УДК 004.056

М. Ю. Могила

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДИК ОЦІНЮВАННЯ РИЗИКІВ ДЛЯ ПІДПРИЄМСТВ В ГАЛУЗІ ІТ

Вінницький національний технічний університет

Анотація
В роботі розглянуто представників які досліджували дане питання, найбільш поширених в зазначеній сфері, Проаналізовано існуючі підходи до визначення ризиків підприємств, досліджено методології оцінювання ризиків інформаційної безпеки. Обґрунтовано вибір методу OCTAVE для даної задачі.
Ключові слова: ризики інформаційної безпеки, процесні ризики, методики оцінювання ризиків

Abstract
The paper considers the representatives who researched this issue, the most common in this area, analyzed the existing approaches to determining the risks of enterprises, studied the methodology for assessing the risks of information security. The choice of OCTAVE method for this task is substantiated.
Keywords: risks of information safety, process risks, techniques of an estimation of risks

Вступ

Нині ризики є одними з основних атрибутів функціонування підприємств, а також під час створення автоматизованих систем і їх складових. Важливо зазначити, що більшість проєктів не доходить до стадії експлуатації. Через те потрібно розуміти відмінність між методиками оцінювання ризиків малих та середніх підприємств галузі ІТ.

Метою роботи є дослідження та аналіз методів оцінки ризику на підприємстві, визначення основних переваг та недоліків, та підбір оптимального методу для ІТ-підприємства, та покращити оцінювання ризиків

Виклад основного матеріалу

Насамперед потрібно сказати, що існують два основних методи оцінювання ризиків: кількісний та якісний.

Якісний аналіз ризику передбачає виявлення джерел та причин ризику, етапів та робіт, при виконанні яких виникає ризик, тобто – встановлення потенційних зон ризику; ідентифікацію (встановлення) усіх можливих ризиків; виявлення практичної користі та можливих негативних наслідків, які можуть виникнути у процесі реалізації рішення, що містить ризик[1].

До якісної оцінки ризиків входять такі елементи як: виявлення ризиків, властивих реалізації передбачуваного рішення; визначення кількісної структури ризиків; виявлення найбільш ризико-небезпечних ділянок в розробленому алгоритмі схвалюваного рішення[2].

В той час як метою кількісний метод являє собою отримання числового вираження окремих ризиків із визначенням характеристик ймовірності та можливих втрат[3].

До кількісної оцінки ризиків відносять[4]:

1. Статистичний метод;
2. Метод експертних оцінок;
3. Метод використання аналогів;
4. Метод критичних значень;
5. Метод оцінки ризику за допомогою «дерева рішень»;
6. Аналіз чутливості;
7. Метод аналогії тощо, розберемо декілька з них детальніше.

Статистичний метод являє собою оцінку ризику на основі досліджуваного показника за певний проміжок часу. Недолік даного методу в тому, що він підходить для визначення ризику для тривалого проміжку часу, але на малий відрізок часу він є малоефективним, тому що вихідні дані можуть бути помилковими, а також потребує великої кількості спостережень.

Метод експертних оцінок являє собою припущення певного експерта або групи експертів.

Перевага даного методу полягає в тому, що є можливість використати суб'єктивну думку особи яка оцінює ризик та врахувати певні фактори, в той час це виступає свого роду недоліком тому, що все залежить від професійності та освіченості людини, тобто грає роль сильний суб'єктивний фактор.

Метод оцінки ризику за допомогою «дерева рішень» полягає в ієрархічній структурній схемі ризиків. Перевагою є те, що можливо оцінити різні шляхи усунення або недопущення ризику та вибрати найбільш ефективний спосіб, а недоліком - він є досить енергозатратний.

Метод аналогії полягає в тому, щоб проаналізувати вже відомі раніше ризики які часто виникають на підприємстві, щоб попередити їх повторне виникнення. Недоліком даного методу є те, що багато ризиків мають специфічні особливості, тому він використовується як допоміжним методом поряд з іншими.

Якщо ж брати до уваги ІТ підприємства було б доцільно проаналізувати програмні забезпечення оцінки ризику.

На сьогодні існує велика кількість програм за допомогою яких можна оцінити ризики на підприємстві, одні удосконалюються інші втрачають свою популярність внаслідок неточності вихідних даних.

На нашу думку, одними із популярних на сьогодні програмних забезпечень (методик) оцінки ризиків є:

1. CRAMM
2. OCTAVE
3. NIST

CRAMM – це метод якому притаманний комплексний підхід до оцінки ризиків, тобто в його структуру входить як кількісний, так і якісний підхід до оцінки ризиків, що дає йому низку переваг таких як: підходить для підприємств з різними типами, на виході отримуємо детальний опис усіх ризиків, доволі прийнятна система моделювання ІТ, і що саме головне, він легкий у реалізації.

В той час даний метод потребує багато часу для аналізу ризиків, потрібен висококваліфікований спеціаліст для реалізації даної методики, а також в результаті буде отримано велику кількість звітів.

Метод OCTAVE - це метод оперативної оцінки критичних загроз, активів і вразливостей. Методика передбачає створення групи аналізу, яка вивчає безпеку. Група аналізу (ГА) включає співробітників бізнес-підрозділів, які експлуатують систему, і співробітників відділу інформаційних технологій [5].

В результаті використання даного методу можна отримати наступні показники : опис стратегії безпеки, можливість вибору скорочення ризиків, буде розроблено план їх скорочення.

Даний метод ефективно застосовувати в ІТ-компаніях які часто звертаються до оцінки ризиків на основі регулярних оцінок та готують план способів або засобів для їх зниження.

NIST - це економічно ефективні заходи безпеки для усього життєвого циклу інформаційних систем[6].

Існує три серії документів NIST у сфері безпеки:

− спеціальні публікації NIST SP 800 Комп'ютерна безпека,

− спеціальні публікації NIST SP 500 Технології комп'ютерних систем,

− спеціальні публікації NIST SP 1800 Практичні настанови з кібербезпеки[6].

Перевагами даного методу є:

− простота у використанні;

− можна використовувати для підприємств різних типів

− в результаті буде отримано детальний опис всіх можливих ризиків

− має своє програмне забезпечення.

Недоліками є:

− процес займає багато часу;

− здебільшого використовується у США, тому що адаптовано під дану країну;

− існують певні шкали (триступеневі), тим самим обмежується її можливості.

У методі CRAMM випущений з уваги перегляд величин ризиків після реалізації контрзаходів. У разі якщо потрібно виконати тільки разову оцінку рівня ІТ-ризиків в компанії будь-якого масштабу, його не доцільно застосовувати, він підійде для управління ІТ-ризиками на базі періодичних оцінок на технічному рівні.

Метод OCTAVE доцільно застосовувати в великих компаніях, яким потрібен чіткий алгоритм дій або план заходів, які допоможуть знизити рівень виникнення регулярних ризиків.

Метод NIST - являється найменш точним із вище перечислених методів тому, що значення змінних, оцінюються за трирівневою шкалою. Такий «строгий» механізм отримання оцінок ризику ставить під сумнів точність результатів.

Проаналізувавши дані, та порівнявши методики оцінки ризиків, ми дійшли до висновку, що найбільш раціональним та ефективним методом оцінки ризику на IT-підприємстві буде - метод OCTAVE, тому що підходить як для малих, так і для великих підприємств і враховує сектор IT, має своє програмне забезпечення, а також основною перевагою для нас є те, що даний метод дає змогу зв'язувати цілі та завдання організації з цілями інформаційної безпеки.

Висновки

В результаті роботи було проведено аналіз та порівняння різних методик оцінювання ризиків, що дало змогу визначити найбільш прийнятну методику оцінювання ризику на IT-підприємстві.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Методи якісного аналізу підприємницьких ризиків [Електронний ресурс] — Режим доступу: http://www.dut.edu.ua/uploads/l_50_49235071.pdf (дата звернення: 02.03.2021).
2. Доценко І.О. Якісні методи оцінки ризиків в системі управлінням підприємством / І.О. Доценко // Матеріали міжнародної науково-практичної конференції «Тенденції управління фінансовими та інноваційними процесами в умовах ринкових перетворень». – Вінниця, 2012. – С 283-285.
3. Методичні основи оцінки ризиків підприємницької діяльності [Електронний ресурс] — Режим доступу: http://www.vestnikdnu.com.ua/archive/201154/171-176.pdf (дата звернення: 02.03.2021).
4. Методичне забезпечення оцінки ризиків підприємства [Електронний ресурс] — Режим доступу: https://periodicals.karazin.ua/soceconom/article/download/4813/4366/#:~:text (дата звернення: 02.03.2021).
5. Потий А.В. Методика оценки критических ресурсов, угроз и уязвимостей безопасности информации для малых предприятий (описание и руководство по применению методики: технический отчет). OCTAVE-S / .В. Потий, Ю.А. Избенко, А.В. Леншин и др. – Х. ХНУРЭ, 2006. – Т. 1. – 144 с
6. Реалізація процесного підходу до керування ризиками інформаційної безпеки в документах NIST [Електронний ресурс] — Режим доступу: https://ela.kpi.ua/bitstream/123456789/23949/1/ITS2017.5.2(9)_09.pdf (дата звернення: 02.03.2021).

Могила Мирослава Юріївна — студент групи 1БС-19Мс, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: miroslavam813@gmail.com

Науковий керівник: ***Баришев Юрій Володимирович*** — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: yuriy.baryshev@vntu.edu.ua

Mohyla Myroslava Yuriivna — student of the 1BS-19Ms group, Faculty of Information Technologies and Computer Engineering, Vinnytsa National Technical University, Vinnytsa, e-mail: miroslavam813@gmail.com

Scientific adviser: ***Baryshev Yurii Volodymyrovych*** — PhD (Eng), Associated Professor of Information Protection Department, Vinnytsia National Technical University, Vinnytsia, e-mail: yuriy.baryshev@vntu.edu.ua