УДК 004.056:005.334

ОБҐРУНТУВАННЯ ВИБОРУ ЕФЕКТИВНОЇ ШКАЛИ ОЦІНКИ ІНФОРМАЦІЙНИХ РИЗИКІВ

Усенко М.О.
e-mail: maksym.usenko1@nure.ua
Науковий керівник – к.т.н., доц. Добринін І.С.
Харківський національний університет радіоелектроніки, каф. ІКІ
ім. В. В. Поповського
м. Харків, Україна

This paper addresses the critical challenge of selecting an optimal scale for information security risk assessment in modern organizational environments. While traditional 3-point and 5-point scales offer simplicity, they often lack the necessary detail for large-scale organizations facing diverse and complex threats. The study justifies the transition to a 9-point scale, grounding its advantages in both mathematical stability and cognitive psychology. Additionally, the study introduces practical models for quantifying incident probability and financial losses using this unified scale.

У сучасному світі безпека інформаційних систем є дуже важливим питанням для організацій різного рівня. Важливою частиною її забезпечення є визначення та мінімізація інформаційних ризиків. Оцінювання інформаційних ризиків є важливим процесом, оскільки він дозволяє ідентифікувати, аналізувати та керувати ризиками, пов'язаними з інформаційними активами. Для оцінювання ризиків можуть бути використані різноманітні методики та стандарти [1].

Зростання кількості та різноманітності наявних інформаційних загроз (зокрема так званий штучний інтелект, квантові обчислення) ускладнює процес оцінювання, роблячи вибір шкали ключовим для коректного ранжування наявних ризиків як при регулярному оцінюванні, так і в умовах переоцінювання при виникненні інцидентів або нових zero-day вразливостей. Зазвичай стандарти та методології (наприклад, ISO/IEC 27005:2022) залишають за спеціалістом, який буде їх використовувати, рішення про застосування якісного чи кількісного (або у деяких випадках й напівкількісного) оцінювання, не кажучи вже безпосередньо про шкалу значень. Таким чином, питання вибору шкали оцінювання є актуальним для будь-якої організації, що прагне забезпечити високий рівень захищеності своїх інформаційних активів, ефективно використовуючи наявні ресурси.

Метою даної роботи є вибір найкращої шкали для оцінювання інформаційних ризиків та формування пропозицій щодо її практичного застосування.

У сфері оцінювання ризиків зазвичай мова йде про 3-значну та 5-значну шкали. Першу застосовують у якісному варіанті (низький, середній та високий рівень). Основною перевагою даної шкали є мінімальна кількість наявних значень, що дозволяє виконувати оцінювання дуже швидко, проте

звідси випливає й недолік – доволі груба оцінка, що є особливо критичним в умовах середніх та великих організацій, тому найбільшої ефективності дана шкала досягає в умовах необхідності проведення оцінювання у малих організаціях або виконання первинного оцінювання з подальшим уточненням кількісними показниками. Щодо 5-значної шкали, то вона може бути як якісною (дуже низький, низький, середній, високий та дуже високий рівень), так і кількісною (1 – 5 балів). Її популярність обумовлена забезпеченням балансу між простотою по відношенню до більших шкал, а також збільшеною деталізацією по відношенню до згаданої вище 3-значної.

Певні стандарти все ж пропонують чітко визначені алгоритми надання оцінок, як наприклад BSI Standard 200-3, де застосовується 4-значна якісна шкала, що збільшує верхню межу класичної 3-значної, впроваджуючи значення «дуже високий».

Проте зазначені вище шкали не надають достатньої деталізації в умовах великих організацій, що стикаються з великою кількістю різноманітних загроз, а отже необхідно розглядати більші шкали. 10 та 12-бальні шкали широко застосовуються у різноманітних сферах, зокрема у освітньому процесі, тоді як 9-бальну шкалу оцінювання застосував Томас Л. Сааті у методі аналізу ієрархій (MAI) [2]. У окремій роботі "Deriving the AHP 1-9 scale from first principles" [3] він показав, чому саме 9-бальна шкала була обрана для використання у розробленому ним методі.

Основою для застосування значень від 1 до 9 у MAI є відомий у психології закон Вебера-Фехнера та ідея ледве помітних відмінностей (just noticeable differences), звідки отримують послідовність 1, 2, …, n. Верхня межа у значення 9 базується на математичній стабільності – власний вектор пріоритетів залишається стабільним лише тоді, коли порівнювані елементи є однорідними (належать до одного порядку величини).

Також, так як у своїй роботі Т. Сааті звертає увагу як на математику, так і на психологію, принагідно зазначити, що згідно з правилом "гаманця Міллера" [4] середньостатистична людина може тримати в робочій пам’яті 7 ± 2 елементи.

Таким чином, 9-бальна шкала задовольняє як математичні, так і психологічні умови формування шкали оцінювання.

З описаного вище зрозуміло, що, з одного боку, 9-бальна шкала пропонує збільшену деталізацію у порівнянні з 3 та 5-бальною, і в той же час є найбільшою шкалою, що зберігає ефективність при обробці людиною, тобто є найкращим вибором з точки зору співвідношення точність/сприйнятність.

Повертаючись до питання вибору шкали оцінювання при застосуванні наявних підходів, доцільно сформувати пропозиції щодо використання 9-бальної шкали. Різні підходи можуть використовувати різні параметри, об’єднуючи та розбиваючи деякі, або ж формуючі нові. Проте універсальними значеннями у питаннях інформаційних ризиків є вірогідність виникнення інциденту та величина наслідків його реалізації,

показником якої зазвичай є величина фінансової втрати. Пропонується виконувати розрахунок даних параметрів за шкалами, які надані в таблиці 1.

Таблиця 1 – Шкала для кількісного оцінювання вірогідності виникнення інциденту та величини наслідків його реалізації

Оцінка	Вірогідність	Втрати (у.о.)
1	1 раз на 3 роки	< 100
2	1 раз на рік	100 – 1000
3	1 раз на пів року	1000 – 10000
4	1 раз на 3 місяці	10000 – 100000
5	1 раз на місяць	100000 – 1000000
6	1 раз на тиждень	1000000 – 10000000
7	1 раз на добу	10000000 – 100000000
8	1 раз на годину	100000000 – 1000000000
9	1 раз на хвилину	> 1000000000

Зрозуміло, що запропонована в таблиці 1 шкала є загальною, тобто має бути додатково скоригована при застосуванні до конкретної організації, зокрема у питанні величини втрат, так як різні підприємства мають різний грошовий обіг, а отже й серйозність втрати певної суми може бути незначною для однієї організації, проте критичною для іншої.

Список використаних джерел:

1. Корченко О. Г., Казмірчук С.В., Ахметов Б.Б., *Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія*, Київ, ЦП «Компринт», 2017 – 435 с.

2. Saaty T.L. Fundamentals of Decision Making and Priority Theory with the Analytic Hierarchy Process. Pittsburgh: RWS Publications, 2013. 477 p.

3. Saaty T.L. Deriving the AHP 1-9 scale from first principles. ISAHP 2001, Berne, Switzerland, August 2-4, 2001. 5 c.

4. The Magical Number Seven, Plus or Minus Two : вебсайт. URL: https://en.wikipedia.org/wiki/The_Magical_Number_Seven,_Plus_or_Minus_Two (дата звернення: 05.03.2026).