УДК 519.71:330(043.2)

Л.М. Радзіховська[1]
Д.Ю. Радзіховський[2]

ОЦІНКА РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЙМОВІРНІСНИМ МЕТОДОМ

[1]Вінницький торговельно-економічний інститут Київського національного торговельно-економічного університету
[2]Вінницький національний технічний університет

Анотація. *У публікації розглянуто особливості ризиків інформаційної безпеки підприємств, оцінку ризиків вказаного виду на основі знаходження математичного очікування втрат.*

Ключові слова: ризик, ймовірнісний метод, інформаційна безпека.

RISK ASSESSMENT OF INFORMATION SECURITY RISKS BY THE PROBABILITY METHOD

Abstract. *The publication considers the features of information security risks of enterprises, risk assessment of this type based on finding the mathematical expectation of losses.*

Keywords: risk, probabilistic method, information security

Нині сучасні підприємства в Україні зазнають ризиків інформаційної безпеки (ІБ). Поняття «інформаційна безпека» включає багато аспектів, трактується дослідниками досить широко, проте, зазвичай під інформаційною безпекою розуміють захищеність інформаційних ресурсів (інформаційних систем підприємств, іншої інформаційної структури і т. ін.) від навмисних або випадкових впливів, що можуть нанести шкоду користувачам цих ресурсів. Зауважимо, що проблеми інформаційної безпеки торкаються всіх рівнів забезпечення інформаційних систем підприємств.

Розглянемо причини виникнення ризиків інформаційної безпеки:

– порушення ІБ відбувається внаслідок впливу стихійних лих (наприклад, потоп, сильний вітер, блискавка, обвал тощо), що непідконтрольні людині;

– соціальні заворушення. Порушення ІБ, яке зумовлене нестабільністю суспільства (наприклад, акти вандалізму, терористичні акти, війни тощо);

– фізичні пошкодження. Порушення ІБ, яке зумовлене навмисним або випадковим фізичним впливом на інформаційну систему або її компоненти (наприклад, вогонь, вода, електростатика, вплив навколишнього середовища (забруднення, пил, корозія, замерзання), руйнування, крадіжка, втрата, невміле поводження з обладнанням / носієм інформації);

– технічні атаки. Порушення ІБ, що зумовлене атакуванням інформаційної системи та використанням її вразливостей в конфігуруванні, протоколах, програмах тощо. Наприклад, мережеве сканування, експлуатація вразливості / бекдору, спроба входу, втручання, відмова в обслуговуванні;

– порушення ІБ через відмову базових компонентів і послуг, що підтримують функціонування системи (наприклад, відмова мережі електроживлення, системи кондиціонування повітря, системи водопостачання);

– технічний збій. Порушення ІБ, спричинене відмовами системи захисту інформації або пов’язаними з нею нетехнічними можливостями. До такого типу ризиків зараховують апаратний, програмний збій, перевантаження, порушення ремонтоздатності [1].

Серед основних завдань забезпечення інформаційної безпеки підприємства (своєчасне виявлення та реагування на загрози при використанні інформаційних систем; створення технологічної та матеріальної бази інформаційної забезпеченості підприємства; координація діяльності суб'єктів в забезпеченні інформаційної безпеки та ін.) одним з найважливіших є завдання оцінки, аналізу та управління ризиками її порушення. Зазвичай ризик при цьому означають як ймовірність реалізації загрози інформаційній безпеці.

Отже, розглянемо, як можливо здійснити оцінку ризиків інформаційної безпеки ймовірнісним методом.

Зауважимо при цьому, що аналізу ризиків інформаційної безпеки присвячено досить мало праць сучасних науковців. Маються на увазі як праці, присвячені визначенню ймовірностей вказаних ризиків,

так і праці, присвячені вивченню наслідків такого виду ризиків. А саме, ризики інформаційної безпеки вивчали Ю. Герасим, Л. Єжова, В. Ромака, М. Рибій.

Оцінка ризиків інформаційної безпеки складається з таких етапів:

– визначення переліку об'єктів, що потребують захисту, інформаційною службою підприємства;

– формування повної множини загроз інформації;

– аналіз і вибір переліку загроз, з огляду на особливості функціонування підприємства;

– виявлення можливих джерел цих загроз;

– визначення імовірності здійснення потенційних загроз із використанням експертної оцінки;

– оцінка можливих збитків в разі здійснення ідентифікованих загроз [2].

Відомо, що ситуація ризику має місце тоді, коли є можливість кількісно і якісно визначити ймовірність настання тієї чи іншої події (ситуацію ризику, можна розглядати як різновид невизначеності, коли настання події ймовірне і може бути визначене).

Так, при кількісному оцінюванні ризику традиційно застосовують наступні головні інструменти: ймовірність появи випадкової величини (P); математичне очікування досліджуваної випадкової величини (M); дисперсія (D); стандартне (середньоквадратичне) відхилення (σ); коефіцієнт варіації.

Для прийняття рішення потрібно знати величину (ступінь) ризику, що вимірюється двома критеріями:

1) середнє очікуване значення (математичне очікування);

2) коливання (мінливість) можливого результату.

Для визначення числового значення ймовірності втрат різних рівнів, як правило, застосовують ймовірнісний підхід. Для оцінки ймовірності втрат необхідно мати дані про діяльність суб'єкта за певний період часу. За наявними даними (проміжок часу фіксується) розраховуються наступні числові характеристики: статистичні ймовірності втрат всіх наявних рівнів. Таким чином, вибір рішення за умов ризику припускає, що ймовірності можливих варіантів обстановки відомі. Ці ймовірності визначаються на основі статистичних даних, а при їх відсутності – на основі експертних оцінок.

Що стосується ризиків інформаційної безпеки, то слід відмітити, що в Україні, на жаль, не проводиться системна аналітична робота по збору статистичних даних про загрози в інформаційній сфері, на основі яких можна визначити потрібні ймовірності та вагові коефіцієнти. Проте, таку інформацію можливо отримати, систематизувати та використовувати, аналізуючи діяльність даного конкретного підприємства чи його аналогів на ринку.

Зауважимо, що у країнах з високорозвиненою інформаційною культурою для оцінки ризиків (у тому числі і інформаційної безпеки) застосовують статистичні показники, вивірені дані, отримані в результаті незалежного аудиту. Так, в США відповідну статистичну інформацію надають правоохоронні органи, міністерство юстиції, IT-компанії, що працюють у сфері інформаційної безпеки.

Отже, за основу ймовірнісного методу аналізу ризику в теорії ризиків береться розрахунок математичного очікування втрат різних рівнів при здійсненні певного виду діяльності.

При здійсненні аналізу ризиків інформаційної безпеки така оцінка розроблена Л.Єжовою і виглядає наступним чином.

Нехай IT-система складається з n структурних елементів: i=1,2,…, n.

Множина загроз інформаційної безпеки щодо елементів системи (j=1,2,…, m):

x_{ij} – втрати системи від здійснення j-ої загрози інформаційної безпеки до i-го елемента.

p_{ij} – ймовірність здійснення j-ої загрози інформаційної безпеки до i-го елемента.

Далі будуємо матрицю втрат системи.

Матриця втрат системи *Таблиця 1*

Загрози \ Об'єкти	1	2	…	m	
1	x_{11}	x_{12}	…	x_{1m}	x_1
2	x_{21}	x_{22}	…	x_{2m}	x_2
…	…	…	…	…	…
n	x_{n1}	x_{n2}	…	x_{nm}	x_n
	y_1	y_2	…	y_m	

x_i=$\sum_{j=1}^{m} x_{ij}$ — максимально можливі втрати і-го об′єкта від загроз.

y_j=$\sum_{i=1}^{n} x_{ij}$ — максимально можливі втрати системи від j-ої загрози.

Також потрібно побудувати матрицю ймовірностей втрат системи.

Як ми наголошували вище, для визначення відповідних ймовірностей можна залучити експертів з інформаційної безпеки (тоді ймовірності обчислюються експертним методом) або зібрати статистику відповідних загроз за певні попередні періоди діяльності підприємства або його аналогів (статистичний шлях знаходження ймовірностей).

Матриця ймовірностей втрат системи *Таблиця 2*

Загрози \ Об'єкти	1	2	…	m
1	p_{11}	p_{12}	…	p_{1m}
2	p_{21}	p_{22}	…	p_{2m}
…	…	…	…	…
n	p_{n1}	p_{n2}	…	p_{nm}

Тоді математичне очікування втрат і-го об'єкта обчислюється так: M(x_i)=$\sum_{j=1}^{m} x_{ij} p_{ij}$. А саме, M($x_i$) — середнє значення можливих втрат і-го об'єкта від здійснення всіх інформаційних загроз.

Математичне сподівання втрат системи від j-ої загрози дорівнює M(y_i)=$\sum_{i=1}^{n} x_{ij} p_{ij}$, а саме, M($y_i$) — середнє значення сукупних втрат системи від j-ої загрози [2].

Розглянута оцінка ризиків інформаційної безпеки на основі знаходження математичного очікування втрат є прикладом застосування класичної схеми оцінювання ризиків саме до ризиків вказаного виду. Вона може бути взята за основу і удосконалена з урахуванням специфіки ризиків інформаційної безпеки.

Таким чином, проблеми оцінки, аналізу ризиків інформаційної безпеки нині є досить актуальними і потребують розв'язання не лише на рівні окремих підприємств, організацій, а й на регіональному та державному рівнях. Також важливим є формування заходів по зниженню та мінімізації ризиків інформаційної безпеки та управління ними, оскільки нехтування вказаним видом ризиків може привести до зниження прибутків, а в найгіршому випадку і до банкрутства підприємств. Отже, подальші дослідження потрібно проводити не лише у галузі вдосконалення способів оцінки ризиків інформаційної безпеки, а й покращення методів зниження та управління ними. Тобто, варто розглянути особливості розподілу, диверсифікації, страхування ризиків інформаційної безпеки.

. СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Lviv Polytechnic National University Institutional Repository [Електронний ресурс] – Режим доступу до ресурсу: http://ena.lp.edu.ua
2. Єжова Л.С. Економічні аспекти ризиків інформаційної безпеки. Сучасна спеціальна техніка. 2011. №3 (26). С. 80-91.

Радзіховська Лариса Миколаївна, кандидат педагогічних наук, доцент, доцент кафедри економічної кібернетики та інформаційних систем, Вінницький торговельно-економічний інститут КНТЕУ, Вінниця, e-mail: larirad@ukr.net

Радзіховський Дмитро Юрійович — студент групи 2БС-18Б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: Dimaradvin@gmail.com.

Radzikhovska Larysa Mykolayivna*, Candidate of Pedagogical Sciences, Associate Professor, Associate Professor of the Department of Economic Cybernetics and Information Systems, Vinnytsia Institute of Trade and Economics KNTEU, Vinnytsia, e-mail: larirad@ukr.net*

Radzikhovskiy Dmytro Y.— Department of Information Techologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, email : Dimaradvin@gmail.com.