Вісник ЛДУБЖД
Bulletin of Lviv State University of Life Safety
https://journal.ldubgd.edu.ua/index.php/Visnuk
ISSN 2078-4643 (print), ISSN 2708-1389 (online)

UDC 004.056.5
DOI: 10.32447/20784643.26.2022.06

This article is an Open Access article distributed under the terms and conditions of the Creative Commons Attribution 4.0 (CC BY 4.0) License (http://creativecommons.org/licenses/by/4.0/).

Л. Ф. Дзюба, О. Ю. Чмир
Львівський державний університет безпеки життєдіяльності, м. Львів, Україна
ORCID: https://orcid.org/0000-0002-4261-6490 – Л. Ф. Дзюба
https://orcid.org/0000-0002-6340-9888 – О. Ю. Чмир
lidadz111@gmail.com

ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ З ВИКОРИСТАННЯМ МЕТОДІВ МАТЕМАТИЧНОЇ СТАТИСТИКИ

Анотація. Інформаційна безпека підприємств для забезпечення конфіденційності, цілісності та доступності інформації є невід'ємною частиною успішної бізнес-діяльності. Результатом реалізації ризиків у сфері інформаційної безпеки для підприємств малого та середнього бізнесу може бути припинення або уповільнення бізнес процесів, втрата конкурентної переваги, збиток для бренду та втрата репутації, судові розгляди та позови. Також збиток підприємства може полягати у втраті клієнтів та прибутку, зниженні вартості бізнесу, витрат на усунення наслідків, штрафи та санкції регулюючих органів. Для організацій та підприємств малого та середнього бізнесу проблеми оцінювання та управління ризиками інформаційної безпеки є надзвичайно актуальними. Тому метою роботи є моделювання інформаційних ризиків підприємства малого бізнесу на підставі порівняння загроз та вразливостей для його інформаційної безпеки з використанням елементів SWOT-аналізу. Для досягнення мети розроблено перелік запитань стосовно загроз та вразливостей інформаційної безпеки підприємства для проведення інтерв'ю з експертами. Перелік загроз містив сім позицій: зовнішні атаки на інформаційні активи підприємства, навмисну некоректну експлуатацію, крадіжки бізнес-інформації, збої в роботі, порушення надання послуг унаслідок стихійних лих, ненавмисну неправильну експлуатацію та непередбачені наслідки від змін. До переліку шести вразливостей включено відсутності системи аварійного електропостачання, відсутність системи регулярного резервного копіювання; двофакторної автентифікації; плинність кадрів (часта зміна персоналу); недостатній рівень фахової підготовки користувачів; ненавмисний витік бізнес-інформації. Узгодженість думок експертів стосовно загроз та вразливостей оцінено коефіцієнтом конкордації Кендалла. Результати експертних оцінок інформаційної безпеки опрацьовано методом попарних порівнянь. Ітераційний алгоритм цього методу реалізовано в середовищі Excel. На підставі векторів коефіцієнтів відносної важливості загроз та коефіцієнтів відносної важливості вразливостей побудовано порівняльну матрицю загроз та вразливостей для підприємства. Матриця загроз та вразливостей є підгрунттям для прийняття управлінських рішень на підприємстві.

Ключові слова: загрози, вразливості, SWOT-аналіз, експертні оцінки, метод попарних порівнянь.

L. F. Dziuba, O. Y. Chmyr
Lviv State University of Life Safety

ASSESSMENT OF INFORMATION SECURITY RISKS USING METHODS OF MATHEMATICAL STATISTICS

Annotation. Information security of enterprises to ensure confidentiality, integrity and availability of information is an integral part of successful business activity. As a result of the implementation of risks in the field of information security for small and medium-sized businesses, business processes may be stopped or slowed down, loss of competitive advantage, damage to the brand and loss of reputation, court proceedings and lawsuits. Also, the loss of the enterprise may consist of the loss of customers and profits, a decrease in the value of the business, the costs of eliminating the consequences, fines and sanctions of regulatory authorities. For organisations and enterprises of small and medium-sized businesses, the problems of assessment and management of information security risks are extremely relevant. Therefore, the purpose of the work is to model the information risks of a small business enterprise based on the comparison of threats and vulnerabilities for its information security using the elements of SWOT analysis. To achieve the goal, a list of questions regarding threats and vulnerabilities of the company's information security has been developed for conducting interviews with experts. The list of threats contained seven items: external attacks on the company's information assets, intentional incorrect exploitation, theft of business information, disruptions in work, disruption of service provision due to natural disasters, unintentional incorrect exploitation and unforeseen consequences from changes. The list of six vulnerabilities includes the absence of an emergency power supply system, the absence of a regular backup system; two-

factor authentication; staff turnover (frequent staff turnover); insufficient level of professional training of users; inadvertent leakage of business information. The consistency of experts' opinions regarding threats and vulnerabilities was assessed by Kendall's concordance coefficient. The results of expert evaluations of information security were processed by the method of pairwise comparisons. The iterative algorithm of this method is implemented in Excel. Based on the vectors of the coefficients of the relative importance of threats and the coefficients of the relative importance of vulnerabilities, a comparative matrix of threats and vulnerabilities for the enterprise was built. The matrix of threats and vulnerabilities is the basis for making management decisions at the enterprise.

Keywords: *threats, vulnerabilities, SWOT analysis, expert assessments,* method of pairwise comparisons.

Вступ (Introduction)

Інтенсивний розвиток інформаційних технологій у сучасному світі зумовлює неабияку увагу до стану інформаційної безпеки. В [1] зазначено, що стан інформаційної безпеки визначається як стан захищеності систем обробки й зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення (у цьому значенні частіше використовують термін «захист інформації»). Загалом для держави [2] інформаційна безпека характеризується ступенем захищеності й, отже, стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості та ін.) стосовно небезпечних (дестабілізаційних, деструктивних, суперечних інтересам країни тощо) інформаційних впливів, причому як до впровадження, так і до вилучення інформації.

Як наголошено в роботі [3], сучасний бізнес зазнає ризиків інформаційної безпеки, що динамічно змінюються. У роботі [4] зазначено, що підхід, заснований на аналізі інформаційних ризиків організації, є найбільш значним для практики забезпечення інформаційної безпеки. Для того, щоб зберегти конкурентоспроможність підприємства, необхідно впроваджувати економічно обґрунтовані заходи захисту цінних інформаційних активів. На стані інформаційної безпеки позначаються такі чинники, як постійне збільшення кількості електронних злочинів, жорсткі й часто змінювані вимоги з боку держави та регуляторів, посилення залежності бізнесу від безперебійної роботи інформаційної системи підприємства.

У роботі [5] досліджено детермінанти виникнення кіберризиків та їх негативний вплив на світову та національну економіки. Якщо великі підприємства мають потужні спеціалізовані відділи з інформаційних технологій, що займаються захистом інформації, то підприємства малого та середнього бізнесу потерпають від витоку, крадіжок, втрат, спотворення, підробок, знищення, копіювання та блокування інформації [6].

У роботі [7] зазначено, що організації малого та середнього бізнесу дедалі більше залежать від інформаційних систем, що робить їх уразливими до витоку даних унаслідок кібератак і комп'ютерних вірусів, втрати даних через людський чинник або збої у роботі носіїв інформації. Згідно з [7], наслідками реалізації ризиків у сфері інформаційної безпеки для підприємств малого та середнього бізнесу є припинення або уповільнення бізнес-процесів, втрата конкурентної переваги, збиток для бренду та втрата репутації, судові розгляди та позови. Окрім того, збиток підприємства може полягати у втраті клієнтів та прибутку, зниженні вартості бізнесу, витрат на усунення наслідків, штрафи та санкції регулюючих органів. Тому для організацій та підприємств малого та середнього бізнесу проблеми оцінювання та управління ризиками інформаційної безпеки з кожним днем стають дедалі актуальнішими.

Відповідно до [8], ризик інформаційної безпеки – це числова (словесна) функція, яка описує ймовірність втілення загроз інформаційній безпеці та величину збитку від їх реалізації внаслідок використання цими загрозами уразливостей активів з метою завдання шкоди організації. Оцінювання ризиків загалом, незалежно від сфери діяльності, є упорядкованим процесом, що складається з певних етапів [9]. Такими етапами є: ідентифікація ризику, аналіз ризику та оцінювання ризику. На кожному з етапів загального оцінювання ризику можливим є використання різних методів або їх поєднання [9]. Для дослідження ризиків інформаційної безпеки використовують кількісні та якісні методи [10]. Вибір певного методу на відповідному етапі дослідження ризику регламентується його ефективністю. На етапі ідентифікації ризику використовують метод SWOT-аналізу. За допомогою цього методу в [1] виконано аналіз сильних і слабких сторін інформаційної безпеки України, виокремлено можливості подальшого її удосконалення та досліджено наявні загрози. В [11] зазначено, що SWOT-аналіз є інструментом стратегічного планування, який використовується для оцінки сильних і слабких сторін підприємства або організації. За допомогою SWOT-аналізу в [12] досліджено тенденції впровадження змішаного навчання в освітній процес закладів

вищої освіти. Технологію проведення SWOT-аналізу для дослідження ризиків інформаційної безпеки описано в роботі [6]. Однак у цій роботі матриця чотирьох елементів, якими є сильні та слабкі сторони підприємства, можливості та загрози стосовно інформаційної безпеки, містить лише по три складники кожного з цих елементів.

Отже, зважаючи на актуальність проблеми захисту інформації, **метою** роботи є моделювання інформаційних ризиків підприємства малого бізнесу на підставі порівняння загроз та вразливостей для його інформаційної безпеки з використанням елементів SWOT-аналізу. Завдання, які потрібно вирішити для досягнення мети: розробити для проведення інтерв'ю з експертами перелік запитань стосовно загроз та вразливостей інформаційної безпеки підприємства; опрацювати результати експертних оцінок методом математичної статистики та отримати матрицю поєднання загроз та вразливостей, яка може бути підгрунттям для прийняття управлінських рішень на підприємстві.

Методи досліджень (Methods)

Для дослідження інформаційної безпеки підприємства малого бізнесу та якісної оцінки інформаційних ризиків використано метод інтерв'ю для опитування експертів та метод SWOT-аналізу. Елементи матриці SWOT-аналізу на підставі опитування експертів розраховано методом попарних порівнянь.

Результати досліджень (Results)

Для комплексної оцінки загроз інформаційній безпеці застосовано метод SWOT-аналізу, який подають [6, 8, 11] у вигляді матриці, що містить елементи: ***S*** (strengths) – сильні сторони підприємства; ***W*** (weaknesses) – слабкі сторони (вразливості) підприємства; *O* (opportunities) – можливості та ***T*** (threats) – загрози для підприємства. Оскільки в роботі досліджено загрози для інформаційної безпеки підприємства та його вразливості, то для опитування експертів розроблено переліки семи загроз ***T*** та шести вразливостей ***W***. До загроз конфіденційності, цілісності та доступності інформації віднесено:

– $\boldsymbol{T_1}$ – зовнішні атаки на інформаційні активи підприємства, що можуть викликати відмову в обслуговуванні та полягати у: зламі ключів і паролів; несанкціонованих спробах доступу та модифікацій мережевого трафіка; перехопленні повідомлень; поширенні комп'ютерних вірусів та спамів; впровадженні шкідливого коду та троянських програм; соціальній інженерії; виконанні зловмисного сканування та зламі веб-сайту підприємства;

– $\boldsymbol{T_2}$ – навмисну некоректну експлуатацію, яка полягає: в отриманні несанкціонованого доступу до інформаційної системи; використанні системи з метою порушення роботи та з метою шахрайства; розкритті інформації, що використовується для входу в систему та бізнес інформації; завантаженні або відправці повідомлень неадекватного змісту; у зміні або додаванні транзакцій, файлів або баз даних; у зміні системних привілеїв без авторизації; у зміні або установці програмного забезпечення (ПЗ) без авторизації; у встановленні недозволеного ПЗ;

– $\boldsymbol{T_3}$ – крадіжки: бізнес інформації; комп'ютерного обладнання; ПЗ; інформації для автентифікації; інформації для ідентифікації особистості та порушення авторських прав на програмне забезпечення;

– $\boldsymbol{T_4}$ – збої в роботі: застосунків, розроблених підприємством та закуплених у сторонніх постачальників; системного ПЗ та комп'ютерного чи мережевого обладнання;

– $\boldsymbol{T_5}$ – порушення надання послуг унаслідок: пошкодження обчислювального центру; втрати обчислювальної техніки або комунікаційних каналів чи послуг; втрати допоміжного обладнання; втрати електроживлення; перевантаження системи або стихійного лиха;

– $\boldsymbol{T_6}$ – ненавмисну неправильну експлуатацію, яка полягає у помилках користувачів або адміністраторів;

– $\boldsymbol{T_7}$ – непередбачені наслідки від змін: бізнес-процесів; ПЗ; бізнес-інформації; в комп'ютерному або комунікаційному устаткуванні.

До вразливостей інформаційної системи підприємства віднесено:

– $\boldsymbol{W_1}$ – відсутність системи аварійного електропостачання;

– $\boldsymbol{W_2}$ – відсутність системи регулярного резервного копіювання;

– $\boldsymbol{W_3}$ – відсутність двофакторної автентифікації;

– $\boldsymbol{W_4}$ – плинність кадрів (часта зміна персоналу);

– $\boldsymbol{W_5}$ – недостатній рівень фахової підготовки користувачів;

– $\boldsymbol{W_6}$ – ненавмисний витік бізнес-інформації.

Для подальшого аналізування інформаційних ризиків створено експертну групу (надалі – експерти ***E***) з осіб, які компетентні в питаннях виробничої діяльності підприємства та знайомі з основами інформаційної безпеки. За рекомендаціями [13] оптимальна чисельність групи становить 7-8 осіб. Учасники експертної групи з 7 осіб (надалі $\boldsymbol{E_1}$ – $\boldsymbol{E_7}$) розташували за пріоритетом загрози ***T*** та вразливості ***W*** інформаційної безпеки підприємства.

Результати опитування експертів відповідно до переліку загроз ***T*** подано у табл. 1.

Експерти розташували загрози в порядку зменшення небезпеки впливу на інформаційну безпеку підприємства. Порядковий номер 1 отримує найнебезпечніша на думку експерта ***E*** загроза, найменш небезпечна номер 7.

Таблця 1

Експертні оцінки загроз T

	E_1	E_2	E_3	E_4	E_5	E_6	E_7
T_1	1	3	2	3	3	3	6
T_2	2	2	4	2	4	2	7
T_3	3	1	5	1	2	1	4
T_4	4	6	6	5	6	4	3
T_5	5	5	1	4	1	5	5
T_6	7	7	3	7	7	7	1
T_7	6	4	7	6	5	6	2

Узгодженість міркувань експертів стосовно загроз інформаційної безпеки підприємства оцінено за допомогою коефіцієнта конкордації Кендалла [13], який становить 0,306, відповідно до даних табл. 1.

Для опрацювання експертних оцінок загроз використано метод попарних порівнянь. Цей метод визначає порядок розміщення загроз з огляду їхньої переваги за допомогою попарного порівняння. Згідно з цим методом, на підставі експертних оцінок (табл. 1) побудовано матриці попарних порівнянь загроз A_r, $r=\overline{1,7}$. Елементи матриць визначено так [12]:

$$A_r=(a_{ij}^r)=\begin{cases}1, & якщо\ \ T_i^r>T_j^r,\\ 0{,}5, & якщо\ \ T_i^r\approx T_j^r,\\ 0, & якщо\ \ T_i^r<T_j^r,\end{cases} \quad (1)$$

де: r – номер експерта, $i,j=\overline{1,7}$ – номери загроз, T_i^r – значення T_i - ої загрози E_r - го експерта.

На підставі (1) з урахуванням даних табл. 1 матриці попарних порівнянь загроз за відповідями семи експертів мають вигляд

$$A_1=\begin{pmatrix}0{,}5&1&1&1&1&1&1\\0&0{,}5&1&1&1&1&1\\0&0&0{,}5&1&1&1&1\\0&0&0&0{,}5&1&1&1\\0&0&0&0&0{,}5&1&1\\0&0&0&0&0&0{,}5&0\\0&0&0&0&0&1&0{,}5\end{pmatrix},\quad A_2=\begin{pmatrix}0{,}5&0&0&1&1&1&1\\1&0{,}5&0&1&1&1&1\\1&1&0{,}5&1&1&1&1\\0&0&0&0{,}5&0&1&0\\0&0&0&1&0{,}5&1&0\\0&0&0&0&0&0{,}5&0\\0&0&0&1&1&1&0{,}5\end{pmatrix},$$

$$A_3=\begin{pmatrix}0{,}5&1&1&1&0&1&1\\0&0{,}5&1&1&0&0&1\\0&0&0{,}5&1&0&0&1\\0&0&0&0{,}5&0&0&1\\1&1&1&1&0{,}5&1&1\\0&1&1&1&0&0{,}5&1\\0&0&0&0&0&0&0{,}5\end{pmatrix},\quad A_4=\begin{pmatrix}0{,}5&0&0&1&1&1&1\\1&0{,}5&0&1&1&1&1\\1&1&0{,}5&1&1&1&1\\0&0&0&0{,}5&0&1&1\\0&0&0&1&0{,}5&1&1\\0&0&0&0&0&0{,}5&0\\0&0&0&0&0&1&0{,}5\end{pmatrix},$$

$$A_5=\begin{pmatrix}0{,}5&1&0&1&0&1&1\\0&0{,}5&0&1&0&1&1\\1&1&0{,}5&1&0&1&1\\0&0&0&0{,}5&0&1&0\\1&1&1&1&0{,}5&1&1\\0&0&0&0&0&0{,}5&0\\0&0&0&1&0&1&0{,}5\end{pmatrix},\quad A_6=\begin{pmatrix}0{,}5&0&0&1&1&1&1\\1&0{,}5&0&1&1&1&1\\1&1&0{,}5&1&1&1&1\\0&0&0&0{,}5&1&1&1\\0&0&0&0&0{,}5&1&1\\0&0&0&0&0&0{,}5&0\\0&0&0&0&0&1&0{,}5\end{pmatrix},$$

$$A_7=\begin{pmatrix}0{,}5&1&0&0&0&0&0\\0&0{,}5&0&0&0&0&0\\1&1&0{,}5&0&1&0&0\\1&1&1&0{,}5&1&0&0\\1&1&0&0&0{,}5&0&0\\1&1&1&1&1&0{,}5&1\\1&1&1&1&1&0&0{,}5\end{pmatrix}.$$

Далі побудовано матрицю X_T математичних сподівань оцінок кожної з загроз, елементи якої визначено так [13]:

$$X_T = (x_{ij}) = \frac{1}{2} + \frac{m_{ij} - m_{ji}}{2m}, \quad (2)$$

де m_{ij} – кількість експертів, які надали перевагу загрозі T_i над загрозою T_j, m_{ji} – кількість експертів, які надали перевагу загрозі T_j над загрозою T_i, $m = 7$ – кількість експертів, причому $x_{ij} + x_{ji} = 1$. Матриця математичних сподівань оцінок загроз має вигляд:

$$X_T = \begin{pmatrix} \frac{1}{2} & \frac{4}{7} & \frac{2}{7} & \frac{6}{7} & \frac{4}{7} & \frac{6}{7} & \frac{6}{7} \\ \frac{3}{7} & \frac{1}{2} & \frac{2}{7} & \frac{6}{7} & \frac{4}{7} & \frac{5}{7} & \frac{6}{7} \\ \frac{5}{7} & \frac{5}{7} & \frac{1}{2} & \frac{6}{7} & \frac{5}{7} & \frac{5}{7} & \frac{6}{7} \\ \frac{1}{7} & \frac{1}{7} & \frac{1}{7} & \frac{1}{2} & \frac{3}{7} & \frac{5}{7} & \frac{4}{7} \\ \frac{3}{7} & \frac{3}{7} & \frac{2}{7} & \frac{4}{7} & \frac{1}{2} & \frac{6}{7} & \frac{5}{7} \\ \frac{1}{7} & \frac{2}{7} & \frac{2}{7} & \frac{2}{7} & \frac{1}{7} & \frac{1}{2} & \frac{3}{7} \\ \frac{1}{7} & \frac{1}{7} & \frac{1}{7} & \frac{3}{7} & \frac{2}{7} & \frac{4}{7} & \frac{1}{2} \end{pmatrix} \quad (3)$$

За допомогою матриці (3) визначено коефіцієнти відносної важливості загроз, тобто сформовано деякий вектор $k_T = [k_1 \quad k_2 \quad k_3 \quad k_4 \quad k_5 \quad k_6 \quad k_7]^T$, який відшукано на підставі ітераційного алгоритму [13]:

1. Початкова умова: $t = 0$, $k_T^{[0]} = (\underbrace{1 \quad 1 \quad \ldots \quad 1}_{m})^T$.

2. Рекурентні співвідношення: $k_T^{[t]} = \frac{1}{\lambda_T^{[t]}} \cdot Y_T^{[t]}$, $\lambda_T^{[t]} = (\underbrace{1 \quad 1 \quad \ldots \quad 1}_{m}) \cdot Y_T^{[t]}$, де: $Y_T^{[t]} = X_T \cdot k_T^{[t-1]}$; $t = \overline{1,m}$, X_T – матриця, елементи якої є математичним сподіванням оцінок кожної з пар загроз, $k_T^{[t]}$ – вектор порядку *t*, побудований із коефіцієнтів відносної важливості даних загроз, $\sum_{i=1}^{m} k_{T,i}^{[t]} = 1$ – умова нормування.

3. Ознакою закінчення алгоритму є умова: $\max | k_T^{[t]} - k_T^{[t-1]} | < E$, де E – задана точність.

У виконаному дослідженні задано точність закінчення алгоритму $E = 0,001$. Відповідно до описаного ітераційного алгоритму виконано декілька кроків до досягнення ознаки його закінчення.

Крок 0. Припускаємо, що

$$k_T^{[0]} = (1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1)^T.$$

Крок 1.

$$Y_T^{[1]} = X_T \cdot k_T^{[0]} = \frac{1}{14}(63 \quad 59 \quad 71 \quad 37 \quad 53 \quad 29 \quad 31)^T;$$

$$\lambda_T^{[1]} = (1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1) \cdot Y_T^{[1]} = 24,5;$$

$$k_T^{[1]} = \frac{1}{\lambda_T^{[1]}} \cdot Y_T^{[1]} \approx (0,184 \quad 0,172 \quad 0,207 \quad 0,108 \quad 0,155 \quad 0,085 \quad 0,09)^T$$

Крок 2.

$$Y_T^{[2]} = X_T \cdot k_T^{[1]} \approx (0,58 \quad 0,542 \quad 0,698 \quad 0,313 \quad 0,488 \quad 0,268 \quad 0,264)^T$$

$$\lambda_T^{[2]} = (1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1) \cdot Y_T^{[2]} \approx 3,153;$$

$$k_T^{[2]} = \frac{1}{\lambda_T^{[2]}} \cdot Y_T^{[2]} \approx (0,184 \quad 0,172 \quad 0,221 \quad 0,099 \quad 0,155 \quad 0,085 \quad 0,084)^T$$

Після другого кроку перевіряємо закінчення алгоритму за умовою заданої точності:

$$\max | k_T^{[2]} - k_T^{[1]} | < 0,001,$$

$$\max(|0,184-0,184|,|0,172-0,172|,|0,221-0,207|,|0,099-0,108|,|0,155-0,155|,$$
$$|0,085-0,085|,|0,084-0,09|) \approx 0,014 > 0,001.$$

Оскільки умову не виконано, продовжуємо наступні кроки.

Крок 3.

$$Y_T^{[3]} = X_T \cdot k_T^{[2]} \approx (0,572 \quad 0,534 \quad 0,693 \quad 0,307 \quad 0,483 \quad 0,268 \quad 0,26)^T$$

$$\lambda_T^{[3]} = (1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1) \cdot Y_T^{[3]} \approx 3,115;$$

$$k_T^{[3]} = \frac{1}{\lambda_T^{[3]}} \cdot Y_T^{[3]} \approx (0,183 \quad 0,171 \quad 0,222 \quad 0,099 \quad 0,155 \quad 0,086 \quad 0,083)^T$$

Знову перевіряємо умову закінчення алгоритму:

$$\max | k_T^{[3]} - k_T^{[2]} | = \max(|0,183-0,184|,|0,171-0,172|,|0,222-0,221|,|0,099-0,099|,$$
$$|0,155-0,155|,|0,086-0,085|,|0,083-0,084|) \approx 0,001.$$

Оскільки умову не виконано, то потрібен ще один крок.

Крок 4.

$$Y_T^{[4]} = X_T \cdot k_T^{[3]} \approx (0,571 \quad 0,534 \quad 0,693 \quad 0,307 \quad 0,483 \quad 0,268 \quad 0,26)^T$$

$$\lambda_T^{[4]} = (1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1) \cdot Y_T^{[4]} \approx 3,115;$$

$$k_T^{[4]} = \frac{1}{\lambda_T^{[4]}} \cdot Y_T^{[4]} \approx (0,183 \quad 0,171 \quad 0,222 \quad 0,099 \quad 0,155 \quad 0,086 \quad 0,083)^T$$

Алгоритм завершуємо, оскільки

$$\max | k_T^{[4]} - k_T^{[3]} | < 0,001.$$

Таким чином, за груповану оцінку ступеня впливу на результат можна взяти вектор коефіцієнтів відносної важливості загроз виду

$$k_T^{[4]} \approx (0,183 \quad 0,171 \quad 0,222 \quad 0,099 \quad 0,155 \quad 0,086 \quad 0,083)^T \quad (4)$$

Відповідно до (4), найбільшою є загроза T_3, а найменшою – загроза T_7.

Описаний ітераційний процес реалізовано у середовищі Excel.

Результати опитування експертів відповідно до сформульованого вище переліку вразливостей W подано в табл. 2. Експерти E розташували вразливості W в порядку зменшення небезпеки впливу на інформаційну безпеку підприємства. Порядковий номер, що дорівнює 1, отримав найнебезпечніший чинник, а найменш небезпечний – номер 6.

Таблиця 2.

Експертні оцінки вразливостей **W**

	E_1	E_2	E_3	E_4	E_5	E_6	E_7
W_1	5	3	1	5	1	1	5
W_2	4	5	4	6	3	3	4
W_3	6	4	5	2	2	2	1
W_4	1	6	3	4	5	6	3
W_5	3	2	2	3	4	5	2
W_6	2	1	6	1	6	4	6

Узгодженість міркувань експертів стосовно вразливостей інформаційної безпеки підприємства оцінено за допомогою коефіцієнта конкордації Кендалла, який становить 0,08 відповідно до даних табл. 2. Оскільки коефіцієнт конкордації достатньо малий (0,08 < 0,2), то практично відсутня узгодженість міркувань експертів стосовно вразливостей підприємства.

За методом попарних порівнянь опрацьовано експертні оцінки вразливостей та отримано порядок розміщення вразливостей з огляду їхньої переваги за допомогою методу попарного порівняння.

На підставі експертних оцінок (табл. 2) побудовано матриці B_r, $r = \overline{1,7}$, попарних порівнянь вразливостей, елементи яких визначено так:

$$B_r = (b_{ij}^r) = \begin{cases} 1, & якщо\ W_i^r > W_j^r, \\ 0,5, & якщо\ W_i^r \approx W_j^r, \\ 0, & якщо\ W_i^r < W_j^r, \end{cases} \quad (5)$$

де: r – номер експерта, $i, j = \overline{1,6}$ – номери вразливостей, W_i^r – значення W_i - ої вразливості E_r - го експерта.

На підставі (5) з урахуванням даних табл. 2 матриці попарних порівнянь вразливостей за відповідями семи експертів набудуть вигляду:

$$B_1 = \begin{pmatrix} 0,5 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0,5 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0,5 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0,5 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0,5 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0,5 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 0,5 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0,5 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0,5 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0,5 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0,5 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0,5 \end{pmatrix},$$

$$B_3 = \begin{pmatrix} 0,5 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0,5 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0,5 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0,5 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0,5 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0,5 \end{pmatrix}, \quad B_4 = \begin{pmatrix} 0,5 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0,5 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0,5 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0,5 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0,5 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0,5 \end{pmatrix},$$

$$B_5 = \begin{pmatrix} 0,5 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0,5 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0,5 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0,5 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0,5 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0,5 \end{pmatrix}, \quad B_6 = \begin{pmatrix} 0,5 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0,5 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0,5 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0,5 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0,5 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0,5 \end{pmatrix},$$

$$B_7 = \begin{pmatrix} 0,5 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0,5 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0,5 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0,5 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0,5 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0,5 \end{pmatrix}.$$

Далі побудовано матрицю X_W математичних сподівань оцінок кожної з вразливостей W, елементи якої визначено відповідно до (2), де m_{ij} – кількість експертів, які надали перевагу вразливості W_i над W_j, m_{ji} – кількість експертів, які надали перевагу вразливості W_j над W_i. Отже, матриця математичних сподівань вразливостей W має вигляд:

$$X_W = \begin{pmatrix} \frac{1}{2} & \frac{5}{7} & \frac{5}{7} & \frac{4}{7} & \frac{3}{7} & \frac{4}{7} \\ \frac{2}{7} & \frac{1}{2} & \frac{2}{7} & \frac{3}{7} & \frac{2}{7} & \frac{4}{7} \\ \frac{2}{7} & \frac{5}{7} & \frac{1}{2} & \frac{5}{7} & \frac{4}{7} & \frac{4}{7} \\ \frac{3}{7} & \frac{4}{7} & \frac{2}{7} & \frac{1}{2} & \frac{1}{7} & \frac{4}{7} \\ \frac{4}{7} & \frac{5}{7} & \frac{3}{7} & \frac{6}{7} & \frac{1}{2} & \frac{3}{7} \\ \frac{3}{7} & \frac{3}{7} & \frac{3}{7} & \frac{3}{7} & \frac{4}{7} & \frac{1}{2} \end{pmatrix} \quad (6)$$

За допомогою матриці (6) та описаного вище ітераційного алгоритму визначено коефіцієнти відносної важливості вразливостей. Ітераційний алгоритм завершено на третьому кроці, оскільки $\max | k_W^{[3]} - k_W^{[2]} | \approx 0,0004 < 0,001$. Отриманий вектор коефіцієнтів відносної важливості вразливостей такий:

$$k_W^{[3]} \approx (0,197 \quad 0,129 \quad 0,185 \quad 0,136 \quad 0,193 \quad 0,16)^T \quad (7)$$

Отже, найважливішою є вразливість W_1, а найменший вплив матиме вразливість W_2.

Обговорення результатів досліджень (Discussion)

На підставі векторів коефіцієнтів відносної важливості загроз (4) та коефіцієнтів відносної важливості вразливостей (7) побудовано порівняльну матрицю загроз та вразливостей (табл. 3). Якщо елемент вектора загроз T є більшим за відповідний елемент вектора вразливостей W, то в табл. 3 на перетині стовпця загроз з рядком вразливостей розміщено знак «+», у протилежному випадку – «0».

Таблиця 3

Порівняльна матриця загроз T та вразливостей W

W \ T	T_1	T_2	T_3	T_4	T_5	T_6	T_7
W_1	0	0	+	0	0	0	0
W_2	+	+	+	0	+	0	0
W_3	0	0	+	0	0	0	0
W_4	+	+	+	0	+	0	0
W_5	0	0	+	0	0	0	0
W_6	+	+	+	0	0	0	0

З табл. 3 видно, що загроза T_3 є пріоритетною, оскільки має найбільше поєднань з вразливостями.

Висновки (Conclusions)

Для оцінювання ризиків інформаційної безпеки з використанням SWOT-аналізу розроблено перелік запитань для опитування експертів стосовно загроз та вразливостей підприємства. Результати експертних оцінок опрацьовано методом попарних порівнянь та побудовано матрицю поєднання загроз та вразливостей.

На підставі експертних оцінок загроз та вразливостей отримано структуровані дані для формування стратегії підприємства щодо інформаційної безпеки. Для даного підприємства пріоритетною є загроза інформаційній безпеці унаслідок крадіжок бізнес інформації; комп'ютерного обладнання; ПЗ; інформації для аутентифікації; інформації для ідентифікації особистості та порушення авторських прав на програмне забезпечення. Тому слід розробити заходи для зменшення впливу цієї загрози.

Зважаючи на мале значення коефіцієнта конкордації оцінок вразливостей, бачимо, що практично відсутня узгодженість міркувань експертів стосовно вразливостей підприємства. Тому доцільно було б провести стосовно вразливостей підприємства нове опитування за більшого обсягу інформації.

Список літератури:

1. Вознюк Є. В. SWOT-аналіз стану інформаційної безпеки України. Науковий часопис НПУ імені М. П. Драгоманова. 2021. Т. 22, № 30. С. 116 – 124. https://doi.org/10.31392/NPU-nc.series22.2021.30.12
2. Глосарій: навчальний енциклопедичний словник-довідник з питань інформаційної безпеки / за заг. редакцією д. політ. н., проф. А.М.Шуляк. 2019. 580 с.
3. Єжова Л. Ф. Економічні аспекти ризиків інформаційної безпеки. Сучасна спеціальна техніка. 2011. № 3(26). С. 80 – 91.
4. Аудит інформаційної безпеки: підручник Ромака В. А. та ін. Львів: СПОЛОМ, 2015. 363 с.
5. Волосович С., Клапків Л. Детермінанти виникнення та реалізації кібер-ризиків. Зовнішня торгівля: економіка, фінанси, право. 2018. № 3. С. 101 – 115.
6. Information Security Risk Analysis SWOT. / Shevchenko H. and an. Cybersecurity Providing in Information and Telecommunication Systems, January 28, 2021, Kyiv, Ukraine. P. 309 – 317. http://ceur-ws.org/Vol-2923/paper34.pdf
7. Віннікова І. І., Марчук С. В. Кібер-ризики як один із видів сучасних ризиків у діяльності малого та середнього бізнесу та управління

ними. Східна Європа: Економіка, бізнес та управління. 2018. Вип. 5 (16). С. 110 – 114.

8. Шевченко С. М., Жданова Ю. Д., Спасітєлєва С. О., Складанний П. М. Проведення SWOT-аналізу оцінювання інформаційних ризиків як засіб формування практичних навичок студентів спеціальності 125 Кібербезпека. Кібербезпека: освіта, наука, техніка. 2020. №2 (10). С.158 – 168. DOI 10.28925/2663-4023.2020.10.158168

9. ДСТУ IEC/ ISO 31010:2013. Керування ризиком. Методи загального оцінювання ризику. [Чинний від 2014-07-01]. Вид. офіц. Київ, Мінекономрозвитку України 2015. 73 с.

10. Архипов О. Є. Вступ до теорії ризиків: інформаційні ризики: монографія. Київ: Нац. акад. СБУ. 2015. 248 с.

11. Akinyemi I., Schatz D., Bashroush R. SWOT-analysis of information security management system ISO 27001. University of East London, Docklands Campus, 4-6 University Way, London E16 2RD.

12. Іващенко М. В.; Бикова Т. Б. SWOT-аналіз процесу впровадження змішаного навчання в закладах вищої освіти. Open educational e-environment of modern University. 2018. № 5. С. 107 – 115.

13. 13. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник, за заг. ред. д-ра техн. наук, професора В. Б. Толубка. Київ: ДУТ. 2015. 288 с.

References:

1. Vozniuk Ye. V. SWOT - analiz stanu informatsiinoi bezpeky Ukrainy. [Swot-analysis of the State of Ukraine's Information Security]. Naukovyi cha-sopys NPU imeni M. P. Drahomanova. 2021. T. 22. № 30. S. 116-124.doi.org/10.31392/NPU-nc.series22.2021.30.12

2. Hlosarii: navchalnyi entsyklopedychnyi slovnyk-dovidnyk z pytan informatsiinoi bezpeky / Za zah. redaktsiieiu d. polit. n., prof. A.M.Shuliak. 2019. 580 s.

3. Yezhova L. F. Ekonomichni aspekty ryzykiv informatsiinoi bezpeky [Economic aspects of information security risks] / Suchasna spetsialna tekhnika. 2011. № 3(26). S. 80 – 91.

4. Romaka V. A., Lahun A. B., Harasym Yu. R., Rak T. Ye., Samotii V. V., Rybii M. M. Audyt informatsiinoi bezpeky [Information security audit]: pidruchnyk. Lviv: SPOLOM, 2015. 363 s.

5. Volosovych S. Determinanty vynyknennia ta realizatsii kiber-ryzykiv / S. Volosovych, L. Klapkiv [Determinants of the cyber-risks arise and realization] // Zovnishnia torhivlia: ekonomika, finansy, pravo. 2018. № 3. S. 101 – 115.

6. Shevchenko H., Shevchenko S., Zhdanova Y., Spasiteleva S. and Negodenko O. Information Security Risk Analysis SWOT. Cybersecurity Providing in Information and Telecommunication Systems, January 28, 2021, Kyiv, Ukraine. P. 309 – 317.

7. Vinnikova I. I., Marchuk S. V. Kiber-ryzyky yak odyn iz vydiv suchasnykh ryzykiv u diialnosti maloho ta serednoho biznesu ta upravlinnia nymy [Cyber - risks as one of the types of modern risks in the activities of small and medium-sized businesses and their management] / Skhidna Yevropa: Ekonomika, biznes ta upravlinnia. 2018. Vyp. 5 (16). C. 110 – 114.

8. Shevchenko S. M. Provedennia SWOT-analizu otsiniuvannia informatsiinykh ryzykiv yak zasib formuvannia praktychnykh navychok studentiv spetsialnosti 125 Kiberbezpeka [Conducting a SWOT-analysis of information risk assessment as a means of formation of practical skills of students speciality 125 cyber security] // S. M. Shevchenko, Yu. D. Zhdanova, S. O. Cpasitielieva, P. M. Skladannyi / Kiberbezpeka: osvita, nauka, tekhnika. 2020, №2 (10). S.158 – 168. DOI 10.28925/2663-4023.2020.10.158168

9. DSTU IES/ ISO 31019:2013. Keruvannia ryzykom. Metody zahalnoho otsiniuvannia ryzyku. [Risk management. Methods of general risk assessment].

10. Arkhypov O. Ye. Vstup do teorii ryzykiv: informatsiini ryzyky [Introduction to risk theory: information risks]: monohr. / O. Ye. Arkhypov. Kyiv: Nats. akad. SBU. 2015. 248 s.

11. Akinyemi I., Schatz D., Bashroush R. SWOT - analysis of information security management system ISO 27001. University of East London, Docklands Campus, 4-6 University Way, London E16 2RD.

12. Ivashchenko M. V.; Bykova T. B. SWOT-analiz protsesu vprovadzhennia zmishanoho navchannia v zakladakh vyshchoi osvity [SWOT-analysis of the implementation of blended learning in institutions of higher education] / Open educational e-environment of modern University. 2018. № 5. S. 107 – 115.

13. Buriachok V. L. Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspect [Information and cyber security: socio-technical aspect:]: pidruchnyk / V. L. Buriachok, V. B. Tolubko, V. O. Khoroshko, S. V. Toliupa; za zah. red. d-ra tekhn. nauk, profesora V. B. Tolubka. Kyiv: DUT. 2015. 288 s.

© Л. Ф. Дзюба, О. Ю. Чмир, 2022.

Науково-методична стаття.
Надійшла до редакції 28.09.2022.
Прийнято до публікації 12.12.2022.