

УДК 338.2:004.056

МЕТОДИ ОЦІНКИ РІВНЯ БЕЗПЕКИ ПІДПРИЄМСТВА: ПІДХОДИ ДО УПРАВЛІННЯ РИЗИКАМИ ТА ЗАБЕЗПЕЧЕННЯ СТАБІЛЬНОСТІ

Шеренок К.К., Антонович В.Д.

e-mail: kostiantyn.sherenok@nure.ua, vladyslav.antonovych@nure.ua

Харківський національний університет радіоелектроніки, каф. ЕК
м. Харків, Україна

In this work, methods for assessing the security level of an enterprise are explored as essential tools for risk management and ensuring business stability. The study focuses on various aspects of security, including physical, informational, and economic protection. Key approaches such as risk analysis, scenario modeling, and the evaluation of existing security systems are discussed. The work also highlights the importance of SWOT analysis, monitoring, and auditing in identifying vulnerabilities and enhancing security strategies. Overall, these methods help minimize risks and ensure reliable protection against both external and internal threats, supporting the enterprise's continuous operation in an uncertain environment.

Методи визначення рівня безпеки підприємства є основою ефективного управління ризиками та забезпечення стабільності його діяльності. В умовах постійних змін в економічному, технологічному та соціальному середовищі питання безпеки підприємства набуває дедалі більшої актуальності, оскільки саме безпека є запорукою його безперебійного функціонування. Сфера безпеки охоплює широкий спектр аспектів: від фізичної безпеки, що включає охорону персоналу, будівель і обладнання, до інформаційної безпеки, захисту від кіберзагроз, а також економічної та фінансової стійкості підприємства.

Оцінка рівня безпеки дає змогу своєчасно виявляти потенційні загрози, мінімізувати їхній вплив на діяльність підприємства та розробляти стратегічні заходи для їх нейтралізації. Завдяки цьому забезпечується надійний захист підприємства від внутрішніх і зовнішніх факторів ризику, що, у свою чергу, підвищує його конкурентоспроможність та стійкість до змін у зовнішньому середовищі [1].

Одним із ключових підходів до оцінювання безпеки виступає аналіз ризиків, який дозволяє системно ідентифікувати можливі загрози, оцінити ймовірність їх виникнення та визначити рівень впливу на функціонування підприємства. Ризики можуть мати різноманітну природу: від природних або техногенних катастроф до економічних криз, змін у законодавстві або зростання кіберзлочинності. Застосування аналізу ризиків на практиці є необхідною умовою для отримання обґрунтованих даних, що лежать в

основі прийняття управлінських рішень, а також для створення ефективної системи реагування на загрози.

Не менш важливою методологією є моделювання та симуляція ймовірних сценаріїв розвитку подій, що потенційно можуть призвести до загроз. Створення комп'ютерних моделей, заснованих на актуальних та історичних даних, дозволяє проаналізувати можливі наслідки кризових ситуацій, таких як природні катаклізми, аварії, витoki інформації або цілеспрямовані атаки з боку зловмисників. Завдяки симуляціям підприємство може не лише прогнозувати розвиток ситуації, а й протестувати різні сценарії реагування, визначити найбільш ефективні протоколи дій та заздалегідь сформулювати комплексну стратегію безпеки [2].

Оцінювання ефективності вже впроваджених систем безпеки також є важливим елементом загальної системи захисту. Це стосується як фізичних систем (наприклад, систем відеоспостереження, охоронної сигналізації, обмеження доступу), так і інформаційних технологій, до яких належать системи кіберзахисту, антивірусне програмне забезпечення, шифрування даних тощо. Перевірка дієвості таких систем проводиться за допомогою аудитів, регулярного тестування, пентестингу та інспекцій, що дозволяє виявляти вразливості, попереджати збої та оперативно вдосконалювати захист.

Ще одним інструментом оцінки безпеки підприємства є SWOT-аналіз, який допомагає виявити внутрішні сильні й слабкі сторони, а також зовнішні можливості та загрози. За допомогою цього методу підприємство отримує глибше розуміння свого становища у середовищі та здатне своєчасно адаптуватися до нових викликів. SWOT-аналіз також дозволяє ідентифікувати напрямки для розвитку системи безпеки, підкріпити конкурентні переваги та зменшити вплив чинників ризику [3].

Значну роль у підтримці високого рівня безпеки відіграє регулярний моніторинг і аудит безпекових процесів. Постійний моніторинг забезпечує контроль за станом захищеності підприємства в режимі реального часу, дозволяє вчасно виявляти загрози та оперативно на них реагувати. Аудит, зі свого боку, дає змогу оцінити відповідність внутрішніх процедур і систем міжнародним стандартам, таким як ISO 27001 чи NIST, і виявити прогалини, що потребують усунення [4, 5].

Визначальними у процесі оцінювання стану безпеки виступають індикатори безпеки, серед яких: кількість зафіксованих інцидентів, середній час реагування на загрози, ступінь відповідності внутрішніх політик вимогам стандартів, рівень поінформованості персоналу про політики безпеки тощо. Такі показники є цінним джерелом інформації для аналізу ефективності заходів, своєчасного оновлення стратегій і прийняття рішень на основі реальних даних.

Таким чином, сучасні методи визначення рівня безпеки підприємства є незамінними інструментами для забезпечення сталого функціонування організації в умовах невизначеності. Кожен із методів – чи то аналіз ризиків, симуляція сценаріїв, аудит або SWOT-аналіз – виконує свою унікальну функцію, але всі вони спрямовані на досягнення спільної мети: збереження безперервності бізнесу, захист ресурсів та забезпечення готовності до нових викликів. Раціональне поєднання цих підходів, адаптоване до специфіки конкретного підприємства, дозволяє створити надійну систему управління безпекою, яка відповідає вимогам сучасного ділового середовища.

Список використаних джерел:

1. Гавловська Н., Матюх С., Любохинець Л. Оцінювання стану економічної безпеки промислового підприємства. *Development Service Industry Management*. 2023. № 1. С. 7-12. URL: [https://doi.org/10.31891/dsim-2023-1\(1\)](https://doi.org/10.31891/dsim-2023-1(1)).

2. Кошельок Г. В., Малікова І. П. Методичні підходи до оцінки економічної безпеки підприємства. *Східна Європа: економіка, бізнес та управління*. 2021. В. 5 (32). С. 62-69. URL: https://www.easterneurope-bm.in.ua/journal/32_2021/11.pdf.

3. Шило Ж. С., Кречко М. Ю. Методи оцінки рівня економічної безпеки підприємства: підходи до оцінювання та забезпечення економічної безпеки. *Вісник НУВГП. Серія «Економічні науки*. 2022. Вип. 2 (98). С. 278-288. URL: <https://ep3.nuwm.edu.ua/24406/1/Ve9824%20%281%29.pdf>.

4. Мешкова-Кравченко Н. В., Тарасюк А. В. Оцінка економічної безпеки підприємства. *Вісник ХНТУ*. 2021. №1 (76). С. 204-212. URL: <https://journals.kntu.net.ua/index.php/visnyk/article/view/632/868>.

5. Шило З. Методика комплексної оцінки рівня економічної безпеки підприємства. *Міжнародний науковий журнал менеджменту, економіки та фінансів*. 2022. Вип. 1 (4). С. 17-25.

6. Polozova T., Cherkashina M., Shapoval O., Romanchik T., Alzoubi Laith Abdel Karim Mohammad. Assessment of risks in conditions of provision of security of economic activities of organizations. *Journal of security and sustainability issues*. 2019. № 8 (4). С. 705-714.

7. Polozova T., Stepanenko S., Murzabulatova O., Ponomarov S. Specific of the creation and functioning of the financial and economic security system of business entities. *Український журнал прикладної економіки та техніки*. 2023. Том. 8. № 3. С. 70-77.