# SNW-АНАЛІЗ МІЖНАРОДНИХ СТАНДАРТІВ З ОЦІНЮВАННЯ ІНФОРМАЦІЙНИХ РИЗИКІВ

Усенко М.О., Добринін І.С.

Харківський національний університет радіоелектроніки,
кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Україна.

E-mail: maksym.usenko1@nure.ua,
ihor.dobrynin@nure.ua

**Abstract**

*The purpose of this paper is to analyze the BSI Standard 200-3, ISO/IEC 27005:2022 and IEC 31010:2019 standards using the SNW analysis method. The strengths, neutrals and weaknesses of the specified standards were identified. To perform this study, analytical work was conducted, in particular literature analysis.*

У сучасному світі велике значення для будь-якої організації має питання забезпечення інформаційної безпеки, що досягається шляхом впровадження системи управління інформаційною безпекою (далі – СУІБ). Одним з етапів процесу створення СУІБ є управління інформаційними ризиками, у результаті чого для кожної організації у певний момент постає питання вибору відповідної методології. Даній проблемі присвячена низка стандартів і методик, зокрема ISO/IEC 27005:2022, IEC 31010:2019, NIST SP 800-39, OCTAVE та інші. Проте, загальноприйнятим є факт, що стандарти від ISO та IEC є найкращими у питаннях роботи з інформаційними ризиками.

Ще одним стандартом, що спеціалізується на питанні управління інформаційними ризиками, але не є так широко використовуваним, як ISO/IEC 27005:2022 або IEC 31010:2019, є німецький BSI Standard 200-3.

Метою цієї роботи є проведення аналізу стандартів BSI Standard 200-3 [1], ISO/IEC 27005:2022 [2] та IEC 31010:2019 [3] з використанням методики SNW-аналізу [4].

Запропонована методика, що зазвичай використовується для оцінювання структури організації, полягає у визначенні сильних, нейтральних та слабких сторін, з метою нейтралізації слабкостей та покращення конкурентоспроможності, або, у даному випадку, аналізу стандартів.

Спочатку розглянемо BSI Standard 200-3. Однією з переваг даного стандарту є надання таблиці з 46-ма базовими загрозами, яка, окрім самих загроз, зазначає також, на які з аспектів захисту інформації (конфіденційність, цілісність, доступність) буде впливати відповідна загроза. Дана таблиця впроваджує можливість швидкого визначення списку базових актуальних загроз для будь-якого цільового об’єкта, після чого виконується пошук додаткових специфічних загроз для кожного конкретного цільового об’єкта. Слід зазначити, що стандарт вважає цільовими об’єктами конкретні елементи інформаційної системи організації, такі як комп’ютери, сервери, маршрутизатори та інші.

Ще одним позитивним аспектом є планування наперед заходів безпеки для загроз, що були визначені як прийнятні, але потенційно можуть зрости у майбутньому, задля їх якнайшвидшого впровадження.

Також до переваг можно віднести простоту і високу швидкість впровадження стандарту, так як він має детальну покрокову інструкцію з оцінювання та обробки ризиків, що супроводжуються прикладами для кожного кроку, та виявляє ризики на основі цільових об’єктів.

До нейтральних елементів стандарту BSI Standard 200-3 належить використання у процесі оцінювання ризиків критеріїв "потенційна шкода" (potential damage), "частота виникнення" (frequency of occurrence) та "рівень ризику" (risk categorie), що базується на двох критеріях, зазначених вище. Для визначення наведених параметрів застосовується методика якісного оцінювання.

Також нейтральним аспектом є використання наступних опцій обробки ризиків: "уникнення ризику" (risk avoidance), "зниження ризику" (risk reduction), "передача ризику" (risk transfer) та "прийняття ризику" (risk acceptance).

Недоліком BSI Standard 200-3 можна назвати сфокусованість стандарту на одному, хоч і чітко визначеному, підході, так як часто, особливо у великих організаціях, може виникати потреба використання декількох методик оцінювання задля отримання більш повної картини.

Щодо ISO/IEC 27005:2022, як сильну сторону можна виділити варіативність на етапі визначення ризиків. Стандарт пропонує два підходи: "підхід на основі подій" (event-based approach) та "підхід на основі активів" (asset-based approach). Перший визначає ризики на основі визначення можливих подій та їх наслідків, що дозволяє виконати більш швидку ідентифікацію, сфокусувавшись на найбільш критичних ризиках. Підхід на основі активів, в свою чергу, визначає ризики, базуючись на активах, загрозах та вразливостях.

Іншим позитивним аспектом є впровадження процесу моніторингу, зокрема циклів управління ризиками: "стратегічний цикл" (strategic cycle) та "операційний цикл" (operational cycle). У першому розглядаються нові загрози, що виникають внаслідок змін у загальному контексті організації, тоді як другий, спираючись на результати стратегічного циклу, визначає, які ризики мають бути переглянуті або додані до процесу управління ризиками.

Нейтральним елементом, аналогічно до BSI Standard 200-3, є використання критеріїв "потенційна шкода" (potential consequences), "частота виникнення" (likelihood) та "рівень ризику" (level of risk) у процесі оцінювання ризиків. Але, на відміну від BSI Standard 200-3, стандарт розглядає методики якісного, напівкількісного та кількісного оцінювання, що можна вважати ще однією перевагою ISO/IEC 27005:2022.

Також нейтральним аспектом є використання наступних опцій обробки ризиків: "уникнення ризику" (risk avoidance), "модифікація ризику" (risk modification), "розподіл ризику" (risk sharing) та "утримання ризику" (risk retention).

До слабкостей можна віднести певну складність і низьку швидкість впровадження, що виникає в результаті пропонування різних підходів та методів оцінювання.

IEC 31010:2019, в свою чергу, надає варіативність на кожному етапі оцінювання ризиків: стандарт пропонує список з 41-ї техніки для "виявлення поглядів" (eliciting views), "ідентифікації ризиків" (risk identification), "аналізу ризиків" (risk analysis) та "оцінки ризиків" (risk evaluation), що є перевагою стандарту.

Іншим позитивним аспектом є впровадження процесу моніторингу, що включає порівняння очікуваних результатів обробки ризиків з отриманими та пошук нових ризиків і неочікуваних змін, що можуть виникнути у майбутньому.

До нейтральних елементів, аналогічно до BSI Standard 200-3 та ISO/IEC 27005:2022, належать критерії процесу оцінювання ризиків "потенційна шкода" (potential consequences) та "частота виникнення" (likelihood). Стандарт розглядає методики якісного, напівкількісного та кількісного оцінювання, що також є перевагою для IEC 31010:2019. Слід зазначити, що формування підсумкового критерію, аналогічного до "рівня ризику" у інших стандартах, що розглядаються, є необов'язковою дією.

Слабкістю стандарту IEC 31010:2019 є його складність і низька швидкість впровадження внаслідок пропонування великої кількості різних технік для оцінювання ризиків та методів оцінювання.

Ще одним негативним елементом стандарту можна назвати відсутність процесу обробки ризиків, адже стандарт фокусується виключно на оцінці ризиків.

Задля наочності результати аналізу наведені у таблиці 1.

**Таблиця 1. Результати аналізу стандартів шляхом використання SNW-аналізу**

| | Сильні сторони | Нейтральні сторони | Слабкі сторони |
|---|---|---|---|
| BSI Standard 200-3 | Таблиця базових загроз.<br><br>Планування заходів безпеки для потенційних ризиків.<br><br>Простота та висока швидкість впровадження. | Використання критеріїв оцінювання ризику "потенційна шкода", "частота виникнення" та "рівень ризику" з методикою якісного оцінювання.<br><br>Використання опцій обробки ризиків: "уникнення ризику", "зниження ризику", "передача ризику" та "прийняття ризику". | Відсутність варіативності. |
| ISO/IEC 27005:2022 | Варіантивність на етапі визначення ризиків.<br><br>Можливість використання якісного, напівкількісного та кількісного оцінювання.<br><br>Впровадження циклів управління ризиками. | Використання критеріїв оцінювання ризику "потенційна шкода", "частота виникнення" та "рівень ризику".<br><br>Використання опцій обробки ризиків: "уникнення ризику", "модифікація ризику", "розподіл ризику" та "утримання ризику". | Складність та низька швидкість впровадження. |
| IEC 31010:2019 | Варіативність на кожному етапі оцінювання ризиків.<br><br>Можливість використання якісного, напівкількісного та кількісного оцінювання.<br><br>Впровадження процесу моніторингу ризиків. | Використання критеріїв оцінювання ризику "потенційна шкода" та "частота виникнення". | Складність та низька швидкість впровадження.<br><br>Відсутність процесу обробки ризиків |

Отже, у роботі показані результати аналізу стандартів BSI Standard 200-3, ISO/IEC 27005:2022 та IEC 31010:2019 з використанням методики SNW-аналізу: визначені їх сильні, нейтральні та слабкі сторони.

## *Література*

1.BSI Standard 200-3: Risk Analysis based on IT Grundschutz : стандарт. Бонн : Federal Office for Information Security, 2017. 45 с.

2. ISO/IEC 27005:2022. ISO : вебсайт. URL: https://www.iso.org/standard/80585.html (дата звернення: 07.11.2024).

3. IEC 31010:2019. ISO : вебсайт. URL: https://www.iso.org/standard/72140.html (дата звернення: 07.11.2024).

4. SNW-аналіз. Вікіпедія : вебсайт. URL: https://uk.wikipedia.org/wiki/SNW-аналіз (дата звернення: 07.11.2024).