 176]:

$$W(X) = w_1(PV_{N.i.j}) + ... + w_к(PV_{N.i.j}) + ... + w_u(PV_{N.i.j}),\ u = \overline{1,m}. \quad (5.25)$$

Крок 3. Оцінювання важливості відомостей.

Цим останнім кроком проводиться розрахунок ***коефіцієнта важливості* (*β*)** відомостей через відношення їх «ваги» до узагальненої «ваги» сформованого переліку *X* відомостей у межах сфери *N* (групи *N.i*) до якої вони входять за формулою [169, 176]:

$$\boldsymbol{\beta} = \frac{w(PV_{N.i.j})}{W(X)}, \quad (5.26)$$

де $w(PV_{N.i.j})$ – середнє значення бального інтервалу прогнозованої СШ відомостей за їх СС; $W(X)$ – сумарне значення прогнозованої СШ переліку *X* відомостей за сферою *N* у балах.

За допомогою проведений розрахунок коефіцієнтів важливості $\beta_{1.i.j}$ відомостей, що становлять ДТ ЗВДТ 2005 та 2010 року у сфері оборони (N=1) результати якого наведено у табл. 22-23 та за отриманими даними побудовано порівняльний графіки їх важливості, що показано на рис. 32 [169, 176].

Таблиця 21

Значення «ваги» відомостей, що становлять ДТ у сфері оборони за статтями ЗВДТ 2005 року

X	$\bar{\iota}_T / \bar{x}_{ЦТ} / \bar{x}_{ОВ}$	$w(PV_{1.i.j})$
		бали
$PV_{1.1.1}$	+/+/+	260
$PV_{1.1.2}$	+/+/+	260
$PV_{1.1.3}$	+/+/+	260
$PV_{1.1.4}$	+/+/+	260
$PV_{1.1.5}$	+/+/-	60
$PV_{1.1.6}$	+/+/-	60
$PV_{1.1.7}$	+/+/-	60
$PV_{1.1.8}$	+/+/+	260
$PV_{1.1.9}$	+/+/-	60
$PV_{1.1.10}$	+/-/-	5
$PV_{1.1.11}$	+/+/-	60
$PV_{1.1.12}$	+/+/-	60
$PV_{1.2.1}$	+/+/-	60
$PV_{1.2.2}$	+/-/-	5
$PV_{1.2.3}$	+/-/-	5
$PV_{1.2.4}$	+/-/-	5
$PV_{1.2.5}$	+/-/-	5
$PV_{1.3.1}$	+/+/+	260
$PV_{1.3.2}$	+/+/-	60
$PV_{1.3.3}$	+/-/-	5
$PV_{1.4.1}$	+/+/-	60
$PV_{1.4.2}$	+/+/+	260
$PV_{1.4.3}$	+/+/+	260
$PV_{1.4.4}$	+/+/-	60
$PV_{1.4.5}$	+/-/-	5
$PV_{1.4.6}$	+/+/+	260
$PV_{1.4.7}$	+/+/-	60
$PV_{1.4.8}$	+/+/-	60
$PV_{1.4.9}$	+/+/-	60
$PV_{1.4.10}$	+/-/-	5
$PV_{1.4.11}$	+/+/-	60
$PV_{1.4.12}$	+/-/-	5
$PV_{1.4.13}$	+/+/-	60
$PV_{1.5.1}$	+/-/-	5
$PV_{1.5.2}$	-/+/-	55
$PV_{1.5.3}$	+/-/-	5
$PV_{1.5.4}$	+/-/-	5
$PV_{1.5.5}$	+/-/-	5
$PV_{1.5.6}$	+/-/-	5
$PV_{1.5.7}$	+/-/-	5
$PV_{1.5.8}$	+/+/-	60
$PV_{1.5.9}$	+/-/-	5
$PV_{1.6.2}$	+/-/-	5
$PV_{1.6.3}$	+/-/-	5
$PV_{1.6.4}$	+/+/-	60
$PV_{1.6.5}$	+/+/-	60
$PV_{1.7.1}$	+/-/-	5
$PV_{1.7.2}$	+/-/-	5
$PV_{1.7.3}$	+/-/-	5
$PV_{1.8.1}$	+/-/-	5
$PV_{1.9.1}$	-/+/-	55
$PV_{1.9.2}$	-/+/+	255
$PV_{1.9.3}$	-/+/-	55
$PV_{1.9.4}$	+/-/-	5
$PV_{1.9.5}$	+/+/-	60
$PV_{1.9.6}$	+/-/-	5
$PV_{1.9.7}$	+/+/-	60
$PV_{1.9.8}$	+/-/-	5
$PV_{1.9.9}$	+/+/-	60
$PV_{1.9.10}$	+/+/-	60
$PV_{1.9.11}$	-/+/-	55
$PV_{1.9.12}$	+/+/-	60
$PV_{1.9.13}$	+/-/-	5
$PV_{1.9.14}$	+/-/-	5
$PV_{1.10.1}$	+/+/-	60
$PV_{1.10.2}$	+/-/-	5
$PV_{1.10.3}$	+/-/-	5
$PV_{1.10.4}$	-/+/-	55
$PV_{1.10.5}$	-/+/-	55
$PV_{1.11.1}$	+/-/-	5
$PV_{1.11.2}$	+/-/-	5
$PV_{1.11.3}$	+/-/-	5
$PV_{1.11.4}$	+/-/-	5
$PV_{1.11.5}$	+/-/-	5
$PV_{1.11.6}$	+/-/-	5
$PV_{1.11.7}$	+/-/-	5
$PV_{1.11.8}$	+/-/-	5
$PV_{1.11.9}$	+/-/-	5
$PV_{1.12.1}$	+/+/-	60
$PV_{1.12.2}$	+/+/-	115
$PV_{1.12.3}$	+/-/-	5
$PV_{1.12.4}$	+/+/-	60
$PV_{1.12.5}$	+/+/-	60

Таблиця 22

Коефіцієнти важливості відомостей, що становлять ДТ ЗВДТ 2005 року

2005р.	$PV_{1.1.j}$	$PV_{1.2.j}$	$PV_{1.3.j}$	$PV_{1.4.j}$	$PV_{1.5.j}$	$PV_{1.6.j}$	$PV_{1.7.j}$	$PV_{1.8.j}$	$PV_{1.9.j}$	$PV_{1.10.j}$	$PV_{1.11.j}$	$PV_{1.12.j}$	$\sum$
$w(PV_{1i.j})$	1665	80	325	1215	150	130	15	5	745	180	45	300	4855
$\beta_{1.i.j}$	0,343	0,0165	0,067	0,25	0,031	0,027	0,003	0,001	0,1534	0,037	0,0093	0,0618	1

Таблиця 23

Коефіцієнти важливості відомостей, що становлять ДТ ЗВДТ 2010 року

2010р.	$PV_{1.1.j}$	$PV_{1.2.j}$	$PV_{1.3.j}$	$PV_{1.4.j}$	$PV_{1.5.j}$	$PV_{1.6.j}$	$PV_{1.7.j}$	$PV_{1.8.j}$	$PV_{1.9.j}$	$PV_{1.10.j}$	$PV_{1.11.j}$	$PV_{1.12.j}$	$\sum$
$w(PV_{1i.j})$	1665	135	325	1215	200	130	15	5	625	180	10	305	4810
$\beta_{1.i.j}$	0,346	0,028	0,067	0,25	0,042	0,027	0,003	0,001	0,134	0,037	0,002	0,063	1

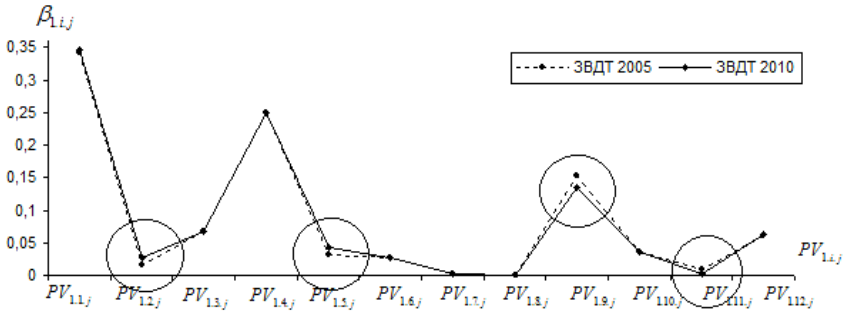


Рис. 32. Графік важливості відомостей, що становлять ДТ у сфері оборони за ЗВДТ 2005 та 2010 року

Результати показали, що найбільшу важливість для національної безпеки України у сфері оборони мають відомості $PV_{1.1.j}$, $PV_{1.4.j}$, $PV_{1.9.j}$ та $PV_{1.12.j}$. Що також підтверджується значенням «питомої ваги» (Q) об'єктів цих відомостей у додатку 1 методики визначення підстав для віднесення відомостей до ДТ та визначення їх СС (див. *Додаток 5*).

Зокрема, порівняльний аналіз виявив суттєві зміни, що відбулись у чотирьох статтях. Вчасності, збільшення коефіцієнта важливості β відбулось у статтях $PV_{1.2.j}$, $PV_{1.5.j}$, що стосується відомостей про: морально-психологічний стан особового складу, вплив соціально-

політичної обстановки в регіонах, узагальнені розрахунки психогенних втрат у воєнний час, кількісні показники фізичних полів корабля, окремі показники характеристик систем управління, організацію скритого управління військами, тощо. Зменшення своєї важливості β відчули статті $PV_{1.9.j}$, $PV_{1.11.j}$, що спричинено: по-перше, виключенням ряду підпунктів цих статей, по-друге, можливим делегуванням відомостей, що становлять ДТ до інших сфер.

Метод нечіткої класифікації відомостей, що становлять державну таємницю за встановленими критеріями

Відомо [3, 32], що при експертизі використовується ЗВДТ [31] та ПСлІ як акти у яких у вигляді статей з коротким описом їх змісту із визначеним СОД зведені відомості, що становлять ДТ і СлІ СРСД. Відповідно МНІ, що містять такі відомості надається ГС «Т», «цілком таємно» (ЦТ) і «особливої важливості» (ОВ) для СІ або гриф «для службового користування» для СлІ. З наведених у [31, 105, 106] даних ЗВДТ і ПСлІ можуть бути представлені у якості СОІМ з наявною онтологічною ієрархією з можливостями визначення цінності (важливості) інформації.

Отже, для розробки ***методу нечіткої класифікації відомостей, що становлять ДТ за встановленими критеріями*** [171] застосовуємо теорію нечітких множин [112, 161, 162], а також СОІМ ЗВДТ [106].

1. Основні параметри методу за встановленими критеріями.

Як відомо з [106], ***СОІМ ЗВДТ*** – це зосереджена сукупність державних інформаційних ресурсів СОДТ, яка складається з орієнтованих інформаційних елементів (клік) об'єднаних у мережу за визначеним (складним) порядком. Такий порядок формує складну інформаційну мережу з визначеною орієнтацією її клік з основними параметрами ЗВДТ.

Для розробки методу обрано ***параметри***, які встановлені вимогами законодавства [3, 31] та існуючими критеріями у сфері ОДТ [38, 64, 125, 106, 169, 170, 171]:

- *перелік* (*або звід*) відомостей, що становлять ДТ – $PV_{N.i.j}$,;

- *об'єкти* (*objects*) відомостей, що становлять ДТ – $O_{N.i.j}$ та їх «питома вага» (*Q*) у балах;

- *показники* (*indicators*) об'єктів відомостей, що становлять ДТ – $I_{N.i.j}$;

- *СС* відомостей, що становлять ДТ (або ГС для МНСІ);

- *«допоміжні слова»*, що вживаються у статтях ЗВДТ – *k*: ОСП, ССП, ОП, СП, О.

Використання математичного апарату теорії нечітких множин для оголошення зазначених параметрів, їх опис, структура та зміст детально приведено у наукових працях [106, 169, 170, 171].

2. Сутність, початкові дані та завдання методу.

Сутність методу полягає у реалізації способу визначення наявності на МНІ відомостей, що становлять ДТ та їх СС за встановленими критеріями для обґрунтування необхідності прийняття заходів, спрямованих на обмеження доступу до цих МНІ – ГС, шляхом оцінювання величини можливої шкоди національній безпеці України у разі розголошення цих відомостей або втрати їх МНІ.

Початковими даними методу є певна визначена сукупність (масив) вхідної інформації ($\overline{X}$), яка містить об'єкти ($\overline{O}$), показники ($\overline{I}$) цих об'єктів й певні умови до них (*k*), що розміщена на МНІ і становлять матеріали експертизи.

Завданням методу є виділення з масиву вхідної інформації ($\overline{X}$) об'єктів відомостей, що становлять ДТ ($O_{N.i.j}$) та їх показники ($I_{N.i.j}$) за наявним переліком (або зводом) статей ЗВДТ з можливою наявністю до цих показників певних умов («допоміжних слів») (*k*) для знаходження окремої статті ($PV_{N.i.j}$) з встановленим до неї значенням функції належності СС $\mu(x_i)$ за кількісною оцінкою величини можливої шкоди (*W*) національній безпеці у разі розголошення таких відомостей або втрати їх МНСІ. У цілому необхідно створити *нечіткий класифікатор відомостей, що становлять ДТ* (НКДТ) за встановленими у [3, 31, 32] критеріями, наявною формальною мовою опису – ЗВДТ [31] та алгоритм класифікації статей СОІМ ЗВДТ – $PV_{N.i.j}$ [106], побудова якого основана на принципах онтологічної ієрархії цінності інформації [105], теорії нечітких множин і засобами імітаційного моделювання [112, 119].

3. Принцип роботи та засоби моделювання методу.

Принцип роботи методу складається з наступних ***етапів*** (рис. 33):

1) формування об'єму (масиву) вхідної інформації $\overline{X}$, що знаходиться на МНІ і підлягає експертизі («*вектор-множина вхідної інформації* $\overline{X}$ »);

2) використання апріорного словника об'єктів $\overline{O}$ (АСО) відомостей, що становлять ДТ або їх класифікатора (наприклад, додаток 1 [6] або (див. *Додаток 5*)) (*«вектор-множина об'єктів* $\overline{O}$ *»*);

3) визначення ймовірності появи окремого об'єкта $P(O_{N.i.j})$ відомостей, що становлять ДТ із встановленим у [38] значенням його «питомої ваги» - *Q*;

4) визначення всіх можливих показників $\overline{I}$, що належать окремому об'єкту $O_{N.i.j}$ відомостей, що становлять ДТ («*вектор-множина показників об'єкта* $\overline{I}$ »);

5) ідентифікація наявних показників $I_{N.i.j}$ об'єкта $O_{N.i.j}$ відомостей, що становлять ДТ за апріорним словником показників $\overline{I}$ об'єктів (АСПО) або їх класифікатором (наприклад, у ЗВДТ за «допоміжними словами» [106] із встановленим до них у [169, 170] значенням функції належності $\mu(k_k)$ (*«показники об'єкту* $I_{N.i.j}$ *»*);

6) формування опису статті відомостей, що становлять ДТ $PV_{N.i.j}$ або ідентифікація існуючої у ЗВДТ (*«вектор-звід* (*перелік*) *відомостей, що становлять ДТ* $\overline{PV}$ *»*);

7) кількісна оцінка величини можливої шкоди (*W*) національній безпеці у разі розголошення цих відомостей $PV_{N.i.j}$ або втрати МНСІ;

8) встановлення СС відомостям $PV_{N.i.j}$ за значенням функції їх належності $\mu(x_i)$ до існуючої статті ЗВДТ або прогнозованої величини можливої шкоди національній безпеці у разі їх розголошення або втрати МНСІ;

9) розрахунок «питомої ваги» $w(x_i)$ та коефіцієнта важливості (β) відомостей $PV_{N.i.j}$ серед переліку існуючих статей ЗВДТ $\overline{PV}$ у сфері *N*;

10) вжиття необхідних заходів забезпечення ОДТ для недопущення зниження рівня ефективності використання об'єкта відомостей, що становлять ДТ (ρ) внаслідок зниження ефективності функціонування СОДТ та рівня захищеності СІ у сфері *N* ($K_{зі\,N}$) у разі їх розголошення або втрати МНСІ.

У результаті виконання вищенаведених етапів сформовані вектори-множини описуються як [171]:

- «*вектор-множина вхідної інформації* $\overline{X}$ »:

$$\{\overline{X}\} = \{\overline{O}_{N.i.j1}, \overline{O}_{N.i.j2}, ..., \overline{O}_{N.i.j.n}\}, \left|\overline{O}\right| = n;$$

- *«вектор-множина об'єктів* $\overline{O}$ *»*:

$$\{\overline{O}\} = \{\overline{I}_{N.i.j1}, \overline{I}_{N.i.j2}, ..., \overline{I}_{N.i.j.m}\}, \left|\overline{I}\right| = m,\ \overline{O} \subseteq \overline{I}, n \le m;$$

- «*вектор-множина показників об'єкта* $\overline{I}$ »:

$$\{\overline{I}\} = \{I_{N.i.j1}, I_{N.i.j2}, ..., I_{N.i.j.q}\}, \left|\overline{PV}_{N.i.j}\right| = N.i.j \ .$$

Описом АСО та АСПО можуть бути розподільчі функції $F_i(O_{N.i.j.1}, O_{N.i.j.2}, ..., O_{N.i.j.n}), i = \overline{1,n}$, та $f_i(I_{N.i.j.1}, I_{N.i.j.2}, ..., I_{N.i.j.m}), i = \overline{1,m}$, апріорні ймовірності появи об'єктів $P(O_{N.i.j})$ відомостей, що становлять ДТ $PV_{N.i.j}$, короткий зміст яких приведено у статтях ЗВДТ, що містить *«вектор-звід* (*перелік*) *відомостей, що становлять ДТ* $\overline{PV}$ *»*.

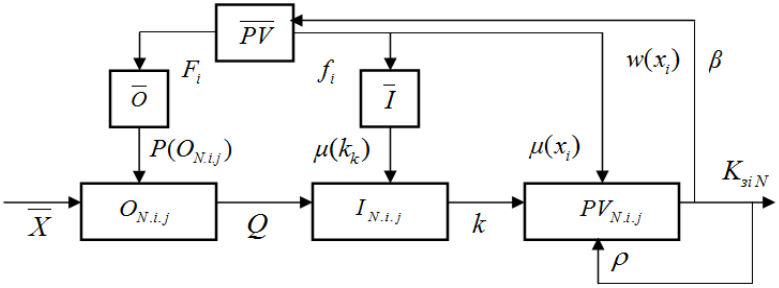


Рис. 33. Принцип роботи методу

З «*вектор-множина вхідної інформації* $\overline{X}$ » розташованої на МНІ ідентифікуються *n*-мірна множина об'єктів $\overline{O}_{N.i.j.n}$ і порівнюється з *«вектор-множина об'єктів* $\overline{O}$ », який міститься в АСО. Далі з отриманої *n*-мірної множини об'єктів $\overline{O}_{N.i.j.n}$ визначаються окремі об'єкти $O_{N.i.j}$ відомостей, що становить ДТ з *m*-мірною множиною їх показників $\overline{I}_{N.i.j.m}$, що порівнюється з «*вектор-множина показників об'єкта* $\overline{I}$ », який містить АСПО. Також розраховуються апріорні ймовірності появи об'єктів $P(O_{N.i.j})$ відомостей, що становлять ДТ. Крім того, число *m* може бути досить велике, а отже, їх обробка вимагатиме великих витрат часу, що неодмінно позначиться на ефективність методу. Тому, на НКДТ покладаються функції виявлення взаємопов'язаних показників $I_{N.i.j}$ об'єктів відомостей, що становлять ДТ $O_{N.i.j}$ для коректного пониження *m*-мірного простору АСПО для того, щоб кількість *q* показників $I_{N.i.j}$ окремого об'єкта $O_{N.i.j}$ була

мінімальною, а інформації (F_i, f_i, P) достатньо для формування достовірного результату.

Результатом роботи методу є рішення НКДТ про належність об'єкта $O_{N.i.j}$ та показників $I_{N.i.j}$ цього об'єкта до відомостей, що становлять ДТ $PV_{N.i.j}$ із значенням його «питомої ваги» за додатком 1 [38]. При цьому дуже важливо, щоб точність класифікації була якомога більше, а час досягнення результату якомога менше. Тому для цього зазвичай використовують набір евристичних правил, як багаторівневого формату нечітких продукційних (логічних) правил «*if-and*(*or*)-*then*» до об'єктів $O_{N.i.j}$ та нечіткий кортеж (5.14) за встановленими «допоміжними словами» до показників $I_{N.i.j}$ цих об'єктів у ЗВДТ:

- *до показників* $I_{N.i.j}$ *об'єктів відомостей, що становлять ДТ* (*нечіткий кортеж* (5.14);
- *до об'єктів* $O_{N.i.j}$ *відомостей, що становлять ДТ* (*нечітке правило*):

$$\begin{cases} if\ (\overline{X}\ is\ \overline{O}_{N.i.j.n}\min)\ then\ (\overline{O}_{N.i.j.n}\ is\ O_{N.i.j}\min)\ PV_{N.i.j}=[b_{1j},b_{2j}] \\ if\ (\overline{X}\ is\ \overline{O}_{N.i.j.n}\ \text{mid})\ then\ (\overline{O}_{N.i.j.n}\ is\ O_{N.i.j}\text{mid})\ PV_{N.i.j}=[W_i,W_j] \\ if\ (\overline{X}\ is\ \overline{O}_{N.i.j.n}\max)\ then\ (\overline{O}_{N.i.j.n}\ is\ O_{N.i.j}\max)\ PV_{N.i.j}=[a_j,c_j] \end{cases};$$

де $\overline{X}, \overline{O}, \overline{I}$ – вхідні величини («*вектор-множина вхідної інформації* $\overline{X}$ », «*вектор-множина об'єктів* $\overline{O}$ », «*вектор-множина показників об'єкта* $\overline{I}$ »); $\min, \text{mid}, \max$ – нечітке число кількості об'єктів вхідної інформації; ОСП, ССП, ОП, СП, О – допоміжні слова.

Кінцевим результатом методу є нечіткий сигнал-рішення у вигляді функції належності $\mu(x_i)$ (див. рис. 30) розпізнаваного об'єкта $O_{N.i.j}$ до відомостей, що становлять ДТ $PV_{N.i.j}$, або іншими словами стаття $PV_{N.i.j}$ ЗВДТ розпізнаваного об'єкта відомостей $O_{N.i.j}$. Еквівалент сигнал-рішення визначається шляхом математичного обчислення (формула (5.1)) при використанні інформації про форму відповідних функцій належності $\mu(x_i)$ та $\mu(k_k)$ (див. рис. 30, 31) та параметрів, якими вони описуються.

Згідно деяких правил [112, 172] відбувається дефазицікація величини, тобто знаходиться реальна величина вихідного сигналу (W) за його нечітким значенням $w(x_i)$, або за значенням коефіцієнта важливості

цих відомостей (β) [169, 170, 176]. Причому на цьому етапі дефазифікація відбувається для кожного правила окремо. Реалізувавши дані залежності засобами імітаційного моделювання у вигляді функціональних блоків системи моделювання *Matlab*, а саме блоком нечіткого моделювання *SubFuzzy* (рис. 34), отримаємо еквівалентну модель НКДТ (рис. 35), яка може бути проаналізована відомими методами.

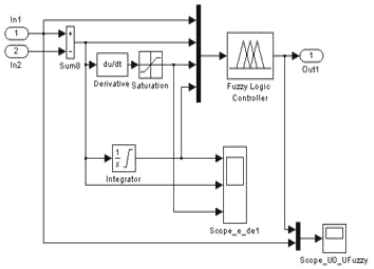


Рис. 33. Структура блоку *SubFuzzy*

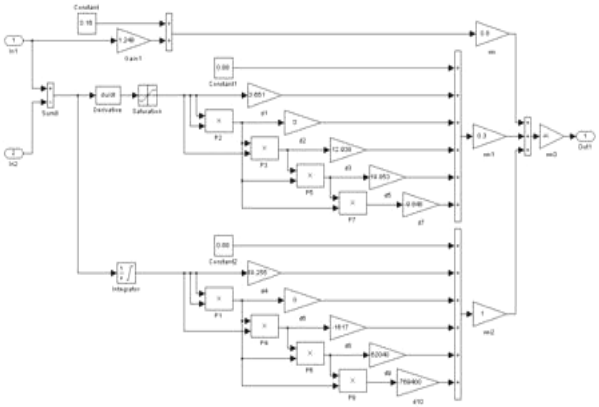


Рис. 34. Еквівалентна модель НКДТ

Запропонований метод полягає у розробці НКДТ, який дозволяє визначати приналежність об'єкта $O_{N.i.j}$ відомостей, що становлять ДТ та його показників $I_{N.i.j}$ до існуючої чи створити нову статтю ЗВДТ $PV_{N.i.j}$. При цьому метод створює АСО та АСПО, що може бути основою автоматизації процесу проведення експертизи МНІ на предмет наявності чи відсутності у них відомостей, що становлять ДТ для окремого СРСД.

Очікується, що на основі використаної формальної мови опису ЗВДТ [31], метод буде підтримувати процес доповнення нових інформаційних елементів (статей) до СОІМ ЗВДТ [106] з багатовимірними просторами показників певних сфер N. При цьому повинні використовуватись відповідні критерії оптимізації, такі як критерії Байеса, критерії якості кластерного аналізу та кластеризації, що забезпечить точність роботи методу.

Сценарний метод оцінювання шкоди, заподіяної витоком секретної інформації

Рівень шкоди, обумовленої розголошенням СІ, є, за «Рекомендаціями…» [38], наслідком дій сторони, що заволоділа цією інформацією. Отже, цим припускається багатоваріантність можливих дій сторони, причому в загальному випадку ці варіанти є різноймовірними. Традиційне зведення множини варіантів до одного найбільш вірогідного для систем, що належать до класу складних (а це насамперед соціальні та соціотехнічні системи), не є прийнятним, бо має суттєво суб'єктивний характер і, крім того, може істотно знизити оцінку шкоди через неврахування інших, менш ймовірних наслідків.

Таким чином, оцінювання остаточної шкоди, обумовленої витоком СІ, має базуватися на врахуванні часткових оцінок шкоди, отриманих за різними варіантами розвитку подій, кожен з яких є наслідком можливих дій сторони, що заволоділа ДТ. Тобто фактично маємо задачу прогнозування подій у складній соціальній системі, зокрема, залежно від конкретної ситуації, в політичній, економічній, соціотехнічній тощо.

Соціальне прогнозування – досить складний процес, точність якого залежить від величезної кількості факторів, одним із яких є використання та дотримання вимог науково обґрунтованих методик генерації та відбору варіантів розвитку прогнозованої ситуації. При цьому, як зазначалося у [123], в даному випадку найбільшої актуальності набуває питання вибору способів та засобів багатоваріантного прогнозу. Деякої риторичності цьому питанню надає загальна визнаність ефективності застосування в таких задачах *методу сценаріїв* [97, 173], або як його називає низка науковців [64, 174, 175] – *сценарного підходу* чи *сценарного аналізу*.

Суттєва особливість сценарного підходу полягає в тому, що він, на відміну від класичних методів математичного прогнозу, не дає кількісної оцінки майбутнього значення певного прогнозованого параметру чи групи параметрів, а формує множину ймовірних станів, до

яких може розвинутися вихідна ситуація під впливом тих чи інших факторів. Це дозволяє стверджувати, що сценарний підхід можна розглядати як специфічний вид соціального планування. За висловом Е. Янга, «сценарій не передбачає майбутнє, а формує його варіант за наявності відповідних передумов» [174], тобто під сценарієм звичайно розуміють опис можливого розвитку подій у певній ситуації.

Суть та схему застосування сценарного підходу можна пояснити на прикладі аналізу функціонування певного соціального об'єкту, процес усталеної і передбачуваної життєдіяльності якого перервався появою аномалії – виникненням надзвичайної (критичної) ситуації. Для прогнозування характеру подальшого функціонування досліджуваного об'єкту генеруються (будуються) так звані сценарії – моделі можливих у майбутньому варіантів перебігу подій.

Відправною, початковою точкою для всіх сценаріїв є момент виникнення критичної ситуації, однак наступний розвиток подій за кожним із сценаріїв має свої індивідуальні особливості та відмінності, а кінцеві події та наслідки реалізації кожного із сценаріїв можуть бути абсолютно різними. Зазвичай метою сценарного прогнозування є аналіз та вивчення складу і послідовності подій кожного із сценаріїв, аналіз причинно-наслідкових зв'язків між подіями та визначення ймовірностей реалізації відповідних сценаріїв разом із оцінкою кінцевого стану досліджуваного об'єкту після завершення кожного зі сценаріїв.

Результатом виконання такого сценарного аналізу частіше за все є прийняття певного рішення та відповідних управлінських дій, які дозволяють у певному сенсі оптимізувати процес виведення соціального об'єкту із виниклої надзвичайної (критичної) ситуації. У ще більш загальній постановці методологія сценарного аналізу має забезпечити прогноз та виявлення можливої появи аномальностей у процесі функціонування соціального об'єкту, тобто розвитку будь-яких надзвичайних ситуацій, альтернативних станові нормального його функціонування.

Формально сценарій *S* можна описати, задавши: а) декомпозицію сценарію на сукупність послідовних подій-сцен, де кожна попередня сцена s_l трансформується $(\rightarrow)$ у наступну s_{l+1}: $\{s_k\}=\{s_1 \rightarrow s_2 \rightarrow ... \rightarrow s_k\}$; б) завершення кожної події s_l характеризується певним станом X_l / s_l досліджуваного об'єкту: $X_l / s_l = [(x_{l1}, x_{l2}, ..., x_{lm},) / s_l]$, $l = \overline{1,k}$, де $x_i, i = \overline{1,m}$ – змінні, що описують функціонування об'єкту у часі; в) ймовірність *p* реалізації сценарію *S* та наслідки *q* цієї реалізації, зокрема *q* може означати певні втрати, які зазнав об'єкт після виходу з надзвичайної ситуації за сценарієм *S*.

Загалом опис сценарію *S* може бути заданий четвіркою:

$$< \{s_k\}, \{X_k / s_k\},\ p,\ q > .$$

Якщо маємо декілька сценаріїв $s_1, s_2, ..., s_n$, які за умовами своєї реалізації утворюють повну групу, то, якщо q за своєю сутністю є характеристикою втрат, можемо визначити ймовірні втрати Q після виходу об'єкту з надзвичайної ситуації як середній ризик [64, 95]:

$$Q = \sum_{i=1}^{n} p_i q_i \ , \qquad (5.27)$$

де $p_i q_i$ – ризик реалізації *i*-ого сценарію.

Вважається, що вперше *метод сценаріїв* застосував Герман Кан для дослідження складних систем [175]. Спочатку сценарії мали суто описовий характер, потім почали використовуватись більш формалізовані конструкції [139]. Існують різні концепції генерації сценаріїв [97-99, 123], однак завершеного вирішення даної проблеми на сьогодні немає.

На практиці для генерації сценаріїв використовується достатньо широкий спектр методів, суттєво відмінних за умовами та особливостями свого застосування [97-99, 123].

Серед формалізованих методів, що дозволяють певною мірою впорядкувати процес якісного аналізу критичної (проблемної) ситуації та створити об'єктивні умови для побудови множини реалістичних варіантів (альтернатив) сценаріїв, можна у якості прикладу навести *метод морфологічного аналізу* [139]. Він достатньо поширений у практичних застосуваннях і, зокрема, для свого використання не вимагає наявності у дослідника якихось специфічних особливих знань чи інструментальних засобів. Суть цього методу полягає у визначенні на класі досліджуваних об'єктів за результатами їх морфологічного аналізу сукупності морфологічних класифікаційних ознак (параметрів) $П_1, П_2, ..., П_к$, що характеризують найбільш суттєві структурні особливості представників досліджуваного класу об'єктів, та завданні для кожного з цих параметрів множини його можливих значень [64, 95]:

$$\{П_{ij}\} = \{П_{i1}, П_{i2}, ..., П_{iq_i}\},\ i = \overline{1,k},\ j = \overline{1,q_i}, \qquad (5.28)$$

де $\{П_{ij}\}$ – морфологічний простір i-ої ознаки $П_i$.

Далі визначається декартів або прямий добуток морфологічних просторів усіх ознак [64, 95]:

$$\pi = \left\{ \Pi_{1j} \right\} \times \left\{ \Pi_{2j} \right\} \times \left\{ \Pi_{3j} \right\} \times ... \times \left\{ \Pi_{kj} \right\}. \qquad (5.29)$$

Множина π являє собою сукупність компонентів, кожний з яких – це кортеж з k елементів, по одному з відповідного вихідного морфологічного простору: з Π_1, з Π_2,..., з Π_k.. Ця множина включає кортежі, які обіймають усі можливі комбінації значень класифікаційних ознак (параметрів) $\Pi_1, \Pi_2, ..., \Pi_к$, утворюючи морфологічну скриню – спільний морфологічний простір для всього класу об'єктів.

Якщо йдеться про генерацію сценаріїв, то кожний кортеж сформованого спільного морфологічного простору являє собою окремий варіант сценарія. Однією з основних проблем у даній ситуації є скорочення кількості згенерованих варіантів. Це обумовлює необхідність вирішення задачі вилучення множини неперспективних (наприклад, малоймовірних) сценаріїв, виокремлення найбільш «раціональних» варіантів, тобто переходу до селекції реалістичних варіантів сценаріїв. У науковій літературі [98] ця частина морфологічного аналізу має власну назву – *синтез раціональних систем на морфологічних множинах*, чим підкреслюється його функціональна відмінність від першої частини методу сценаріїв – *методу морфологічної скрині*.

Загалом процедура розроблення сценаріїв, їх співставлення та аналіз потребують розв'язку низки задач, особливістю яких є наявність значної кількості латентних властивостей, показників, змінних, що не дозволяють прямого спостереження та вимірювання, характеризуються суттєвою інформаційною невизначеністю. В цій ситуації єдино можливим способом розв'язання подібних задач є застосування експертних методів спільно з ефективною апостеріорною обробкою отриманих експертних оцінок [115-122, 138, 144, 169].

При застосуванні сценарного аналізу до задач, пов'язаних з аналізом загроз щодо СІ, моментом виникнення критичної (проблемної) ситуації слід вважати саме реалізацію певної загрози відносно цієї інформації. Відповідно до процедури сценарного аналізу, слід згенерувати множину сценаріїв можливого розвитку подій, обумовлених реалізацією загрози СІ та оцінити наслідки розвитку подій за кожним із сценаріїв [95]. Якщо наявна множина сценаріїв дозволяє обрахувати часткову шкоду окремо за кожним з них та вказати часткову ймовірність реалізації кожного, можна побудувати певну ієрархічну структуру, зображену на рис. 36.

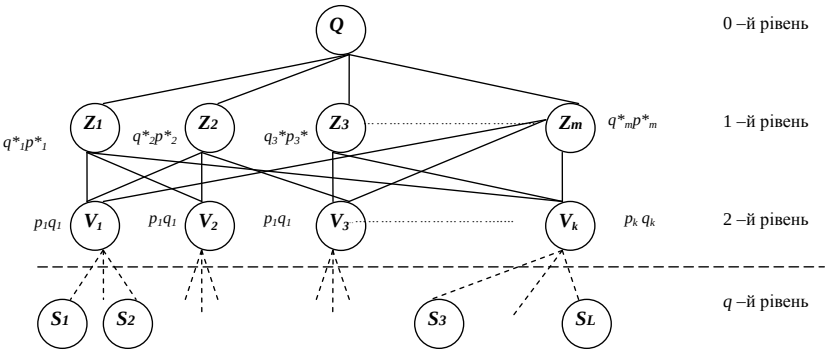


Рис. 36. Ієрархічне представлення результатів застосування сценарного підходу до обчислення СШ, заподіяної витоком СІ

Фокусом Q цієї ієрархії є кількісне значення сумарного збитку, розрахованого на певній множині незалежних подій $\{Z_i\}$, $i=\overline{1,m}$, кожній з яких можна зіставити часткову ймовірність p_i^* та частковий збиток q_i^*. Особливістю цієї ієрархії є можливість застосування апарату статистичних ризиків для розрахунку сумарного збитку як середнього ризику [64, 95] або, за прийнятою в літературі із захисту інформації термінологією, інформаційного ризику [26, 40, 41, 55, 100, 101, 138]:

$$Q=\sum_{i=1}^{m} p_i^* q_i^* \cdot \qquad (5.30)$$

Часткові ймовірності p_i^* та часткові збитки q_i^*, що є параметрами незалежних подій $\{Z_i\}$, $i=\overline{1,m}$, які утворюють перший рівень ієрархії, визначаються через ймовірності і збитки подій, що є результатами розвитку відповідних сценаріїв $\{Cu_j\}$, $j=\overline{1,k}$.

Абстрактність структури наведеної на рис. 36 вимагає більш детальних пояснень стосовно формалізму її ієрархії. Перш за все зупинимось на утворенні рівнів 0, 1, 2 (над пунктирною горизонтальною лінією) та взаємозв'язків між ними, що є ключовим моментом для застосування сценарного підходу до обчислення сумарного збитку.

Припустимо, що утворення збитків є наслідком незалежного розвитку множини сценаріїв $\{Cu_j\}$, $j=\overline{1,k}$, які розгортаються після втрати секретної інформації. За певний часовий інтервал T результатом реалізації цих сценаріїв стають відповідні незалежні події V_j, які, таким чином, є індикаторами завершення певних сценаріїв. Наша схема

набуває статичного вигляду, множина подій $\{V_j\}$, для кожної з яких визначена ймовірність P_j (ймовірність розвитку сценарію $Сц_j$), утворює поле подій, кожному з елементів якого можливо зіставити часткові збитки q_i^*. Однак безпосереднє обчислення середнього ризику на множині $\{V_j\}$ є неможливим через те, що ця сукупність подій не утворює повної групи. Тому виконується трансформація множини подій $\{V_j\}$ у скінченну множину $\{Z_i\}$, елементи якої відповідають комплексу умов, обов'язкових для повної групи, а саме попарна несумісність подій:

$$Z_i \bigcap Z_r = \varnothing, \quad i \neq r, \tag{5.31}$$

$$\bigcup_{i=1}^{m} Z_i = \Omega, \tag{5.32}$$

де Ω – достовірна подія.

Множині подій $\{Z_i\}$ зіставляється множина ймовірностей цих подій $\{P(Z_i)\} = \{p^*_i\}$, для якої справедливі ймовірності співвідношення, характерні щодо елементів повної групи [64, 95]:

$$P(\bigcup_{i=1}^{m} Z_i) = \sum_{i=1}^{m} P(Z_i) = \sum_{i=1}^{m} p_i^* = 1, \tag{5.33}$$

$$P(Z_i \bigcap Z_r) = 0, i \neq r. \tag{5.34}$$

Завдяки цьому стає можливим застосування апарату середніх ризиків для обчислення СШ Q.

Методику утворення повної групи подій розглянемо на прикладі, що припускає певну змістовну інтерпретацію, використавши для цього наведений у «Рекомендаціях…» [38] приклад визначення ступеня важливості інформації щодо бойової частоти системи керування нового зразка оперативно-тактичної ракети шляхом прогнозування дій сторони, що оволоділа цими відомостями. Нехай за результатами аналізу експертами можливих варіантів розвитку подій у ситуації, виниклій через витік інформації, найбільш ймовірними є припущення, що сторона, яка отримала цю інформацію, використає її для:

1) розробки засобів та методів радіоподавлення системи керування ракетою;

2) планування проведення військових операцій з врахуванням перспектив можливої нейтралізації дій нової оперативно-тактичної ракетної системи супротивної держави;

3) використання здобутої інформації у розробці та модифікації власних оперативно-тактичних ракетних систем;

4) передачі інформації союзникам чи іншим третім сторонам.

Тобто, маємо чотири варіанти розвитку подій (сценарії $Сц_1$, $Сц_2$, $Сц_3$, $Сц_4$), ймовірність яких визначається частковими ймовірностями p_1, p_2, p_3, p_4, а завершення – подіями-індикаторами V_1, V_2, V_3, V_4. Розгортання кожного з цих сценаріїв пов'язане з цілком конкретною сукупністю активів, серед яких у загальному випадку можна виділити три групи:

перша – це активи, що зазнали уражень безпосередньо через витік інформації про бойові частоти;

друга – активи, задіяні для ліквідації цих уражень та відновлення нормального рівня боєздатності оперативно-тактичних ракетних комплексів;

третя – активи (фінансово-економічні, технічні, людські тощо), які вирішено доцільним залучити для створення або підсилення СЗІ (остання група активів є спільною для усіх чотирьох сценаріїв).

Таким чином, *сценарний метод*, окрім всього іншого, дає змогу обрахувати за кожним зі сценаріїв частковий рівень втрат, обумовлених витоком інформації, який дорівнює сукупній вартості груп активів, пов'язаних з відповідним сценарієм. Часткові вихідні дані за кожним сценарієм наведено у табл. 24.

Таблиця 24

Вихідні дані за кожним сценарієм

варіанти розвитку події	*ймовірність реалізації*	*шкода від реалізації*
V_1	p_1	q_1
V_2	p_2	q_2
V_3	p_3	q_3
V_4	p_4	q_4

Спробуємо використати ці дані для визначення інтегрованих втрат, обумовлених витоком інформації. Зазначимо, що події V_1, V_2, V_3, V_4 не є несумісними, вони можуть відбуватися одночасно, а можуть й не відбуватися зовсім, тобто множина $\{V_j\}, j=\overline{1,4}$ не задовольняє вимогам до повної групи подій.

Тому постає завдання формування повної множини $\{Z_i\}$ елементарних подій, яка пов'язана із вихідною множиною $\{V_j\}$, але, на відміну від неї, задовольняє вимоги, що висуваються до повної групи. Кожна з подій $\{Z_i\}$ $i=\overline{1,m}$ являє собою суміщення чотирьох подій з множини V_1, V_2, V_3, V_4 або множини доповнюючих (протилежних) подій $\overline{V_1},\overline{V_2},\overline{V_3},\overline{V_4}$. Принциповою при формуванні елементарних подій $\{Z_i\}$, $i=\overline{1,m}$ є вимога врахування в їх структурі усіх можливих сполучень елементів множини $\{V_j\}$ включно із самою множиною цих подій та порожньою множиною $\varnothing$ (останній відповідає ситуація, в якій жоден із сценаріїв не реалізувався за час *T*).

Впорядкувати множину можливих станів системи подій $\{Z_i\}$, $i=\overline{1,16}$, сформованих на множині подій вихідної системи $\{V_j\}$, $j=\overline{1,4}$ можливо шляхом запровадження кількісного показника d числа сполучень множини $\{V_j\}$, одночасно присутніх (існуючих) після закінчення розвитку сценаріїв, тобто $d=1,2,3,4,0$ (останнє значення 0 відповідає ситуації, в котрій не відбулась жодна з подій множини).

У процесі формування подій множини $\{Z_i\}$ повинна зберегтися вся інформація про можливі стани вихідної системи подій $\{V_j\}$, зокрема про всі можливі сполучення цих подій, що виникли як наслідок розвитку сценаріїв, тобто всі ці можливі стани мають бути представлені у структурі подій множини $\{Z_i\}$.

На відміну від подій $\{V_j\}$, $j=\overline{1,4}$, жодна з подій $\{Z_i\}$, $i=\overline{1,16}$ не може з'явитись одночасно з іншою, лише поодинці, відтак результатом розвитку сценаріїв має бути обов'язкова поява однієї з подій множини $\{Z_i\}$.

Виходячи з цих принципів, для чотирьох перших елементарних подій маємо:

$$Z_1=V_1\cap\overline{V_2}\cap\overline{V_3}\cap\overline{V_4},\ Z_2=\overline{V_1}\cap V_2\cap\overline{V_3}\cap\overline{V_4},$$
$$Z_3=\overline{V_1}\cap\overline{V_2}\cap V_3\cap\overline{V_4},\ Z_4=\overline{V_1}\cap\overline{V_2}\cap\overline{V_3}\cap V_4.$$

Зважаючи на структуру наведених елементарних подій, легко обчислити часткові ймовірності їх реалізації. Так, для Z_i отримуємо: $P(Z_i)=p_1^*=p_1(1-p_2)(1-p_3)(1-p_4)$, формули для ймовірностей p_2^*, p_3^*,

p_4^* формуються таким же чином з використанням ймовірностей P_j для подій V_j та $(1-p_r)$ для доповнюючих подій $\overline{V_r}$.

Шість наступних елементарних подій $Z_5 \div Z_{10}$ будуть містити попарні сполучення елементів множини $\{V_j\}$, наприклад:

$$Z_5 = V_1 \cap V_2 \cap \overline{V_3} \cap \overline{V_4},\ Z_6 = \overline{V_1} \cap V_2 \cap \overline{V_3} \cap V_4,\ Z_{10} = \overline{V_1} \cap \overline{V_2} \cap V_3 \cap V_4.$$

Відповідно для обчислення ймовірностей цих елементарних подій отримуємо [64, 95]:

$$P(Z_5) = p_5^* = p_1 p_2 (1-p_3)(1-p_4), \tag{5.35}$$

$$P(Z_{10}) = p_{10}^* = (1-p_1)(1-p_2) p_3 p_4. \tag{5.36}$$

Події $Z_{11} \div Z_{14}$ у свою чергу включатимуть потрійні сполучення подій з множини $\{V_j\}$: $Z_{11} = V_1 \cap V_2 \cap V_3 \cap \overline{V_4}$,…, $Z_{14} = \overline{V_1} \cap V_2 \cap V_3 \cap V_4$ й характеризуватимуться відповідно ймовірностями виду [64, 95]:

$$p_{11}^* = p_1 p_2 p_3 (1-p_4), \ldots, p_{14}^* = (1-p_1) p_2 p_3 p_4. \tag{5.37}$$

Структура події Z_{15} враховує останнє можливе сполучення подій з множини $\{V_j\}$: $Z_{15} = V_1 \cap V_2 \cap V_3 \cap V_4$, ймовірність якого визначається очевидним виразом [64, 95]:

$$p_{15}^* = p_1 p_2 p_3 p_4. \tag{5.38}$$

Остання елементарна подія множини $\{Z_i\}$ має врахувати можливість відсутності реалізації будь-якого зі сценаріїв множини $\{Sc_j\}$: $\overline{V_1 \cup V_2 \cup V_3 \cup V_4}$, у термінах обчислення подій ми маємо [64, 95]:

$$Z_{16}^* = \Omega \setminus \bigcup_{j=1}^{4} V_j\ . \tag{5.39}$$

Ймовірність цієї елементарної події дорівнює [64, 95]:

$$p_{16}^* = \prod_{j=1}^{4} (1-p_j), \tag{5.40}$$

У повному обсязі множина структур подій та вирази для обчислення відповідних ймовірностей p_i^* наведені у табл. 25.

Таблиця 25

Трансформація «природної» множини подій $\{V_j\}$, $j=\overline{1,4}$

у повну групу «штучних» подій $\{Z_i\}$, $i=\overline{1,16}$

Z_i	d	Зміст (структура) події z_i	$P(Z_i)=p_i^*$	q_i^*
Z_1	1	$V_1\cap\overline{V_2}\cap\overline{V_3}\cap\overline{V_4}$	$p_1(1-p_2)(1-p_3)(1-p_4)$	q_1
Z_2	1	$\overline{V_1}\cap V_2\cap\overline{V_3}\cap\overline{V_4}$	$(1-p_1)p_2(1-p_3)(1-p_4)$	q_2
Z_3	1	$\overline{V_1}\cap\overline{V_2}\cap V_3\cap\overline{V_4}$	$(1-p_1)(1-p_2)p_3(1-p_4)$	q_3
Z_4	1	$\overline{V_1}\cap\overline{V_2}\cap\overline{V_3}\cap V_4$	$(1-p_1)(1-p_2)(1-p_3)p_4$	q_4
Z_5	2	$V_1\cap V_2\cap\overline{V_3}\cap\overline{V_4}$	$p_1p_2(1-p_3)(1-p_4)$	q_1+q_2
Z_6	2	$V_1\cap\overline{V_2}\cap V_3\cap\overline{V_4}$	$p_1(1-p_2)p_3(1-p_4)$	q_1+q_3
.....	…	……	……	……
Z_{10}	2	$\overline{V_1}\cap\overline{V_2}\cap V_3\cap V_4$	$(1-p_1)(1-p_2)p_3p_4$	q_3+q_4
Z_{11}	3	$V_1\cap V_2\cap V_3\cap\overline{V_4}$	$p_1p_2p_3(1-p_4)$	$q_1+q_2+q_3$
Z_{12}	3	$V_1\cap V_2\cap\overline{V_3}\cap V_4$	$p_1p_2(1-p_3)p_4$	$q_1+q_2+q_4$
Z_{13}	3	$V_1\cap\overline{V_2}\cap V_3\cap V_4$	$p_1(1-p_2)p_3p_4$	$q_1+q_3+q_4$
Z_{14}	3	$\overline{V_1}\cap V_2\cap V_3\cap V_4$	$(1-p_1)p_2p_3p_4$	$q_{21}+q_3+q_4$
Z_{15}	4	$V_1\cap V_2\cap V_3\cap V_4$	$p_1p_2p_3p_4$	$q_1+q_2+q_3+q_4$
Z_{16}	0	$\Omega\setminus(V_1\cup V_2\cup V_3\cup V_4)$	$(1-p_1)(1-p_2)(1-p_3)(1-p_4)$	0

В загальному випадку кількість елементів множини $\{Z_i\}$ визначається формулою (5.7), зокрема, для $k=4$ отримуємо $m=16$.

При формуванні множини подій $\{Z_i\}$ враховано всі можливі варіанти перебігу подій, що могли статися в ході реалізації сценаріїв (збережені усі можливі сполучення подій з множини $\{V_j\}$, включаючи і повну відсутність подій), тобто в цьому сенсі немає втрат інформації при трансформуванні множини подій $\{V_j\}$ в множину $\{Z_i\}$. Однак елементарні події повної множини $\{Z_i\}$ попарно незалежні і утворюють повну групу подій, що дозволяє застосувати до них математичний

апарат теорії статистичних ризиків, зокрема обчислити середній ризик у традиційній формі за формулою (5.30).

Вирази для обчислення часткової шкоди $\{Q_i^*\}$, $i=\overline{1,16}$, прийнявши гіпотезу адитивності часткової шкоди, доволі нескладно отримати, аналізуючи логічну структуру подій $\{Z_i\}$. Так для $z_1 = V_1 \cap \overline{V}_2 \cap \overline{V}_3 \cap \overline{V}_4$ маємо [64, 95]:

$$q_1^* = q(V_1 \cap \overline{V}_2 \cap \overline{V}_3 \cap \overline{V}_4) = q_1. \qquad (5.41)$$

Відповідно, $q_2^* = q_2, ..., q_4^* = q_4$. Аналогічним чином для подій $z_5 \div z_{10}$ отримуємо: $q_5^* = q_1 + q_2, ..., q_{10}^* = q_3 + q_4$, для z_{11}: $q_{11}^* = q_1 + q_2 + q_3$, для z_{15}: $q_{15}^* = \sum_{j=1}^{4} q_j$. Очевидно, що для події z_{16} (відсутність будь-яких подій з множини $\{V_j\}$) часткова шкода відсутня: $q_{16}^* = 0$. В упорядкованому вигляді вирази для обчислення шкоди q_i^* наведено в останньому стовпчику табл. 25.

Застосування запропонованого методу сценаріїв потребує окремих методичних зауважень. Перш за все, якщо вважати відомими значення ймовірностей $\{p_j\}$ та збитків $\{q_j\}$ і не цікавитися походженням цієї інформації (припустити її абсолютний експертний характер), то при проведенні аналізу за методом сценаріїв можна обмежитися трьома верхніми рівнями схеми, зображеної на рис. 36. Однак за необхідності обґрунтування чи пояснення кількісних значень цих оцінок виникає проблема деталізації і висвітлення їх появи, що в свою чергу викликає виникнення додаткових рівнів передподій (третього, четвертого,..., наступного). Наприклад, для пояснення збитків за Cu_1, Cu_2 необхідно проаналізувати дії сторони, що отримала інформацію, і відповідно власні дії із запобігання негативним наслідкам дій супротивної сторони, зокрема витрати на нейтралізацію та протидію можливим загрозам, обумовленим витоком інформації.

Економіко-вартісна складова цього аналізу дасть обґрунтування оцінки збитків, а професійно орієнтована дозволить об'єктивно оцінити залишкові ймовірності загроз.

Тобто четвертий рівень ієрархії – це взаємопов'язаний перелік негативних дій супротивної сторони та відповідного комплексу заходів з їх нейтралізації для кожного із сценаріїв, що дає змогу простежити

природу (джерела) виникнення збитків та складові, що формують кількісні показники ймовірностей $\{P_j\}$.

Деталізація елементів четвертого рівня, наприклад, визначення конкретних механізмів та методів захисту, що складають комплекс захисних заходів, утворює нижчий (п'ятий) рівень ієрархії.

Слід зауважити, що надмірна конкретизація в задачах прогнозу, особливо із застосуванням методів експертного оцінювання, може іноді заважати [64], тож доцільність використання нижчих рівнів ієрархізації (від четвертого рівня і далі) слід визначати за кожним сценарієм окремо, приймаючи до уваги специфіку проблем енної галузі, рівень обізнаності експертів тощо. Крім того, після формування початкового списку сценаріїв при переході до аналізу варто врахувати можливості та результати їх взаємного впливу за умови одночасного розгортання (посилення, доповнення чи взаємну нейтралізацію) [123].

Метод визначення рівня компетентності членів експертної комісії при державних експертах з питань таємниць

При розробці методів експертного оцінювання шкоди національній безпеці у сфері ОДТ виникають проблеми, викликані неповнотою і недостовірністю ретроспективних та прогнозованих даних фахівців ЕК, що залучаються до підготовки рішень та висновків ДЕТ, які виникають при виконанні процедури віднесення інформації до ДТ, зміни СС цієї інформації, розсекречування та засекречуванні МНСІ (рис. 37).

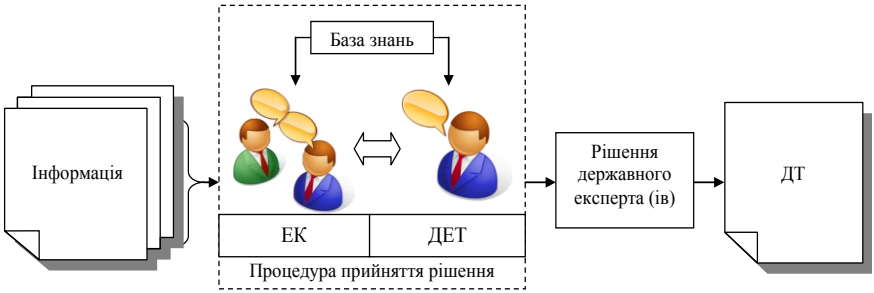


Рис. 37. Процес експертного оцінювання відомостей та прийняття рішення

ЕК, використовуючи свої знання, досвід, інтуїцію, а також колективний підхід до вироблення рекомендацій на початкових етапах вирішення завдань, визначає і (або) прогнозує вихідні дані щодо шкоди національній безпеці України у разі розголошення конкретної СІ. Як наслідок, надає власним рішенням відповідний СС такої інформації, що

відносить її до ДТ, або робить висновок про скасування цього рішення залежно від важливості змісту відомостей. Змісту відомостей, що становлять ДТ присвоюється СС, а її матеріальним носіям ГС – «ОВ», «ЦТ», «Т».

У разі наявності такої інформації в акті експертизи зазначаються, які саме відомості становлять ДТ, з посиланням на статті ЗВДТ, пункти РПВДТ, та, за необхідності, наводиться їх стислий зміст, а також робляться посилання на сторінки, пункти, абзаци, речення, у яких вони містяться (див. *Додаток 4*).

У працях [177, 178] наведено достатньо багато підходів до дослідження рівня компетентності експертів, що базуються значною мірою на методах елементарної алгебри [177], понятійному апараті психології [178] і суб'єктивних судженнях. Їх недоліками, з огляду до сфери ОДТ, є [122]: несистемний підхід до формалізації проблеми і класифікації інформації за змістом відомостей; недостатня поінформованість експертів ЕК про конкретний об'єкт експертизи; нечітка постановка завдання перед ЕК, а також відсутність єдиного формування вихідних даних і результатів експертизи (кількісної оцінки відомостей) процедури прийняття рішення щодо віднесення відомостей до ДТ.

Удосконалено та адаптовано до сфери ОДТ ***метод визначення рівня компетентності членів ЕК при ДЕТ*** [122] за допомогою використання компонентів *моделі ІППШ* (див. п.5.1) при експертному визначення виду СС відомостей, а саме у вигляді балів – за середнім значенням прогнозованої величини СШ ($\overline{\boldsymbol{W}_{cc}}$), інтервалу – за критерієм визначення СС ($W_i < \boldsymbol{W}_{cc} < W_j$) та ЛЗ «СС» – «ОВ», «ЦТ», «Т».

Класифікуємо види можливих ***відповідей*** **(*Z*)** щодо типу надання СС наступним чином:

Z_1 – «число» ($\overline{W_T} = 5$, $\overline{W_{ЦТ}} = 55$, $\overline{W_{OB}} = 200$);

Z_2 – «інтервал» ($1 \le W_T < 10$, $10 \le W_{ЦТ} < 100$, $100 \le W_{OB} \le 300$);

Z_3 – «нечіткий інтервал» («ОВ», «ЦТ», «Т»).

Проведемо визначення рівня компетентності членів ЕК на основі аксіоми незміщеності, згідно з якою рішення більшості є компетентним, і, як наслідок, найкомпетентнішим будемо вважати того експерта, розбіжність суджень якого із рішенням ЕК є мінімальною. Нехай n – кількість експертів, m – кількість відповідей, при чому $m = \sum_{i=1}^{3} m_i$, де m_i – кількість відповідей i-го виду, i = 1,…3, викладеної вище

класифікації Z. Необхідно визначити рівні компетентності експертів ЕК γ_j, $j = 1,\ldots n$.

Сутність методу полягає у визначенні матриць, що містять значення розбіжностей суджень членів ЕК, їх аналізі та перетвореннях, у результаті яких будуть визначені рівні компетентності експертів. Для подальшої алгоритмізації методу базовим варіантом вважатимемо випадок відсутності інформації про рівні компетентності членів ЕК. Залежно від виду відповіді визначимо процедури оцінювання рівня компетентності.

Визначення компетентності експертів ЕК для відповіді виду Z_1. Експерт для кожних q-х відомостей, $q = \overline{1,m_1}$, визначає кількість відповідей k_q і надає кожній відповіді певний бал a_{ij} i-го експерта за відповідь на j-і відомості згідно з можливим СС. Відповіді даного виду впорядковані за збільшенням балів (грифа секретності), тобто має місце кількісна або змістовна градація.

Методом експертного опитування формуємо числову матрицю [177]:

$$A = (a_{ij})_{i=1,\ j=1}^{n\quad m_1}. \tag{5.42}$$

Формується послідовність трикутних матриць [122, 177]:

$$\{T_1^k\}_{k=\overline{1,m_1}}, \text{ де } T_1^k = (t_{ij}^k)_{i,j=1}^n,\ t_{ij}^k = \left|a_{ik} - a_{jk}\right|,\ i > j \text{ при } i \le j,\ t_{ij}^k = 0. \tag{5.43}$$

Обчислюються елементи матриці $T_1^{k'} = (t_{ij}^{k'})_{i,j=1}^n, t_{ij}^{k'} = 1/t_{ij}^k$ при $i > j$ і $t_{ij}^k \neq 0$, якщо $i > j$ і $t_{ij}^k = 0$, то раціонально покласти $t_{ij}^{k'} = \dfrac{2}{\min\limits_{t_{ij}^{'} \neq 0} t_{ij}^k}$, інші нульові елементи залишаються без змін. Як наслідок, $T_1^{'} = \left(t_{ij}^{'}\right)_{i,j=1}^n$, де $t_{ij}^{'} = \sum\limits_{k=1}^{m_1} t_{ij}^{k'}$ при $i > j$, а якщо $i \le j$, то $t_{ij}^{'} = 0$.

Нормуванням елементів матриці $T_1^{'}$ отримаємо [122, 177]:

$$T_1 = (t_{ij})_{i,j=1}^{n},\ t_{ij} = \frac{t_{ij}'}{\sum\limits_{i>1} t_{ij}'} \text{ при } i > j\,. \tag{5.44}$$

Якщо за відповідями виду Z_1 є необхідність у попередньому висновку про компетентність членів ЕК, то здійснюється її обчислення за формулою [122, 177]:

$$\gamma_p = \sum_{\substack{ij=1 \\ i>j \\ (j=p)\vee(i=p)}}^{n} t_{ij} \Big/ \sum_{p=1}^{n} \sum_{\substack{ij=1 \\ i>j \\ (j=p)\vee(i=p)}}^{n} t_{ij}\,,\ p = \overline{1,n.} \tag{5.45}$$

Визначення компетентності експертів ЕК для відповіді виду Z_2.

Методом експертного опитування формуємо матрицю $A = (a_{ij})_{i=1,\,j=1}^{n\quad 2m_2}$, де

$a_{ij} =$ { число – лівий кінець інтервалу відповіді *i*-го експерта на *j*-і відомості, де $j = 2k-1,\ k = \overline{1,m_2}$,
число – правий кінець інтервалу відповіді *i*-го експерта на *j*-і відомості, де $j = 2k,\ k = \overline{1,m_2}$.

Формуємо послідовність трикутних матриць $\{T_2^k\}_{k=\overline{1,m_2}}$, де $T_2^k = (t_{ij}^k)_{i,j=1}^{k}$ і

$$t_{ij}^k = \frac{1}{2}\chi(\min\{a_{il}, a_{jl}\} \ge \max\{a_{iq}, a_{jq}\})(\min\{a_{il}, a_{jl}\} - \max\{a_{iq}, a_{jq}\}) \times$$
$$\times\left(\frac{1}{a_{il} - a_{iq}} + \frac{1}{a_{jl} - a_{jq}}\right), \tag{5.46}$$

де $l = 2k,\ q = 2k-1,\ k = \overline{1,m_2}, i > j$ і $t_{ij}^k = 0$ при $j \ge i$. Наступні дії виконуються аналогічно крокам відповіді виду Z_1.

Визначення компетентності членів ЕК для відповіді виду Z_3. Методом експертного опитування визначаємо ЛЗ «СС» («ОВ», «ЦТ», «Т») у вигляді набору елементів $(\underline{W}_i^k, \overline{W}_j^k, w(PV_{1.i.j})^k, Q_{1.i}^k, \psi_n^k, T_н^k)$, $k = \overline{1,m_3}$.

Для ЛЗ "СС" набір необхідних елементів матиме наступний вигляд:

$$\text{«Т»} = (\underline{W_T}, \overline{W_T}, Q_{1.i}, w(PV_{1.i.j}), \psi_n^k, T_T);$$

$$\text{«ЦТ»} = (\underline{W_{ЦТ}}, \overline{W_{ЦТ}}, Q_{1.i}, w(PV_{1.i.j}), \psi_n^k, T_{ЦТ});$$

$$\text{«ОВ»} = (\underline{W_{OB}}, \overline{W_{OB}}, Q_{1.i}, w(PV_{1.i.j}), \psi_n^k, T_{OB}),$$

де $w(PV_{1.i.j})$ – "вага" *j*-х пунктів *i*-х статей переліку відомостей $PV_{1.i.j}$, що становлять ДТ у сфері оборони; $Q_{1.i}$ – максимальна "питома вага" об'єктів відомостей ДТ *i*-х статей ЗВДТ у сфері оборони; $T_н$ – строк дії рішення про віднесення відомостей до ДТ та їх СС ($T_T = 5$, $T_{OB} = 10$, $T_{ЦТ} = 30$ років).

Для кожного експерта обчислюємо абсолютне значення параметра максимальної впевненості у визначеній СС відомостей, що становлять ДТ [122, 177]:

$$\psi_n^k = \frac{T_н^k}{2}(\underline{W_i} + \overline{W_j})_n + \frac{T_н^k}{4}(w(PV_{1.i.j}) - Q_{1.i})_n \Big/ 100\%\ ,\ k = \overline{1, m_3}. \qquad (5.47)$$

Обчислюємо елементи матриці $T_3^k = (t_{ij}^k)_{i,j=1}^n$, де

$$t_{ij}^k = \frac{\left|\psi_i^k - \psi_j^k\right|}{\max\limits_i \psi_i^k - \min\limits_i \psi_i^k}, \quad i, j = \overline{1,n},\ i > j,\ k = \overline{1,m_3}. \qquad (5.48)$$

Далі необхідно отримані матриці T_3^k додати і проводити обчислення аналогічно крокам відповіді виду Z_1.

Наприклад, необхідно визначити рівні компетентності п'ятьох членів ЕК з питань таємниць за відомостями ДТ, що мають СС – «ОВ», «ЦТ», «Т» для відповідей виду Z_3, статей $PV_{1.1.j}$, $PV_{1.4.j}$, $PV_{1.9.j}$ ЗВДТ з максимальною «питомою вагою» об'єктів цих відомостей та з найбільшою прогнозованою СШ національній безпеці України у разі їх розголошення (табл. 26).

Таблиця 26

Результати експертного опитування

№ (n)	Номер питання														
	1					2					3				
	Т					ЦТ					ОВ				
	$\underline{W_T}$	$\overline{W_T}$	Q_{1i}	$w(PV_{1i,j})$	ψ_n^k	$\underline{W_{ЦТ}}$	$\overline{W_{ЦТ}}$	Q_{1i}	$w(PV_{1i,j})$	ψ_n^k	$\underline{W_{OB}}$	$\overline{W_{OB}}$	Q_{1i}	$w(PV_{1i,j})$	ψ_n^k
1	2	4	300	745	5,712	50	60	300	1215	33,93	120	160	300	1665	172,81
2	7	8	300	745	5,937	48	70	300	1215	34,33	135	170	300	1665	176,56
3	6	7	300	745	5,887	65	80	300	1215	35,68	110	200	300	1665	177,31
4	8	9	300	745	5,987	30	40	300	1215	31,93	150	170	300	1665	178,81
5	4	5	300	745	5,787	98	99	300	1215	37,18	200	260	300	1665	199,81

Значення ψ_n^k, $k=\overline{1,m_3}$, отримано за формулою (5.47). Далі обчислюються елементи (5.48) і формуються матриці T_3^k [122, 177]:

$$T_3^k=\begin{pmatrix} t_{12} & 0 & 0 & 0 \\ t_{13} & t_{23} & 0 & 0 \\ t_{14} & t_{24} & t_{34} & 0 \\ {}_{15} & t_{25} & t_{35} & t_{45} \end{pmatrix}; \qquad (5.49)$$

$$T_3^1=\begin{pmatrix} 0,(81) & 0 & 0 & 0 \\ 0,(63) & 0,(18) & 0 & 0 \\ 1 & 0,(18) & 0,(36) & 0 \\ 0,2(36) & 0,(54) & 0,(36) & 0,(72) \end{pmatrix}; \quad T_3^2=\begin{pmatrix} 0,76 & 0 & 0 & 0 \\ 0,(3) & 0,26 & 0 & 0 \\ 0,38 & 0,46 & 0,71 & 0 \\ 0,62 & 0,54 & 0,29 & 0,1 \end{pmatrix};$$

$$T_3^3=\begin{pmatrix} 0{,}14 & 0 & 0 & 0 \\ 0{,}17 & 0{,}03 & 0 & 0 \\ 0{,}22 & 0{,}08 & 0{,}06 & 0 \\ 1 & 0{,}86 & 0{,}83 & 0{,}78 \end{pmatrix}.$$

Розраховуються матриці $T_3^{k'}$, елементи яких є оберненими до елементів T_3^k, і обчислюються їх суми [122, 177]:

$$T_3^{k'} = \begin{pmatrix} t_{12}^{-1} & 0 & 0 & 0 \\ t_{13}^{-1} & t_{23}^{-1} & 0 & 0 \\ t_{14}^{-1} & t_{24}^{-1} & t_{34}^{-1} & 0 \\ t_{15}^{-1} & t_{25}^{-1} & t_{35}^{-1} & t_{45}^{-1} \end{pmatrix}; \qquad (5.50)$$

$$\begin{pmatrix} 1,22 & 0 & 0 & 0 \\ 1,56 & 5,56 & 0 & 0 \\ 1 & 5,56 & 2,78 & 0 \\ 4,24 & 1,82 & 2,78 & 1,37 \end{pmatrix} + \begin{pmatrix} 1,32 & 0 & 0 & 0 \\ 3,3 & 3,85 & 0 & 0 \\ 2,63 & 2,17 & 1,41 & 0 \\ 1,61 & 1,85 & 3,45 & 1 \end{pmatrix} +$$

$$+ \begin{pmatrix} 7,14 & 0 & 0 & 0 \\ 5,88 & 33,3 & 0 & 0 \\ 4,55 & 12,5 & 16,67 & 0 \\ 1 & 1,16 & 1,21 & 1,28 \end{pmatrix} = \begin{pmatrix} 9,68 & 0 & 0 & 0 \\ 10,75 & 42,74 & 0 & 0 \\ 8,18 & 20,23 & 20,86 & 0 \\ 6,85 & 4,83 & 7,44 & 3,65 \end{pmatrix}.$$

Далі знаходяться абсолютні значення рівнів компетентності за формулою (5.45), а нормуючи їх, визначаються відносні рівні компетентності експертів ЕК $\overline{\gamma_1} = 0,42$; $\overline{\gamma_2} = 0,57$; $\overline{\gamma_3} = 0,63$; $\overline{\gamma_4} = 0,59$; $\overline{\gamma_5} = 0,74$. Якщо вважати, що відносний рівень компетентності перебуває у межах $0 < \overline{\gamma_n} \le 1$, то отримані результати свідчать про досить «високий» рівень компетентності експертів, який перевищує 0,5 загального рівня компетентності всієї ЕК.

Визначено рівень компетентності членів ЕК при ДЕТ з використанням кількісного оцінювання важливості інформації з метою якісного віднесення її до ДТ у сфері оборони, зміни ступеня її секретності та розсекречування. Це, у свою чергу, дасть змогу сформувати якісний склад ЕК та визначити оптимальний СС, що в свою чергу вплине на обсяг фінансування заходів, необхідних для охорони такої інформації.

Розділ 6. СИСТЕМА ОЦІНЮВАННЯ ШКОДИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ У РАЗІ ВИТОКУ ДЕРЖАВНОЇ ТАЄМНИЦІ

6.1. Методологія синтезу системи оцінювання шкоди національній безпеці у разі витоку державної таємниці

Відомо, що методологічний базис є найважливішим компонентом теорії захисту інформації, який складається з сукупності методів і моделей, необхідних і достатніх для досліджень проблем і вирішення практичних завдань відповідного призначення. У зв'язку з цим на особливу увагу заслуговує завдання оцінювання шкоди національній безпеці України у разі витоку ДТ. Проте, при практичному використанні існуючих засобів забезпечення сфери ОДТ члени ЕК при ДЕТ не завжди можуть чітко детермінувати оціночні параметри, оскільки їх часто виражають в якісній формі.

Тому, особливий інтерес представляють системи, які дозволяють ефективно проводити оцінювання шкоди (з врахуванням якісної і кількісної оцінки) в нечіткому слабоформалізованому середовищі. У зв'язку з цим, розроблено *методологію синтезу системи оцінювання шкоди національній безпеці України у разі витоку ДТ*.

Використовуючи відомий підхід [112] до побудови методологій (синтезу систем оцінки рівня безпеки інформації в комп'ютерних системах, оцінки систем технічного захисту інформації на програмно-керованих автоматичних телефонних станцій і вибору найкращого варіанту на базі інтегрованої оцінки рівня гарантій захищеності інформаційних ресурсів), а також логіко-лінгвістичний підхід, пропонується, на підставі розроблених *моделей* (див. п. 5.1) та *методів* (див. п. 5.2), ***методологія синтезу системи оцінювання шкоди національній безпеці України у разі витоку ДТ*** [169, 176].

Вона містить десять ***етапів*** (рис. 38):

1-2) *кваліфікація порушення та ідентифікація можливих атак;*

3-4) *ідентифікація загроз та відомостей, що становлять ДТ;*

5) *визначення ідентифікуючих та оціночних параметрів;*

6) *оцінювання важливості відомостей за сферами ДТ;*

7) *визначення рівня компетентності;*

8) *оцінювання основних коефіцієнтів;*

9) *інтерпретація іншого тяжкого наслідку;*

10) *оцінка величини сукупної шкоди національній безпеці.*

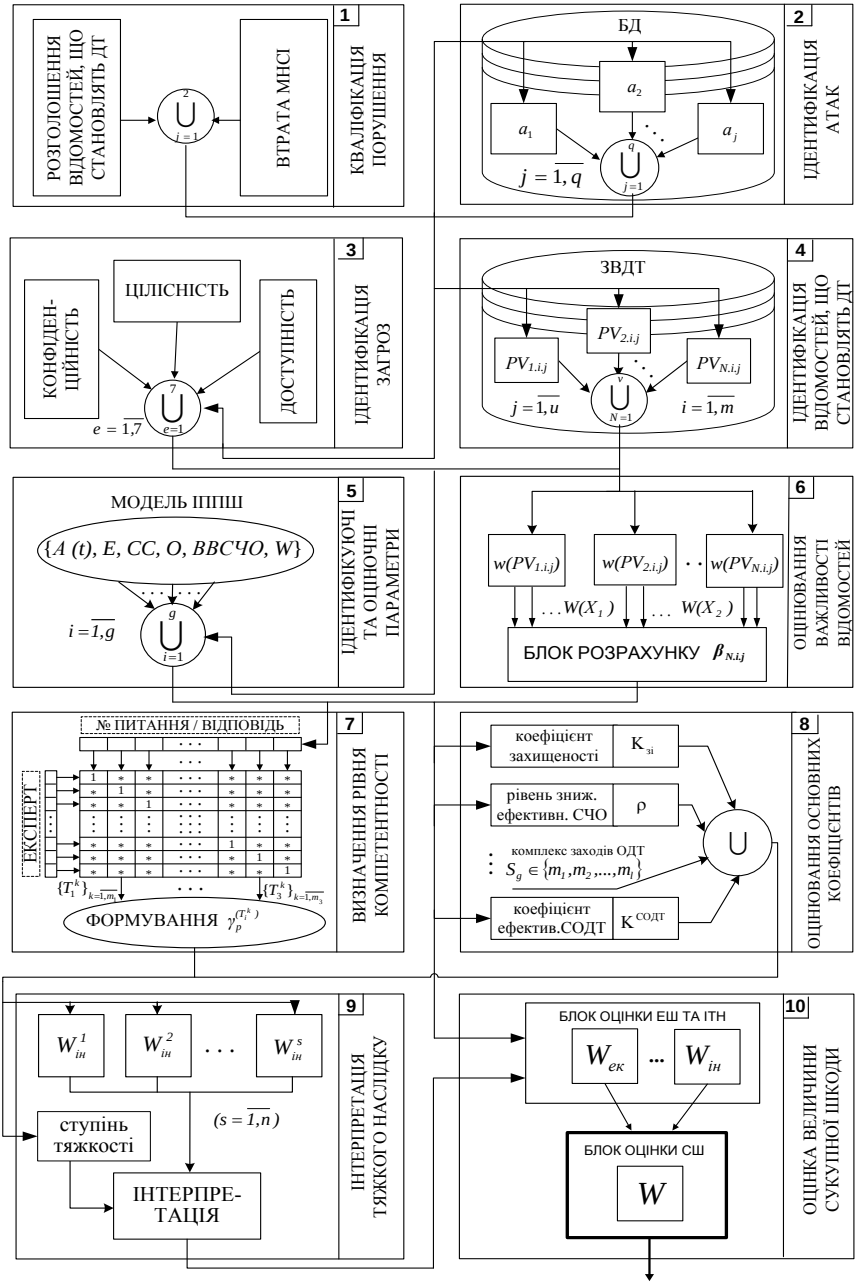


Рис. 38. Схема методології синтезу системи оцінювання шкоди національній безпеці України у разі витоку ДТ

Проведемо детального опису кожного з етапів [169, 176].

Етап 1-2. Кваліфікація порушення та ідентифікація можливих атак. На перших етапах для кваліфікації ***порушення (подій)*** **(*E*)** та ідентифікації можливих ***атак*** **(*A*)** необхідно виконати крок 1 «*Методу аналізу і оцінки величини можливої шкоди національній безпеці у сфері ОДТ*» (див. п. 5.2), використовуючи при цьому засіб забезпечення сфери ОДТ – розділ 6 колонка 3 «Звіту про стан забезпечення ОДТ» [29] і методику оцінювання ефективності функціонування СОДТ [125].

Етап 3. Ідентифікація загроз. Наступним етапом проводиться ідентифікація основних ***загроз*** **(*T*)** направлених на запобігання порушення (П) властивостей захищеності інформації (конфіденційності (К), цілісності (Ц), доступності (Д)) при e=7 як: t_1 = «ПК»; t_2 = «ПЦ»; t_3 = «ПД»; t_4 = «ПКЦ»; t_5 = «ПКД»; t_6 = «ПЦД»; t_7 = «ПКЦД», що визначають вимоги до функціонування складу комплексу засобів захисту автоматизованих систем для обробки інформації однієї або кількох категорій конфіденційності в РСО СРСД, де організовано та забезпечено РС з метою ефективного функціонування СОДТ. Множина таких загроз T приймає вигляд: $T = \{t_e\}, e = \overline{1, 7}.$

Етап 4. Ідентифікація відомостей, що становлять ДТ. Даний етап проводить за кроком 2 «*Методу аналізу і оцінки величини можливої шкоди національній безпеці у сфері ОДТ*» ідентифікацію ***відомостей, що становлять ДТ*** **(x_i)** відносно яких відбулися *E*, *A*, що призвели до *T*, використовуючи при цьому такі засоби забезпечення сфери ОДТ: розділ 6 колонка 6 «Звіту про стан забезпечення ОДТ» [29] та ЗВДТ [31].

Етап 5. Визначення ідентифікуючих та оціночних параметрів. На цьому етапі для створення можливості ЕК при ДЕТ у процесі оцінювання використовувати ширший спектр необхідних величин **<*E*, *A*, x_i, *CC*, *S*, K_{3i}, ρ, *ВВСЧО*, K_c, *W*>**, пропонується використовувати *модель ІПППШ*, яка отримана на основі розроблених моделей (див. п. 5.1).

За результатами проведення п'ятого етапу формується набір оцінних параметрів, які необхідні для систем оцінювання шкоди національній безпеці у сфері ОДТ на етапах 8-10.

Етап 6. Оцінювання важливості відомостей. Цей етап повністю виконується «*Методом оцінювання важливості відомостей за сферами ДТ*» (див. п. 5.2), який за 3 кроки оцінює одну із основних властивостей відомостей, що становлять ДТ – ***важливість*** **($\beta_{N.i.j}$)**. У якості засобів використовується методика визначення підстав для віднесення відомостей до ДТ та визначення їх СС (див. п.1.3), а також ЗВДТ [31].

Етап 7. Визначення рівня компетентності. На даному етапі проводиться визначення рівня ***компетентності*** **(γ_p)** членів ЕК при

ДЕТ за допомогою удосконаленого «*Методу визначення рівня компетентності членів ЕК при ДЕТ*» (див. п. 5.2). В основу методу, на відміну від відомих, покладено застосування набору оціночних параметрів моделі ІППШ у комбінованих видах суджень експерта відповіді якого формують трикутні матриці і після нормування їх елементів проводиться визначення рівня компетентності (формула (5.45)).

Етап 8. Оцінювання основних коефіцієнтів. Проводиться оцінювання основних коефіцієнтів, які характеризують: а) рівень зниження ефективності **(ρ)** використання СЧО відомостей; б) ефективність фукнціонування СОДТ **($K^{СОДТ}$)**; в) захищеність інформації **($K_{зі\,N}$)**; г) ступінь можливого старіння відомостей **(K_c)**; д) інші стани забезпечення ОДТ тощо.

Даний етап потребує використання методики оцінювання ефективності СОДТ, проведення кроків 3-10 «*Методу аналізу і оцінки величини можливої шкоди національній безпеці у сфері ОДТ*» та засобів забезпечення сфери ОДТ: розділи «Звіту про стан забезпечення ОДТ» [29] та ЗВДТ [31]. За його результатами проводиться обґрунтування величини фінансування заходів на ОДТ для забезпечення РС та кількісний розрахунок ***показника ЕШ*** **($W_{ек}$)** та ***ІТН*** **($W_{ін}$)** у балах.

Етап 9. Інтерпретація тяжкого наслідку. На передостанньому етапі, використовуючи методику визначення підстав для віднесення відомостей до ДТ, а саме *перелік ІТН* (див. п. 1.3), що містить п'ять сформованих категорій можливих наслідків за ступенем їх тяжкості, проводиться інтерпретація ***прогнозованої*** бальної величини ***шкоди*** **($W_{ін}$)** до опису тяжкого наслідку, що мав місце. Результатом етапу є остаточна кількісна та якісна оцінка величини можливої шкоди від ІТН.

Етап 10. Оцінка величини сукупної шкоди. На останньому етапі проводиться остаточний розрахунок величини ***СШ*** **($Ц_W$)**, яка складається із суми загальної вартісної величини ***ЕШ*** **($Ц_{W_{ек}}$)** та ***ІТН*** **($Ц_{W_{ін}}$)** з урахуванням можливого існування закону старіння до цих відомостей за рішенням ДЕТ. Отримане кінцеве значення показника СШ показує вартісну (грошову) величину можливої шкоди національній безпеці України у разі витоку ДТ.

На підставі запропонованої методології можна будувати як програмні, так і програмно-апаратні системи, призначені для ефективного оцінювання шкоди національній безпеці України у сфері ОДТ, які використовують як вхідні дані різні набори оцінних параметрів, що дозволяє підвищити гнучкість і розширює можливості застосування існуючих засобів, що функціонують як в детермінованому, так і в нечіткому слабоформалізованому середовищі.

Структурна схема системи оцінювання шкоди національній безпеці у разі витоку державної таємниці

На основі *критеріїв визначення СС відомостей, що становлять ДТ* за формумали (1.4)-(1.6) та спираючись на досвід наукових праць [137, 138], запропоновано (рис. 39) ***структурну схему системи оцінювання шкоди національній безпеці у разі витоку ДТ***, яка містить БД з п'ятьма таблицями: засоби M_c ($c=\overline{1,p}$, де c – покажчик (номер) поточного ідентифікатору засобу) забезпечення сфери ОДТ, що містять необхідні вхідні набори параметрів для оцінювання; критерії C_y ($y=\overline{1,3}$, де y – покажчик (номер) поточного ідентифікатору критерію) – СС відомостей, що становлять ДТ («Т» (y=1), «ЦТ» (y=2), «ОВ» (y=3)); значення критеріїв W_{yj}, де j – покажчик (номер) поточного ідентифікатору критерію $j=\overline{1,n}$, а n – кількість критеріїв; загальна зібрана довідкова інформація про кожний засіб забезпечення сфери ОДТ.

У модулі процесу вибірки «МПВ» здійснюється вибір необхідного критерію і його значення, які задовольняють ДЕТ. До нього надходять дані із засобів забезпечення сфери ОДТ, критерії та їх значення за допомогою сформованої БД, які татож формують компоненти *моделі ІППШ* (див. п. 5.1). Ці дані обробляються методами оцінювання шкоди національній безпеці у сфері ОДТ і після цього передаються, враховуючи при необхідності визначений рівень компетентності членів ЕК при ДЕТ, в модуль генерації звіту «МГЗ», де формується звіт результатів експертного оцінювання.

Роботу такої системи можна представити у вигляді виконання трьох етапів [169, 179]:

Етап 1. Визначення ідентифікуючих та розрахунок оціночних компонент моделі ІППШ. На цьому етапі використовується такі інтегровані БД: *модель СОІМ ЗВДТ* (див. п. 5.1); *перелік «питомої ваги» (Q) об'єктів $O_{N.i.j}$ відомостей, що становлять ДТ* (див. *Додаток 5*); *таблиця ідентифікації СЧО*.

Етап 2. Проводиться розрахунок величини ЕШ та шкоди від ІТН з метою отримання прогнозованої (бальної) величини СШ національній безпеці у сфері ОДТ за критеріями визначення СС відомостей, що становлять ДТ щодо яких відбулося порушення (подія *Е*). Застосовуюстья БД *переліку категорій тяжкості ІТН, їх бальне значення та опис* (див. п.1.3); *інтервальнне значення критеріїв визначення СС відомостей* (1.4)-(1.6).

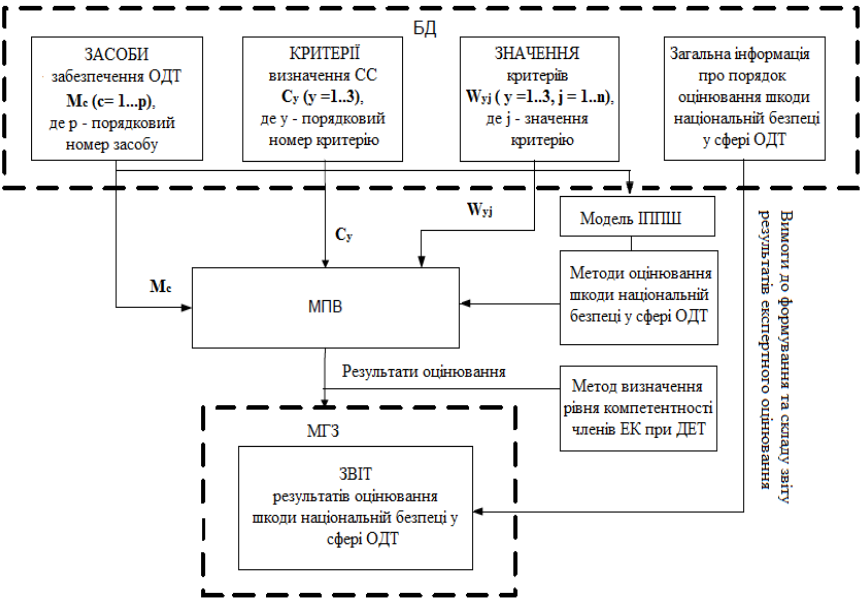


Рис. 39. Структурна схема системи оцінювання шкоди національній безпеці України у разі витоку ДТ

Етап 3. Інтерпритація отриманого значення прогнозованої ЕШ та ІНТ до вартісного (грошового) їх значення, розрахунок обґрунтованих витрат та нанесених втрат (збитків) до та після подій *E*, отримання вартісного (грошового) значення СШ національній безпеці у сфері ОДТ з можливістю застосування ДЕТ закону старіння інформації та врахування рівня компетентності членів ЕК. Використовуються *інтегровані БД* та засіб забезпечення сфери ОДТ – «*Звіт про стан забезпечення ОДТ*» [29].

Запропонована система дасть змогу розрахувати вартісну величину СШ нанесеної національній безпеці у разі розголошення ДТ чи втрати МНСІ, тим самим забезпечити виконання норм Закону України «Про державну таємницю» [3], зокрема ст. 9, 11, і допоможе судам загальної юрисдикції, що здійснюють судочинство у справах про злочини, які завдають шкоди національній безпеці України, визначити належну міру покарання за нанесені порушення (події) у сфері ОДТ.

Базовий алгоритм роботи системи

Алгоритму роботи системи передбачає існування початкових (вхідних) та статистичних (звітних) даних для отримання кінцевого результату. У якості вхідних даних для системи оцінювання шкоди національній безпеці у разі витоку ДТ є відомості про наявність порушення (події *E*) або експертиза МНІ та ініціатор її проведення (СРСД, ДЕТ). Робота алгоритму відбувається шляхом виконання послідовності з 13 елементарних кроків (блоків), а процес їхнього виконання є алгоритмічним, що забезпечує властивість дискретності.

До основних блоків схеми алгоритму роботи системи (рис. 40) на основі методології синтезу та структурної схеми віднесено [169, 179]:

Блок 1 – введення початкових даних експертної оцінки (СРСД, порушення (події), відомостей, що оцінюються (стаття ЗВДТ та її СС));

Блок 2 – визначення об'єкту ($O_{N.i.j}$) відомостей, його «питома вага» (*Q*), ідентифікація СЧО (ВВСЧО (*k*));

Блок 3 – формування та визначення «ваги» переліку *X* відомостей, що становлять ДТ, які забезпечують функціонування об'єкту $O_{N.i.j}$ і наявні в РСО СРСД;

Блок 4 – розрахунок ефективності функціонування СОДТ ($K^{СОДТ}$) та рівня зниження функціонування СЧО (ρ);

Блок 5 – розрахунок прогнозованої (бальної) величини можливої ЕШ ($W_{ек}$) та ІТН ($W_{ін}$), його опис та категорія тяжкості для національної безпеки;

Блок 6 – введення дати засекречування відомостей за рішенням ДЕТ та дати інформування про виникнення щодо них подій Р або В зі звіту про стан забезпечення ОДТ в РСО СРСД;

Блок 7 – визначення кількості років зберігання та охорони цих відомостей ($T_ф$);

Блок 8 – введення фінансової бухгалтерської звітності щодо величини витрат на забезпечення заходів ОДТ за кожен визначений рік у блоці 7;

Блок 9 – вартісний розрахунок величини ЕШ ($Ц_{W_{ек}}$) та шкоди від ІТН ($Ц_{W_{ін}}$) національній безпеці України у разі витоку ДТ;

Блок 10 – розрахунок СШ ($Ц_W$) національній безпеці України у разі витоку ДТ;

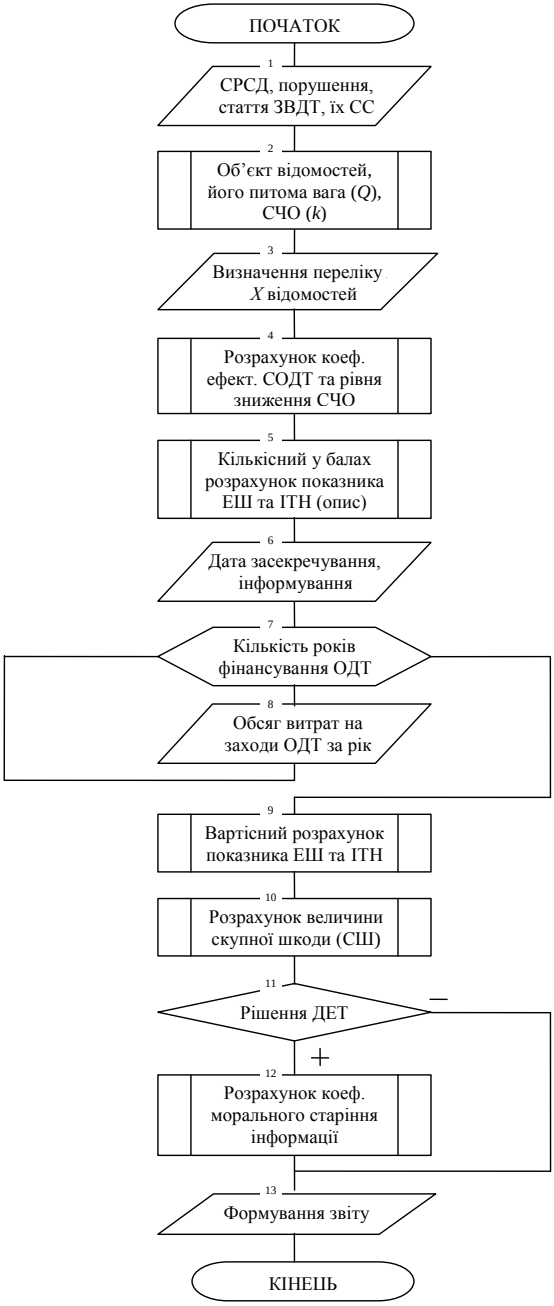


Рис. 40. Блок-схема алгоритму роботи системи

Блок 11 – прийняття рішення ДЕТ щодо застосування коефіцієнту морального старіння (K_c) інформації у зв'язку з необхідністю розсекречування цих відомостей або втрати їх актуальності чи важливості;

Блок 12 – розрахунок коефіцієнту морального старіння (K_c);

Блок 13 – автоматизоване формування звіту з результатами та відомостями експертного оцінювання.

Важливою властивістю розробленого алгоритму є масовість, або можливість застосування до різних вхідних даних.

Необхідною умовою, яка задовольняє алгоритм, є детермінованість, або визначеність. Це означає, що виконання команд алгоритму відбувається у єдиний спосіб та призводить до однакового результату для однакових вхідних даних. Вхідні дані алгоритму можуть бути обмежені набором припустимих вхідних даних. Застосування алгоритму до неприпустимих вхідних даних може призводити до того, що алгоритм ніколи не працюватиме, або потрапить в тупиковий стан (зависання) з якого не зможе продовжити виконання. Заповнення блоків, що потребує введення необхідних даних є обов'язковим для виконання розрахункових дій та операцій в системі оцінювання шкоди національній безпеці України у разі витоку ДТ.

6.2. Програмна реалізація та експериментальне дослідження системи оцінювання шкоди національній безпеці України у разі витоку державної таємниці

Програмна реалізація системи

На основі розробленої *методології синтезу, структурної схеми та алгоритму роботи* (див. п. 6.1) проведено програмну реалізацію системи оцінювання шкоди національній безпеці України у разі витоку ДТ, яка являє собою повноцінний ***програмний продукт* (*комп'ютерна програма*) *«Система аналізу і оцінки величини можливої шкоди національній безпеці держави у сфері ОДТ»*** (див. *Додаток 11*) [169, 179].

Запропонована програма буде корисна для ДЕТ у процесі проведення експертної оцінки процедури віднесення відомостей до ДТ з встановленням їх СС шляхом визначення та обґрунтування величини можливої шкоди національній безпеці України у разі витоку ДТ. Також даний програмний продукт може використовуватись при підготоці експертного висновку з розрахунку величини СШ (збитку) національній безпеці держави при виникненні порушень у сфері ОДТ, а саме у разі розголошення відомостей, що становлять ДТ чи втрати МНСІ.

Рекомендації по встановленню програми:

Бажано виконувати встановлення програми в директорію за замовчуванням (C:\) або в іншу директорію (не системну) і запуск без прав адміністратора (мається на увазі звичайний запуск, а не запуск із контекстного меню за посиланням “Run as administrator”).

До системних директорій відносяться:

1. C:\Program Files.
2. C:\Program Files (x86).
3. C:\Users.

Далі з папки проекту або за допомогою створеного на робочому столі ярлика програми запустити роботу програми, а саме файлу з назвою *Система ОШ НБ ОДТ.exe* тестування якого і буде проводитися. Головне вікно програми являє собою єдине повноцінне середовище роботи експерта, яке зручне у використанні та має прив’язку до основних інтегрованих баз даних, які підключаються автоматично при заповненні відповідних полів. Зовнішній вигляд початку роботи програми показано на рис. 41.

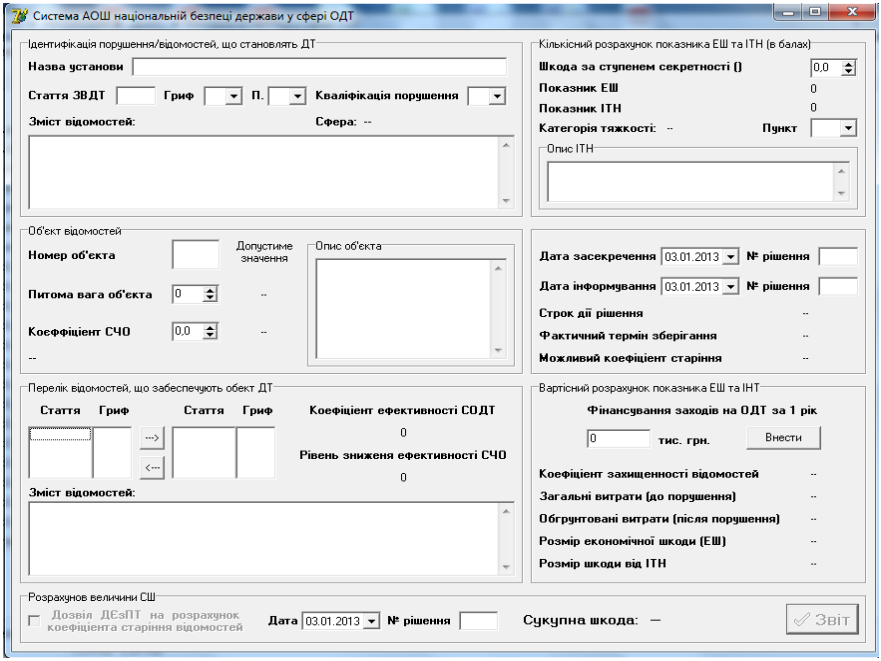
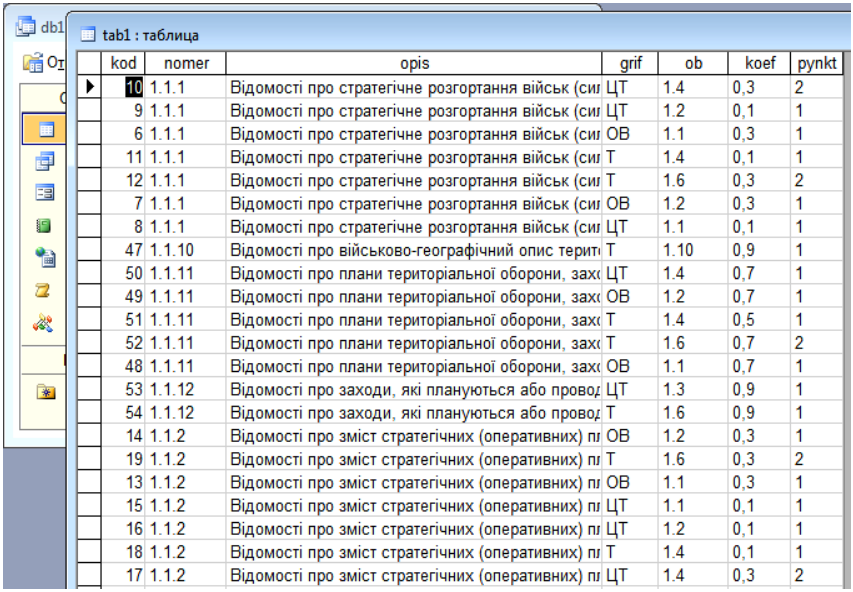


Рис. 41. Головне вікно системи оцінювання шкоди національній безпеці України у разі витоку ДТ

Принцип роботи програми вимагає поетапного виконання структурних логічних блоків системи:

1) ідентифікація порушення / відомостей, що становлять ДТ;
2) об’єкт відомостей;
3) перелік відомостей, що забезпечують об’єкт ОДТ;
4) кількісний розрахунок показника ЕШ та ІТН (в балах);
5) визначення коефіцієнта морального старіння відомостей;
6) вартісний розрахунок показника ЕШ та ІТН;
7) розрахунок величини СШ.

У *першому* блоці програми проводиться заповнення повної або скороченої назви установи – ініціатора експертизи. Далі проводиться ідентифікація відомостей, що становлять ДТ та її СС (гриф) за допомогою інтегрованої бази даних *db1.mdb*, яка містить таблицю 1 (*tab1*) статей ЗВДТ [31], що зображено на рис. 42. У цьому ж блоці зазначається вид порушення (події *E*) – розголошення (Р) чи втрата (В), що відбулися за вказаною статею. У діалогових полях приводиться загальний зміст (опис) відомостей, що становлять ДТ та визначається їх сфера застосування (*N*).



kod	nomer	opis	grif	ob	koef	pynkt
10	1.1.1	Відомості про стратегічне розгортання військ (сил	ЦТ	1.4	0,3	2
9	1.1.1	Відомості про стратегічне розгортання військ (сил	ЦТ	1.2	0,1	1
6	1.1.1	Відомості про стратегічне розгортання військ (сил	ОВ	1.1	0,3	1
11	1.1.1	Відомості про стратегічне розгортання військ (сил	Т	1.4	0,1	1
12	1.1.1	Відомості про стратегічне розгортання військ (сил	Т	1.6	0,3	2
7	1.1.1	Відомості про стратегічне розгортання військ (сил	ОВ	1.2	0,3	1
8	1.1.1	Відомості про стратегічне розгортання військ (сил	ЦТ	1.1	0,1	1
47	1.1.10	Відомості про військово-географічний опис терит	Т	1.10	0,9	1
50	1.1.11	Відомості про плани територіальної оборони, захо	ЦТ	1.4	0,7	1
49	1.1.11	Відомості про плани територіальної оборони, захо	ОВ	1.2	0,7	1
51	1.1.11	Відомості про плани територіальної оборони, захо	Т	1.4	0,5	1
52	1.1.11	Відомості про плани територіальної оборони, захо	Т	1.6	0,7	2
48	1.1.11	Відомості про плани територіальної оборони, захо	ОВ	1.1	0,7	1
53	1.1.12	Відомості про заходи, які плануються або провод	ЦТ	1.3	0,9	1
54	1.1.12	Відомості про заходи, які плануються або провод	Т	1.6	0,9	1
14	1.1.2	Відомості про зміст стратегічних (оперативних) пл	ОВ	1.2	0,3	1
19	1.1.2	Відомості про зміст стратегічних (оперативних) пл	Т	1.6	0,3	2
13	1.1.2	Відомості про зміст стратегічних (оперативних) пл	ОВ	1.1	0,3	1
15	1.1.2	Відомості про зміст стратегічних (оперативних) пл	ЦТ	1.1	0,1	1
16	1.1.2	Відомості про зміст стратегічних (оперативних) пл	ЦТ	1.2	0,1	1
18	1.1.2	Відомості про зміст стратегічних (оперативних) пл	Т	1.4	0,1	1
17	1.1.2	Відомості про зміст стратегічних (оперативних) пл	ЦТ	1.4	0,3	2

Рис. 42. База даних ЗВДТ (*tab1*)

Наступним *другим* блоком системи проводиться визначення об’єкта цих відомостей чи його складової частини (СЧО). За визначенням статі

ЗВДТ автоматизовано ідентифікується об’єкт відомостей, його опис та значення «питомої ваги», яка міститься у інтегрованій базі даних *db1.mdb* у таблицю 2 (*tab2*) значень «питомої ваги» об’єктів (див. *Додаток 5*), що показано на рис. 43.

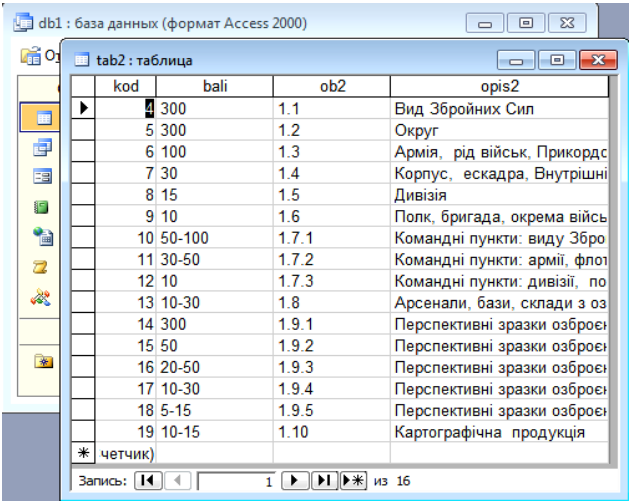


Рис. 43. Перелік «питомої ваги» об’єктів (*tab2*)

Наступним *третім* логічним блоком системи є формування переліку відомостей, що становлять ДТ, які містять ідентифікований об’єкт або СЧО в РСО СРСД при цьому використовується таблиця 1 (*tab1*) статей ЗВДТ інтегрованої бази даних *db1.mdb*. Далі шляхом застосування розроблених *методів* (див. п.5.2) проводиться розрахунок коефіцієнтів ефективності системи ОДТ ($K^{СОДТ}$) та оцінки рівня зниження ефективності використання СЧО (ρ).

Четвертий блок, використовуючи критерії визначення СС відомостей, що становлять ДТ та метод аналізу і оцінки величини можливої шкоди національній безпеці у сфері ОДТ, визначає потенційну прогнозовану величину ЕШ та ІТН у балах на основі приведеного значення інтервалу шкоди за СС відомостей, що міститься у таблиці 3 (*tab3*) та наводить опис і категорію тяжкості ІТН за визначеною у таблиці 4 (*tab4*) сферою при порівнянні отриманого значення бальної величини до приведеної у таблиці 5 (*tab5*) переліку ІТН [38] інтегрованої бази даних *db1.mdb*, які показані на рис. 44- 46.

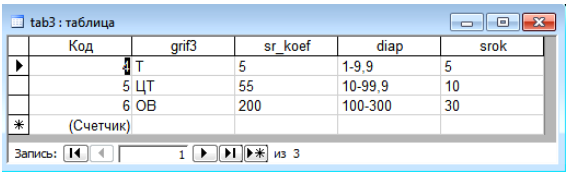


Рис. 44. Значення інтервалу шкоди за СС відомостей (*tab3*)

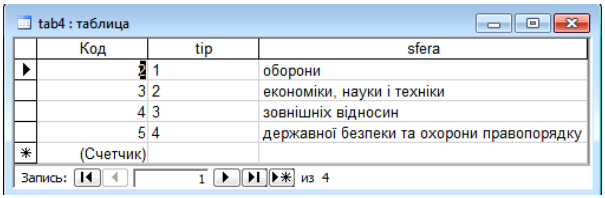


Рис. 45. Значення інтервалу шкоди за СС відомостей (*tab3*)

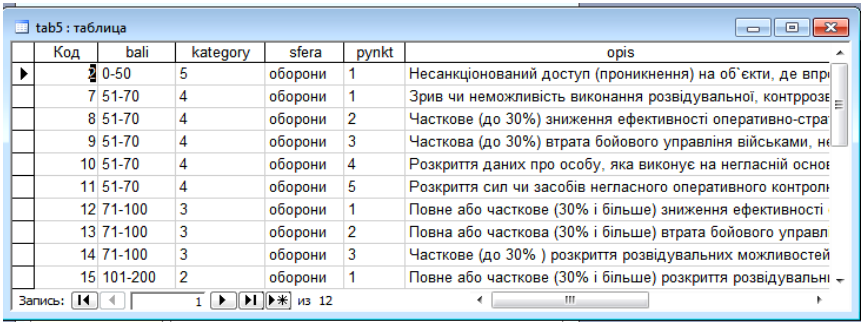


Рис. 46. Перелік категорій тяжкості ІТН та їх бальне значення (*tab5*)

Далі *п'ятим* блоком проводяться введення додаткової інформації щодо певних уточнюючих дат (дата засекречування відомостей та дата інформування про розголошення чи втрату) для подальшого розрахунку можливого коефіцієнту морального старіння цих відомостей у разі їх потенційного розсекречування ДЕТ .

У *шостому* блоці системи вносяться відповідні суми витрат на ОДТ відомостей в РСО для подальшого визначення величини обґрунтованих витрат, розміру ЕШ та шкоди від ІТН як величини СШ національній безпеці у разі розголошення відомостей, що становлять ДТ чи втрати МНСІ. Загальний процес аналізу і оцінки величини можливої шкоди національній безпеці у разі витоку ДТ даної системи показано на рис. 47.

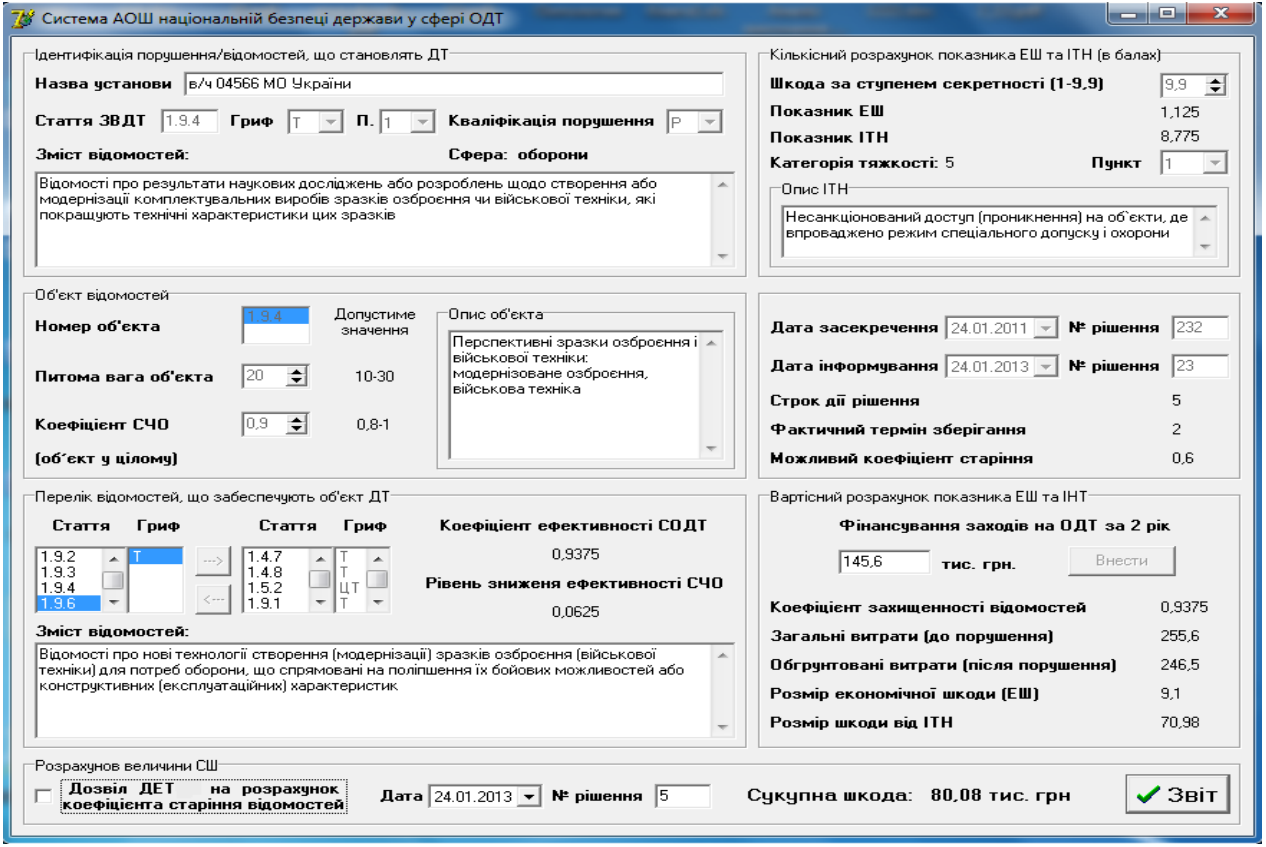


Рис. 47. Система оцінювання шкоди національній безпеці України у разі витоку ДТ

Кінцевим *сьомим* блоком є отримання результату проведеного оцінювання (величини СШ національній безпеці у сфері ОДТ) з можливістю автоматизованого формування експертного висновку у вигляді друкованого звіту формату А4 та за рішенням ДЕТ може застосовувати розрахований у п'ятому блоці коефіцієнт морального старіння, що показано на рис. 48, 49.

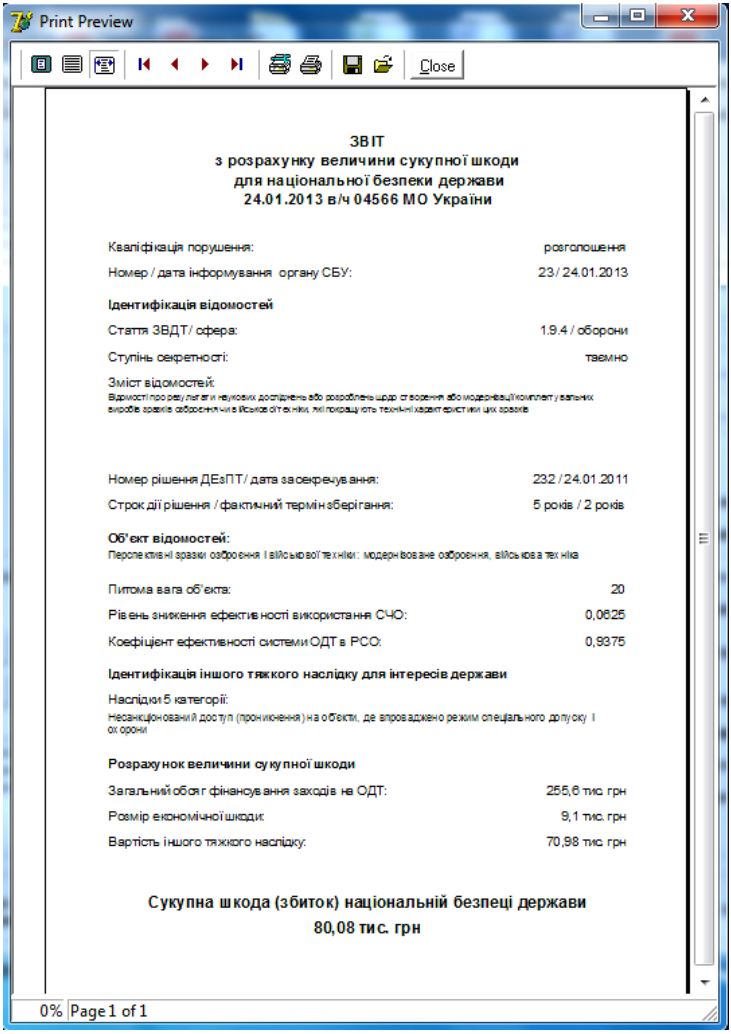
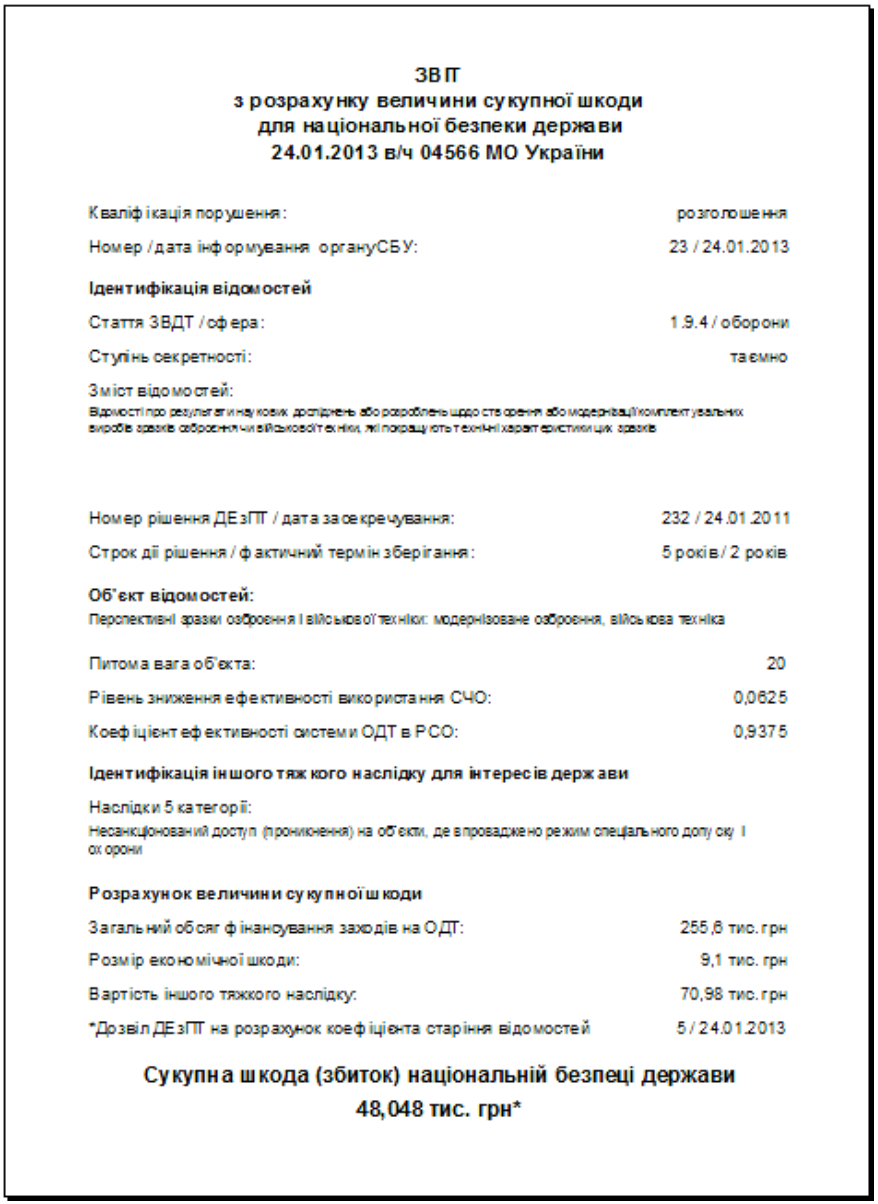


Рис. 48. Формування Звіту отриманих результатів системи оцінювання шкоди національній безпеці України у разі витоку ДТ без застосуванням коефіцієна морального старіння інформації



ЗВІТ
з розрахунку величини сукупної шкоди
для національної безпеки держави
24.01.2013 в/ч 04566 МО України

Кваліфікація порушення:	розголошення
Номер / дата інформування органуСБУ:	23 / 24.01.2013

Ідентифікація відомостей

Стаття ЗВДТ / офера:	1.9.4 / оборони
Ступінь секретності:	таємно

Зміст відомостей:
Відомості про результати наукових досліджень або розроблень щодо створення або модернізації комплектувальних виробів зразків озброєння чи військової техніки, які покращують технічні характеристики цих зразків

Номер рішення ДЕзПТ / дата засекречування:	232 / 24.01.2011
Строк дії рішення / фактичний термін зберігання:	5 років / 2 років

Об'єкт відомостей:
Перспективні зразки озброєння і військової техніки: модернізоване озброєння, військова техніка

Питома вага об'єкта:	20
Рівень зниження ефективності використання СЧО:	0,0625
Коефіцієнт ефективності системи ОДТ в РСО:	0,9375

Ідентифікація іншого тяжкого наслідку для інтересів держави

Наслідки 5 категорії:
Несанкціонований доступ (проникнення) на об'єкти, де впроваджено режим спеціального допуску і охорони

Розрахунок величини сукупної шкоди

Загальний обсяг фінансування заходів на ОДТ:	255,6 тис. грн
Розмір економічної шкоди:	9,1 тис. грн
Вартість іншого тяжкого наслідку:	70,98 тис. грн
*Дозвіл ДЕзПТ на розрахунок коефіцієнта старіння відомостей	5 / 24.01.2013

Сукупна шкода (збиток) національній безпеці держави
48,048 тис. грн*

Рис. 49. Звіт отриманих результатів
системи оцінювання шкоди національній безпеці України у разі витоку ДТ
із застосуванням коефіцієна морального старіння інформації

Експериментальне дослідження системи

З метою верифікації розроблених методів, моделей та комп'ютерної програми проведено експериментальне дослідження (експеримент) системи сутність якого полягає у визначенні можливих помилок системи, адекватності її реагування на СС відомостей до яких відбулися події E та у здатності до гнучкого розрахунку і адаптацію при зміні вхідних даних при експертному оцінюванні шкоди національній безпеці. Для проведення дослідження обрані наступні *випадки* [169, 180]:

- порівняння величини можливої шкоди від СС відомостей;
- порівняння величини можливої шкоди від строків зберігання та охорони відомостей.

У *першому випадку* виконано обчислення та порівняльний аналіз величини можливої СШ за СС при розголошенні відомостей $PV_{1.3.1}$.

Вхідні дані для розрахунку приведені у табл. 27, а їх результати показано рис. 50.

Таблиця 27

Порівняння величини можливої шкоди від СС відомостей

Відомості, що становлять ДТ	СС	Строк (роки)		Фінансування заходів на ОДТ (тис. грн.)	Величина можливої шкоди (тис. грн.)			
		$T_н$	$T_ф$		ЕШ	ІТН	СШ	СШ*
1.3.1	Т	5	2	244	20,667	40,741	61,381	36,829
	ЦТ	10			62	268,336	330,336	264,269
	ОВ	30			124	702,584	826,584	771,451

Примітка. * - застосування коефіцієнту морального старіння інформації.

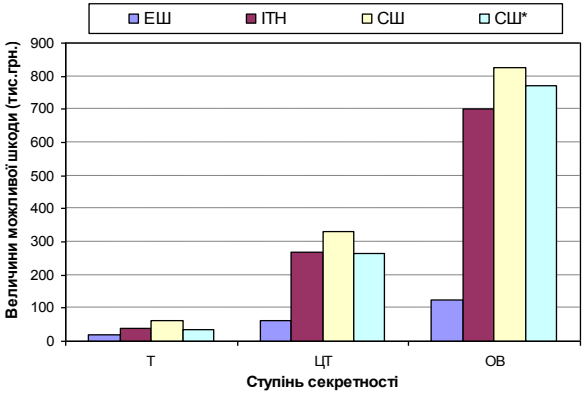


Рис. 50. Порівняння величини можливої шкоди від СС відомостей

У *другому випадку* виявлено динаміку зміни величини СШ в залежності від строків зберігання відомостей $PV_{1.9.6}$ та обсягів фінансування заходів на їх охорону.

В табл. 28 та відповідно на рис. 51 приведені результати експерименту другого випадку.

Таблиця 28

Порівняння величини можливої шкоди від строків зберігання та охорони відомостей

Відомості, що становлять ДТ	СС	Строк (роки)		Фінансування заходів на ОДТ (тис. грн.)	Величина можливої шкоди (тис. грн.)			
		$T_н$	$T_ф$		ЕШ	ІТН	СШ	СШ*
1.9.6	Т	5	1	85,87	14,312	107,135	121,447	97,158
			2	87,45	14,575	109,104	123,679	74,207
			3	90,15	15,025	112,472	127,497	50,999
			4	93,33	15,555	116,44	131,995	26,399
			5	95,07	15,845	118,611	134,456	0

Примітка. * - застосування коефіцієнту морального старіння інформації.

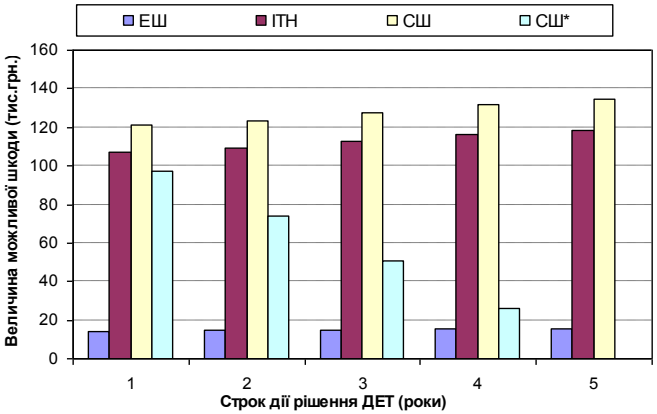


Рис. 51. Порівняння величини можливої шкоди від строків зберігання та охорони відомостей

За допомогою розробленого програмного забезпечення проведено моделювання роботи системи оцінювання шкоди національній безпеці України у разі витоку ДТ.

ВИСНОВКИ

Охорона ДТ є окремим сегментом національної безпеки України, визначеним чинною політикою інформаційної безпеки, де одним із основних її положень є виділення окремої категорії відомостей, що складають ДТ. Дана процедура пов'язана з аналізом і оцінкою важливості СІ саме у контексті загроз національній безпеці України та можливої шкоди від їх реалізації. Існуюча процедура визначення цієї шкоди базується на емпіричних підходах, яким властивий високий рівень суб'єктивізму та низька точність отриманих результатів. Тому актуальною є задача розроблення науково обґрунтованої методології оцінювання шкоди, заподіяної витоком СІ, зокрема моделей, методів, критеріїв і систем, що застосовуються для цього і врахувати існуючі в цій сфері напрацювання, що базуються на осмисленні багаторічного позитивного досвіду у сфері ОДТ.

Розглянуті нормативно-правові та соціально-організаційні аспекти ОДТ, проведено критичний аналіз чинних методичних настанов, рекомендацій та процедур оцінювання можливої шкоди у разі розголошення ДТ або втрати її матеріальних носіїв, запропоновано оригінальні експертно-аналітичні підходи до визначення цінності СІ та обсягів втрат у разі її витоку.

У науковій роботі виконані дослідження, які можуть бути використані при розробці ефективних систем за запропонованою методологією синтезу, яка заснована на створених моделях засобів, моделі ІППШ та методах оцінювання шкоди національній безпеці України у разі витоку ДТ.

У ході вирішення поставлених задач були отримані такі результати:

1. На підставі проведеного аналізу базових понять та існуючих засобів, запропоновано визначення величини можливої шкоди національній безпеці держави у сфері ОДТ для однозначного детермінування відповідних процесів і параметрів та їх використання при створенні спеціальних інструментальних засобів.

2. Розроблено моделі ЗВДТ та ПСлІ у сфері оборони у якості складних орієнтованих інформаційних мереж, а також модель експертного оцінювання МНІ на наявність відомостей, що становлять ДТ та визначення ступеня їх секретності з метою отримання набору узагальнюючих параметрів шкоди.

3. Розроблено інтегровану модель представлення параметрів шкоди, яка за рахунок узагальнення ідентифікуючих та оціночних параметрів, відображених десятикомпонентним кортежем, дозволяє формувати необхідні множини даних для аналізу і оцінки шкоди при використанні існуючих засобів у сфері ОДТ.

4. Запропоновано методи оцінювання шкоди національній безпеці України у разі витоку ДТ, які на основі використання узагальненої моделі ІППШ і логіко-лінгвістичного підходу, дозволяють використовувати засоби оцінювання з інтегрованими можливостями, які використовують в якості вхідних даних динамічно змінювані набори детермінованих і нечітко визначених оціночних параметрів для встановлення та обґрунтування величини можливої шкоди національній безпеці держави у разі розголошення СІ чи втрати МНСІ, визначення рівня компетентності членів ЕК при ДЕТ під час віднесення відомостей до ДТ і визначення ступеня їх секретності, оцінювання важливості цих відомостей відносно визначених сфер ДТ, сценарного методу оцінювання шкоди, заподіяної витоком СІ тощо.

5. Отримала подальший розвиток методологія синтезу систем оцінювання шкоди національній безпеці, яка дозволила за рахунок формалізації та узагальнення процесу застосування розробленої моделі ІППШ, моделей засобів і запропонованих методів сформувати процес оцінювання шкоди з використанням величин заданих множин існуючих інструментальних засобів у сфері ОДТ.

6. Розроблено структурну схему системи оцінювання шкоди національній безпеці у сфері ОДТ, яка за рахунок підсистем обробки первинних параметрів і формування даних, що реалізують запропоновані моделі та методи, дозволяє перетворювати і формувати дані, як у кількісній (бальній), так і у вартісній (грошовій) інтерпретації.

7. На базі запропонованої методології та структурної схеми, розроблена прикладна програмна система оцінювання шкоди національній безпеці України у сфері ОДТ, в якій за рахунок можливості динамічної зміни різних наборів параметрів, досягнута висока інтеграція функціональних можливостей, гнучкість і зручність її використання, для ефективного вирішенні завдань як в детермінованому, так і в нечіткому, слабоформалізованому середовищі.

8. Проведено експериментальне дослідження ПЗ системи оцінювання шкоди національній безпеці у сфері ОДТ з метою верифікації розроблених моделей та методів, методології синтезу і структурної схеми. Впровадження та практичне використання зазначених розробок підтвердило достовірність теоретичних гіпотез і висновків наукової роботи.

СПИСОК ЛІТЕРАТУРИ

1. Про основи національної безпеки України / Верховна Рада України; Закон від 19.06.2003 № 964-IV {редакція від 20.07.2010} // [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/964-15

2. Конституція України / Верховна Рада України; Конституція, Закон від 28.06.1996 № 254к/96-ВР {версія від 25.01.2012} // [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/254к/96-вр

3. Про державну таємницю / Верховна Рада України; Закон від 21.01.1994 № 3855-XII {редакція від 24.02.2011} // [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/3855-12/page

4. Бортвінкін О.В. Система охорони державної таємниці. Історичний аспект / Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – №13. – 2006. – С.83-88 // [Електронний ресурс]. – Режим доступу: http://pnzzi.kpi.ua/13/13_p83.pdf

5. Історія охорони державної таємниці в Україні: монографія / О.В. Ботвінкін, В.М. Шлапаченко, В.П. Ворожко, А.С. Пашков. – К.: Наук.-вид. відділ НА СБ України, 2008. – 155 с.

6. Охорона державних секретів незалежної України (Історично-правові нариси) / Й. У. Мастяниця, Л.Є. Шиманський, О.В. Олійник, В.П. Ворожко // За заг. ред. П.О. Мисника, О.В. Зайчука. – К.: Інститут законодавства Верховної Ради України, 2010. – 128 с.

7. Нарис історії охорони державної таємниці в Україні: монографія / В.П. Ворожко, Б.В. Бернадський, О.В. Бортвінкін / Наукове видання. – К., 2012. – 188 с.

8. Професійна юридична система НАУ-Online – пошукова інтернет-версія правових систем / Нормативно-правові документи // [Електронний ресурс]. – Режим доступу: http://zakon.nau.ua

9. Про інформацію / Верховна Рада України; Закон від 02.10.1992 № 2657-XII {редакція від 09.05.2011} // [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2657-12

10. Про Службу безпеки України / Верховна Рада України; Закон 25.03.1992 від № 2229-XII {редакція від 05.01.2012} // [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/2229-12

11. Про доступ до публічної інформації / Верховна Рада України; Закон від 13.01.2011 № 2939-VI // [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2939-17

12. Закон України «Про доступ до публічної інформації»: інформаційний прорив в Україні / Мін'юст України; Роз'яснення від

13.05.2011 // [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/n0031323-11

13. Про захист персональних даних / Верховна Рада України; Закон від 01.06.2010 № 2297-VI // [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2297-17

14. Про оперативно-розшукову діяльність / Верховна Рада України; Закон від 18.02.1992 № 2135-XII {редакція від 12.06.2011} // [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2135-12

15. Кримінальний кодекс України / Верховна Рада України; Кодекс України, Кодекс, Закон від 05.04.2001 № 2341-III {редакція від 17.01.2012} // [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/ show/2341-14

16. Кримінально-процесуальний кодекс України / Верховна Рада УРСР; Кодекс України, Закон, Кодекс від 28.12.1960 № 1001-05 // [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/1001-05

17. Про Положення про державного експерта з питань таємниць / Президент України; Указ від 23.04.1994 № 185/94 // [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=185%2F94

18. Про Положення про Державний комітет України з питань державних секретів та технічного захисту інформації / Президент України; Указ, Положення від 05.11.1996 № 1047/96 // [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/1047/96

19. Про деякі питання передачі державної таємниці іноземній державі чи міжнародній організації / Президент України; Указ від 14.12.2004 № 1483/2004 // [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/1483/2004

20. Про Положення про порядок підготовки документів щодо надання доступу до державної таємниці іноземцям та особам без громадянства / Президент України; Указ, Положення від 17.07.2006 № 621/2006 // [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws /show/621/2006

21. Про Перелік посадових осіб, на яких покладається виконання функцій державного експерта з питань таємниць / Президент України; Указ, Перелік від 01.12.2009 № 987/2009 // [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/987/2009

22. Про Положення про технічний захист інформації в Україні / Президент України; Указ від 27.09.1999 № 1229/99 {редакція від 04.05.2008} // [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/1229/99

23. Про Положення про порядок здійснення криптографічного захисту інформації в Україні / Президент України; Указ від 22.05.1998 № 505/98 {редакція від 12.09.2009} // [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/505/98

24. Про види, розміри і порядок надання компенсації громадянам у зв'язку з роботою, яка передбачає доступ до державної таємниці / Кабінет Міністрів України; Постанова, Положення від 15.06.1994 № 414 // [Електронний ресурс].– Режим доступу: http://zakon1.rada.gov.ua/laws/show/414-94-п

25. Про проведення експертизи цінності документів / Кабінет Міністрів України; Постанова, Порядок від 08.08.2007 № 1004 {редакція від 01.11.2011} // [Електронний ресурс].– Режим доступу:http://zakon2.rada.gov.ua/laws/show/1004-2007-п

26. Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію / Кабінет Міністрів України; Постанова, Інструкція від 27.11.1998 № 1893 {редакція від 01.11.2011} // [Електронний ресурс].– Режим доступу: http://zakon2.rada.gov.ua/laws/show /1893-98-п

27. Про внесення змін до постанови Кабінету Міністрів України від 27 листопада 1998 р. № 1893 / Кабінет Міністрів України; Постанова від 17.11.2004 № 1547 {редакція від 17.11.2004} // [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/1547-2004-п/ ed20111101

28. Про внесення змін до деяких постанов Кабінету Міністрів України з питань доступу до інформації / Кабінет Міністрів України; Постанова від 07.09.2011 № 938 // [Електронний ресурс].– Режим доступу: http://zakon2.rada.gov.ua/laws/show/938-2011-п

29. Про затвердження форм звіту про стан забезпечення охорони державної таємниці та інструкцій щодо порядку їх заповнення та подання / Служба безпеки України; Наказ, Інструкція, Форма [...] від 28.11.2008 № 841// [Електронний ресурс]. – Режим доступу:http://zakon2.rada.gov.ua/laws/show/z1163-08

30. Про затвердження Положення про експертні комісії з питань державної таємниці / Служба безпеки України; Наказ від 14.12.2004 № 696 // [Електронний ресурс].– Режим доступу: http://zakon.nau.ua/doc/?uid=1092.10.0

31. Про затвердження Зводу відомостей, що становлять державну таємницю / Служба безпеки України; Наказ, Звід від 12.08.2005 № 440 {редакція від 21.11.2011} // [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/z0902-05

32. Щодо порядку організації та проведення експертиз на предмет наявності чи відсутності у матеріальних носіях інформації відомостей,

що становлять державну таємницю / Служба безпеки України; Методичні рекомендації, від 28.10.2008 № 26/6-7850 // [Електронний ресурс].– Режим доступу: http://www.customs.com.ua/php/document.php?ISN=40688

33. Про затвердження Переліку психічних захворювань (розладів), які можуть завдати шкоди охороні державної таємниці і за наявності яких допуск до державної таємниці громадянинові не надається / МОЗ України, Служба безпеки України; Наказ, Перелік від 13.05.2002 № 174/136 // [Електронний ресурс].– Режим доступу: http://zakon2.rada.gov.ua/laws/show/z0458-02

34. Про затвердження Положення про державну експертизу в сфері технічного захисту інформації / Держспецзв'язку України; Наказ, Положення, Заява [...] від 16.05.2007 № 93 // [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/z0820-07

35. Про затвердження Положення про державну експертизу в сфері криптографічного захисту інформації / Держспецзв'язку України; Наказ, Положення, Форма типового документа [...] від 23.06.2008 № 100 // [Електронний ресурс].– Режим доступу: http://zakon2.rada.gov.ua/laws/show/z0651-08

36. Про затвердження Посібника керівникам підприємств, установ, організацій Міністерства транспорту України з організації роботи та здійснення повноважень з забезпечення охорони державної таємниці / Міністерство транспорту України; Наказ № 86 від 10.02.2003 // [Електронний ресурс]. – Режим доступу: http://ukraine.uapravo.net/data/base41/ukr41941.htm

37. Про затвердження Порядку державного обліку секретних науково-дослідних, дослідно-конструкторських робіт і дисертацій / МОН України; Наказ, Порядок, Картка [...] від 09.06.2009 № 494 // [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/z0606-09

38. Методичні рекомендації державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня їх секретності / Державний комітет України з питань державних секретів та технічного захисту інформації; Збірка №8, Наказ № 23 від 9 лютого 1998 – К., 1998. – С.4-14.

39. Рекомендації з організації діяльності експертних комісій при державних експертах з питань таємниць / Державний комітет України з питань державних секретів та технічного захисту інформації; Збірка №8, Наказ № 22 від 9 лютого 1998 – К., 1998. – С.15-24.

40. Захист інформації з обмеженим доступом: збірник нормативних документів // Уклад. В.П. Ворожко, О.Г. Корченко. – К.: КМУЦА, 1999. – 283 с.

41. Нормативно-правове забезпечення інформаційної безпеки: Збірник нормативно-правових документів / Уклад. О.Г. Корченко, Ю.О. Дрейс. – Житомир: ЖВІ НАУ, 2010. – 280 с.

42. Артемов В.Ю. Законодавче забезпечення охорони державної таємниці в умовах становлення національної державності / В.Ю. Артемов, А.С. Пашков // Інформаційна безпека. – Вип. №1(3). – 2010. – С.45-50.

43. Божков І.І. Державна таємниця та система її охорони / Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – №4. – 2002. – С.7-10 // [Електронний ресурс]. – Режим доступу: http://pnzzi.kpi.ua/4/04_p7.pdf

44. Пашков А.С. Структура та основні елементи системи охорони державної таємниці // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.:ВІКНУ, 2008. – №16. – С.140-147.

45. Пашков А.С. Основні елементи системи охорони державної таємниці / «Сучасні проблеми захисту інформації з обмеженим доступом»: Доповіді та тези доповіді міжвідомчої наук.-практ. конфер. (20–21 листопада 2008р.) – К.: НАУ, НА СБ України. – 2008. – С.41-43.

46. Пашков А.С. Система охорони державної таємниці та її роль в забезпеченні інформаційної безпеки / Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – Вип. №22. – 2009. – С.168-171.

47. Пашков А.С. Охорона інформації з обмеженим доступом як складова захисту національних інформаційних ресурсів / А.С. Пашков, Н.М. Берназ, О.С. Лєнков // Інформаційна безпека. – Вип. №1(1). – 2009. – С.124-127.

48. Пашков А.С. Загальні принципи охорони державної таємниці / Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – Вип. №17. – 2009 // [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/portal/natural/Znpviknu/2009_17/vip17-29.pdf

49. Шлапоченко В.М. Принципи організації збереження секретної інформації / В.М. Шлапоченко, О.А. Колеснік // ЗНП НА СБ України – 2003. – №8. – С.3-7.

50. Ємельянов С.Л. Проблемні аспекти організаційно-правового захисту державної таємниці в Україні / Інформаційна безпека. – Вип. №1 (5). – 2011. – С.36-44

51. Нормування роботи підрозділів режимно-секретних органів / В.П. Ворожко, О.Є. Муратов, О.І. Матяш // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – №2(13). – 2006. – С.100-102 // [Електронний ресурс]. – Режим доступу: http://pnzzi.kpi.ua/13/13_p100.pdf

52. Сидоренко С.М. До питання інформаційно-аналітичного забезпечення діяльності режимно-секретних органів / «Актуальні проблеми управління інформаційною безпекою держави»: Збірник матеріалів наук.-практ. конф., 22 березня 2011, Частина 1. – К.: Вид-во НА СБ України, 2011. – С.285-296.

53. Архипов О.Є. Щодо методики реалізації процедури віднесення інформації до секретної / О.Є. Архипов, В.П. Ворожко // Правове, нормативне та метрологічне забезпечення захисту інформації в Україні. – Вип. №2(17). – 2008. – С.10-15 // [Електронний ресурс]. – Режим доступу: http://pnzzi.kpi.ua/17/17_p11.pdf

54. Архипов О. Є. Проблеми методичного забезпечення віднесення відомостей до інформації з обмеженим доступом в Україні / О.Є. Архипов, І.П. Касперський // Правова інформатика. – № 3(11). – 2005. – С.61-66.

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

56. Архипов О.Є. Теоретико-методичні засади оцінювання шкоди, обумовленої розголошенням секретної інформації / Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Вип. №2(17). – 2008. – С.16-23 // [Електронний ресурс]. – Режим доступу: http://pnzzi.kpi.ua/17/17_p16.pdf

57. Корченко О.Г. Удосконалення проведення процедури прийняття рішень державних експертів з питань таємниць у сфері оборони засобами інформаційних технологій // О.Г. Корченко, Ю.О. Дрейс // «Сучасні проблеми захисту інформації з обмеженим доступом»: міжвідомча наук.-практ. конф.: Тези доп. – К.: НАУ, НА СБ України, 2008. – С.62-63.

58. Корченко О.Г. Система підтримки прийняття рішень державних експертів з питань таємниць у сфері оборони / О.Г. Корченко, Ю.О. Дрейс // Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення : IV наук.-техн. конф. : Тези доп. – К.: НТУУ ВІТІ «КПІ», 2008. – С.188.

59. Михайлов В. Предотвращение ущерба национальной безопасности Украины – предусмотренный законодательством повод к засекречиванию информации / В. Михайлов, А. Муратов // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – №2(13). – 2006. – С.112-118 // [Електронний ресурс]. – Режим доступу: http://pnzzi.kpi.ua/13/13_p112.pdf

60. Рубанов В.А. От «культа секретности» – к информационной культуре / В.А. Рубанов // Коммунист. – № 13. – 1988. – С.24–30.

61. Соснін О.В. Проблеми теорії і практики засекречування інформації / Захист інформації. – Том 11, № 2(43) (2009). – С.4-10.

62. Фатьянов А.А. Проблемы защиты конфиденциальной информации, не составляющей государственную тайну / А. А. Фатьянов. // Информационное общество. – 1997. – №1. – С.49–56.

63. Постатейный комментарий к Закону Российской Федерации «О государственной тайне» / Бюро научно-технической информации «Техника для спецслужб» // [Электронный ресурс]. – Режим доступа: http://www.bnti.ru/showart.asp?aid=393&lvl=02

64. Архипов О. Є. Критерії визначення можливої шкоди національній безпеці України у разі розголошення інформації, що охороняється державою: монографія / О.Є. Архипов, О.Є. Муратов. – К: Наук.-вид. відділ НА СБ України, 2011. – 195 с.

65. Актуальные проблемы совершенствования законодательства о государственной тайне / Комитет Государственной Думы Российской Федерации по безопасности; материалы Парламентских слушаний 14.10.2008 // [Электронный ресурс]. – Режим доступа: http://www.komitet2-16.km.duma.gov.ru/site.xp/052051124051050056.html

66. Государственная тайна и ее защита в Российской Федерации: Учебное пособие / Под общ. ред. М.А. Вуса и А.В. Федорова. – [3-е изд.] – СПб.: Изд-во Р.Асланова «Юридический центр Пресс», 2007. – 752 с.

67. Швырков А.В. Методический подход к оценке ущерба в стоимостном выражении, наносимого безопасности Российской Федерации в результате несанкционированного (неправомерного) распространения сведений, составляющих государственную тайну / А.В. Швырков // Вопросы защиты информации: научно-практический журнал. – 2006. – №2(73). – С.30-35.

68. Седень С.Н. Основы защиты информации, составляющей государственную тайну. Курс лекций / Московский инженерно-физический институт. – 2002. – М.: МИФИ // [Электронный ресурс]. – Режим доступа: http://labs.rulezz.ru/study/16/5

69. Саати Т.Л. Математические модели конфликтных ситуаций. Пер. с англ. Под ред. И. А. Ушакова. – М. : «Сов. радио», 1977. – 304 с. // [Электронный ресурс]. – Режим доступа: http://scilib-military.narod.ru/Saati/contents.htm

70. Саати Т.Л. Принятие решений при зависимостях и обратных связях: Аналитические сети. Пер. с англ. / Науч. ред. А.В. Андрейчиков, О.Н. Андрейчикова. – М.: Издательство ЛКИ, 2008. – 360с. // [Электронный ресурс]. – Режим доступа: http://nashaucheba.ru/v15515/?cc=1&view=djvu

71. Муратов О.Є. Основні положення порядку засекречування інформації у США / О.Є. Муратов, В.П. Ворожко // Безпека інформації. – Том 17, № 1 (2012). – С.4-9.

72. Ворожко В.П. Система засекречивания и рассекречивания информации в США / Безопасность информации. – 1997. – №1(8). – С. 48-53.

73. Classified National Security Information. Executive Order 13526. Presidential Documents.// Federal Register. – Vol. 75. – No 2. – p. 707-731.

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

75. Угода між Урядом України та Урядом Сполучених Штатів Америки про охорону секретної інформації у сфері оборони // Відомості Верховної Ради України. – 2004. – №36. – ст.441.

76. Сидоренко С.М. Організаційно-правові засади охорони державної таємниці в Естонській республіці, Румунії, Чеській республіці / «Актуальні проблеми управління інформаційною безпекою держави»: Збірник матеріалів науково-практичної конференції, 30 березня 2012р., м.Київ. – К.: Наук.-видав. відділ НА СБ України, 2012. – С.219-223.

77. Про державні таємниці / Естонська Республіка; Закон від 25 січня 2007 року {зі змінами та доповненнями від 22 липня 2011 року} // [Електронний ресурс]. – Режим доступу: http://www.legalltext.ee/en/andmebass/ava.asp?m=022

78. Про служби безпеки / Естонська Республіка; Закон від 20 грудня 2000 року {зі змінами та доповненнями від 19 червня 2002 року} [Електронний ресурс]. – Режим доступу: http://www.legalltext.ee/en/andmebass/ava.asp?m=022

79. Про затвердження норм про захист секретної інформації НАТО в Румунії / Постанова № 353 від 15 квітня 2002 року // [Електронний ресурс]. – Режим доступу: http://www.orniss.ro/en/index.html

80. Телеховський Ю.Г. Реформування спеціальних служб Словаччини: досвід для України / Стратегічні пріоритети, №4 (25), 2012. – С. 210-214.

81. Про Державне агентство національної безпеки / Республіка Болгарія; Закон від 20 грудня 2007 року // [Електронний ресурс]. – Режим доступу: http://law.dir.bg/reference.php?f=zdans-07

82. Авдошин І.В. Особливості діяльності спецслужб естонської республіки з питань охорони державної таємниці / «Актуальні проблеми управління інформаційною безпекою держави»: Збірник матеріалів науково-практичної конференції, 30 березня 2012р., м.Київ. – К.: Наук.-видав. відділ НА СБ України, 2012. – С.152-157.

83. Про захист секретної інформації / Республіка Болгарія; Закон від 30 квітня 2002 року // [Електронний ресурс]. – Режим доступу: http://law.dir.bg/reference.php?f=zzki-02

84. Телеховський Ю.Г. Реформування спеціальних служб Румунії: досвід для України / Стратегічні пріоритети, №3 (20), 2011. – С. 154-158.

85. Сирота Т. В. Категорії відомостей, які складають таємницю за законодавством України та іноземних держав / «Актуальні проблеми управління інформаційною безпекою держави»: Збірник матеріалів науково-практичної конференції, 30 березня 2012р., м.Київ. – К.: Наук.-видав. відділ НА СБ України, 2012. – С.229-234.

86. Архипов О. Є. Системні аспекти оцінювання рівня важливості секретної інформації / О. Є. Архипов, В. П. Ворожко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Вип.2 (15). – 2007. – С.10-12.

87. Мельников В. В. Защита информации в компьютерных системах / В. В Мельников. – М.: Финансы и статистика; Электроинформ, 1997. – 368 с.

88. Харкевич А. А. О ценности информации / А. А. Харкевич // Проблемы кибернетики. – 1960. – №4. – С.14–21.

89. Стратанович Р. Л. О ценности информации / Р. Л. Стратанович // Изв. АН СССР. Техническая кибернетика. – 1965. – №5. – С.3–12.

90. Бонгард М. М. Проблемы узнавания / М. М. Бонгард. – М.: Наука, 1967. – 320 с.

91. Архипов О. Є. Визначення цінності конфіденційної інформації / О. Є. Архипов // «Інтернет-освіта-наука-2010», VII міжнародна конференція ІОН-2010, 28 вересня-3 жовтня 2010: Збірник матеріалів конференції. – Вінниця: ВНТУ, 2010. – С.377–379.

92. Архипов А. Е. Применение мотивационно-стоимостных моделей для описания вероятностных соотношений в системе "атака-защита" / А. Е. Архипов, С. А. Архипова // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К. – 2008. – Вип.1 (16). – С.57–61.

93. Богуш В. М. Інформаційна безпека держави / В. М. Богуш, О. К. Юдін. – К.: «МК-Прес», 2005. – 432 с.

94. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты / В. В. Домарев. – К.: ООО «ТИД ДС», 2001. – 688 с.

95. Архипов О. Є. Застосування методології передбачення для оцінювання шкоди, заподіяної витоком секретної інформації / О. Є. Архипов, І. П. Касперський // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К. – 2007. – Вип.2 (15). – С.13–19.

96. Ефимов А. Н. Информация: ценность, старение, рассеяние / А. Н. Ефимов. – М.: Знание, 1978. – 64 с.

97. Згуровський М. З. Сценарний аналіз як системна методологія передбачення / М. З. Згуровський // Системні дослідження та інформаційні технології. – 2002. – № 1. – С. 5–36.

98. Катренко А. В. Системний аналіз об'єктів та процесів комп'ютеризації / А. В. Катренко. – Львів: «Новий світ», 2000. – 424 с.

99. Сурмин Ю. П. Теория систем и системный анализ / Ю.П. Сурмин – К.: МАУП, 2003. – 368 с.

100. Інформаційні технології. Настанови з керування безпекою інформаційних технологій (ІТ). Частина 3. Методи керування захистом ІТ. (ISO/IEC TR 13335–3) : ДСТУ ISO/IEC TR 13335–3. – (Чинний з 2004-10-01) – К.: Держспоживстандарт України, 2005. – ІІІ. 76 с. – (Національний стандарт України).

101. Information Technology – Security techniques – Information security risk management. (ISO/IEC 27005:2008). – ISO/IEC JTC 1/SC 27, 2008. – 62 p.

102. Архипов А. Е. Технология построения комбинированных измерительных шкал для оценивания значимости информации / А.Е. Архипов // Адаптивные системы автоматического управления. – 2008. – № 13(33). – С.153–158.

103. Архипов О. Є. Моделювання і прогнозування в соціальній сфері: Навч.-метод. посіб. / О.Є. Архипов, С.А. Архіпова. – К.: ІВЦ Видавництво «Політехніка», 2001. – 60 с.

104. Архипов О. Є. Щодо методики ідентифікації та оцінювання активів системи інформаційних технологій /О.Є. Архипов // Захист інформації. – №1 (50), 2011. – С.42-47.

105. Архипов О.Є. Застосування онтологічної ієрархії у задачах визначення цінності інформації / О.Є. Архипов, М.А. Петренко // Захист інформації. – Вип. №1(54). – 2012. – С.45-52.

106. Корченко О. Г. Модель складної орієнтованої мережі ЗВДТ / О. Г. Корченко, О. Є. Муратов, Ю. О. Дрейс, І. О. Козлюк // Захист інформації. – №3 (52), 2011. – С.87-93.

107. Петренко Н. Компьютерные онтологии и онтолого-управляемая архитектура информационных систем / Krassimir Markov, Vitalii Velychko, Oleksy Voloshin // Information Models of Knowledge. - Kiev, Ukraine – Sofia, Bulgaria, 2010. – С.86-92.

108. Рогушина Ю. В. Використання методу індуктивного виведення для вдосконалення онтології предметної області пошуку / Ю. В. Рогушина, І. Ю. Гришанова // Системні дослідження та інформаційні технології. – №1, 2007. – С.62-70.

109. Справочник проектировщика АСУ ТП / Г. Л. Смилянский, Л. З. Амлинский, В. Я. Баранов и др.; Под ред. Г. Л. Смилянского. – М.: Машиностроение, 1983. – 527 с.

110. Информационные технологии управления / Под ред. Ю. М. Черкасова. – М. :ИНФРА-М, 2001. – 216 с.

111.Суппес П. Основы теории измерений / П. Суппес, Дж. Зиннес // Психологическое измерение. – М.: Мир, 1976. – 220 с.

112. Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / А. Г. Корченко. – К.: «МК-Пресс», 2006. – 320 с.

113. Архипов О. Є. Системні аспекти оцінювання рівня важливості секретної інформації / О. Є. Архипов, В. П. Ворожко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. К., – 2007. – Вип.2 (15). – С.10–12.

114. Носок С. О. Методи обробки експертних даних в задачі автоматизації профвідбору. Дисертація на здобуття наукового ступеня канд. техн. наук. / С. О. Носок. – К.: 2007. – 160 с.

115. Архипов А. Е. Технологии экспертного оценивания в задачах защиты информации / А.Е. Архипов, С.А. Архипова, С.А. Носок // Інформаційні технології та комп'ютерна інженерія. – 2005. – № 2. – С.89–94.

116. Архипов А. Е. Применение методов кластеризации в задаче обработки данных экспертного опроса / А.Е. Архипов, С.А. Архипова, С.А. Носок, И.В. Пишко // Радіоелектроніка, інформатика, управління. – 2003. – № 2(10). – С.104–108.

117. Архипов А. Е. Применение кластерного анализа для структурирования данных экспертного опроса / А.Е. Архипов, С.А. Архипова, С.А. Носок // Адаптивные системы автоматического управления. – 2003. – №6(26). – С.55–61.

118. Архипов О. Є. Модели оценивания компетентности экспертов по данным многообъектной экспертизы / «Інтернет-освіта-наука-2010», сьома міжнародна конференція ІОН-2010, 28 вересня-3 жовтня 2010: Зб. мат. конф. / О.Є. Архипов, С.А. Архипова. – Вінниця: ВНТУ, 2010. – С.191–194.

119. Архипов О. Є. Математичне моделювання соціальних систем і процесів: Навч.-метод. посібник / О.Є. Архипов, С.А. Архипова. – К. : ІВЦ Видавництво «Політехніка», 2002. – 60 с.

120. Архипов А. Е. Модели компетентности експерта/А.Е. Архипов, С.А. Архипова, С.А. Носок // Міжнародна наукова конференція Інтелектуальні системи прийняття рішень та прикладні аспекти інформаційних технологій (ISMIT-2006), м. Євпаторія, 15-19 травня 2006, том 1. – С.22-25.

121. Архипов А. Е. О построении модели компетентности эксперта / А.Е. Архипов, С.А. Архипова, С.А. Носок // Системні технології. Системи управління, контролю та технічної діагностики: Зб. наук. праць. – Вип.8 – Дніпропетровськ: «Системні технології», 2006. – С.22-25.

122. Дрейс Ю. О. Визначення рівня компетентності експертів експертної комісії з питань державної таємниці / Ю.О. Дрейс, О.Г. Корченко // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : Зб. наук. праць. – Житомир : ЖВІ НАУ, 2011. – Вип. 4. – С.190-196.

123.Грабовецький Б. Є. Економічне прогнозування і планування / Б. Є. Грабовецький. – К.: Центр навчальної літератури, 2003. – 188 с.

124.Матвієнко В. Я. Прогностика / В. Я. Матвієнко. – К: Українські пропілеї, 2000. – 484 с.

125. Оцінювання ефективності системи охорони державної таємниці : Монографія / О. Є. Архипов, І. Т. Бородавко, В. П. Ворожко. – К.: Вид-во НА СБ України, 2007. – 62 с.

126. Змитрович А.И. Интеллектуальные информационные системы. - Мн.: НТОО «Тетра Системс», 1997. – 368 с.

127. Основи інформаційних систем / В.Ф. Ситник, Т.А. Писаревска, Н.В. Єрьоміна, О.С. Краєва.: З ред. В.Ф. Ситника. - К.: КНЕУ, 1997. – 252 с.

128. Конеев Н. Р. Информационная безопаснсть предприятия / Н. Р. Конеев, А. В. Беляев. – С-Пб.: БХВ-Петербург, 2002. - 752 с.

129. Организация работы с документами / В. А. Кудряев и др. – М.: ИНФРА-М, 1998. – 575 с.

130. Защита информационных ресурсов государственного управления / А. С. Гринберг, Н. Н. Горбачев, А. А. Тепляков. – М.: ЮНИТА-ДАНА, 2002. – 327 с.

131. Особенности использования средств технической защиты информации от утечки за счет побочных электромагнитных излучений и наводок/ А. Е. Архипов, В. Н. Луценко, В. А. Худяков // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, №4. – К., 2002.-С. 178-182.

132. Захист інформації в телекомунікаційних мережах та системах зв'язку: Навч.-метод. посіб./ А.Є. Архипов, В.М. Луценко, В.О. Худяков – К.: ІВЦ «Видавництво «Політехніка», 2003. – 40 с.

133. Нестеренко М.П. Стільниковий телефон – новітнє джерело соціальних проблем та загроз / М.П. Нестеренко, В.В. Шорошев // Бизнес и безопасность. - № 5. – 2004. – С.64-66.

134. Коротєєв І.М. Навмисний силовий вплив як негативне явище сучасних інформаційних технологій// Бизнес и безопасность. – 2005. - №5 – С.2-3.

135. Мусиенко Д. Защита электронного оборудования от деструктивного воздействия беспроводных технических средств // Бизнес и безопасность. – 2005. - №5. – С .37-42.

136. Архипов А.Е. Задачи и проблемы обеспечения комплексных систем защиты информации / А.Е. Архипов, В.П. Ворожко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, № 6. – К., 2003. – С.137-140.

137. Архипов А.Е. Применение среднего риска для оценивания эффективности защиты информационных систем / А.Е. Архипов // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні., № 3(14) – К., 2006. – С.60-67.

138. Анализ и оценивание рисков информационной безопасности: монографія / [Корченко А.Г., Архипов А.Е., Казмирчук С.В.]. – К.: ООО «Лазурит-Полиграф», 2013. – 275 с.

139.Качинський А.Б. Безпеки, загрози і ризик: Наукові концепції та математичні методи. – К., 2003. – 472 с.

140. Гостев И.М. Безопасность – бесполезная трата денег или их выгодное вложение? // Конфидент. Защита информации. - № 5. – 2003. – С.16-18.

141.Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / С.А. Петренко, С.В.Симонов. – М.: Компания Ай Ти; ДМК Пресс, 2004. – 348 с.

142. Защита информационных ресурсов государственного управления / Гринберг А.С., Горбачев Н.Н., Тепляков А.А. – М.: Юнити-ДАНА, 2003. – 327 с.

143. Андрощук Г.А. Экономическая безопасность предприятия: защита коммерческой тайны / Г.А. Андрощук, П.П. Крайнев. – К.: Изд. Дом «Ин Юре», 2000. – 400 с.

144. Экспертиза в системе ТЗИ на основе нечетких множеств / А.Г. Корченко, В.Г. Потапов, В.А. Рындюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, №7. – К., 2003. – С.118-127.

145. Домарев В.В. Защита информации и безопасность компьютерных систем. – К.: «ДиаСофт», 1999. – 480 с.

146. Зегжда Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. – М.:Горячая линия – Телеком, 2000. – 452 с.

147. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт**.**

148. Нове в законодавстві про інформацію / Мін'юст України; Лист від 21.06.2011 // [Електронний ресурс]. – Режим доступу: http://zakon4.rada. gov.ua/laws/show/n0038323-11

149. Головань С.М. Класифікація інформації на основі законодавчих актів України / Сучасний захист інформації. – Вип. №1. – 2010. – С.4-7

150. Головань С.М. Класифікація інформації / Вісник Східноукраїнського національного університету ім. В. Даля. – Вип. №7 (161). – Луганськ.: Вид-во СНУ ім. В. Даля. – 2011, Ч. 1. – С.322-326.

151. Прокоф'єва Д.М. Дослідження змісту категорій інформації з обмеженим доступом відповідно до чинного законодавства України / Центр інформаційної безпеки // [Електронний ресурс]. – Режим доступу: http://www.bezpeka.com/ru/lib/spec/law/art8.html

152.Турченко О. Щодо поняття професійної таємниці / Правничий часопис донецького університету. – Вип № 1 (19). – 2008. – С.53 // [Електронний ресурс]. – Режим доступу:http://www.nbuv.gov.ua/portal/Soc_Gum/Pchdu/2008_1/10.htm

153. Про банки і банківську діяльність / Верховна Рада України; Закон від 07.12.2000 № 2121-III // [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2121-14

154. Цивільний кодекс України. Стаття 1076. Банківська таємниця // http://yurist-online.com/ukr/uslugi/yuristam/kodeks/003/1076.php

155. Носік Ю. Правовий режим банківської таємниці в Україні / Тайны нформационной безопасности / НДЦ «ТЕЗІС» НТУУ «КПІ» // [Електронний ресурс]. – Режим доступу: http://www.idportal.org/page-id-658.htm

156. Бараннік Р.В. Особливості охорони інформації, що становить таємницю у кримінальному судочинстві / Р.В. Бараннік, П.Г. Назаренко // Адвокат. – Вип. №4. – 2011. – С.15-18 // [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/portal/Soc_Gum/Advokat/2011_4/2011-4Barannik_Nazarenko.pdf

157. Засада гласності та її обмеження в кримінальному судочинстві: Автореф. дис.. канд. юрид. наук: 12.00.09 / В.В. Король;. Львів. нац. ун-т ім. І. Франка. – Львів., 2002. – 21 с. – укр. // [Електронний ресурс]. – Режим доступу: http://studrada.com.ua/content/король-вв-засада-гласності-та-її-обмеження-в-кримінальному-судочинстві-2002р

158. Кримінально-процесуальний кодекс України. Розділ другий. Порушення кримінальної справи, дізнання і досудове слідство. Глава 10. Дізнання. Стаття 121. Недопустимість розголошення даних досудового слідства // [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?page=2&nreg=1002-05

159. Перевалова Л.В. Захист конфіденційної інформації: проблеми та шляхи вирішення / Л.В. Перевалова, С.В. Кваша. – Вісник Національного технічного університету «Харківський політехнічний інститут». Збірник наукових праць. Тематичний випуск: Актуальні проблеми розвитку українського суспільства. – Харків: НТУ «ХПІ», 2011. – № 30. – С. 55-61

160. Про засади запобігання і протидії корупції / Верховна Рада України; Закон, Форма типового документа, Декларація від 07.04.2011

№ 3206-VI // [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/3206-17

161. Корченко О.Г. Нечітке моделювання лінгвістичної змінної “інформація” за змістом відомостей та видом операцій, що виконуються над нею / О.Г. Корченко, Ю.О. Дрейс // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : Зб. наук. праць. – Вип.2. – Житомир: ЖВІ НАУ, 2009. – С.102–108.

162.Корченко О.Г. Нечітке моделювання вхідної інформації АРМ державного експерта з питань таємниць / О.Г. Корченко, Ю.О. Дрейс // Актуальні проблеми забезпечення інформаційної безпеки держави : Наук.-практ. конф. : Тези доп. – К.: Вид-во НА СБ України, 2009. – С.190-191.

163.Складні мережі / [Ю. Головач, О. Олємской, К. фон Фербер, Т. Головач, О. Мриглод, І. Олємской, В. Пальчиков]. – Львів. : Журнал фізичних досліджень. Том 10, число 4. – 2006. – С.247-289 // [Електронний ресурс]. – Режим доступу:http://www.ktf.franko.lviv.ua/JPS/2006/4/pdf/247_289.pdf

164. Національна безпека: український вимір: щокв. наук. зб. / Рада нац. безпеки і оборони України, Ін-т пробл. нац. безпеки; редкол.: Горбулін В.П. (голов. ред.)[та ін.]. – К., 2008. – Вип. 1-2 (20-21). – 160 с.

165. Ландэ Д.В. Интернетика: Навигация в сложных сетях: модели и алгоритмы / Д.В. Ландэ, А.А. Снарский, И.В. Безсуднов. – М.: Либроком (Editorial URSS). – 2009. – 264 с. // [Электронный ресурс]. – Режим доступа: http://webground.sut

166. Ланде Д. В. Новітні підходи й технології інформаційно-аналітичної підтримки прийняття рішень / Національна безпека: український вимір: щоквартальний науковий збірник / Рада нац. безпеки і оборони України, Ін-т пробл. нац. безпеки; редкол.: Горбулін В.П. (голов. ред.) [та ін.]. – К., 2008. – Вип. 1-2 (20-21). – С.87-105.

167.Перелік службової інформації Збройних сил України / Генеральний штаб Збройних сил України; Наказ №180 від 20.09.2011.

168. Корченко О.Г. Модель складної орієнтованої інформаційної мережі службової інформації у сфері оборони – Переліку службової інформації Збройних Сил України / О.Г. Корченко, Ю.О. Дрейс // Захист інформації і безпека інформаційних систем : І Міжнар. наук.-техн. конф. : Тези доп. – Львів. : НУ “Львівська політехніка”, 2012. – С.10-11.

169. Моделі та методи оцінювання шкоди національній безпеці у сфері охорони державної таємниці [Текст] : автореф. дис. ... канд. техн. наук : за спец. 21.05.01 – інформаційна безпека держави / Дрейс Юрій Олександрович; Нац. авіац. ун-т. – К., 2013. – 20 с.

170. Корченко О.Г. Метод аналізу і оцінки величини можливої шкоди національній безпеці держави у сфері охорони державної

таємниці / О.Г. Корченко, С.В. Казмірчук, Ю.О. Дрейс // Захист інформації. – №3 (56). – К. : НАУ, 2012. – С.5-18.

171. Дрейс Ю.О. Метод нечіткої класифікації відомостей, що становлять державну таємницю за встановленими критеріями / Вісник Національного університету «Львівська політехніка»: Автоматика, вимірювання та керування. – 2013. – №774. – С.10-17.

172. Поршнев С.В. MATLAB 7. Основы работы и программирования. Учебник – М.: ООО «Бином-Пресс», 2011. – 320 с.

173. Литвиненко О.В. Спеціальні інформаційні операції та пропагандистські кампанії / О. В. Литвиненко. – К.: ВКФ «Сатсанга», 2000. – 222 с.

174. Янг Э. Прогнозирование научно-технического прогресса / Э. Янг. – М.: Прогресс, 1974. – 219 с.

175. Жерардэн Л. Исследование альтернативных картин будущего: Метод составления сценариев. Руководство по научно-техническому прогнозированию / Жерардэн Л. – М.: Прогресс, 1977. – 132 с.

176. Дрейс Ю.О. Розрахунок коефіцієнтів захищеності відомостей, що становлять державну таємницю / Ю.О. Дрейс, Н.С. Вишневська, Ю.Є. Хохлачова // Захист інформації. – №3 (48). – К. :НАУ. – 2010. – С.10-14.

177. Гнатієнко Г.М. Експертні технології прийняття рішень : монографія / Г.М. Гнатієнко, В. Є. Снитюк. – К. : ТОВ «Маклаут», 2008. – 444 с.

178. Катренко А.В. Теорія прийняття рішень / А.В. Катренко, В.В. Пасічник, В.П. Пасько. – К.: Видавнича група BHV, 2009. – 448 с.

179.Корченко О.Г. Методологія синтезу та програмна реалізація системи оцінювання шкоди національній безпеці у сфері охорони державної таємниці / О.Г. Корченко, М.Г. Луцький, М.В. Захарова, Ю.О. Дрейс // Захист інформації. – Том 15, №1 (2013). – С.14-20.

180. Дрейс Ю.О. Експериментальне дослідження системи оцінювання шкоди національній безпеці у сфері охорони державної таємниці / Захист інформації. – Том 15, № 4 (2013). – С.337-345.

ДОДАТКИ

Додаток 1

(*Форма А, зразок*) *Додаток N 2 до* [17]

Таємно

(після заповнення)

Прим. N_____

ЗАРЕЄСТРОВАНО
Державним комітетом України
з питань державних секретів
за N___ від "__" _____року

РІШЕННЯ
державного експерта з питань таємниць про
віднесення відомостей до державної таємниці
N _____ від "__" _____року

Державний експерт (и) з питань таємниць

_____
(прізвище, ім'я та по батькові)

_____,
(державний орган, посада)

розглянувши відповідно до Закону України "Про державну таємницю" відомості (пропозиції* про віднесення відомостей до державної таємниці) про _____
_____
_____
_____

* Якщо пропозиції про віднесення відомостей до державної таємниці внесені державним органом, вказати повну його назву.

ВСТАНОВИВ (ЛИ):

Ці відомості належать до сфери _____
(оборони, економіки, науки і техніки,

_____
зовнішніх відносин, державної безпеки і охорони правопорядку)

Їх розголошення може призвести до _____
(особливо тяжких або тяжких)

наслідків для діяльності держави в зазначеній сфері або завдати шкоди її економічним чи політичним інтересам: _____
(зазначити, в чому

_____
конкретно виявлятимуться ці наслідки чи шкода інтересам держави)

_____

На підстави викладеного –

ВИРІШИВ (ЛИ):

1. Віднести зазначені вище відомості до державної таємниці та визначити ступінь їх секретності _____
("особливої важливості", "цілком таємно", "таємно")

2. Надати право доступу до цих відомостей і приймати рішення про допуск до них інших осіб відповідно до їх службових обов'язків керівникам

_____
(зазначити міністерства, інші центральні органи державної виконавчої влади,
_____
підприємства, установи, організації, які залучені до виконання державного завдання чи
_____
реалізації політичного рішення, пов'язаного з використанням цих відомостей)

3. Визначений ступінь секретності цих відомостей має чинність до "___"_____199__року, після чого він підлягає перегляду з метою_____.
(зниження на один ступінь, скасування, продовження строку)

Державний експерт (и) з питань таємниць _____
(підпис)

М.П.

Відмітки Державного комітету України з питань державних секретів:

Відомості, зазначені у цьому рішенні, внесені до Зводу відомостей, що становлять державну таємницю, "_"_____199__року за N_____.

Голова Комітету _____ "___"_____199__року.
(підпис)

Відомості, зазначені у цьому рішенні, вилучені зі Зводу відомостей, що становлять державну таємницю, "___"_____ року на підставі висновку державного експерта з питань таємниць від "__"_____199__року N_____.

Голова Комітету _____ "___"_____199__року.
(підпис)

Відомості, зазначені у цьому рішенні, вилучені зі Зводу відомостей, що становлять державну таємницю, "___"_____ року у зв'язку із закінченням строку дії ступеня секретності, визначеного для них у пункті 3 цього рішення.

Голова Комітету _____ "___"_____199__року.
(підпис)

Додаток 2
(*Форма Б, зразок*) *Додаток N 3 до* [17]
Прим. N_____

ЗАРЕЄСТРОВАНО
Державним комітетом України
з питань державних секретів
за N_____ від _____

ВИСНОВОК
державного експерта з питань таємниць
про розсекречування відомостей
N _____ від "__" _____року

Державний експерт (и) з питань таємниць
_____
(прізвище, ім'я та по батькові)
_____,
(державний орган, посада)
розглянувши відповідно до Закону України "Про державну таємницю" відомості (пропозиції* про розсекречування відомостей) про _____
_____
_____
_____
_____
_____,
які згідно з рішенням від "___"_____199__року N_____
державного експерта з питань таємниць
_____
(прізвище, ім'я та по батькові)
_____
віднесені до державної таємниці з наданням їм ступеня секретності
_____,_____
_____
* Якщо пропозиції про розсекречування відомостей внесено державним органом, вказати повну його назву.

ВСТАНОВИВ:

Ці відомості втратили важливість для діяльності держави у сфері
_____,
(оборони, економіки, зовнішніх відносин, державної безпеки і охорони правопорядку)
їх розголошення не може призвести до негативних наслідків для цієї сфери або завдати шкоди політичним чи економічним інтересам держави.

У зв'язку з цим

ЗРОБИВ ВИСНОВОК:

1. Вважати зазначені вище відомості такими, що відповідають / не становлять ступеню секретності "цілком таємно", "таємно" / державної таємниці (зайве викреслити).

2. Вважати рішення державного експерта з питань таємниць від "___"_____199__року N_____ таким, що втратило чинність.

Підпис (и)

М.П.

Відмітки Державного комітету України з питань державних секретів:

Відомості, зазначені у цьому висновку, вилучені зі Зводу відомостей, що становлять державну таємницю, "___"_____199_року, про що зроблено відмітку у рішенні державного експерта з питань таємниць від "___"_____199__року N_____, вказаному у пункті 2 цього рішення.

Голова Комітету _____ "___"_____199__року.
(підпис)

Додаток 3

до пункту 11 [30]

_____
(гриф обмеження доступу)

ПРОТОКОЛ N ___

Присутні:

Голова комісії _____
(прізвище та ініціали)

Секретар _____
(прізвище та ініціали)

Члени комісії: _____
(прізвище та ініціали)

_____
(прізвище та ініціали)

_____
(прізвище та ініціали)

Доповідач _____
(прізвище та ініціали)

Питання, які розглядалися:_____
_____
_____
_____
_____

Вирішили: _____
_____
_____

Пропозиції та зауваження до протоколу:_____
_____
_____
_____

Голова комісії _____ _____
(підпис) (ініціали та прізвище)

Секретар _____ _____
(підпис) (ініціали та прізвище)

Члени комісії: _____ _____
(підпис) (ініціали та прізвище)

_____ _____
(підпис) (ініціали та прізвище)

_____ _____
(підпис) (ініціали та прізвище)

"___" _____ 20__ р.

Додаток 4

до пункту 13 [30]

_____
(гриф обмеження доступу)

ЗАТВЕРДЖУЮ

_____
(посада керівника підприємства, у
станови й організації)

_____ _____
(підпис) (ініціали та прізвище)

"___" _____20__ р.

АКТ ЕКСПЕРТИЗИ

Експертна комісія

_____
(найменування підприємства, установи, організації)

у складі

_____
(посада, прізвище та ініціали)

_____

розглянула_____
(вид та стислий зміст документа, іншого матеріального

_____
носія інформації, номер, дата реєстрації)

_____

Зробила висновок:

_____
_____
_____

Голова комісії _____ _____
(підпис) (ініціали та прізвище)

Члени комісії: _____ _____
(підпис) (ініціали та прізвище)

_____ _____
(підпис) (ініціали та прізвище)

_____ _____
(підпис) (ініціали та прізвище)

"___" _____ 20__ р.

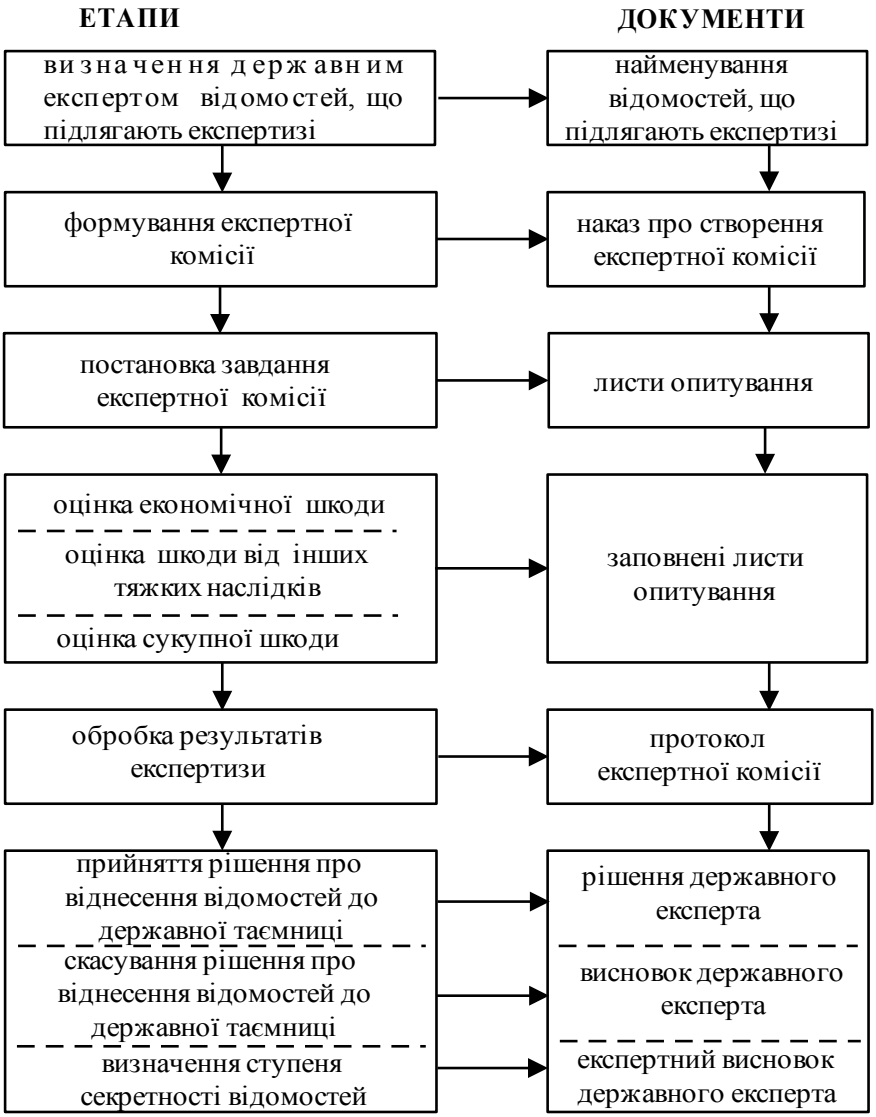
Додаток 5
(*Додаток 1* [38])

"ПИТОМА ВАГА" ОБ'ЄКТІВ

№ п/п	Сфера діяльності, об'єкти	Значення питомої ваги
	1. ОБОРОНА	
1.1	Вид Збройних Сил	300
1.2.	Округ	300
1.3.	Армія, рід військ, Прикордонні війська	100
1.4.	Корпус, ескадра, Внутрішні війська МВС	30
1.5.	Дивізія	15
1.6.	Полк, бригада, окрема військова частина	10
1.7.	Командні пункти: - виду Збройних Сил, округу, - армії, флотилії, корпусу, ескадри, Прикордонних військ, Національної гвардії, Цивільної оборони - дивізії, полку, бригади	 50-100 30-50 10
1.8.	Арсенали, бази, склади з озброєнням, військовою та спеціальною технікою, ремонтні частини, підприємства	10-30
1.9.	Перспективні зразки озброєння і військової техніки: - стратегічне озброєння - оперативно - тактичне озброєння - озброєння, військова техніка на якісно новому рівні - модернізоване озброєння, військова техніка - засоби військового зв'язку, радіоелектронної боротьби, вимірювальна та спеціальна техніка	 300 50 20-50 10-30 5-15
1.10.	Картографічна продукція	10-15
	2. ЕКОНОМІКА	
2.1.	Мобілізаційні потужності створення державних матеріальних резервів: - міністерством, відомством - підприємством, установою, організацією	 100 10-20
2.2.	Формування, фінансування та виконання оборонного замовлення: - Міністерством промислової політики - іншим міністерством, відомством - підприємством, установою, організацією	 300 100 10-50
2.3.	Об'єкти атомної енергетики	10-30
2.4.	Об'єкти енергопостачання	10-15
2.5.	Залізничні вузли	10-30
	3. ДЕРЖАВНА БЕЗПЕКА	
3.1.	Системи і комплекси урядового і спеціального зв'язку	50
3.2.	Державні шифри	500
3.3.	Системи та засоби криптографічного захисту інформації.	50-100
3.4.	Перспективні технічні системи і засоби розвідки	20-50
3.5.	Спеціальні технічні засоби оперативно-розшукового застосування.	5-15
3.6.	Технічні засоби охорони, сигналізації.	10-15

Додаток 6
(*Додаток 2* [38])

ПРОЦЕДУРА ПРОВЕДЕННЯ ЕКСПЕРТИЗИ



Додаток 7
(*Додаток 3* [38])

ЛИСТ ОПИТУВАННЯ ЧЛЕНА ЕКСПЕРТНОЇ КОМІСІЇ

1.	Відомості, що підлягають експертизі	
2.	Сфера (сфери) діяльності, до якої відносяться відомості	
3.	Об'єкт, який містить відомості, що підлягають експертизі, їх "питома вага" (у балах)	
4.	Прогнозні дії сторони, що оволоділа відомостями	
5.	Складова частина (елемент) об'єкта, що безпосередньо підпадає під дію сторони, що оволоділа відомостями, її відносна вартість від вартості об'єкта (%)	
6.	Зниження ефективності (%) використання складової частини об'єкта (або об'єкта в цілому) внаслідок дії сторони, що оволоділа відомостями	
7.	Величина економічної шкоди (у балах)	
8.	Інші тяжкі наслідки від втрати відомостей, рівень шкоди (у балах)	
9.	Сукупна шкода у балах	

Додаток 8
(*Додаток 4* [38])

ПРОТОКОЛ
засідання експертної комісії

1.Відомості, що підлягають експертизі.

2. Сфера діяльності, до якої відносяться відомості.

3. Об'єкт, який містить відомості, що підлягають експертизі, його "питома вага".

4. Прогнозні дії сторони, що оволоділа відомостями.

5. Складова частина (елемент) об'єкту, що безпосередньо підпадає під дію іноземної держави, її відносна вартість від вартості об'єкта (%).

6. Зниження ефективності (%) використання СЧО (або об'єкта в цілому) внаслідок дії сторони, що оволоділа відомостями.

7.Величина економічної шкоди внаслідок втрати відомостей.

8.Інші тяжкі наслідки, рівні їх шкоди.

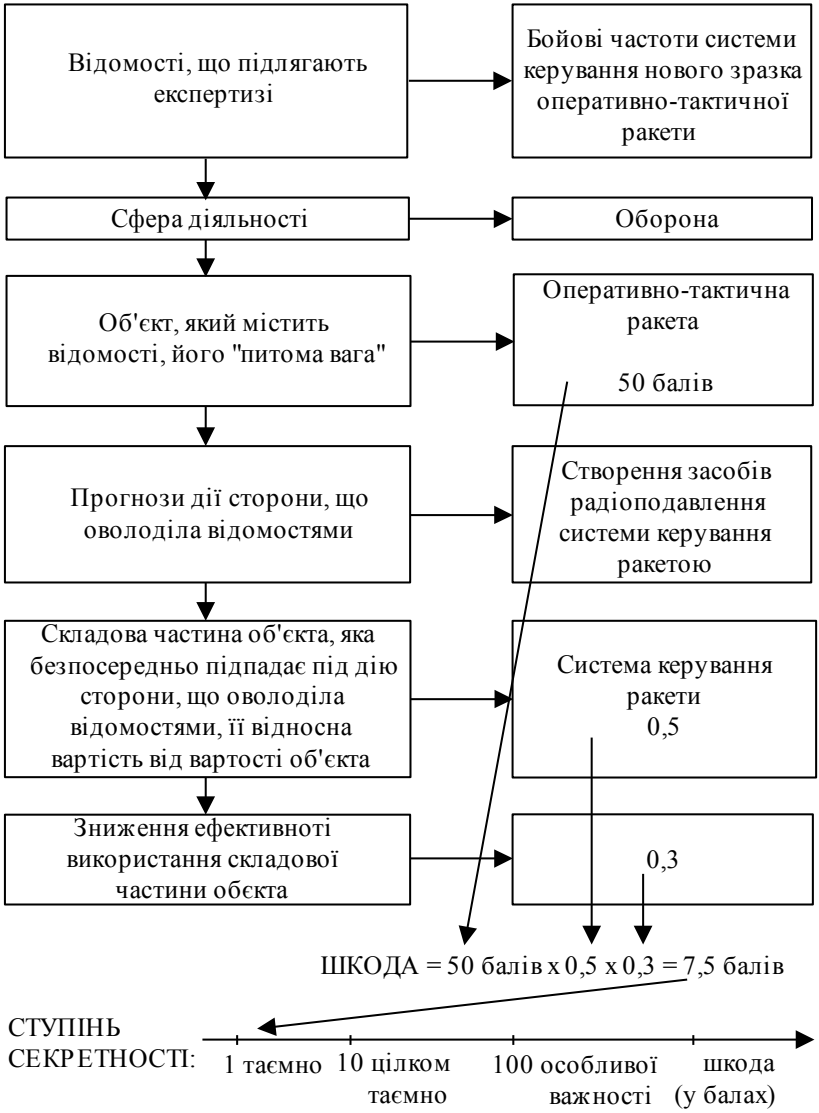
9. Сукупна шкода .

10. Ступінь секретності відомостей.

Секретар комісії_____
Члени експертної комісії_____
(підписи)
"___" _____ 19___р.

Додаток 9
(*Додаток 5* [38])

ПРИКЛАД ЕКСПЕРТНОГО ВИЗНАЧЕННЯ ШКОДИ ВІД ВТРАТИ ВІДОМОСТЕЙ І СТУПЕНЯ ЇХ СЕКРЕТНОСТІ



Додаток 10
(*Додаток 5* [38])

ПРИКЛАД ЕКСПЕРТНОГО ВИЗНАЧЕННЯ ШКОДИ ВІД ВТРАТИ ВІДОМОСТЕЙ І СТУПЕНЯ ЇХ СЕКРЕТНОСТІ

Додаток 11

УКРАЇНА

ДЕРЖАВНА СЛУЖБА ВЛАСНОСТІ УКРАЇНИ ІНТЕЛЕКТУАЛЬНОЇ

СВІДОЦТВО

про реєстрацію авторського права на твір

№ 48712

Комп'ютерна програма "Система аналізу і оцінки величини можливої шкоди національній безпеці держави у сфері охорони державної таємниці"

(вид, назва службового твору)

Автор(и) **Корченко Олександр Григорович, Дрейс Юрій Олександрович**

(повне ім'я, псевдонім (за наявності))

Авторські майнові права належать **Національний авіаційний університет, пр-т Космонавта Комарова, 1, м. Київ, 03680**

(повне ім'я фізичної та/або повне офіційне найменування юридичної особи, адреса)

Дата реєстрації 11.04.2013

Державна служба інтелектуальної власності України. Ідентифікаційний код 37553256

Голова Державної служби інтелектуальної власності України

М.В. Ковіня

Н а у к о в е в и д а н н я

Корченко Олександр Григорович
Архипов Олександр Євгенійович
Дрейс Юрій Олександрович

ОЦІНЮВАННЯ ШКОДИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ У РАЗІ ВИТОКУ ДЕРЖАВНОЇ ТАЄМНИЦІ

Монографія

Друкується в авторській редакції

Підписано до друку 10.07.2014. Формат 60х84/16
Друк офсетний. Папір офсетний.
Надруковано в Україні.
Тираж 300 прим.

Надруковано в друкарні ТОВ «Наш формат»,
01042, м.Київ, вул. Фрунзе, 84

332