

УДК 65.012.8

## ЗАСТОСУВАННЯ МЕТОДОЛОГІЇ ПЕРЕДБАЧЕННЯ ДЛЯ ОЦІНЮВАННЯ ШКОДИ, ЗАПОДІЯНОЇ ВИТОКОМ СЕКРЕТНОЇ ІНФОРМАЦІЇ

Олександр Архипов, Ігор Касперський \*

Національний технічний університет України „КПІ”

\*Інститут захисту інформації з обмеженим доступом Національної академії СБ України

**Анотація:** Викладено методику розрахунку кількісного значення сукупної шкоди, обумовленої витоком інформації, шляхом застосування сценарного підходу у прогнозуванні розвитку подій, які відбулися внаслідок цього витоку.

**Summary:** The article is devoted to usage of scenario method for determining range of data leak damage.

**Ключові слова:** Метод сценарію, державна таємниця, інформаційний ризик, середній ризик.

### I Вступ

Відповідно до вимог чинного законодавства віднесення інформації до державної таємниці та визначення ступеня секретності таких даних проводиться шляхом визначення шкоди від розголошення цієї інформації. Міра шкоди, завданої розголошенням інформації, також є кваліфікуючою ознакою при визначенні виду та ступеня юридичної відповідальності за пов'язані з цим наслідком діяння.

Центральним суб'єктом процесу віднесення інформації до державної таємниці є державні експерти з питань таємниць (далі - держексперти), які відповідно до ст. 9. Закону України «Про державну таємницю» [1] уповноважені визначати підстави, за якими інформацію має бути віднесено до державної таємниці та ступінь секретності інформації, віднесеної до державної таємниці. Для вирішення цього завдання держексперти мають право створювати експертні комісії, порядок функціонування яких визначено Положенням про експертні комісії з питань державної таємниці [2] та Методичними рекомендаціями державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня їх секретності (далі - Методичні рекомендації) [3].

В попередніх публікаціях нами розкрито загальні недоліки викладеної в Методичних рекомендаціях методики віднесення інформації до державної таємниці та сучасні дієві підходи отримання та обробки оціночних суджень членів експертних комісій, які можливо використати в роботі держекспертів [4 – 6]. В цій статті запропоновано власне бачення методичних підходів до визначення шкоди, завданої розголошенням інформації та можливостей застосування методу сценаріїв.

Отож відповідно до п. 3.1 Методичних рекомендацій з метою визначення належності відомостей до державної таємниці рівень потенційної сукупної шкоди від розголошення інформації обраховується шляхом сумування показників економічної та іншої шкоди, яка може бути завдана внаслідок такого розголошення. Обрахування іншої шкоди (це шкода, яка не піддається економічному розрахунку) проводиться в балах відповідно до шкали можливих негативних наслідків, наведених у п. 3.2 Методичних рекомендацій.

Розрахунок економічної шкоди здійснюється шляхом знаходження різниці між показником ефективності використання виділених коштів для забезпечення діяльності об'єкта за умов збереження інформації про нього у таємниці та того самого показника після розголошення цих даних. Визначення показника економічної шкоди проводиться в умовних одиницях – балах відповідно до визначеною у додатку 1 до Методичних рекомендацій «питомою вагою» окремих важливих об'єктів.

Невирішеним залишається завдання щодо способів обрахування величини економічної шкоди, яку відповідно до п. 5.1 та додатку 3 до Методичних рекомендацій члени експертних комісій визначають окремо через прогнозування дії сторони, що оволоділа відомостями, визначення складової частини об'єкта, яка безпосередньо підпадає під дії сторони, що оволоділа відомостями, її відносна вартість у відсотках до вартості об'єкта та ступеня зниження ефективності використання складової частини об'єкта або об'єкта в цілому внаслідок дії сторони, що оволоділа відомостями.

### II Постановка задачі

Як бачимо, віднесення інформації до державної таємниці відбувається шляхом прогнозування наслідків від її розголошення. 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.

Однак 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.

Як нами зазначалося раніше [7], в цьому випадку більш обґрунтованим буде прогнозування на основі розгляду кількох варіантів розвитку подій з наступною математичною обробкою сукупності отриманих результатів. Таким чином, актуальності набуває питання вибору способів та засобів багатоваріантного прогнозу. Деякої риторичності цьому питанню надає загальна визнаність ефективності застосування в таких випадках методу сценаріїв [8, 9], або як його називає низка науковців [10, 11, 12] – сценарний підхід чи сценарний аналіз.

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 розвинути 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" [13].

### III Основні аспекти застосування сценарного підходу до обрахування загальної шкоди від втрати інформації, що становить державну таємницю

Під сценарієм будемо розуміти опис можливого розвитку подій в певній ситуації. Вважається, що вперше метод сценаріїв застосував Герман Кан для дослідження складних систем [14]. Спочатку сценарії мали суто описовий характер, потім почали використовуватись більш формалізовані конструкції [15]. Існують різні концепції методу генерації сценаріїв [11, 12, 16, 17], однак універсального чи завершеного вирішення даної проблеми на сьогодні немає. Ми приєднуємося до думки Катренка А. В. щодо ефективності застосування для розв'язання даної проблеми системного підходу [18].

Якщо наявна множина сценаріїв дозволяє обрахувати часткову шкоду окремо за кожним з них та вказати часткову ймовірність реалізації кожного з цих сценаріїв, можна побудувати певну ієрархічну структуру, зображену на рис. 1.

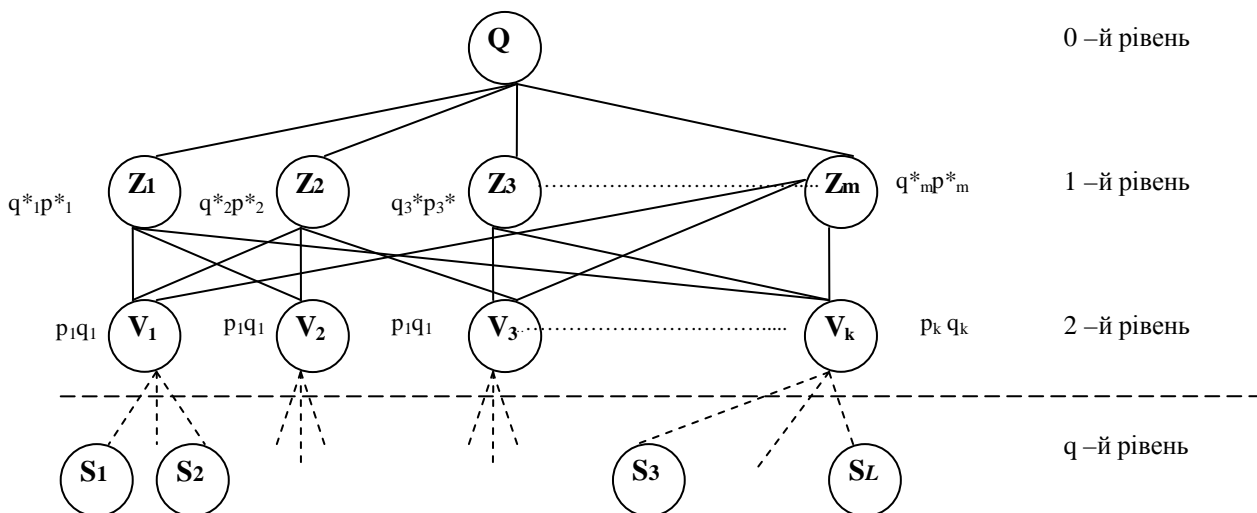


Рисунок 1 – Ієрархічне представлення результатів застосування сценарного підходу до обчислення сукупної шкоди, заподіяної втратою секретної інформації

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 [19] або, за прийнятою в літературі з захисту інформації термінологією, інформаційного ризику [20, 21].

$$Q = \sum_{i=1}^m p_i^* q_i^* \quad (1)$$

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  $\{C_{ij}\}$ ,  $j = \overline{1, k}$ .

Абстрактність наведеної на рис. 1 структури 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  $\{C_{ij}\}$ ,  $j = \overline{1, k}$ , 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  $C_{ij}$ ), утворює поле подій, кожному з елементів якого можливо співставити часткові збитки  $q_j^*$ . 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

$$Z_i \cap Z_r = \emptyset, i \neq r, \quad (2)$$

$$\bigcup_{i=1}^m Z_i = \Omega, \quad (3)$$

де  $\Omega$  - достовірна подія.

Множині подій  $\{Z_i\}$  зіставляється множина ймовірностей цих подій  $\{P(Z_i)\} = \{p_i^*\}$ , для якої справедливі ймовірнісні співвідношення, характерні щодо елементів повної групи:

$$P\left(\bigcup_{i=1}^m Z_i\right) = \sum_{i=1}^m P(Z_i) = \sum_{i=1}^m p_i^* = 1, \quad (4)$$

$$P(Z_i \cap Z_r) = 0, i \neq r. \quad (5)$$

Завдяки цьому стає можливим застосування апарату середніх ризиків для обчислення сукупної шкоди  $Q$ .

Методику утворення повної групи подій розглянемо на прикладі, що припускає певну змістовну інтерпретацію, використавши для цього наведений у Методичних рекомендаціях випадок розголошення інформації стосовно робочих частот керування ракетами системи ППО, яка стоїть на озброєнні.

Отже можливо припустити, що внаслідок отримання названої інформації сторона використовує її для:

1. планування проведення військових операцій у повітряному просторі сторони, яка втратила інформацію;
2. розробки засобів та методів знешкодження системи ППО в країнах, у яких вона стоїть на озброєнні;
3. створення власних систем ППО на основі здобутої інформації;
4. передачі інформації союзникам чи іншим третім сторонам.

Тобто маємо чотири варіанти розвитку подій (сценарії  $C_{c1}$ ,  $C_{c2}$ ,  $C_{c3}$ ,  $C_{c4}$ ), ймовірність яких визначається частковими ймовірностями  $p_1$ ,  $p_2$ ,  $p_3$ ,  $p_4$ , а завершення – подіями-індикаторами  $V_1$ ,  $V_2$ ,  $V_3$ ,  $V_4$ .

Перший з перерахованих варіантів у мирний час може нанести максимальну шкоду одразу після втрати секретної інформації і до виявлення потерпілою стороною факту цієї втрати. У другому випадку реальна шкода може бути нанесена не лише до виявлення факту витоку, а і до повної нейтралізації наслідків витоку. Оцінити вартісну шкоду у третьому та четвертому випадках значно складніше, проте будемо вважати це вже зробленим. Сукупні вихідні дані за кожним сценарієм наведено в табл. 1.

Таблиця 1

| Варіанти розвитку події | Вірогідність реалізації | Шкода від реалізації |
|-------------------------|-------------------------|----------------------|
| $V_1$                   | $p_1$                   | $q_1$                |
| $V_2$                   | $p_2$                   | $q_2$                |
| $V_3$                   | $p_3$                   | $q_3$                |

|       |       |       |
|-------|-------|-------|
| $V_4$ | $p_4$ | $q_4$ |
|-------|-------|-------|

Події  $V_1, V_2, V_3, V_4$ . не є несумісними, вони можуть відбуватися одночасно, а можуть й не відбуватися зовсім, тобто множина  $\{V_j\}, j=1,4$  не задовольняє вимогам до повної групи подій.

Тому постає завдання формування повної множини  $\{Z_i\}$  елементарних подій, яка пов'язана з вихідною множиною  $\{V_j\}$ , але на відміну від неї задовольняє вимогам, що висувуються до повної групи. Кожна з подій

$\{Z_i\} i=1, m$  являє собою суміщення чотирьох подій з множини  $V_1, V_2, V_3, V_4$ . або множини доповнюючих подій  $\overline{V_1}, \overline{V_2}, \overline{V_3}, \overline{V_4}$  Принциповою при формуванні елементарних подій  $\{Z_i\} i=1, m$  є вимога врахування в їх структурі всіх можливих сполучень елементів множини  $\{V_j\}$  включно із самою множиною цих подій та порожньою множиною  $\emptyset$  (останній відповідає ситуація, в якій жоден із сценаріїв не реалізувався за час T).

Впорядкувати множину можливих станів системи подій  $\{Z_i\}, i=1,16$ , сформованих на множині подій вихідної системи  $\{V_j\}, j=1,4$  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 якій не відбулась жодна з подій множини).

В 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  $C_{c1} \div C_{c4}$ , тобто всі ці можливі стани мають бути представлені у структурі подій множини  $\{Z_i\}$ .

На відміну від подій  $\{V_j\}, j=1,4$ , жодна з подій  $\{Z_i\}, i=1,16$  не може з'явитись одночасно з іншою лише поодиноці, 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:  $Z_5 = V_1 \cap V_2 \cap \overline{V_3} \cap \overline{V_4}$ ,  $Z_6 = \overline{V_1} \cap V_2 \cap \overline{V_3} \cap \overline{V_4}$  ...,  $Z_{10} = \overline{V_1} \cap \overline{V_2} \cap V_3 \cap V_4$ .

Відповідно для обчислення ймовірностей цих елементарних подій отримуємо:

$$P(Z_5) = p^*_5 = p_1 p_2 (1-p_3)(1-p_4), \quad (6)$$

$$P(Z_{10}) = p^*_{10} = (1-p_1)(1-p_2)p_3 p_4 \quad (7)$$

Події  $Z_{11} \div Z_{14}$  у свою чергу включатимуть потрібні 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 обмеженими ймовірностями виду:

$$p^*_{11} = p_1 p_2 p_3 (1-p_4), \dots, p^*_{14} = (1-p_1) p_2 p_3 p_4 \quad (8)$$

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

$$p^*_{15} = p_1 p_2 p_3 p_4 \quad (9)$$

Остання елементарна подія множини  $\{Z_i\}$  має врахувати можливість відсутності реалізації будь-якого з сценаріїв множини  $\{C_{c_j}\}$ :  $\overline{V_1 \cup V_2 \cup V_3 \cup V_4}$ : у термінах обчислення подій ми маємо:

$$Z^*_{16} = \Omega \setminus \bigcup_{j=1}^4 V_j \quad (10)$$

Ймовірність цієї елементарної події дорівнює

$$p_{16}^* = \prod_{j=1}^4 (1 - p_j) \quad (11)$$

В повному обсязі множина структур подій та вирази для обчислення відповідних ймовірностей  $p_i^*$  наведені в таблиці 2.

Таблиця 2 - Трансформація "природної" множини подій  $\{V_j\}, j=1,4$  у множину "штучних" подій  $\{Z_i\}, i=1,16$ , відмінністю якої є виконання вимог щодо утворення повної групи подій

| $Z_i$ | $d$ | 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   | $V_1 \cap \overline{V_2} \cap V_3 \cap \overline{V_4}$            | $p_1(1-p_2)p_3(1-p_4)$         | $q_1 + q_3$             |
| ....  | ... | .....   | .....                          | .....                   |
| $Z_0$ | 2   | $\overline{V_1} \cap \overline{V_2} \cap V_3 \cap V_4$            | $(1-p_1)(1-p_2)p_3p_4$         | $q_3 + q_4$             |
| $Z_1$ | 3   | $V_1 \cap V_2 \cap V_3 \cap \overline{V_4}$                       | $p_1p_2p_3(1-p_4)$             | $q_1 + q_2 + q_3$       |
| $Z_2$ | 3   | $V_1 \cap V_2 \cap \overline{V_3} \cap V_4$                       | $p_1p_2(1-p_3)p_4$             | $q_1 + q_2 + q_4$       |
| $Z_3$ | 3   | $V_1 \cap \overline{V_2} \cap V_3 \cap V_4$                       | $p_1(1-p_2)p_3p_4$             | $q_1 + q_3 + q_4$       |
| $Z_4$ | 3   | $\overline{V_1} \cap V_2 \cap V_3 \cap V_4$                       | $(1-p_1)p_2p_3p_4$             | $q_2 + q_3 + q_4$       |
| $Z_5$ | 4   | $V_1 \cap V_2 \cap V_3 \cap V_4$                                  | $p_1p_2p_3p_4$                 | $q_1 + q_2 + q_3 + q_4$ |
| $Z_6$ | 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:

$$m = \sum_{d=0}^k c_k^d = 2^k, \quad (12)$$

де  $c_k^d$  - число сполучень з  $k$  елементів по  $d$ , зокрема для  $k=4$  отримуємо  $m=16$ .

При формуванні множини подій  $\{Z_i\}$  враховано усі можливі варіанти перебігу подій, що могли статися в ході реалізації сценаріїв  $Sc_1 \div Sc_4$  (збережені усі можливі сполучення подій з множини  $\{V_j\}$ , включно з повною відсутністю 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 (1).

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:

$$q_1^* = q(V_1 \cap \overline{V_2} \cap \overline{V_3} \cap \overline{V_4}) = q_1 \quad (13)$$

Відповідно, маємо  $q^*_2 = q_2, \dots, q^*_4 = q_4$ . Аналогічним чином для подій  $z_5 \div z_{10}$  отримуємо:  $q^*_5 = q_1 + q_2, \dots, q^*_{10} = q_3 + q_4$ , 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 часткової шкоди  $q^*_i$  наведено у останньому стовпчику таблиці 2.

Застосування запропонованого методу сценарію потребує і 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 можливо обійтись трьома верхніми рівнями схеми, зображеної на рис. 1. Однак за необхідності обґрунтування чи пояснення кількісних значень цих оцінок виникає проблема деталізації і висвітлення їх появи, що в свою чергу викликає появу додаткових рівнів передподій (третього, четвертого,  $q$ -того). Наприклад, для пояснення збитків за  $C_{\Sigma 1}, C_{\Sigma 2}$  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 дозволить отримати обґрунтування оцінки збитків, а професійно орієнтована дозволить об'єктивно оцінити залишкові імовірності 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 п'ятий рівень ієрархії.

Слід зауважити, що надмірна конкретизація в задачах прогнозу, особливо із застосуванням методів експертного оцінювання, може іноді заважати [10]. Тому доцільність використання нижчих рівнів ієрархізації (від четвертого рівня і далі) слід визначати за кожним сценарієм окремо, приймаючи до уваги специфіку проблем даної 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) [6].

#### IV Висновки

Застосування запропонованих у статті методичних підходів до оцінки шкоди від витоку інформації дозволить більш об'єктивно визначати наявність чи відсутність підстав віднесення інформації до державної таємниці та ступень їх секретності.

*Література:* 1. Закон України “Про державну таємницю” від 21. 09. 1999 р. // Відомості Верховної Ради 1999, N 49. 2. Положення про експертні комісії з питань державної таємниці. Затв. Наказом Служби безпеки України від 04. 01. 2005р. № 696 // Офіційний Вісник України, 2005, N 2, ст. 107. 3. Методичні рекомендації державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня їх секретності. Затв. Наказом Державного комітету України з питань державних секретів та технічного захисту інформації від 9 лютого 1998 року № 23. 4. Архипов О. Є. Касперський І. П. Проблеми функціонування організаційних механізмів віднесення відомостей до інформації з обмеженим доступом в Україні // Четверта науково-технічна конференції «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні», 1 – 3 березня 2006 року, Тези доповідей, К.: НТУУ «КПІ», 2006р., С.22. 5. Архипов О. Є. Касперський І. П. Проблеми методичного забезпечення віднесення відомостей до інформації з обмеженим доступом в Україні // Правова інформатика, 2006, №3 (11), С.61 – 66. 6. Архипов О. Є. Касперський І. П. Проблеми методики отримання та обробки оціночних суджень членів експертних комісій створюваних державними експертами з питань таємниць // Правова інформатика, 2006, № 4 (12), С. 80 – 87. 7. Архипов О. Є. Касперський І. П. Проблеми методичного забезпечення віднесення відомостей до інформації з обмеженим доступом в Україні // Правова інформатика, 2006, № 3 (11), С.61 – 66. 8. Литвак Б. Г. Разработка управленческого решения. - М.: Дело, 2000.- 392 с. 9. Грабовецький Б. Є. Економічне прогнозування і планування. – К.: Центр навчальної літератури, 2003. – 188 с. 10. Литвиненко О. В. Спеціальні інформаційні операції та пропагандистські кампанії. – К.: ВКФ “Сатсанга”, 2000.- 222 с. 11. Згуровський М. З. Сценарний аналіз як системна методологія передбачення // Системні дослідження та інформаційні технології. – 2002. - №1. –С. 5-36. 12. Качинський А. Б. Безпека, загрози і ризик: наукові концепції та математичні методи. – К.: 2003. – 472 с. 13. Янг Э. Прогнозирование научно-технического прогресса. – М.: Прогресс, 1974.- 219 с. 14. Жерардэн Л. Исследование альтернативных картин будущего: Метод составления сценариев. Руководство по научно-

технічному прогнозуванню. - М. Прогресс, 1977. **15.** Качинський А. Б. Безпека, загрози і ризик: наукові концепції та математичні методи. - К.: 2003. - 472 с. **16.** Грабовецький Б. Є. Економічне прогнозування і планування. - К.: Центр навчальної літератури, 2003. - 188 с. **17.** Литвак Б. Г. Разработка управленческого решения. - М.: Дело, 2000.- 392с. **18.** Катренко А. В. Системний аналіз об'єктів та процесів комп'ютеризації. - Львів: "Новий світ - 2000". -424с. **19.** Пугачев В. С. Теория вероятности и математическая статистика. - М.: Наука, Главная редакция физико-математической литературы, 1979. - 496 с. **20.** Петренко С. А. Управление информационными рисками.- М.: Компания АйТи; ДМК Пресс, 2004.- 384 с. **21.** Петренко С. А., Петренко А. А. Аудит безопасности. Internet .- М.: ДМК Пресс, 2002.- 416 с.

УДК 681.391

## АНАЛИЗ РЕЗУЛЬТАТОВ ЭКСПЕРИМЕНТАЛЬНЫХ АРТИКУЛЯЦИОННЫХ ИССЛЕДОВАНИЙ МАСКИРОВАННОЙ ШЕПОТНОЙ РЕЧИ

*Владимир Журавлёв, Александр Храмов\*, Сергей Завьялов\**

*Киевский национальный технический университет Украины (НТУУ "КПИ"),*

*\*Запорожский национальный технический университет*

*Анотація.* Розглянута методика і результати артикуляційних випробувань сигналів маскованої шепітної мови. На основі аналізу характеристик залежності експериментальної розбірливості фонем від відношення "сигнал – завада" зроблено висновки про природну постійність завадостійкості шепітних фонем, що вокалізуються.

*Summary.* The new method of speech research is proposed. The analysis of the results of articulation researches of whisper speech words and phonemes noise-immunity is realized. On the base of dependence analysis of phoneme experimental legibility from the ratio signal / noise the conclusion as to noise-immunity nature constant of vocalized phonemes in the word structure was made.

*Ключевые слова:* Шепотный речевой сигнал, артикуляционные исследования, помехоустойчивость фонем.

### I Введение

На сегодняшний день акустическая и виброакустическая защита выделенных помещений от несанкционированного доступа представляет наиболее динамично развивающееся направление комплексной защиты информации. В первую очередь это обусловлено уникальными особенностями речевого информационного ресурса, который является первичным общедоступным выражением результата мыслительного процесса человека, оперативностью обмена, высокой конфиденциальностью некоторых сообщений, а также возможностью идентификации личности говорящего. Вышеприведенные аргументы в основном определяют актуальность проблемы защиты речевого информационного ресурса.

Речевой сигнал имеет особую структуру, в которой закодирована семантическая информация. Поэтому процесс слухового восприятия речи представляет собой, прежде всего, процесс расшифровки и распознавания семантического и аутентификационного содержания информации, содержащейся в речевом сигнале аудитора. Исследование процесса преобразования центральной нервной системой акустических признаков речевого сигнала в его фонетическое и смысловое содержание, является одной из актуальных проблем в современной науке. Одной из задач этой проблемы является изучение помехоустойчивости различных речевых сигналов, обладающих информационной составляющей. Одной из реализаций речевого обмена является т. н. "шепотная речь" – речевой сигнал, в котором отсутствует составляющая вибрации голосовых связок, однако присутствует информационная составляющая. Авторы не обнаружили в открытых источниках информации о помехоустойчивости шепотной речи, поэтому её анализ, по нашему мнению, будет интересен в части познания и исследования частных реализаций природного процесса обмена информацией.

### II Постановка задачи

В соответствии с законом Украины [1], целью информационной защиты является предотвращение утечки, хищения, утраты, искажения и подделки (имитации) информации. На данном этапе анализа считаем целесообразным применяя метод декомпозиции представить речевой сигнал (РС) в виде двух составляющих – информационной и аутентификационной. Информационная составляющая РС включает в себя "что" говорит диктор, а аутентификационная – "как" он это "что" артикулирует. С точки зрения информационной