УДК 330.131.7

Герасименко О.М., к.е.н., докторант
Черкаський національний університет імені Богдана Хмельницького

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ТА ПРОГРАМНИХ МЕТОДИК ІДЕНТИФІКАЦІЇ, АНАЛІЗУ ТА ОЦІНКИ РИЗИКІВ У ЗАБЕЗПЕЧЕННІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Герасименко О.М. Порівняльний аналіз методів та програмних методик ідентифікації, аналізу та оцінки ризиків у забезпеченні економічної безпеки підприємства. У статті досліджено методи ідентифікації, аналізу та оцінки ризиків згідно з міжнародними стандартами з ризик-менеджменту. Здійснено визначення методів обробки ризиків та можливість їх використання на тому чи іншому етапі роботи з ризиками. Розглянуто загальний підхід до прийняття рішення щодо обробки ризику згідно з IEC/ISO 31010, що можна поділити на три діапазони. Проведено порівняльну характеристику програмних засобів обробки ризику для різних підприємств. Проаналізовано суть програмних методик оцінки ризиків та основну їх характеристику.

Ключові слова: методи аналізу та оцінки, ризики, ризик-менеджмент, економічна безпека, обробка ризику, програмні засоби оцінки ризиків.

Герасименко Е.М. Сравнительный анализ методов и программных методик идентификации, анализа и оценки рисков в обеспечении экономической безопасности предприятия. В статье исследованы методы идентификации, анализа и оценки рисков согласно международным стандартам риск-менеджмента. Осуществлено определение методов обработки рисков и возможность их использования на том или ином этапе работы с рисками. Рассмотрен общий подход к принятию решения по обработке риска согласно IEC/ISO 31010, который можно разделить на три диапазона. Проведена сравнительная характеристика программных средств обработки риска для различных предприятий. Проанализированы суть программных методик оценки рисков и их основная характеристика.

Ключевые слова: методы анализа и оценки, риски, риск-менеджмент, экономическая безопасность, обработка риска, программные средства оценки рисков.

Herasymenko O.M. Comparative analysis of methods and software methods for identifying, analyzing and assessing risks in ensuring economic safety of the enterprise. The article analyzes the methods of identification, analysis and risk assessment in accordance with international risk management standards. The definition of methods of risk processing and the possibility of their use at one or another stage of work with risks. The author considers the general approach to risk decision making according to IEC / ISO 31010, which can be divided into three ranges. A comparative description of software tools for risk management for different enterprises is conducted. The essence of software methodologies for risk assessment and their main characteristics is analyzed.

Key words: methods of analysis and evaluation, risks, risk management, economic security, risk management, software risk assessment tools.

Постановка проблеми. Питання економічної безпеки сьогодні є одним із пріоритетних у державі. Забезпечення економічної стабільності та безпеки держави реалізується через стабілізацію суб'єктів господарської діяльності, що становлять економічне підґрунтя. В умовах геополітичної та економічної нестабільності реальний сектор економіки потерпає від безлічі економічних викликів, дестабілізуючих чинників, небезпек, загроз і ризиків. Для побудови ефективного господарюючого суб'єкта необхідно вчасно адаптовуватися до змінності зовнішнього та внутрішнього середовища з урахуванням інтересів стейкхолдерів. Реалізація забезпечення ризикоорієнтованого управління підприємства для забезпечення економічної безпеки підприємства на практиці здійснюється за допомогою низки методів та програмних засобів з обробки ризиків. Різні техніки, методики, методи та програмні засоби здатні допомогти реалізовувати на практиці процедури ідентифікації, аналізу та оцінки ризиків.

Аналіз останніх досліджень і публікацій. Віддаючи належне науковцям, результати досліджень яких сприяли становленню безпекознавства та ризик-менеджменту як сучасних галузей науки, доцільно зазначити, що нині відсутній теоретичний і апробований практично ризикоорієнтований підхід до управління економічною безпекою підприємств. У дослідженнях і публікаціях вітчизняних учених економіко-управлінський аспект забезпечення економічної безпеки підприємств має фрагментарний характер. Наявні наукові розробки переважно сфокусовані на технічних, інформаційних, силових аспектах забезпечення безпеки, а не на технологіях протидії ризикам та їх імовірним наслідкам.

Постановка завдання. Мета дослідження полягає у систематизації та узагальненні теоретичних даних щодо методів та програмних методик ідентифікації, аналізу та оцінки ризиків підприємств. Для досягнення поставленої мети необхідним є вирішення таких завдань: дослідження методик та підходів у практиці світового ризик-менеджменту; розгляд загального підходу до прийняття рішення щодо обробки ризику; проведення порівняльної характеристики програмних засобів обробки ризику.

Виклад основних результатів. Важливо, щоб форма, метод оцінки та її результат відповідали низці критеріїв: обґрунтованість та відповідність ситуації, представлення результатів у зручному для розуміння та способу обробки вигляді, забезпечення прозорості, відтворення та можливості перевірки. Вибираючи метод для обробки ризику, необхідно враховувати: кількісні та якісні цілі дослідження; ступінь деталізації роботи з ризиком; тип та обсяг аналізованих ризиків; потенційний розмір наслідків; рівень експертизи та необхідних ресурсів; доступність інформації та даних; потребу в майбутньому в модифікації/модернізації оцінки ризиків; будь-які регуляторні та договірні вимоги.

Ресурси та можливості, що можуть вплинути на вибір методу обробки ризику: навички, досвід, здатність та можливості групи, що займається обробкою ризику; обмеження за часом та іншими ресурсами; достатність бюджету, за необхідності потреба у зовнішніх ресурсах. Ризики можуть бути комплексними, як, наприклад, у складних системах, в яких досить часто необхідно оцінювати ризики всієї системи, ніж обробляти кожен компонент окремо, без урахування взаємодії. Непрямий вплив та залежність ризиків повинні бути зрозумілі, щоб забезпечити управління одного ризику без створення неприйнятної ситуації в іншому місці. Розуміння комплексного характеру ризику або сукупності ризиків підприємства є вирішальним під час вибору відповідних методів або технік оцінки ризику.

Таких методик та підходів у практиці світового ризик-менеджменту існує досить багато, розглянемо основні з них, що найбільш застосовні до практики оцінки ризиків вітчизняних підприємств (табл. 1).

Табл. 1 ілюструє методи аналізу та оцінки ризиків на підприємстві та їх застосовність на тому чи іншому етапі роботи з ризиками. Так, позначення SA означає рекомендацію даного методу до застосування, NA – неприйнятність використання методу на даному етапі та A – застосовність методу.

Існують такі ризики, які вимагають принципово індивідуального підходу до оцінки. Розглянуті методи пропонують як загальноприйняті, так і специфічні підходи до оцінки. Істотним приводом для вибору певного методу оцінки є профіль діяльності підприємства. Використання тільки одного методу в оцінці ризиків не дає повної, точної та достовірної інформації, саме тому пропонується застосовувати в сукупності й інші методи для прийняття найбільш ефективного та оптимального рішення.

Оцінка ризиків здійснюється, по-перше, з погляду їх повного впливу для тих ризиків, які є наявними, по-друге, з урахуванням нетто-впливу після застосування методів управління, тобто оцінка залишкових ризиків. Під час оцінки ризиків використовуються дані, отримані в процесі аналізу ризиків для прийняття рішень у майбутньому.

У результаті оцінка ризику може призвести до:

- перегляду цілей;
- прийняття ризику (тобто нічого не застосовується);
- перегляду варіантів обробки ризику (критичності ризику);
- проведення додаткового аналізу для кращого розуміння ризику;
- підтримки наявних заходів контролю.

Загальний підхід до прийняття рішення щодо обробки ризику можна поділити на три діапазони згідно з IEC/ISO 31010 [1]:

- нижній діапазон – рівень ризику вважається незначним або настільки малим, що немає необхідності у заходах із його обробки;

Таблиця 1

Застосовність підходів до оцінки ризиків

Підходи та методики	Процес оцінки ризику				
	Іденти-фікація ризику	Аналіз ризику			Оцінка ризику
		Наслідки	Ймовір-ність	Рівень ризику	
«Мозковий штурм»	SA	NA	NA	NA	NA
Структуроване або напівструктуроване опитування	SA	NA	NA	NA	NA
Метод Делфі	SA	NA	NA	NA	NA
Контрольні листи	SA	NA	NA	NA	NA
Попередній аналіз небезпек (PHA)	SA	NA	NA	NA	NA
Дослідження небезпеки та працездатності (HAZOP)	SA	SA	A	A	A
Аналіз небезпек та критичні контрольні точки (HACCP)	SA	SA	NA	NA	SA
Оцінка екологічного ризику (оцінка токсичності)	SA	SA	SA	SA	SA
Структурована методика «А що, якщо…?» (SWIFT)	SA	SA	SA	SA	SA
Аналіз сценаріїв	SA	SA	A	A	A
Аналіз впливу на діяльність	A	SA	A	A	A
Аналіз початкової причини	NA	SA	SA	SA	SA
Аналіз характеру та наслідки відмов	SA	SA	SA	SA	SA
Аналіз «дерева» несправностей	A	NA	SA	A	A
Аналіз «дерева» подій	A	SA	A	A	NA
Аналіз причини і наслідків	A	SA	SA	A	A
Причинно-наслідковий аналіз	SA	SA	NA	NA	NA
Аналіз рівнів захисту (LOPA)	A	SA	A	A	NA
Аналіз «дерева» рішень	NA	SA	SA	A	A
Аналіз надійності оператора	SA	SA	SA	SA	A
Аналіз схеми «краватка- метелик»	NA	A	SA	SA	A
Технічне обслуговування задля забезпечення надійності	SA	SA	SA	SA	SA
Аналіз паразитних ланцюгів	A	NA	NA	NA	NA
Аналіз Маркова	A	SA	NA	NA	NA
Імітаційне моделювання за допомогою методу Монте- Карло	NA	NA	NA	NA	SA
Байєсова статистика і мережа Байєса	NA	SA	NA	NA	SA
Криві FN	A	SA	SA	A	SA
Показники ризику	A	SA	SA	A	SA
Матриця наслідків і ймовірностей	SA	SA	SA	SA	A
Аналіз витрат та вигід	A	SA	A	A	A
Багатокритеріальний аналіз рішень (MCDA)	A	SA	A	SA	A

Джерело: складено на основі [1]

- середній діапазон – ураховуються витрати та вигоди, при цьому можливості збалансовані з потенційними наслідками;

- верхній діапазон – рівень ризику вважається неприйнятним незалежно від того, які вигоди може принести діяльність, обробка ризику необхідна незалежно від її вартості.

За такого підходу застосовується в практиці забезпечення економічної безпеки система критеріїв ALARP (as low as reasonably practicable). Для визначення пріоритетності ризику можна використовувати показник RPN (Risk priority number) – число пріоритетності ризику як спосіб його оцінки, що використовується в аналізі видів та наслідків відмов.

Окрім вищерозглянутих методик обробки ризику, сьогодні існує досить велика кількість різноманітних програмних продуктів, що дають змогу в електронному вигляді проводити ідентифікацію, аналіз та оцінку ризиків у компанії незалежно від галузі її господарювання. Так, проведено аналітичний огляд таких найрозповсюджених програмних продуктів (табл. 2).

Як і методи обробки ризику, програмні засоби доцільно поділити на методики, що використовують оцінку ризику на якісному рівні, та кількісні методики, згідно з якими ризик оцінюється через числове значення, а також змішані методики, що поєднують елементи двох попередніх. Більшість із програмних методик працює з інформаційними ризиками, створює історичну базу даних для подальших оцінок ризиків, складає картографію ризиків, проводить аналіз та оцінку згідно з міжнародними стандартами з управління ризиками в тій чи іншій сфері. Розглянуті в табл. 2 програмні засоби розраховані як на малі, так і на середні й великого розміру компанії.

Таблиця 2

Порівняльна характеристика програмних засобів обробки ризику

№	Назва методики	Суть методики	Інтернет-сторінка	Компанія-розробник
1.	CRAMM	Одна з перших методик аналізу ризиків у сфері інформаційної безпеки. Метод аналізу та управління ризиками, що є урядовим стандартом Великої Британії та широко розповсюджений у всьому світі. Передбачає комплексний підхід до оцінки ризиків, поєднуючи кількісні та якісні методи оцінки. Універсальний метод для компаній різних галузей та розмірів. Методика не враховує супровідної документації, такої як опис бізнес-процесів або звітів за проведеними оцінками ризиків. У методиці відсутні процес інтеграції способів управління та опис призначення способу; моніторинг ефективності способів управління, що використовуються та способів управління залишковими ризиками; перерахунок максимально допустимих величин ризиків; процес реагування на події. Методика передбачає залучення спеціалістів, тривалість процесу оцінки ризику, трудомісткість та високу вартість ліцензії.	http://www.cramm.com/	Central Computer and Telecommunications Agency (UK), Insight Consulting (Siemens)
2.	vsRisk	Програмне забезпечення для оцінки ризиків інформаційної безпеки відповідно до міжнародних стандартів ISO 27001 та BS 7799-3. Програмний продукт, створений для спрощення процедури оцінки ризиків, містить інтегровану, постійно поновлювану базу даних загроз та небезпек.	https://www.itgovernance.co.uk/	IT Governance, Vigilant Software
3.	RiskWatch	Фактично є американським стандартом у галузі аналізу та управління ризиками. Як критерії для оцінки та управління ризиками використовується прогнозування річних утрат та оцінка ROI. Даний метод може використовуватися, якщо необхідно провести аналіз ризиків на програмно-технічному рівні захисту без обліку організаційних та адміністративних факторів. Перевагою методу є зрозумілий інтерфейс та значна гнучкість самого методу, за рахунок можливості введення нових категорій, питань, описів та ін.	https://www.riskwatch.com/	RiskWatch Inc.
4.	OCTAVE	Методика проведення оцінки ризиків організації вирізняється тим, що весь процес аналізу здійснюється працівниками організації, без залучення зовнішніх консультантів. Для визначення заходів протидії загрозам у методиці пропонуються каталоги засобів. Передбачене також розроблення планів зниження ризиків декількох типів: довготермінові, на середню перспективу, перелік завдань на найближчий час. Документація за даною методикою загальнодоступна та безкоштовна.	https://www.cert.org/octave	Software Engineering Institute Carnegie Mellon University
5.	RA2 art of risk	Методика містить простий процесний підхід. Процес управління ризиками може налаштовуватися під потреби контрактної компанії. Для успішної оцінки та управління ризиками необхідно збирати інформацію з різних джерел у компанії. Також до методики додається спеціальний модуль для зібрання інформації для процесу оцінки ризиків. Після завершення процесу створюється архів для збереження результатів, які можуть використовуватися у майбутньому як історичні дані для подальших оцінок.	http://www.aexis.de/	AEXIS Security Consultants, XiSEC Consultants Ltd
6.	Method-Ware	Методика відповідає австралійському стандарту Australian/New Zealand Risk Management Standard (AS/NZS 4360:1999) і стандарту ISO17799. Методика дає змогу задати модель інформаційної системи з позиції інформаційної безпеки, ідентифікувати ризики, загрози, втрати у разі реалізації подій. Основними етапами роботи є: опис контексту, ідентифікація ризиків, оцінка загроз та можливого збитку, вироблення управлінських заходів та розроблення плану відновлення та дій у надзвичайних ситуаціях.	http://www.methodware	Methodware (Jade Software Corporation)
7.	Microsoft Security Assessment Tool	Методика, пропонована компанією Microsoft, ділить процес оцінки ризиків на етапи: планування, розроблення основи для успішної оцінки ризиків; координований збір даних, збір інформації про ризики; пріоритезація ризиків, ранжування виявлених ризиків на основі повторюваного процесу.	http://www.microsoft.com	Microsoft Corporation
8.	Proteus Enterprise	Методика вміщує засоби контролю відповідності та геп аналізу, оцінку впливу на бізнес, оцінку ризиків, управління безперервністю бізнесу, управління інцидентами, управління активами та організаційними ролями, а також депозитарій політик та засобів планування. Система здатна масштабуватися для великої компанії, також дає змогу проводити онлайн-аудити у внутрішніх підрозділах та у зовнішніх постачальників.	https://proteuscyber.com/	InfoGov

9.	Citicus ONE vR3.2	Методика спрямована на високорівневе управління бізнес-ризиками в галузі інформаційної безпеки. Дає змогу вимірювати ступінь відповідності вимогам законодавства, нормативної бази, стандартів та внутрішніх політик організації. Збір даних за активами, загрозами та вразливостями здійснюється через веб-форми. Методика дає змогу створити карту ризиків, що пов'язує між собою п'ять факторів ризику: слабкі місця контролю, особливі обставини, вплив на бізнес, рівень загрози та критичність активу. Програмний засіб зорієнтований на невеликі організації.	https:// www.citicus.com/	Citicus Limited
10.	Lightwave Security Secure-Aware v3.7.2	Методика включає в себе чотири модулі: політика та обізнаність, відповідність, управління ризиком та управління безперервністю бізнесу. Вона містить набори вимог для оцінки відповідності стандартам ISO 2700x, PCI DSS и CoBIT 4.1. Методика оцінки та обробки ризику сумісна з ISO 27001/27002. Три чинники ризику: вплив на бізнес, небезпеки та загрози оцінюються за допомогою спеціальних опитувальних листів.	http://www. lightwaveps.com/	Lightwave Security

Джерело: складено автором на основі [2–5]

Зазвичай це коштовні програми, передплата на які здійснюється щороку, у рамках якої проводиться протягом року технічна підтримка.

Висновки. Сучасні умови господарювання, в яких функціонують вітчизняні підприємства, призводять до необхідності вдосконалення системи обробки ризиків. Розглянуті методи, методики та програмні засоби ідентифікації, аналізу та оцінки ризиків дають змогу проводити якісну обробку ризиків, побудувати ефективний механізм їх попередження, орієнтований на вирішення проблем стабілізації та розвитку виробничих підприємств, можуть використовуватися як інструментарій під час прийняття рішень та реалізації рішень в управлінні виробництвом.

Список літератури:

1. Національний стандарт України керування ризиком. Методи загального оцінювання ризику (IEC/ISO 31010:2009, IDT) ДСТУ IEC/ISO 31010:2013. URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66723.
2. Баранова Е.К. Методики анализа и оценки рисков информационной безопасности. *Образовательные ресурсы и технологии.* 2015. № 1(9). С. 73–79.
3. Астахов А. Сравнение программных продуктов для управления рисками информационной безопасности. URL: http://iso27000.ru/blogi/aleksandr-astahov/sravnenie-programmnyh-produktov-dlya-upravleniya-riskami-informacionnoi-bezopasnosti.
4. Астахов А. Искусство управления информационными рисками. М.: ДМК Пресс, GlobalTrust, 2009. 312 с.
5. Нестеров С. Методики и программные продукты для оценки рисков. URL: www.intuit.ru.