УДК 004.056.53 **Цуркан В.В.**

СИСТЕМА ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ПІДТРИМКИ ПРОЦЕСІВ ПРИЙНЯТТЯ РІШЕНЬ ПРО ВИБІР ЗАСОБІВ ОБРОБЛЯННЯ РИЗИКУ

Створено структурну схему системи інформаційно-аналітичної підтримки процесів прийняття рішень про вибір засобів обробляння ризику. Розроблено алгоритм та макет програмного засобу на основі запропонованого структурно рішення. Використання програмного засобу дозволяє отримувати порівнювані та відтворювані результати визначення кількісних оцінок ризику в умовах невизначеності.

Ключові слова: система інформаційно-аналітичної підтримки процесів прийняття рішень, визначення оцінок ризику, порівнюваність, відтворюваність, засіб обробляння ризику.

Забезпечення інформаційно-аналітичної підтримки процесів прийняття рішень в системах управління інформаційною безпекою здійснюється шляхом оцінювання ризику. Для цього необхідно вибрати метод визначення якісних або кількісних оцінок, результати використання якого задовольнятимуть таким вимогам як [1-3]:

1. Порівнюваність (comparability) – характеризує можливість порівняння оцінок ризику з іншими результатами їх визначення шляхом встановлення ступеня відмінності між ними [4].

2. Відтворюваність (reproducibility) – характеризує ступінь близькості один до одного результатів визначення оцінок ризику різними експертами шляхом використання одного й того ж методу при однакових початкових даних [5].

При цьому виконання означених вимог щодо якісних оцінок ускладнене тим, що результати їх визначення, по-перше, отримуються на основі суб'єктивних суджень експертів, а, по-друге, представляються в порядковій шкалі.

Розглянуті обмеження відсутні для статистичних та ймовірнісних методів визначення кількісних оцінок, але на практиці для їх використання складно накопичити достатній обсяг статистик втрат унаслідок реалізацій загроз.

Це пов'язано з необхідністю обробляння будь-якого негативного прояву ризику з метою унеможливлювання його повторення в майбутньому. Тому система управління інформаційною безпекою постійно змінюється і, як наслідок, кількісні оцінки ризику визначаються в умовах невизначеності. У цьому випадку можливе використання експертних методів, проте характерним для них обмеженням є складність отримання відтворюваних результатів. Здебільшого, це пов'язано з суб'єктивністю суджень експертів, проблематичністю їх підбору, комплектування груп, накопичення, обробляння та аналізування експертних оцінок [6].

Уодночас, для автоматизування процесу визначення оцінок ризику на основі проаналізованих методів розроблено різноманітні комерційні програмні засоби, наприклад [7]: RiskWatch, OCTAVE, CRAMM, RA2 art of risk, ГРИФ 2006, КЭС «АванГард», BCM-Analyser, Microsoft Security Assessment Tool, vsRisk, Citicus ONE, Lightwave Security SecureAware, Proteus Enterprise, Rsam, Secure Win Auditor, IT GRC Solution, RiskVision, Total Protection for Compliance, Skybox 4000, Network Advisor & Vulnerability Advisor, Callio Secura 17799, COBRA, BuddySystem, MethodWare, PTA Risk Assessment Tool, RiskOptix, EnterpriseRisk Register, Risk Check, RiskPAC, Abriska 27001, CA GRC Manager, Archer Risk Management, Modulo Risk Manager. У зв'язку з цим, їх цінність обумовлена методом, який покладено в основу кожного з них [8].

Як наслідок, використання означених засобів дозволяє визначати:

1. Якісні оцінки, наприклад: Callio Secura 17779, КЭС «АванГард», RiskWatch.
2. Кількісні оцінки: наприклад: RiskWatch, @RISK, CRAMM.

Аналіз найбільш розповсюджених програмних засобів щодо встановлення можливості отримання порівнюваних і відтворюваних результатів визначення оцінок ризику наведено в таблиці 1 [7-10]. З огляду на неї, при використані проаналізованих засобів складно отримати як порівнювані, так і відтворюванні результати. Це пов'язано з тим, що в основу більшості з них покладено експертний метод.

Тому результати визначаються переважно в порядковій шкалі, зокрема [10]: 0, 1 – «ніколи», 2, 3 – «рідко», 4, 5, 6 – «іноді»; 7,8 – «звично»; 9, 10 – «завжди» (RiskWatch); 1 – «низький»; 2 – «середній»; 3 – «високий» (Callio Secura 17779, OCTAVE); 1 – «тривіальний»; 2,3 – «мінорний»; 4,5 – «значний»; 6,7 – «великий»; 8 – «катастрофічний» (RA2 art of risk).

Примітка:

1. Позначення: задовольняє характеристиці – «+»; не задовольняє характеристиці – «–».
2. Нумерація програмних засобів позначає номера засобу в списку, а не його пріоритет стовно інших засобів.

Таким чином, при визначенні оцінок ризику шляхом використання ймовірнісних, статистичних, експертних методів та розроблених на їх основі програмних засобів практично складно отримати як порівнювані, так і відтворювані результати. Тому для забезпечення і, як наслідок, обґрунтування інформаційно-аналітичної підтримки процесів прийняття рішень доцільно розробити більш гнучкий інструментарій [11]. Зважаючи на це, метою даної роботи є розробляння системи інформаційно-аналітичної підтримки процесів прийняття рішень про вибір засобів обробляння ризику в умовах невизначеності. Для досягнення сформованої мети розроблено структурну схему (рис. 1) системи інформаційно-аналітичної підтримки процесів прийняття рішень на основі методів запропонованих в [6, 12]. Вона складається з двох модулів – МПЛВ та МВКОР.

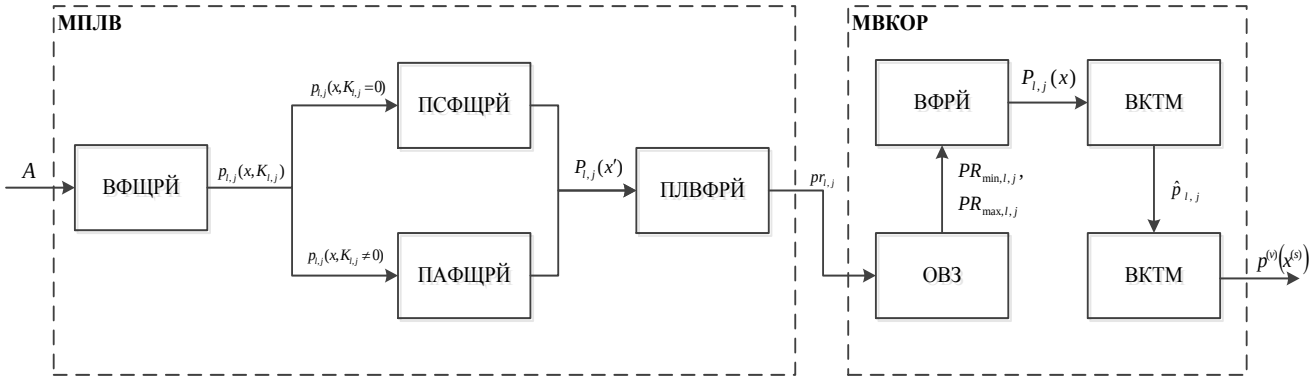

Рис. 1. Структурна схема системи інформаційно-аналітичної підтримки прийняття рішень

МПЛВ, – модуль побудови лінійного відображення, призначений для лінійного відображення нелінійної функції розподілу ймовірностей нанесення втрат унаслідок реалізації загрози на основі отриманих від розпорядника інформаційного активу даних, зокрема:

$$A=\bigcup_{l=1}^{L} A_l,\ A_l=\{O_l, I_l, x_{оч,l}\},\ l\in\{1,\ L\},$$

$$I_l=\{i_{l,j}\mid \bigcup_{t_{l,j}\in T_l}\ \bigcup_{x_{l,j}\in X_l}(i_{l,j}=<t_{l,j},x_{l,j}>)\},\ j\in\{1,n_l\},\ I_l=T_l\times X_l,$$

де: A_l – підмножина множини інформаційних активів A, що містить дані про l інформаційний актив у межах розробляння системи управління інформаційною безпекою, зокрема: про розпорядника інформаційного активу – O_l, про актуальні впорядковані пари (загроза/втрати) – I_l, очікувані втрати на експлуатування l інформаційного активу – $x_{оч,l}$;

$i_{l,j}$ – j актуальна впорядкована пара (загроза/втрати) для l інформаційного активу;

$t_{l,j}$ – j актуальна загроза для l інформаційного активу;

n_l – кількість актуальних загроз для l інформаційного активу

$x_{l,j}$ – діапазон втрат на відновлення l інформаційного активу, $x_{l,j}=[x_{\min,l,j},\ x_{\max,l,j})$;

$x_{\min,l,j}$ – втрати на відновлення l інформаційного активу за відсутності реалізацій j актуальної загрози, $x_{\min,l,j}=0$;

$x_{\max,l,j}$ – втрати на відновлення l інформаційного активу внаслідок реалізацій j актуальної загрози $x_{\max,l,j} > 0$.

Модуль побудови лінійного відображення складається з:

1. Блоку вибору функції щільності розподілу ймовірностей (ВФЩРЙ) – функція $p_{l,j}(x, K_{l,j})$ щільності розподілу ймовірностей вибирається за формою кривої (коефіцієнт асиметрії: $K_{l,j} = 0$ – симетрична, $K_{l,j} \neq 0$ – асиметрична) та значенням її похідної в точці найбільш очікуваних втрат $x_{оч,l}$. Якщо значення коефіцієнта асиметрії $K_{l,j} = 0$ – перетворення $p_{l,j}(x, K_{l,j})$ здійснюється в блоці ПСФЩРЙ (пункт 2), інакше в блоці ПАФЩРЙ (пункт 3).

2. Блоку перетворення функції щільності розподілу ймовірностей з симетричною формою кривої до нормального закону (ПСФЩРЙ) – функція $p_{l,j}(x, K_{l,j} = 0)$ відображається функцією $P_{l,j}(x')$ розподілу ймовірностей нормального закону, наприклад [13], шляхом введення констант нормування.

3. Блоку перетворення функції щільності розподілу ймовірностей з асиметричною формою кривої до нормального закону (ПАФЩРЙ) – функція $p_{l,j}(x, K_{l,j} \neq 0)$ відображається функцією $P_{l,j}(x')$ розподілу ймовірностей нормального закону шляхом перетворення значень x величини втрат X.

4. Блоку побудови лінійного відображення нелінійної функції розподілу ймовірностей нормального закону (ПЛВФРЙ) – побудова лінійного відображання $f_{l,j}$ функції $P_{l,j}(x')$ здійснюється на основі представлення нормального еквівалентного відхилення n_σ нормованою випадковою величиною, що розподілена за нормальним законом.

МВКОР, – модуль визначення кількісних оцінок ризику, призначений для кількісного оцінювання ризику на основі лінійного відображення функції розподілу ймовірностей нанесення втрат унаслідок реалізації загрози. Він складається з:

1. Блоку оцінювання впливу загрози на безпеку інформаційного активу (ОВЗ) – вплив загрози оцінюється шляхом визначення значень однорідної лінійної функції $pr_{l,j}$, як узагальнення $f_{l,j}$, на основі даних про втрати $[x'_{\min,l,j}, x'_{\max,l,j})$ на відновлення інформаційного активу A_l. В результаті цього отримуємо мінімальну $PR_{\min,l,j}(x'_{\min,l,j}, pr_{\min,l,j})$ та максимальну $PR_{\max,l,j}(x'_{\max,l,j}, pr_{\max,l,j})$ оцінки впливу загрози.

2. Блоку визначення функції розподілу ймовірностей нанесення втрат унаслідок реалізації загрози (ВФРЙ) – функція $P_{l,j}(x)$ розподілу ймовірностей визначається на основі мінімальної $PR_{\min,l,j}$ та максимальної $PR_{\max,l,j}$ оцінок впливу загрози на безпеку інформаційного активу A_l.

3. Блоку визначення координат точки максимуму функції щільності розподілу ймовірностей (ВКТМ) – координати точки $\hat{p}_{l,j}(x_{оч,l,j}, p_{оч,l,j})$ максимуму функції $p_{l,j}(x)$ щільності розподілу ймовірностей визначаються шляхом числового диференціювання функції $P_{l,j}(x)$.

4. Блоку відображення координат точки максимуму на матриці ризику, (ВКТМ) – координати точки $\hat{p}_{l,j}$ відображаються на матриці ризику, приклад зображення якої показано на рисунку 2.

На основі запропонованого структурного рішення розроблено макет програмного засобу визначення кількісних оцінок ризику в умовах невизначеності для інформаційно-аналітичної підтримки прийняття рішень про вибір засобів його обробляння, алгоритм роботи якого представлено на рисунку 3.

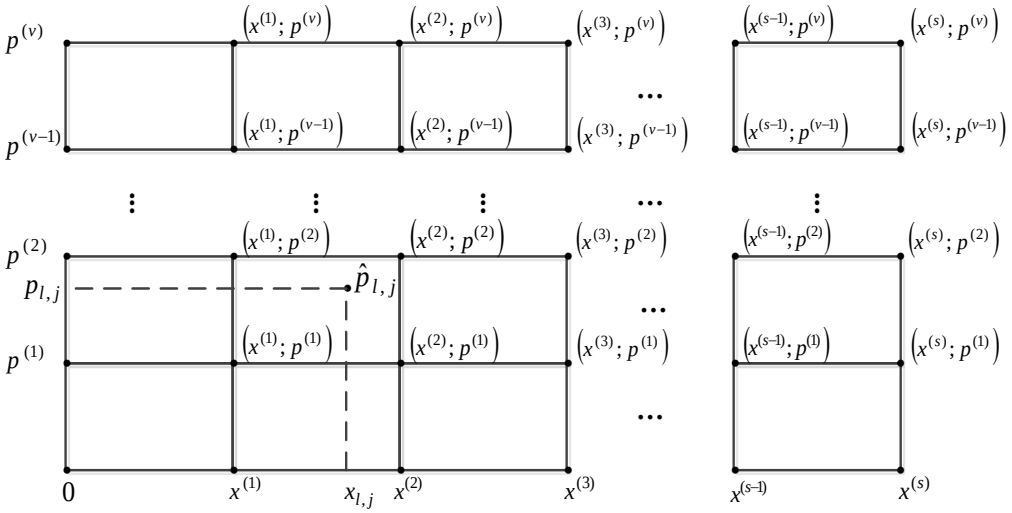

Рис. 2. Матриця ризику з нанесеними координатами точки $\hat{p}_{l,j}$ максимуму, де: $x^{(s)}$ - максимальне значення величини втрат; $p^{(v)}$ - максимальне значення функцій щільності розподілу ймовірностей нанесення втрат

З огляду на рисунок 3, охарактеризуємо етапи алгоритму визначення кількісних оцінок ризику в умовах невизначеності:

1. Введення початкових даних $L, O_l, n_l, t_{l,j}, x_{l,j}, x_{оч,l}$.

2. Визначення кількісних оцінок ризику для l інформаційного активу (етапи 3-10).

3. Визначення кількісної оцінки ризику j актуальної загрози l інформаційному активу (етапи 5-10).

4. Вибір функції $p_{l,j}(x)$ щільності розподілу ймовірностей нанесення втрат унаслідок реалізації j актуальної загрози l інформаційному активу.

5. Перетворення функції $p_{l,j}(x)$ до функції $P_{l,j}(x')$ розподілу ймовірностей нормального закону в залежності від значення коефіцієнта асиметрії $K_{l,j}$. Якщо $K_{l,j} = 0$, то перетворення здійснюється за допомогою процедури «ПАФЩРЙ» (блок 6), інакше процедури «ПСФЩРЙ» (блок 7).

6. Перетворення функції $p_{l,j}(x)$ з асиметричною формою кривої ($K_{l,j} \neq 0$) до функції $P_{l,j}(x')$ розподілу ймовірностей нормального закону.

7. Перетворення функції $p_{l,j}(x)$ з симетричною формою кривої ($K_{l,j} = 0$) до функції $P_{l,j}(x')$ розподілу ймовірностей нормального закону.

8. Визначення оцінок $pr_{l,j}$ впливу j актуальної загрози на l інформаційний актив.

9. Визначення функції $P_{l,j}(x)$ розподілу ймовірностей нанесення втрат унаслідок реалізації j актуальної загрози l інформаційному активу.

10. Визначення координат точки $\hat{p}_{l,j}$ максимуму шляхом числового диференціювання функції $P_{l,j}(x)$.

11-14. Виведення результатів визначення кількісних оцінок ризику для L інформаційних активів.

Таким чином, на основі запропонованого структурного рішення щодо створення системи інформаційно-аналітичної підтримки прийняття рішень можливе розробляння програмних засобів, які на відміну від існуючих (таблиця 1) дозволяють, по-перше, отримувати порівнюванні і відтворювані результати визначення кількісних оцінок ризику в умовах невизначеності, і, як наслідок, по-друге, обґрунтовувати інформаційно-аналітичну

підтримку процесів прийняття рішень. Завдяки цьому можна підвищити їх ефективність шляхом обґрунтованого вибору засобів обробляння ризику.

Таблиця 1

Програмні засоби для визначення оцінок ризику

№ з/с	Назва інструментального засобу	Вимоги до результатів		Країна	Ціна, USD
		Порівнюваність	Відтворюваність		
1.	ГРИФ 2006	+	–	Росія	675
2.	BCM-Analyser	+	–	Росія	635
3.	КЭС «АванГард»	–	–	Росія	1112
4.	RiskWatch	+	–	США	5500
5.	RA2 art of risk	–	–	США	2355
6.	@RISK	+	–	США	3920
7.	COBRA	–	–	США	1500
8.	OCTAVE	–	–	США	1995
9.	Callio Secura 17779	–	–	Канада	2999
10.	CRAMM	–	–	Великобританія	955
11.	vsRisk	–	–	Великобританія	1896
12.	Proteus Enterprise	+	–	Великобританія	2290

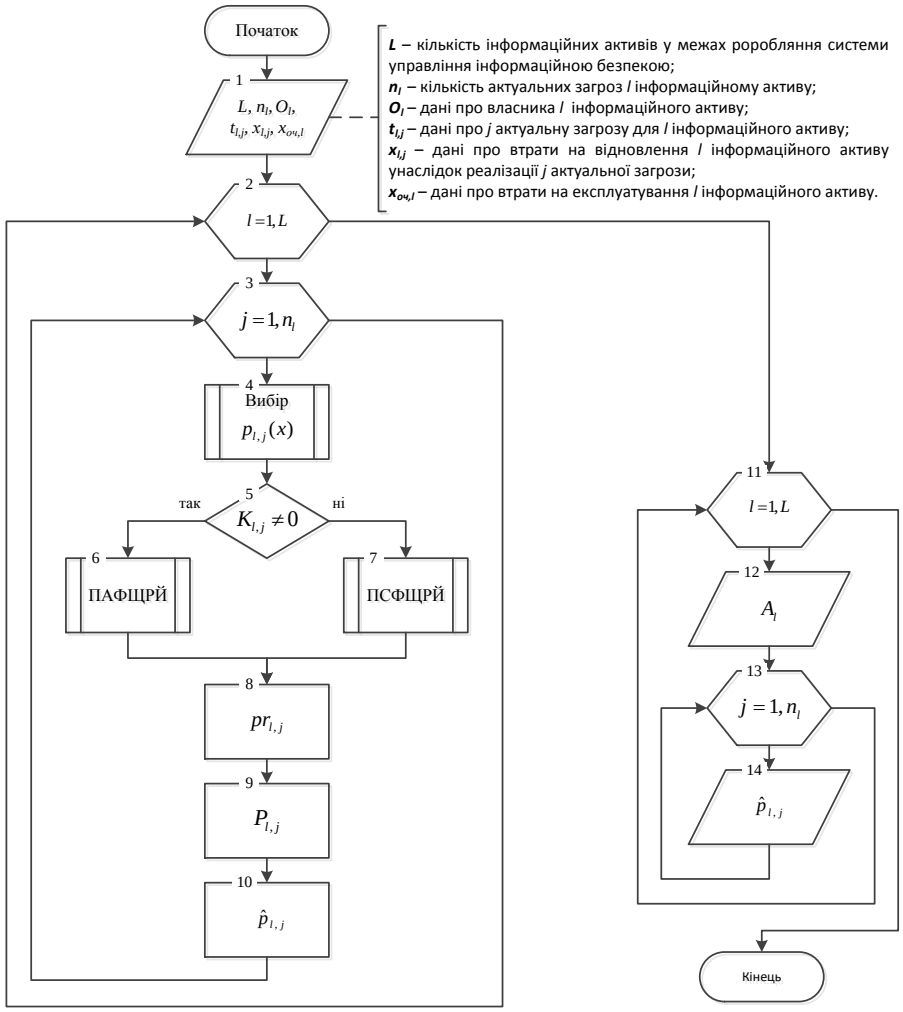

Рис. 3. Блок-схема алгоритму визначення кількісних оцінок ризику в умовах невизначеності

ЛІТЕРАТУРА

1. Інформаційні технології. Методи та засоби досягнення інформаційної безпеки. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, IDT): ДСТУ ISO/IEC 27001:2010. – [Чинний від 2012-07-01]. – К.: Держспоживстандарт України, 2012. – (Національний стандарт України)

2. Мохор В.В. Изложение стандарта «ISO 31000:2009 Risk management – principles and guidelines» на русском языке / А.М. Богданов, В.В. Мохор // Das Management. – 2011. – № 3. – С. 5-18.

3. Information technology. Security techniques. Information Security Risk Management: BS ISO/IEC 27005:2008. – [2008-06-30]. – London: British Standards Institution, 2008. – 64 p. (International Standard).

4. Великий тлумачний словник сучасної української мови (з дод. і допов.) / Уклад. і голов. ред. В.Т. Бусел. – К.; Ірпінь: ВТФ «Перун», 2005. – 1725 с.

5. Точність (правильність і прецизійність) методів та результатів вимірювання. Частина 1. Основні положення та визначення (ISO 5725:1994, IDT): ДСТУ ГОСТ ИСО 5725-1:2005. – [Чинний від 2006-07-01]. – К.: Держспоживстандарт України, 2006. – 31 с. – (Національний стандарт України) – рос.

6. Цуркан В.В. Пробит-анализ рисков безопасности информации / В.В. Цуркан, В.В. Мохор // Захист інформації. – 2010. – № 3. – С. 28-34.

7. Астахов А. Искусство управления информационными рисками [Электронный ресурс]. – Режим доступа: http://анализ-риска.рф/. – Дата доступа: август 2012. – Название с экрана.

8. Лопарев С.А. Анализ инструментальных средств оценки рисков утечки информации в компьютерной сети предприятия / С.А. Лопарев, А.А. Шелупанов // Вопросы защиты информации. – 2003. – № 4. – С. 2-4.

9. Программные средства управления безопасностью [Электронный ресурс]. – Режим доступа: http://shop.globaltrust.ru/show_cat2.php?grid=5061&PHPSESSID=46bc8689d76d86c66d627d27df3c9418. – Дата доступа: август 2012. – Название с экрана.

10. Луцкий М.Г. Современные средства управления информационными рисками / М.Г. Луцкий, Е.В. Иванченко, А.Г. Корченко, С.В. Казмирчук, А.А. Охрименко // Защита информации – 2012. – №1. – С. 5-16.

11. Литвак Б.Г. Экспертные оценки и принятие решений. – М.: Патент, 1996. – 271 с.

12. Цуркан В.В. Визначення кількісних оцінок рівнів ризику при розробленні системи керування безпекою інформації в умовах недостатності статистичних даних / В.В. Цуркан // Моделювання (Київ, 11-12 січ. 2012 р.): XXXI наук.-техн. конф.: тези доп. – К.: ПП «Системи, технології, інформаційні послуги», 2012. – С. 22.

Лямин О. О. О предельном поведении мощностей критериев в случае обобщенного распределения Лапласа / О.О. Лямин // Информатика и ее применения. – 2010. – Т. 4, № 3. – С.

Надійшла: 28.07.2012 р.

Рецензент: д.т.н., професор Корченко О.Г.