



МАТЕРІАЛИ  
ДРУКУЮТЬСЯ  
УКРАЇНСЬКОЮ,  
АНГЛІЙСЬКОЮ ТА  
ПОЛЬСЬКОЮ  
МОВАМИ

ЗБІРНИК НАУКОВИХ ПРАЦЬ

# ВІСНИК ЛЬВІВСЬКОГО ДЕРЖАВНОГО УНІВЕРСИТЕТУ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

№ 26, 2022

заснований у 2007 році

## РЕДАКЦІЙНА КОЛЕГІЯ:

**Головний редактор:** ПОПОВИЧ Василь, д.т.н., проф., Україна; **Заступник головного редактора:** СМОТР Ольга, к.т.н., доц., Україна; **Заступник головного редактора:** МЕНЬШИКОВА Ольга, к.ф.-м.н., доц., Україна; **Відповідальний секретар:** ІВАНУСА Андрій, к.т.н., доц., Україна.

**07 Управління та адміністрування (073 «Менеджмент»):** БАШИНСЬКИЙ Олег, к.т.н., доц., Україна; БЛОЩИЦЬКИЙ Андрій, доктор наук, проф., Астана IT Університет, Казахстан; ГОЛОВАТИЙ Роман, к.т.н., Україна; ЗАЧКО Олег, д.т.н., проф., Україна; КОБИЛКІН Дмитро, к.т.н., Україна; РАТУШНИЙ Роман, д.т.н., проф., Україна; СОДОМА Руслана, к.е.н., доц., Україна; ТРИГУБА Анатолій, д.т.н., проф., Україна; ХІРОШІ Танака, доктор наук, проф., Університет Кей'о, Японія.

**10 Природничі науки (101 «Екологія»):** БОСАК Павло, к.т.н., Україна; БУЧАВИЙ Юрій, к.б.н., доц., Україна; ГІЛЛМОР Гевін, кандидат наук, Університет Бат-Спа, Великобританія; ГОЦІЙ Наталія, к.с.-г.н., Україна; ГРИНЧИШИН Наталія, к.с.-г.н., доц., Україна; КУЗИК Андрій, д.с.-г.н., проф., Україна; МАЖЕЙКЕНА Аусра, доктор наук, проф., Вільнюський технічний університет Гедимінаса, Литва; СИДОРЕНКО Володимир, д.т.н., доцент, Україна; ТЕЛАК Оксана, доктор наук, проф., Головна школа пожежної служби, Польща; ШМАНДІЙ Володимир, д.т.н., проф., Україна; ШУПЛАТ Тарас, к.с.-г.н., Україна.

**12 Інформаційні технології (122 «Комп'ютерні науки», 125 «Кибербезпека»):** БАБЧЕВ Сергій, д.т.н., проф., Україна; БОРЗОВ Юрій, к.т.н., доц., Україна; БУНЬ Ростислав, д.т.н., проф., Україна; БУРАК Назарій, к.т.н., доц., Україна; ГАРАСИМЧУК Олег, к.т.н., доц., Україна; ЖУРАВЕЛЬ Ігор, д.т.н., проф., Україна; КОВАЛЬ Мирослав, д.пед.н., проф., Україна; КОЗЯР Михайло, д.пед.н., проф., Член-кореспондент НАПН України, Україна; МАЛЕЦЬ Ігор, к.т.н., доц., Україна; МАРТИН Євген, д.т.н., проф., Україна; ПОЛОТАЙ Орест, к.т.н., Україна; ПРИДАТКО Олександр, к.т.н., доц., Україна; САМОТИЙ Володимир, д.т.н., проф., Україна; СОВИН Ярослав, к.т.н., доц., Україна; ТКАЧУК Ростислав, д.т.н., проф., Україна; ЯЩУК Валентина, к.е.н., доц., Україна.

**16 Хімічна та біоінженерія (161 Хімічні технології та інженерія):** ГУЛАЙ Любомир, д.х.н. проф., Україна; ДМИТРІВ Григорій, к.х.н., доц., Україна; ЛАВРЕНЮК Олена, к.х.н., доц., Україна; МАЙДЕР-ЛОПАТКА Малгоржата, кандидат наук, Головна школа пожежної служби, Польща; МИХАЛЧКО Борис, д.х.н., проф.,

Україна; НАГУРСЬКИЙ Олег, д.т.н., проф., Україна; ЛЕВИЦЬКИЙ Володимир, д.т.н., проф., Україна; П'ЄЦ Роберт, кандидат наук, Головна школа пожежної служби, Польща.

**18 Виробництво та технології (183 Технології захисту навколишнього середовища):** АБРАМОВИЧ Анна, кандидат наук, Сілезький університет у Катовіце, Польща; БЛОУС Оксана, д.ф.-м.н., проф., Віденський університет, Австрія; ГЕНИК Ярослав, д.с.-г.н., доц., Україна; ХАЙЛЬМЕЙЕР Герман, д.т.н., проф., Університет технологій та гірничої справи Фрайберга, Німеччина; ГУМНИЦЬКИЙ Ярослав, д.т.н., проф., Україна; КОВРОВ Олександр, д.т.н., проф., Україна; ПЕТЛЮВАНІЙ Михайло, к.т.н., доц., Україна; САБАДАШ Віра, д.т.н., проф., Україна; САЙ Катерина, к.т.н., доц., Україна; СТЕПОВА Катерина, к.т.н., доц., Україна; ХРОМ'ЯК Уляна, к.т.н., Україна; ЮРЧЕНКО Валентина, д.т.н., проф., Україна; ЯЦІШИН Теодозія, д.т.н., доц., Україна.

**26 Цивільна безпека (261 Пожежна безпека, 263 Цивільна безпека):** БАЛАНЮК Володимир, д.т.н., проф., Україна; ГАВРИСЬ Андрій, к.т.н., доц., Україна; ДОНЧЕВ Тодор, кандидат наук, доц., Кінгстонський університет, Великобританія; ЄМЕЛЬЯНЕНКО Сергій, к.т.н., Україна; КАРАБИН Василь, д.т.н., доц., Україна; КОВАЛИШИН Василь, д.т.н., проф., Україна; МОРИЦ Євген, д.т.н., Державна служба України з надзвичайних ситуацій, Україна; ПАЗЕН Олег, к.т.н., Україна; РЕНКАС Артур, к.т.н., Україна; РУДИК Юрій, д.т.н., доц., Україна; САМБЕРГ Андре, д.т.н., проф., член програмного комітету Міжнародного товариства управління в надзвичайних ситуаціях (ТІЕМС), Бельгія; СКРАБАЧ Олександра, доктор наук, професор, Військово-технічний університет у Варшаві, Польща; СТАРОДУБ Юрій, д.ф.-м.н., проф., Україна; ТАЦІЙ Роман, д.ф.-м.н., проф., Україна; ТЕЛАК Єжи, доктор наук, Академія спортивної освіти, Польща; ЧЕБЕРЯЧКО Сергій, д.т.н., проф., Україна; ШУКІС Ріголдас, кандидат наук, Вільнюський технічний університет ім. Гедиміна, Литва; ЯКОВЧУК Роман, д.т.н., доц., Україна; ЯРОШ Войцех, кандидат наук, Головна школа пожежної служби, Польща.

**27 Транспорт (275 Транспортні технології):** ГАЩУК Петро, д.т.н., проф., Україна; ДОМІНІК Андрій, к.т.н., доц., Україна; ЗАПОРОЖЕЦЬ Олександр, доктор наук, проф., Інститут авіації, Польща; НЕМІЙ Степан, к.т.н., доц., Україна; ПАСНАК Іван, к.т.н., доц., Україна; РОЙКО Юрій, к.т.н., доц., Національний університет «Львівська політехніка», Україна; ТУРПАК Сергій, д.т.н., проф., Україна.

ISSN 2078-4643 (print)  
ISSN 2708-1389 (online)

DOI: 10.32447/20784643.26.2022.00

**ЗАСНОВНИК І ВИДАВЕЦЬ**

Львівський державний університет  
безпеки життєдіяльності (ЛДУ БЖД)

**ЗАРЕЄСТРОВАНО**

Державною реєстраційною службою України  
12.03.2015 р. Серія КВ №20328-11128Р

**ВНЕСЕНО ДО ПЕРЕЛІКУ ФАХОВИХ ВИДАНЬ УКРАЇНИ  
ЯК ДРУКОВАНЕ ПЕРІОДИЧНЕ ВИДАННЯ КАТЕГОРІЇ «Б»**  
(Наказ МОН України від 02.07.2020 року №886 та від 24.09.2020 року №1188)

**ВНЕСЕНО ДО БІБЛОГРАФІЧНИХ БАЗ ДАНИХ:**  
«*НАУКОВА ПЕРІОДИКА УКРАЇНИ*» В НАЦІОНАЛЬНІЙ БІБЛІОТЕЦІ УКРАЇНИ  
ІМ. В.І. ВЕРНАДСЬКОГО, «*ULRICH'S PERIODICALS DIRECTORY*»,  
«*GOOGLE SCHOLAR*» та ін.

**Рекомендовано до друку рішенням Вченої ради ЛДУ БЖД**  
(Протокол № 5 від 14.12.2022 р.)

**Літературний редактор**

Падик Г.М.

**Технічний редактор**

Сорочич М.П.

**Комп'ютерна верстка**

Беседа А.В.

**Друк на різнографі**

Петролюк Н.І.

**Відповідальний за друк**

Беседа А.В.

**АДРЕСА РЕДАКЦІЇ:**

ЛДУ БЖД, вул. Клепарівська, 35, м. Львів, 79007

**Контактні телефони:**

(032) 233-24-79, тел/факс 233-00-88

**E-mail:**

visnyk@ldubgd.edu.ua

Збірник наукових праць "Вісник Львівського державного університету безпеки життєдіяльності" видається в університеті з 2007 року. Запланована періодичність: 2 рази на рік. Тематична спрямованість: цивільна безпека, пожежна безпека, менеджмент, екологія, комп'ютерні науки та інформаційні технології, кібербезпека, хімічні технології та інженерія, технології захисту навколишнього середовища, транспортні технології (за видами), публікація рекламних матеріалів та матеріалів конференцій, семінарів.

Здано в набір 15.12.2022. Підписано до друку 16.12.2022.

Формат 60x84<sup>1/3</sup>. Папір офсетний. Ум. друк. арк. 6,65.

Гарнітура Times New Roman. Друк на різнографі

Наклад: 100.

**Друк:** Сектор видавничої діяльності ЛДУ БЖД

вул. Клепарівська, 35, м. Львів, 79007.

## ЗМІСТ

### ЕКОЛОГІЯ

*П. В. Босак, О. В. Стокалюк*  
МОДЕЛЮВАННЯ ПОШИРЕННЯ  
ЗАБРУДНЮЮЧИХ РЕЧОВИН У ДОВКІЛЛЯ З  
ПОРОДНИХ ВІДВАЛІВ ВУГІЛЬНИХ ШАХТ  
НОВОВОЛИНСЬКОГО  
ГІРНИЧОПРОМИСЛОВОГО РАЙОНУ

*І. С. Федів, К. В. Степова, Р. М. Конанець*  
ВПЛИВ МЕТОДУ МОДИФІКУВАННЯ НА  
СОРЕБЦІЙНІ ВЛАСТИВОСТІ  
КЛИНОПТИЛОЛІТУ

*В. І. Шуригін, В. В. Карабин*  
ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ  
МІГРАЦІЇ ВУГЛЕВОДНІВ У АЛЮВІАЛЬНИХ  
ВІДКЛАДАХ РІКИ СТРИЙ ВНАСЛІДОК  
ОДНОРАЗОВОГО СКИДУ НАФТИ

### КОМП'ЮТЕРНІ НАУКИ

*Є. В. Мартин, В. С. Яковчук, О. В. Придатко*  
РОЗРОБКА КОНЦЕПЦІЇ ІНФОРМАЦІЙНОЇ  
ГРАФІЧНОЇ ТЕХНОЛОГІЇ МОДЕЛЮВАННЯ  
ТРАЄКТОРІЙ ОБГОНУ ДЛЯ ПОЖЕЖНИХ  
АВТОМОБІЛІВ

*О. В. Хлевной, Д. А. Райта, Н. Є. Бурак,  
Ю. О. Борзов*  
ВИЗНАЧЕННЯ ПАРАМЕТРІВ РУХУ  
ЕВАКУАЦІЙНИХ ПОТОКІВ ІЗ  
ЗАСТОСУВАННЯМ ШТУЧНИХ  
НЕЙРОННИХ МЕРЕЖ

### КІБЕРБЕЗПЕКА

*Л. Ф. Дзюба, О. Ю. Чмир*  
ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ  
БЕЗПЕКИ З ВИКОРИСТАННЯМ МЕТОДІВ  
МАТЕМАТИЧНОЇ СТАТИСТИКИ

### ТЕХНОЛОГІЇ ЗАХИСТУ НАВКОЛИШНЬОГО СЕРЕДОВИЩА

*О. І. Бедратюк, С. О. Ємельяненко,  
В. М. Марич, В. Л. Петровський, Ю. І. Рудик*  
НОВІ ПЕРСПЕКТИВИ ДЛЯ РОБОТИ  
ДОСЛІДНО-ВИПРОБУВАЛЬНИХ  
ЛАБОРАТОРІЙ

### ПОЖЕЖНА БЕЗПЕКА

*В. М. Баланюк, О. І. Гірський, О. І. Герасим'юк,  
В. С. Мирошкін, В. С. Пікус*  
ПРОБЛЕМИ НОРМАТИВНО-ТЕХНІЧНОГО  
ЗАБЕЗПЕЧЕННЯ ВИПРОБУВАНЬ ТА ЯКОСТІ  
ПРОДУКЦІЇ ВОГНЕГАСНИХ СИСТЕМ ТА  
ЗАСОБІВ В УКРАЇНІ

## CONTENTS

### ECOLOGY

5 *P. V. Bosak, O. V. Stokalyuk*  
MODELING DISTRIBUTION OF  
POLLUTANTS ORIGINATING FROM COAL  
WASTE DUMPS OF THE  
NOVOVOLYNSK MINING AREA  
IN THE ENVIRONMENT

14 *I. Fediv, K. Stepova, R. Konanets*  
EFFECT OF DIFFERENT MODIFICATION  
METHODS ON THE SORPTION  
PROPERTIES OF CLINOPTILOLITE

20 *V. I. Shuryhin, V. V. Karabyn*  
EXPERIMENTAL STUDIES OF  
HYDROCARBON MIGRATION IN ALLUVIAL  
SEDIMENTS OF THE RIVER STRYI AS A  
RESULT OF A SINGLE OIL DISCHARGE

### COMPUTER SCIENCE

29 *E. V. Martyn, V. S. Yakovchuk, O. V. Pridatko*  
DEVELOPMENT OF THE CONCEPT OF  
INFORMATION GRAPHIC TECHNOLOGY OF  
MODELING OF OVERTAKING  
TRAJECTORIES FOR FIRE VEHICLES

40 *O. Khlevnoy, D. Raita, N. Ye. Burak, Yu. Borzov*  
MOVEMENT PARAMETERS  
DETERMINATION OF EVACUATION FLOWS  
USING ARTIFICIAL NEURAL NETWORKS

### CYBERSECURITY

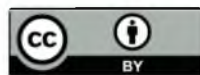
47 *L. F. Dziuba, O. Y. Chmyr*  
ASSESSMENT OF INFORMATION SECURITY  
RISKS USING METHODS  
OF MATHEMATICAL STATISTICS

### TECHNOLOGIES OF ENVIRONMENT PROTECTION

55 *O. I. Bedratyuk, S. O. Yemelyanenko,  
V. M. Marych, V. L. Petrovskiy, Yu. I. Rudyk*  
NEW PERSPECTIVES FOR THE WORK  
OF RESEARCH AND TESTING  
LABORATORIES

### FIRE SAFETY

67 *V. M. Balanyuk, O. I. Hirskiy, O. I. Gerasimiyuk,  
V. S. Myroshkin, V. S. Pykus*  
PROBLEMS OF REGULATORY AND  
TECHNICAL SECURITY TESTS AND PRODUCT  
QUALITY OF FIRE EXTINGUISHING SYSTEMS  
AND EQUIPMENT IN UKRAINE



*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](mailto: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 підґрунтям 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 економіку. 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 підґрунтям 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:

– *T*<sub>1</sub> – 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;

– *T*<sub>2</sub> – 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;

– *T*<sub>3</sub> – крадіжки: бізнес інформації; комп'ютерного обладнання; ПЗ; інформації для автентифікації; інформації для ідентифікації особистості та порушення авторських прав на програмне забезпечення;

– *T*<sub>4</sub> – збої в роботі: застосунків, розроблених підприємством та закуплених у сторонніх постачальників; системного ПЗ та комп'ютерного чи мережевого обладнання;

– *T*<sub>5</sub> – 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;

– *T*<sub>6</sub> – ненавмисну неправильну експлуатацію, яка полягає у помилках користувачів або адміністраторів;

– *T*<sub>7</sub> – непередбачені наслідки від змін: бізнес-процесів; ПЗ; бізнес-інформації; в комп'ютерному або комунікаційному устаткуванні.

До вразливостей інформаційної системи підприємства віднесено:

– *W*<sub>1</sub> – відсутність системи аварійного електропостачання;

– *W*<sub>2</sub> – відсутність системи регулярного резервного копіювання;

– *W*<sub>3</sub> – відсутність двофакторної автентифікації;

– *W*<sub>4</sub> – плінність кадрів (часта зміна персоналу);

– *W*<sub>5</sub> – недостатній рівень фахової підготовки користувачів;

– *W*<sub>6</sub> – 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 *E*<sub>1</sub> – *E*<sub>7</sub>) 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.

Таблиця 1

Експертні оцінки загроз Т

	$E_1$	$E_2$	$E_3$	$E_4$	$E_5$	$E_6$	$E_7$
$T_1$	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 парних порівнянь. Цей метод визначає порядок розміщення загроз з огляду їхньої переваги за допомогою парного порівняння. Згідно з цим методом, на підставі експертних оцінок (табл. 1) побудовано матриці

парних порівнянь загроз  $A_r$ ,  $r = \overline{1, 7}$ . Елементи матриць визначено так [12]:

$$A_r = (a_{ij}^r) = \begin{cases} 1, & \text{якщо } T_i^r > T_j^r, \\ 0.5, & \text{якщо } T_i^r \approx T_j^r, \\ 0, & \text{якщо } T_i^r < T_j^r, \end{cases} \quad (1)$$

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 парних порівнянь загроз за відповідями семи експертів мають вигляд

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

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

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

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

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

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

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

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:

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

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

$$k_T^{[0]} = \underbrace{(1 \ 1 \ \dots \ 1)}_m^T$$

1. Початкова умова:  $t = 0$ ,

$$k_T^{[t]} = \frac{1}{\lambda_T^{[t]}} \cdot Y_T^{[t]}$$

2. Рекурентні співвідношення:

$$\lambda_T^{[t]} = \underbrace{(1 \ 1 \ \dots \ 1)}_m \cdot Y_T^{[t]}$$

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

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

**Крок 1.**

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

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

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

**Крок 2.**

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

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

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

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.**

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

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

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

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.**

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

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

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

Алгоритм завершуємо, оскільки

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

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

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

(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:

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

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:

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

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:

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

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  $W$

$T \backslash W$	$T_1$	$T_2$	$T_3$	$T_4$	$T_5$	$T_6$	$T_7$
$W_1$	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-ризик 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., Спасітелева С. О., Складаний 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 ІЕС/ 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. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толопа 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 odyv 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). С. 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. Spasitielieva, 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: sotsiotekhnichniy aspekt [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.