# СЦЕНАРНИЙ ПІДХІД ДО ОЦІНКИ РИЗИКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Снігуров А.В., Слюсар Н.М., Діденко Є.С.

Кафедра «Інфокомунікаційної інженерії ім. В.В. Поповського»,
Харківський національний університет радіоелектроніки, Україна

E-mail: arkadii.snihurov@nure.ua,
natalia.sliusar@nure.ua,
yevheniia.didenko@nure.ua

**Abstract**

*The report analyzes the role of such a process as information security risk assessment in the organization's information security system, suggests a scenario approach for information security risk assessment. The level of vulnerability to be taken into account in the information security risk indicator is proposed to be calculated using the CVSSv3.1 methodology.*

Оцінка ризиків інформаційної безпеки (ІБ) є одним з ключових процесів при побудові як систем менеджменту інформаційної безпеки (СМІБ), так і розробки систем захисту складних інформаційних систем (ІС). Фактично результат оцінки ризиків ІБ це прогноз потенційних проблем, потенційних втрат внаслідок реалізації загроз ІБ. Даний процес тісно пов'язаний з іншими процесами, такими як обробка інцидентів ІБ, аудит (внутрішній та зовнішній), оцінка рівня ІБ менеджментом. Останні три процеси мають за метою оцінку поточного стану з ІБ СМІБ (ІС) та порівняння його з прогнозом враховуючі цілі та завдання ІБ та критерії оцінки ефективності СМІБ (системи захисту ІС). При знаходженні невідповідностей стану ІБ встановленим цілям та критеріям здійснюється переоцінка ризику ІБ та вводяться корегуючі дії. Спрощена структура взаємозв'язку даних процесів при плануванні та забезпеченні ІБ в організації (в ІС) представлена на рис.1.

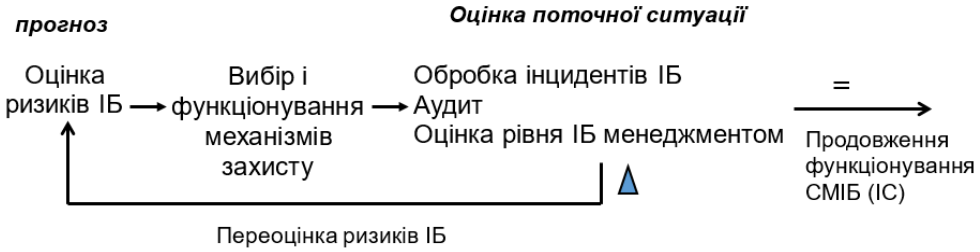


**Рис. 1. Спрощена структура взаємозв'язку процесів при плануванні та функціонуванні СМІБ (системи захисту ІС)**

Вимоги та порядок оцінки ризиків представлені в ряді стандартів [1, 2 та інші]. Відповідно цим нормативним документам одним з основних етапів оцінки ризику є оцінка ймовірнісних характеристик ризику (якісна, кількісна або змішана). Ймовірнісними характеристиками в структурі ризику ІБ є ймовірність реалізації загрози (середньогодова частота загроз - Annualized Rate of Occurrence) та ймовірність вразливості (коефіцієнт впливу - Exposure Factor). Наявність певної інформаційної невизначеності відповідно ризикових ситуацій призводить до того, що фахівці ІБ, які проводять оцінку ризику ІБ, можуть оцінити дані показники помилково. Для зменшення даної проблеми в стандарті [2] пропонуються ряд методів, до яких відносяться: структурований аналіз сценаріїв методом «що, якщо?» (SWIFT), аналіз сценаріїв, аналіз впливу на бізнес (BIA), аналіз первопричини (RCA), аналіз видів та наслідків відмов (FMEA), аналіз дерева несправностей (FTA), аналіз дерева подій (ETA), аналіз

причин та наслідків, аналіз рівнів захисту (LOPA), аналіз дерева рішень, аналіз впливу людського фактора (HRA), криві FN, індекси ризику, матриця наслідків і ймовірностей, аналіз ефективності витрат (CBA), мультикритеріальний аналіз рішень (MCDA).

На даний момент багато публікацій по питанням оцінки ризику ІБ, в тому числі [3,4,5]. В доповіді запропонований механізм оцінки ймовірнісних показників ризику ІБ на підставі аналізу сценаріїв реалізації загроз ІБ з врахуванням існуючих вразливостей системи, що захищається. Для реалізації даного підходу формується множина можливих сценаріїв $C_x = \{a_1, a_2, ..., a_X\}$ реалізації загроз для конкретної організації (ІС). Для формування даної множини сценаріїв розробляється модель порушника, при які визначаються множина типів потенційних порушників $\Pi_y = \{b_1, b_2, ..., b_Y\}$, їх потенціал.

Далі формується матриця (1), в якій для кожного сценарію визначається ймовірність його реалізації для кожного типу порушників.

$$M_{сценаріїв} = \begin{array}{c|cccc} & \Pi_1 & \Pi_2 & ... & \Pi_Y \\ C_1 & P_1^1 & P_1^2 & ... & P_1^Y \\ C_2 & P_2^1 & P_2^2 & ... & P_2^Y \\ ... & ... & ... & ... & ... \\ C_X & P_X^1 & P_X^2 & ... & P_X^Y \end{array}$$

де $P_x^y$ – ймовірність реалізації х – го сценарія у – м типом порушника, $x = \overline{1, X}$, $y = \overline{1, Y}$, $P_x^y = [0,1]$ відповідно до його потенціалу.

Далі формується матриця ймовірності атаки конкретної організації (ІС) кожним з типів порушників, яка враховує їх наміри:

$$\Pi_y = \begin{array}{c|c} \Pi_1 & P_1 \\ \Pi_2 & P_2 \\ ... & ... \\ \Pi_Y & P_Y \end{array}$$

де $P_y$ – ймовірність атаки організації (ІС) у – м типом порушника, $y = \overline{1, Y}$, $P_y = [0,1]$.

Ймовірність реалізації кожного сценарію визначається з виразу:

$$Pc_x = \sum_{y=1}^{Y} P_x^y \cdot P_y .$$

Для кожного сценарія визначається рівень вразливості, який пропонується розраховувати на підставі методичного апарату стандарту Національного інституту стандартів і технологій США Common Vulnerability Scoring System (CVSS) v3.1 [6, 7]:

$$M_{сценаріїв} = \begin{array}{c|c} C_1 & V_1 \\ C_2 & V_2 \\ ... & ... \\ C_X & V_X \end{array}$$

де $V_x$ - рівень вразливості для сценарію х, $x = \overline{1, X}$. Даний показник отримається шляхом поділу рівня вразливості, який розрахований онлайн калькулятором методики CVSS, на 10 для приведення в шкалу [0,1].

Тоді ризик інформаційної безпеки для кожного з сценаріїв атаки можна розрахувати з виразу:

$$R_x = Pc_x \cdot V_x .$$

Такий підхід дозволяє побудувати стратегію захисту організації (ІС) відповідно до прогнозу дій потенційних порушників, їх можливостей по реалізації атаки.

## *Л*ітература

1. Міжнародний стандарт ISO/IEC 27001-2013. Інформаційні технології. Методи забезпечення безпеки. Системи менеджменту інформаційної безпеки. Вимоги. / ISO, 2013. – 38 ст.
2. Міжнародний стандарт ISO/IEC 31010-2009. Менеджмент ризику. Методи оцінки ризику. / ISO, 2009. – 74 ст.
3. Kuzminykh I, Ghita B., Sokolov V., Bakhshi T. Information Security Risk Assessment. Encyclopedia. - 2021, N 1. – 602 – 617 pp.
4. Снігуров А.В., Сацюк Д. В. Ризики інформаційної безпеки сучасних систем електронного документообігу. Інформатика, управління та штучний інтелект. Тези восьмої міжнародної науково-технічної конференції. Харків: НТУ "ХПІ". - 2021. - С. 126.
5. Снігуров А.В., Сацюк Д. В. Підхід до оцінки вразливостей до інформаційних атак систем електронного документообігу з використанням методики CVSSv3. Інформатика, управління та штучний інтелект. Тези восьмої міжнародної науково-технічної конференції. Харків: НТУ "ХПІ". - 2021. - С. 127.
6. Common Vulnerability Scoring System. [Електронний ресурс]. Режим доступу: https://www.first.org/cvss/.
7. Common Vulnerability Scoring System Version 3.1 Calculator. [Електронний ресурс]. Режим доступу: https://www.first.org/cvss/calculator/3.1.