ЗМІСТ

УДК 004.057:681.3.064 **Л.В. Бурячок, В.Л. Бурячок, В.В. Семко**

ТЕХНОЛОГІЯ ПРОВЕДЕННЯ ПОРІВНЯЛЬНОГО АНАЛІЗУ ТА ОЦІНЮВАННЯ СТАНУ ЗАХИЩЕНОСТІ АВТОМАТИЗОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Запропоновано підхід щодо проведення порівняльного аналізу автоматизованих інформаційних систем на підставі заздалегідь обраного набору ознак (властивостей) та комплексного показника якості системи, а також оцінювання ступеня їх захищеності з точки зору дій системного адміністратора щодо забезпечення конфіденційності інформації, її цілісності і доступності.

***Ключові слова*:** безпека, метод, показники якості, інформаційна система, загроза.

Вступ і постановка завдання. Формування та розвиток сучасного інформаційного суспільства базується на синтезі двох інформаційно-комунікаційних технологій (ІКТ) – комп'ютерної і телекомунікаційної та визначається двома простими, але дуже змістовними законами. Перший закон сформульовано одним із засновників корпорації Intel Гордоном Муром. Говорячи про те, що "… кількість транзисторів у процесорах збільшуватиметься вдвічі кожних півтора роки …", фактично пояснює появу на рубежі тисячоліть засобів обчислювальної техніки. Другий закон належить Роберту Меткалфу, винахіднику найпоширенішої на сьогодні технології комп'ютерної мережі Internet. Говорячи про те, що "… цінність мережі знаходиться у квадратичній залежності від кількості вузлів, які є її складовими …" він фактично констатує, що основу сучасного інформаційного суспільства становлять ІТ системи (ІТС) та мережі різного призначення [1]. Неконтрольоване зростання впливу ІКТ та ІТС на постіндустріальне суспільство, поява небезпеки розриву між інформаційною елітою та споживачами призвело, у свою чергу, до суттєвого ускладнення завдань із добування даних, що необхідні органам державного та військового управління для прийняття виважених, адекватних умовам обстановки рішень, а також їх захисту від різного роду деструктивних впливів – викликів, фактично неприхованих кібернетичних злочинів і загроз.

Аналіз останніх досліджень і публікацій. На сьогодні цю проблему висвітлено в багатьох публікаціях зарубіжних і вітчизняних авторів [2]. Найвідомішими серед них є роботи Возженікова А.В., Ліпкан В.А., С.В. Ленкова, Мірошниченко В.М., Хорошка В.А., Ярочкіна В.І., Мініхена К.А., М. Лібіцкі, О. Шермана та інших фахівців. В них розглядається сучасний науково-методичний апарат порівняльного аналізу автоматизованих інформаційних систем (АІС), проте комплексного дослідження проблеми оцінювання ступеня їх захищеності для надійного забезпечення розв'язання завдань інформаційної діяльності не проводиться. Тому, враховуючи реалії сьогодення, вона потребує більш глибокого вивчення.

Актуальність та мета статті. Все це фактично дає можливість стверджувати, що проблеми забезпечення безпеки сучасних АІС, як для України, так і для переважної більшості інших держав світу стають нині особливо актуальними. Відповідно, метою статті є формування підходу щодо проведення порівняльного аналізу АІС на підставі заздалегідь обраного набору ознак (властивостей), а також оцінювання ступеня захищеності таких систем з точки зору дій системного адміністратора щодо забезпечення конфіденційності інформації, її цілісності та доступності.

Виклад основного матеріалу. Під АІС – інформаційними, інформаційно-аналітичними, інформаційно-пошуковими та аналогічними їм системами, згідно [3], розуміють інформаційні системи (ІС), що складаються з персоналу і комплексу засобів автоматизації його діяльності та реалізують інформаційну технологію виконання встановлених функцій. Вони мають одну загальну мету – задоволення потреб користувачів у забезпеченні надійного і своєчасного подання повної, достовірної, конфіденційної інформації, а також її повній та ефективній обробці. Ступінь виконання цих потреб характеризує якість функціонування ІС з погляду конкретного користувача.

Задача полягає в тому, щоб:

по-перше, визначити набір ознак (властивостей), що найбільш повно характеризують

конкретну ІС і визначити чисельне значення показника важливості (ваги важливості) кожного з них у рішенні властивих ІС функцій;

по-друге, провести порівняльний аналіз якості альтернативних варіантів архітектури і топології ІС з врахуванням отриманих вагових коефіцієнтів кожної ознаки (властивості).

В основу методу, який пропонується для рішення поставленої задачі покладено науково-методичний апарат експертних оцінок, що одержав у свій час назву «Метод Дельфі». Для одержання експертної оцінки в групу експертів варто включити: представників розробника; представників Замовника; представників науково-дослідних установ Замовника; фахівців-експлуатаційників; кваліфікованих користувачів.

Сукупність показників (характеристик) якості, що перебувають на одному рівні ієрархії визначається експертами для кожної ІС й формується за окремими групами ознак (властивостей). Кількість показників в ознаці не повинна перевищувати $7 \div 9$ (людина із середніми здібностями не може порівнювати одночасно більше ніж $\triangleleft 7 + 2 \triangleright$ об'єктів). Якщо число показників (характеристик) якості перевищує сім, то експертам пропонується розбити таку групу ознак на декілька підгруп. Це в подальшому сприятиме підвищенню погодженості результатів експертного опитування. Припустимо, що для визначення якості емпіричної ІС використовують такі ознаки (властивості), як:

надійність – здатність ІС безвідмовно та з великою ймовірністю протягом заданого періоду часу виконувати функції при заданих умовах на вихідних даних з області визначення;

ефективність – відношення рівня послуг, надаваних ІС користувачеві при заданих умовах, до обсягу використовуваних ресурсів;

ступінь складності спеціального програмного забезпечення (СПЗ) – характеризує структуру побудови програми, взаємозв'язок її окремих частин і т.д.;

функціональність – здатність ІС виконувати набір функцій, що задовольняють заданим або уявним потребам користувачів.

Кожна з них може бути охарактеризована додатковими показниками (табл.1).

Будемо виходити з того, що для одержання незалежних експертних результатів треба опитати, наприклад, десять фахівців з різних організацій, яким необхідно щодо обраних ознак (властивостей), що характеризують конкретну ІС заповнити відповідну таблицю-анкету (табл. 1). При цьому кожен експерт у відповідності зі своїми вимогами повинен ранжирувати обрані ознаки (властивості) по одному альтернативному рішенню – якості ІС.

<u>На першому етапі</u> роботи кожним експертом разом із Замовником призначаються вагові коефіцієнти важливості для γ_{il} - *l-го* показника *i-ї* ознаки (властивості) і R_i *-ї* ознаки (властивості). Для цього доцільно використати наступну шкалу:

5 – досить важливо, щоб даний показник мав високе значення;

4 – важливо, щоб даний показник мав високе значення;

3 – добре б мати високе значення даного показника;

2 - до деякої міри корисно мати високе значення даного показника;

1 – при низьких значеннях даного показника відчутних втрат не передбачається, - виходячи при цьому з того, що вага найменш відповідальної ознаки (властивості) має дорівнювати одиниці.

<u>На другому етапі</u> роботи кожним експертом здійснюється розрахункова оцінка *l-го* показника *i-ї* ознаки (властивості) - K_{il} , з погляду повноти реалізації властивої йому функції:

$$K_{il} = \frac{\eta_l}{\eta_{l_{идеал}}}, \quad i = \overline{1,n}, \quad l = \overline{1,n_i}. \qquad (1)$$

де η_l – рахункова кількість одиниць *l-го* показника *i-ї* ознаки (властивості), що характеризують повноту реалізації тієї або іншої функції;

$\eta_{l_{идеал}}$ – ідеальна кількість таких одиниць (повинна бути визначена в технічних умовах на створення ІС та відповідному технічному завданні);

n – число ознак (властивостей); n_i – число показників *i-ї* ознаки (властивості).

Таблиця 1

Оцінка ознак і показників якості ІС

Властивість ІС	**Вага властивості** R_i	**Показник властивості**			**Вага показника властивості** γ_{il}	**Розрахункова оцінка показника властивості**			**Знаки: Краще «+»; гірше «-»**	**Комплексна оцінка властивості** $R^j_{q_{il}}$
		Функція, що притаманна показнику	**Міра вимір у**	**Шкала виміру**		**Рахункова кількість** η_l	**ідеальна кількість** $\eta_{l_{идеал}}$	**Значення** K_{il}		
Надійність		Завершеність: наробіток на відмову при відсутності рестарту.	год.	10-1000						
		Стійкість: наробіток на відмову при наявності автоматичного рестарту	год.	10-1000						
		Відновлюваність: тривалість відновлення	хв.	10^{-2}-10						
		Доступність-готовність: відносний час працездатного функціонування	імовір-ність	0. 7-0.99						
Ефективність		Час відгуку: час одержання результатів на типове завдання	сек.	1-1000						
		Пропускна здатність: число типових завдань, що виконують в одиницю часу	число у хв.	1-1000						
		Відносна величина використання ресурсів ЕОМ при нормальному функціонуванні програмного засобу	імовір-ність	0. 7-0.99						
Ступінь складності спеціального ПЗ		Вивчаємість: тривалість вивчення програмного забезпечення	год.	1-1000						
		Змінюваність: тривалість підготовки змін програмного забезпечення.	год.	1-1000						
		Простота установки: тривалість інсталяції програмного забезпечення.	год.	1-100						
		Заміщуваність: тривалість заміни компонентів програмного забезпечення.	год.	1-100						
Функціональність		Відповідність реалізованої функціональності, закладеній в ТЗ і наведеній у документації	-	1-10						
		Взаємодія з іншими інформаційними системами й погодженість при збереженні даних	-	1-10						
		Тривалість роботи ІАС і повнота контролю її стану	год.	10-1000						

Таким чином, такі, здавалось би кількісно невимірні ознаки (властивості) як: «функціональність», «надійність», «ефективність» й «ступінь складності СПЗ», - можуть бути виражені через чисельні показники. Причому $K_{il} \in [0,1]$.

<u>На третьому етапі</u> роботи кожен експерт проводить комплексну оцінку *i-ї* ознаки (властивості). При цьому $x^j_{q_{il}}$ - ранг *i-ї* ознаки (властивості) по альтернативному рішенню q, приписуваний j-м експертом обчислюється по формулі:

$$x_{q_{il}}^{j} = \frac{1}{n_i} \cdot \sum_{l=1}^{n_i} \left(K_{il} \cdot \gamma_{il} \right) , \; q = \overline{1,Q} , \tag{2}$$

де K_{il} – експертна оцінка *l-го* показника *i-ї* ознаки (властивості);

γ_{il} – ваговий коефіцієнт важливості *l-го* показника *i-ї* ознаки (властивості);

Q – загальна кількість ІС, що підлягають оцінюванню.

На цьому ж етапі експертами на підставі отриманих комплексних оцінок *i-ї* ознаки (властивості) попередньо визначається ступінь впливу кожної з ознак (властивостей) на якість досліджуваної ІС. Для цього в передостанній графі таблиці-анкети (табл. 1) прописують знак (+), який означає, що якість ІС поліпшується з поліпшенням даної ознаки (властивості), або знак (-), який означає, що якість ІС погіршується з погіршенням даної ознаки (властивості).

<u>На четвертому етапі</u>:

по-перше, формується узагальнена таблиця з комплексних оцінок *i-х* ознак (властивостей) для досліджуваної ІС підтримки прийняття управлінських рішень, отриманих кожним з експертів у ході виконання попередніх етапів роботи;

по-друге, здійснюється сумарне ранжирування по альтернативному рішенню q:

$$\sum_{j=1}^{m} x_{q_1}^{j}, \quad \sum_{j=1}^{m} x_{q_2}^{j}, \quad .... \tag{3}$$

де x – ранг i-*ї* ознаки по альтернативному рішенню q ($q = 1$), приписуваного j-м експертом; m – кількість задіяних в роботі експертів.

по-третє, визначається коефіцієнт згоди W_q між існуючими думками фахівців за формулою [4, 5]:

$$W_q = \frac{\sum_{i=1}^{n} \left\{ \sum_{j=1}^{m} \left(x_{q_i}^{j} \right) - \frac{1}{2} \cdot m \cdot (n+1) \right\}^2}{\frac{1}{12} \cdot m^2 \cdot \left(n^3 - n \right) + m \cdot \frac{1}{12} \cdot \sum_{t_j} \left(t_j^3 - t_j \right)} \tag{4}$$

де t_j - число повторень кожного рангу в ранжируванні, даному j-м експертом.

Якщо $W_q = 0$, то погоджена точка зору фахівців з даного ранжирування відсутня. Якщо $W_q = 1$ - погодженість думок повна. Для оцінювання значимості результатів при $n \le 7$ варто використати розподіли Фішера, при $n > 7$ - розподіл χ^2.

Припустимо, що в ході оцінювання деякої ІС підтримки прийняття управлінських рішень була сформована наступна таблиця (табл. 2) округлених даних:

Таблиця 2

Узагальнені результати

№ експерта	**Ознака (властивість)** $x_{q_{il}}^{j}$			
	Надійність	**Ефективність**	**Ступінь складності СПЗ**	**Функціональність**
1	1	2	4	3
2	2	3	1	4
3	3	2	1	4
4	1	2	3	4
5	1	3	4	2
6	1	2	3	4
7	1	2	4	3
8	2	3	1	4
9	3	4	2	1
10	1	2	4	3

Сумарні ранги ознак (властивостей) $x_{\sum}$	**16**	**25**	**27**	**32**
Ранжирування ознак (властивостей)	**1**	**2**	**3**	**4**

Виходячи зі значень, наведених у таблиці 2, коефіцієнт згоди, розрахований по формулі (4) буде дорівнювати:

$$W_q = \frac{\sum_{i=1}^{4}\left\{\sum_{j=1}^{10}\left(x_{q_i}^{j}\right) - \frac{1}{2}\cdot 10\cdot(4+1)\right\}^2}{\frac{1}{12}\cdot 10^2\cdot\left(4^3-4\right)} \approx 0.268\cdot$$

Застосувавши для оцінки значимості отриманого результату статистичні таблиці розподілу Фішера для $n=4$ й $W_q = 0.268$ можна зробити висновок, що погодженість між думками експертів існує з імовірністю ≈ 0.99. Представивши результати таблиці 2 (сумарні ранги ознак/властивостей) у вигляді вектора-рядка: $x_{\sum} = \left\| x_{q_{il}}^{j} \right\| = \|16 \;\; 25 \;\; 27 \;\; 32\|$ і позначивши вагу найбільш відповідальної ознаки (властивості) через $v_1 = 2$, а найменш відповідальної ознаки (властивості) через $v_4 = 1$ по формулі [6, 7]:

$$v_q = v_4 + \frac{y_q - y_4}{y_1 - y_4}\cdot\left(v_1 - v_4\right) \qquad (5)$$

знайдемо ваги інших ознак (властивостей), де:

$y_1 = 16$ - сумарний ранг найбільш відповідальної ознаки;

$y_4 = 32$ - сумарний ранг найменш відповідальної ознаки.

Після обчислень отримаємо: $v_2 = 1.44$, $v_3 = 1.31$.

Провівши нормування розрахованих ваг ознак (властивостей) - v_1, v_2, v_3 і v_4, сформуємо таблицю 3.

Таблиця 3

Нормовані ваги ознак (властивостей)

№ властивості	**Ознака (властивість)**			
	Надійність	**Ефективність**	**Ступінь складності СПЗ**	**Функціональність**
Нормована вага ознаки (властивості) $v_q^{норм}$	0.347	0.250	0.227	0.176

Для збільшення коефіцієнта згоди W_q по ранжируванню пропонованих ознак (властивостей) можливо по черзі виключати одного або декількох експертів [7]. Виключається або ж пояснює свій підхід до ранжирування ознак (властивостей), як правило, експерт, думка якого найбільше впливає на загальний коефіцієнт згоди інших фахівців. Після цього по формулах (1) – (2) визначається значення комплексної оцінки *i-ї* ознаки (властивості), а по формулі (5) – їхня вага. Остаточне нормування ваг досліджуваних ознак (властивостей), що характеризують конкретну ІС, визначається для максимального коефіцієнта згоди.

На п'ятому етапі проводиться порівняння нормованої величини значення, що прийняла дана ознака (властивість) і припустимих значень, визначених у технічних умовах на створення ІС та відповідному технічному завданні. При виконанні умови ознака (властивість) позначається як така, що позитивно пройшла випробування.

На шостому етапі обчислюється [8 - 10] комплексний показник якості досліджуваної ІС по альтернативному рішенню q, – K_q^{total} за формулою:

$$K_q^{total} = \left(\frac{1}{n} \cdot \sum_{i=1}^{n} \left(v_{q_i}^{норм} \cdot R_i^{ЛПР} \right) \right) \cdot 100\% \qquad (6)$$

де $v_{q_i}^{норм}$ – нормована вага *i-ї* ознаки (властивості);

n – число ознак (властивостей).

Для визначення вагового коефіцієнта $R_{ij}^{ЛПР}$ кожної з ознак (властивостей) використовують дані з матриці вагових коефіцієнтів, складеної на основі думок експертів за результатами заповнення таблиці-анкети (табл. 1):

$$\begin{vmatrix} R_{11} & \dots & R_{1j} & \dots & R_{1m} \\ \dots & \dots & \dots & \dots & \dots \\ R_{i1} & \dots & R_{ij} & \dots & R_{im} \\ \dots & \dots & \dots & \dots & \dots \\ R_{n1} & \dots & R_{nj} & \dots & R_{nm} \end{vmatrix}, i = \overline{1,n} \ , \ j = \overline{1,m},$$

де n – число ознак (властивостей); m – кількість задіяних в роботі експертів.

Ваговий коефіцієнт $R_i^{ЛПР}$ розраховується як середнє значення вагового коефіцієнта важливості кожної з ознак (властивостей), визначене m незалежними експертами:

$$R_i^{ЛПР} = \sum_{j=1}^{m} R_{ij}^{нор} \Big/ \sum_{j=1}^{m} \sum_{i=1}^{n} R_{ij}^{нор} \qquad (7)$$

де $R_{ij}^{нор}$- нормована вага ранг *i-ї* ознаки (властивості) по альтернативному рішенню q, приписувана j-м експертом:

$$R_{ij}^{нор} = R_{ij} \Big/ \sum_{i=1}^{n} R_{ij}$$

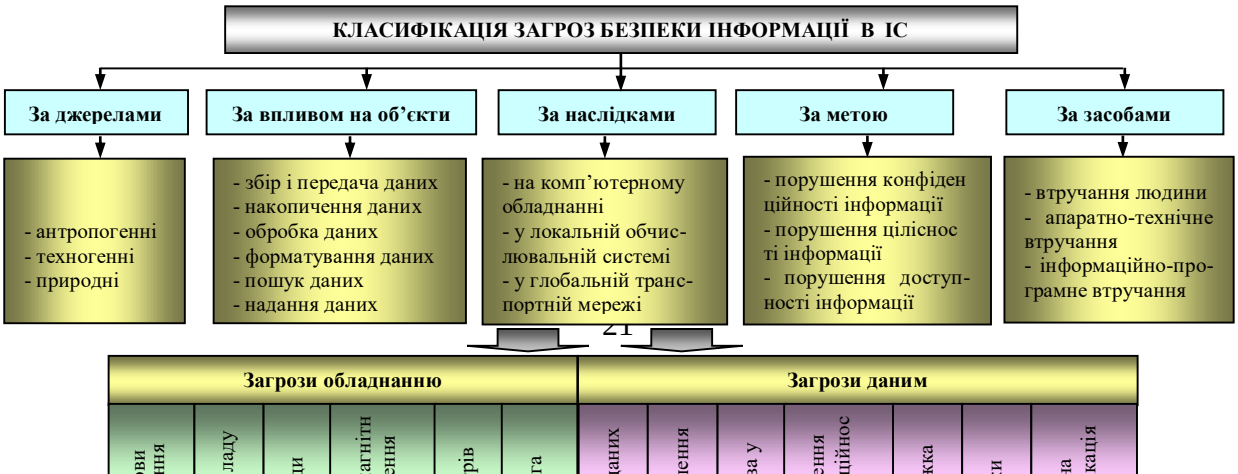
Якщо розгляду підлягає декілька альтернативних рішень q ІС, то остаточний вибір серед них раціонального варіанта буде здійснюватися на підставі наступного правила:

–якщо $K_q^{total} \geq K_{q+1}^{total}$, то q-й варіант ІС є більше якісним у порівнянні з $q+1$ та навпаки;

–якщо $K_q^{total} = K_{q+1}^{total}$, то варіанти рівнозначні.

За раціональний вибирають той варіант ІС, якому відповідає $K_q^{total} = \max$.

<u>На сьомому етапі</u> оцінюються події, які шляхом потенційно можливого впливу на ІС прямо та/або опосередковано можуть завдати збитку її власникам і користувачам. Вони класифікуються за такими основними ознаками (рис. 1): за метою реалізації, за джерелами, за засобами, за методами і наслідками, а також за принципами, характером та способами впливу на певний об'єкт. При цьому найбільший інтерес з позицій класифікації кібернетичних злочинів і загроз за схемою, пропонованою Конвенцією Ради Європи 2001 року по боротьбі з кіберзлочинністю становлять загрози безпеці інформації в ІС за метою реалізації. Вони полягають у порушенні конфіденційності інформації, її цілісності, працездатності ІС та/або доступності до інформації, що в ній циркулює тощо.



При цьому *до загроз порушення конфіденційності інформації в ІС* згідно з [11, 12] належать, як правило, спроби несанкціонованого: читання або копіювання як відкритої, так і конфіденційної інформації, імпорту або експорту такої інформації, а також обміну нею між елементами обчислювальної мережі, що відносяться до різних класів захищеності тощо. З урахуванням положень [13], вони ймовірно можуть бути реалізовані неавторизованим користувачем за умови подолання ним засобів: організаційного обмеження доступу (p_{ood}); охоронної сигналізації (p_{oc}); захисту від вірусних атак ($p_{атак}$); канального захисту від несанкціонованого доступу із телекомунікаційної мережі до ресурсів ЛОМ ($p_{кзткм}$); управління доступу, включаючи засоби управління фізичним доступом до приміщень, системних блоків, клавіатури тощо ($p_{уфд}$), а також адміністрування доступу до відповідних суб'єктів і об'єктів з використанням механізмів загального і спеціального ПЗ ($p_{ад}$). Виходячи з такого ймовірність подолання неавторизованим користувачем зазначених засобів захисту може бути визначена з виразу:

$$p_{пзз} = p_{уфд} \cdot p_{ад} \cdot \left[1-\left(1-p_{ood}\right)\cdot\left(1-p_{oc}\right)\cdot\left(1-p_{атак}\right)\cdot\left(1-p_{кзктм}\right)\right]. \quad (8)$$

Подальше розкриття змісту інформації з обмеженим доступом може статися лише за умови, якщо порушник після її отримання:

знає мову, якою інформація представляється (ймовірність події - $p_{мова}$);

знає і може застосовувати програмні засоби або апаратуру криптографічного перетворення (ймовірність події - $p_{пз/ктп}$);

має необхідні ключі або ключові набори для такого перетворення (ймовірність події - $p_{ключі}$).

Виходячи з такого ймовірність подолання неавторизованим користувачем засобів криптографічного захисту з урахуванням положень [13] може бути визначена з виразу:

$$p_{кзі} = p_{мова} \cdot p_{пз/ктп} \cdot p_{ключі}. \quad (9)$$

Тоді ймовірність порушення конфіденційності інформації з подоланням розглянутих вище засобів може бути визначена як:

$$P_{ПКІ} = p_{кзі} \cdot \left[1-\left(1-p_{пзз}\right)\right]. \quad (10)$$

До загроз порушення цілісності інформації в ІС, як відомо [11, 12], належать: несанкціонована модифікація та/або видалення програм і даних; вставка, зміна або видалення даних в елементах протоколу в процесі обміну між абонентами обчислювальної мережі; втрата даних у результаті збоїв, порушення працездатності елементів обчислювальної мережі або некомпетентних дій суб'єктів доступу тощо. Вони ймовірно можуть бути реалізовані неавторизованим користувачем за умови подолання ним засобів:

організаційного обмеження доступу, охоронної сигналізації та управління доступом, включаючи засоби управління фізичним доступом до приміщень, системних блоків, клавіатури тощо та адміністрування доступу, як й при аналізі загроз конфіденційності інформації (ймовірність такої події - $p_{пзз}$ визначена раніше);

захисту цілісності від загроз у телекомунікаційних мережах ($p_{цткм}$);

захисту від спеціальних впливів на інформацію по ТКМ ($p_{сп.вп}$);

контролю та поновлення цілісності інформації ($p_{конт.ц}$).

З урахуванням можливостей попереднього підходу, ймовірність порушення цілісності $P_{ПЦІ}$ може бути знайдена з виразу:

$$P_{ПЦІ} = p_{конт.ц} \cdot \left[1-\left(1-p_{пзз}\right)\cdot\left(1-p_{сп.вп}\right)\cdot\left(1-p_{цткм}\right)\right]. \quad (11)$$

До загроз порушення доступності інформації в ІС згідно з [11, 12] відноситься: повторення або вповільнення елементів протоколу; придушення обміну в телекомунікаційних мережах; використання помилок або недокументованих можливостей служб і протоколів передачі даних для ініціювання відмови в обслуговуванні; перевитрата обчислювальних або телекомунікаційних ресурсів тощо. Вони, як і в попередніх випадках, можуть бути реалізовані за умови подолання неавторизованим користувачем систем управління доступом до інформаційних ресурсів ЛОМ (ідентифікації, автентифікації, надання певних повноважень чи привілеїв, з наступною їх перевіркою під час кожної із спроб доступу до ресурсів) та фільтрації. Виходячи з такого стійкість системи управління доступом - (в розумінні ймовірності її не подолання) визначається стійкістю процесів ідентифікації та автентифікації самого адміністратора безпеки, як користувача з найширшими повноваженнями:

$$p_{ссуд} = 1 - p_{пзз}. \quad (12)$$

Ця задача може вирішуватися застосуванням у ІС засобів фільтрації типу міжмережних екранів (*firewall*, брандмауерів), сервісів-посередників (*proxyservices*) тощо. При середній тривалості обслуговування в ІС одного запиту і пуассонівському законі розподілу ймовірностей впливу, ймовірність того, що під час звернення до ресурсу він уже використовується, згідно [13] дорівнює:

$$p_{вик.рес} = 1 - p_0 = 1 - \exp\left\{-t_{вик.рес}\cdot\lambda_{зап}\right\}, \quad (13)$$

де p_0 – ймовірність відсутності впливів (ймовірність того, що на певному часовому інтервалі виникне рівно нуль впливів);

$t_{вик.рес}$ – середнє значення часу використання ресурсу.

Враховуючи таке ймовірність порушення доступності ресурсу з урахуванням положень [13] дорівнюватиме:

$$P_{ПДІ} = 1 - \left(1-p_{вик.рес}\right)\cdot\left(1-p_{ссуд}\right). \quad (14)$$

Виходячи з наведених вище формульних залежностей комплексна величина ймовірності порушення системи захисту інформації у ІС та їх специфічному класі – ЛОМ за метою реалізації з урахуванням пропозицій [13, 14] може бути, як результат, знайдена з виразу:

$$P_{ПСЗІ} = 1 - \left(1-P_{ПКІ}\right)\cdot\left(1-P_{ПЦІ}\right)\cdot\left(1-P_{ПДІ}\right). \quad (15)$$

Висновок

Використання даної методики дозволить кінцевому користувачеві:

– визначати рівень впливу кожної ознаки (властивості) на якість функціонування ІС;

– обчислювати комплексні показники якості досліджуваних ІС та на їх основі здійснювати порівняльний аналіз існуючих альтернативних рішень;

– проводити аналіз чутливості комплексних показників якості при зміні міркувань учасників експертної групи з метою перевірки коректності побудованої моделі якості обраного варіанту ІС;

– забезпечити стійкість та ефективність ІС за рахунок підвищення ступеня живучості, надійності, завадозахищеності та інформаційної безпеки використовуваних у ній технічних засобів;

– обґрунтувати необхідність спільного використання різнорідних сил і засобів у рамках єдиної ІС за рахунок зменшення участі людини в зборі, обробці, аналізі та розподіленні інформації тощо.

На підставі отриманих результатів особа, що приймає рішення зможе серед деякого розмаїття альтернативних рішень обрати раціональний з точки зору якості варіант ІС та сформувати рекомендації з підвищення ефективності, продуктивності та надійності її застосування.

Література

1. Бурячок В.Л. Вплив загроз антропогенного і техногенного характеру на стан безпеки ІТ-систем та соціальних інститутів провідних країн світу і України / В.Л.Бурячок, Я.В.Невойт, Л.В.Бурячок/ Науково-технічний журнал «Сучасний захист інформації» Державного університету телекомунікацій. № 4, 2015, с. 29 – 43

2. Бурячок В.Л. Використання методу експертного аналізу для визначення якості автоматизованих інформаційних систем та їхньої порівняльної оцінки /В.Л.Бурячок/ Збірник наукових праць ЦНДІ ОВТ ЗС України, 2006, № 15. с. 18 – 30

3. ДСТУ 2226-93 Автоматизовані системи. Терміни і визначення.

4. Кендал М. Ранговые корреляции. /Пер. с англ. – М.: Статистика, 1975. – 213 с.

5. Добров Г.И., Ершов Ю.А., Левин Е.И., Смирнов Л.П. Экспертные оценки в научно-техническом прогнозировании /Под общ. ред. В.С. Михалевича. – Киев: Наукова думка 1974. – 160 с.

6. Дэвид Г. Метод парных сравнений /Пер. с англ. – М.: Статистика, 1976. – 568 с.

7. Бешелев С. Д., Гурвич Ф. Г. Экспертные оценки. – М.: Наука, 1973. – 263 с.

8. Осипов Н.В., Нечаев А.Н. и др. Методика статистической обработки коллективных экспертных оценок. Деп.. в УкрНИИНТИ 20.0985, № 2247. Библ. Ук. ВИНИТИ № 1 (171), 1986. б/о 1362.

9. Чирков В.Г. Выбор рациональных технических решений. – К.: Техника, 1991. –159 с. (Б-ка инженера).

10. Бурячок В.Л. Вибір раціонального для модернізації зразка (системи) ОВТ серед сукупності конкуруючих на підставі техніко-економічних коефіцієнтів порівняльного воєнно-економічного аналізу. //Збірник наукових праць/ ЦНДІ ОВТ ЗС України. Вип. 7. – К.: ЦНДІ ОВТ, 2001. – С. 17-26.

11. Домарев В.В. Защита информации и безопасность компьютерных систем. – К.: Изд-во ДиаСОФТ, 1999. – 992 с.

12. Ленков С.В. Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегудов Д.А., Хорошко В.А. Под ред.В.А.Хорошко. – К.:Арий, 2008. – Том 1, - 464 с. – Том 2, 344 с.

13. Василенко В.С., Бордюк О.С., Полонський С.М. Оцінювання ризиків безпеці інформації в локальних обчислювальних мережах. [Електронний ресурс]. – Режим доступу: http://www.rusnauka.com/11_EISN_2010/Informatica/ 64068.doc.htm

14. Бурячок В.Л. Алгоритм оцінювання ступеня захищеності спеціальних інформаційно-телекомунікаційних систем / В.Л.Бурячок / Науково-технічний журнал «Захист інформації» Національного авіаційного університету, № 3, 2011, с. 19 – 27.

Надійшла 24.11.2016 р. Рецензент: д.т.н., проф. Горбенко І. Д.