КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (14), 2021
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2021.14.158175
УДК 004.94:519.21

Шевченко Світлана Миколаївна
канд. пед. наук, доцент,
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID ID: 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

Жданова Юлія Дмитрівна
канд. ф.-м. наук, доцент,
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID ID: 0000-0002-9277-4972
y.zhdanova@kubg.edu.ua

Кравчук Катерина Володимирівна
магістр Факультету інформаціонних технологій та управління
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID ID: 0000-0002-3589-8784
kvkravchuk.fitu20@kubg.edu.ua

МОДЕЛЬ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ

Анотація. Дане дослідження присвячене проблемі захисту інформаційних ресурсів на засадах ризик-орієнтованого підходу для малого та середнього бізнесу з наголосом на оцінці ризиків інформаційної безпеки (ІБ). Аналіз наукових джерел дозволив охарактеризувати сутність ризико-орієнтованого підходу і сформулювати основні положення для створення моделі захисту інформації на основі даної технології. Змістова лінія моделі акцентує увагу на проведення якісної та кількісної оцінки ризику ІБ, а саме, SWOT-аналіз, статистичний метод, метод експертних оцінок та метод Монте-Карло. Описано покрокову процедуру здійснення етапів аналізу та впровадження даних методів для оцінки ризиків ІБ. Для отримання цілісної карти відносно ризиків ІБ на початковому етапі пропонується провести SWOT-аналіз, зокрема виділити слабкі сторони бізнесу та зовнішні і внутрішні загрози. Для обчислення кількісної оцінки ризику ІБ застосувати статистичний метод, якщо є достатня кількість аналітичних звітів. У протилежному випадку реалізувати метод експертних оцінок. На заключному кроці згенерувати сценарій методом Монте-Карло. Для ефективного опису контексту кожного інформаційного ресурсу скористатися технологією формування множини пар «загроза – уразливість».
Обґрунтовано актуальність та можливості використання даної моделі в якості методології заисту інформації для малого та середнього бізнесу.

Ключові слова: ризики інформаційної безпеки (ІБ); SWOT-аналіз; статистичні методи; метод експертних оцінок; метод Монте-Карло; загрози; уразливості; модель захисту інформації.

1. ВСТУП

Постановка проблеми. Аналіз загроз та уразливостей інформаційних ресурсів з метою визначення оцінки ризиків ІБ є найбільш важливим елементом політики безпеки ІТ-інфракструктури компанії, зокрема, для малого та середнього бізнесу. Як свідчать статистичні дані [1] кіберзлочинність обходиться малому та середньому бізнесу більш ніж 2,2 мільйона доларів на рік; 43% кібератак орієнтовані на малий бізнес; 60% малих

підприємств, які стали жертвами кібератаки, припиняють свою діяльність упродовж шести місяців; 47% малих підприємств не розуміють, як захистити себе від кібератак; 3 із 4 малих підприємств заявляють, що у них немає персоналу для вирішення проблем IT-безпеки; 91% підприємств не мають страховки кібер-відповідальності. Лише 14% малих підприємств оцінюють свою здатність знижувати кіберризики та атаки як високоефективні. Тому проблема захисту інформації для малого та середнього бізнесу є першочерговою і потребує постійного удосконалення

Аналіз останніх досліджень і публікацій. Дослідженню проблем і створенню методик та моделей, пов'язаних з якісною та кількісною оцінкою ризиків ІБ з метою управління захистом інформації, присвячено достатню кількість наукових праць. Це підтверджує актуальність та важливість даної теми.

Так, у науковому дослідженню [2] представлено методологічний підхід до зниження ризику ІБ у розподілених системах обробки та зберігання даних внаслідок впровадження хмарних технологій; розробка [3] описує процес оцінки ризиків ІБ через математичний апарат нечіткої логіки; команда вчених у роботі [4] окреслюють впровадження в процес аналізу ризику ІБ мережу Байєса та дерева подій. У дослідженнях [5 - 7] пропонується в якості системної методології захисту інформації підхід, пов'язаний з оцінюванням ризиків ІБ та на цій основі управління ними. Така технологія отримала назву «ризик-орієнтований підхід».

Аналіз даних та інших досліджень дозволив виділити наступні характеристики у процесі управління ризиками ІБ: незалежно від галузі застосування етапи управління ризиками ІБ практично є незмінними відповідно до міжнародних стандартів у даній сфері. Тому для ефективності та результативності потрібно шукати шляхи комбінацій та поєднань різних методів для аналізу ризиків ІБ з метою управління ними.

Висвітлені проблеми дають переконливе уявлення про актуальність даного дослідження і визначають його мету.

Мета статті. Мета роботи полягає в розробці та обґрунтуванні моделі захисту інформації на засадах ризик-орієнтованого підходу для малого та середнього бізнесу, яка включає кількісний та якісний підходи до оцінки ризиків ІБ.

2. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Ризик інформаційної безпеки – це числова (словесна) функція, яка описує ймовірність втілення загроз ІБ та величини збитку від їх реалізації внаслідок використання цими загрозами уразливостей активів з метою нанесення шкоди організації [8].

Під управлінням ризиками ІБ (ризик-менеджмент) розуміють безперервний циклічний процес, який містить наступні етапи: ідентифікація ризиків (збір інформації щодо активів, джерел загроз, класифікація загроз та уразливостей; ранжування ризиків); аналіз ризику (якісний та кількісний підхід до оцінки ризику); оцінювання ризику (процес порівняння кількісно оціненого ризику з даними критеріями ризику для визначення значущості ризику ІБ); обробка ризику та прийняття. На рисунку 1 представлено алгоритм процесу управління ризиками ІБ [9].

В якості системної методології захисту інформації виділяють підхід, пов'язаний з оцінюванням ризиків ІБ, та на цій основі управління ними. Така технологія отримала назву «ризик-орієнтований підхід». Ризик-орієнтований підхід до забезпечення інформаційної безпеки – прийняття управлінських рішень на підставі аналізу порівняння

поточних ризиків інформаційної безпеки з прийнятними [10]. Процес управління ризиками ІБ істотно залежить від збору інформації про актив, який потрібно захистити, його уразливості, загрози та їх джерела, а також наскільки об'єктивно буде здійснена оцінка відповідного ризику на основі наданої інформації.

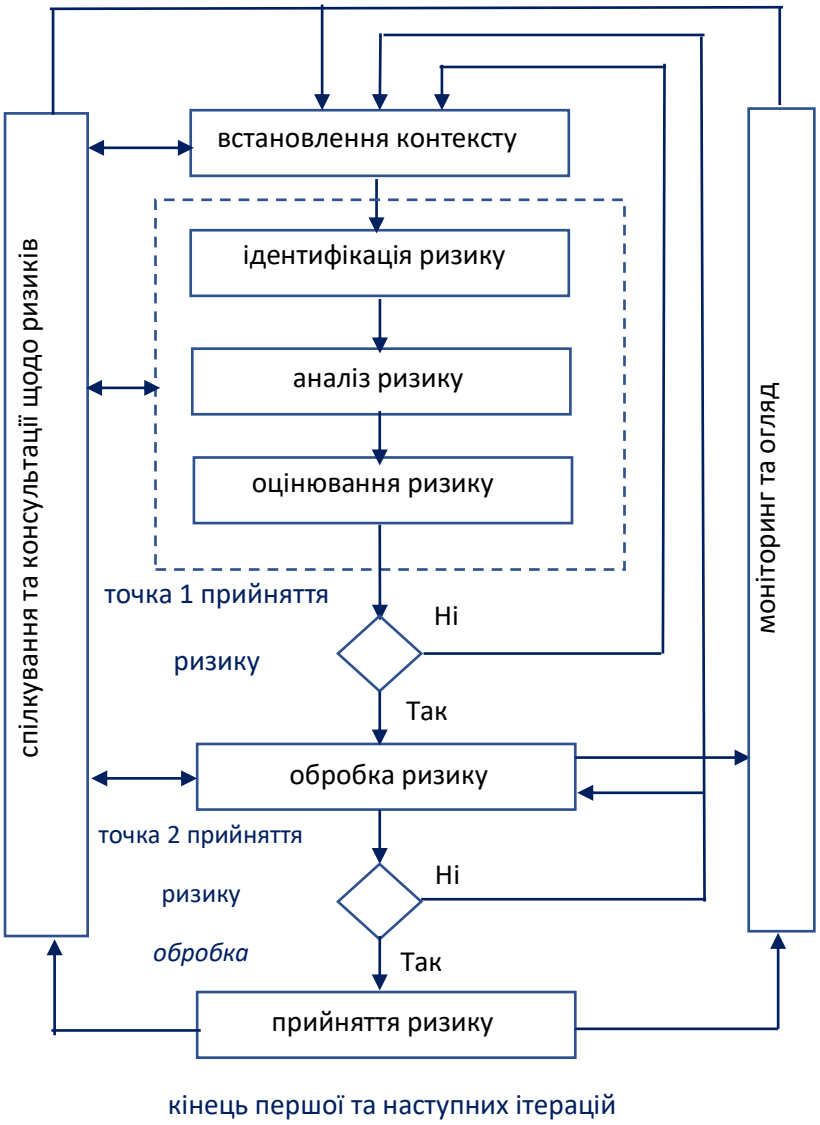


Рис. 1. Алгоритм процесу управління ризиками ІБ

Існує два підходи до процесу оцінки ризиків: кількісний та якісний.

Кількісні методи оцінки ризиків надають математичний опис ризику, основними його параметрами є: «ймовірність» (виражає ймовірність використання загрозою уразливість активу) та «наслідки» (вага негативного впливу ризику на діяльність суб'єкта чи розмір збитків від реалізації несприятливої події). В таблиці 1 представлені види кількісних методів, їх переваги та недоліки.

ISSN 2663 - 4023

Таблиця 1

Характеристика, переваги та недоліки методів кількісної оцінки ризиків ІБ

Категорія	Характеристика	Переваги	Недоліки
Статистичні	Знаходження вибіркового середнього, вибіркового середнього квадратичного відхилення, коефіцієнта варіації	Досить висока точність, можливість моделювання сценаріїв.	Має бути великий обсяг минулих даних
Метод побудови дерева рішень	В процесі розглядаються різні варіанти рішення (гілки дерева), які можуть бути прийняті.	Досить висока точність оцінки, можливість різних сценаріїв розвитку події.	Високі витрати при великій кількості розглядуваних сценаріїв.
Метод аналізу чутливості	Виявлення чутливості показників, що оцінюються, до змін значень вхідних даних.	Можливість вирішення проблеми щодо варіювання характеристик інциденту.	Недооблік кореляції між різними характеристиками.
Аналіз сценаріїв	Розробка плану сценарію розвитку	Можливо застосувати до різних варіантів реалізації інцидентів.	Вимагається великий об'єм вхідних даних, низька ймовірність точного прогнозування для різних сценаріїв.
Метод Монте-Карло	Визначає параметри розподілу випадкової величини та оцінює ризик на основі розрахунку відповідних математичних показників та побудови гістограми й полігону розподілу певного ризику.	Можливість побудувати моделі досить складних систем та процесів, можливість застосувати для різних розподілів вхідних даних	Висока складність методу, потреба у великій кількості вхідних даних, складність розрахунків.
Метод аналогій	Визначення наслідків впливу несприятливих факторів на інші аналогічні процеси.	Відносно невисока вартість, простота в розрахунках.	Невисока точність, складність у підборі аналогів.

Якісно оцінений ризик характеризує джерело загрози та її вид і відповідно уразливість інформаційного активу. В таблиці 2 запропоновано методи якісної оцінки ризиків ІБ.

Таблиця 2

Характеристика, переваги та недоліки методів якісної оцінки ризиків ІБ

Категорія	Характеристика	Переваги	Недоліки
Метод експертних оцінок	Оцінка ризику здійснюється на основі суб'єктивних думок експертів в окремій галузі.	Відсутність необхідності в точних вхідних даних	Суб'єктивність експертних думок, складність в процесі залучення незалежних експертів.

SWOT-аналіз	Стратегія компанії на перетині загроз (внутрішніх та зовнішніх) та слабких сторін (уразливостей)	Відсутність необхідності в точних вхідних даних	Суб'єктивність думок команди, складність в процесі залучення незалежних експертів.

3. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

3.1. Постановка завдання

Більшість підприємств малого та середнього бізнесу з різних причин не мають можливості здійснювати повну оцінку захищеності цінних інформаційних ресурсів. Тому на етапі впровадження частина науковців, і ми згодні з ними, рекомендують застосовувати кількісну оцінку рівня ризику. У цьому випадку є доцільним визначення ймовірності загроз та використання уразливості активу даною загрозою, вартості активу (включає як початкову вартість, так і вартість на встановлення у разі виходу з ладу). Як результат цього етапу – обрахування ступеня ризику та створення ранжованого списку у порядку спадання. Такий підхід дає змогу точніше описувати і створювати політику безпеки на підприємстві. Обов'язковим в цьому процесі є визначення ліміту на вартість системи захисту інформаційних ресурсів.

Слід також відмітити, що наукових дослідженнях [11] зустрічається теза про недоцільність проведення оцінки ризиків ІБ для кожного цінного активу, аргументуючи це тим, що великі підприємства мають обширну кількість інформаційних ресурсів і, є очевидним, що ідентифікація по кожному з них – громіздка та недоцільна робота. Однак, для малого та середнього бізнесу вважаємо за необхідне саме інвентаризацію кожного інформаційного ресурсу для встановлення ступеня ризику ІБ з метою захисту інформації, що й покладено в основу нашого дослідження.

На підставі викладеного наше дослідження спрямовуємо на виконання наступних завдань:

1) виокремити етапи процесу оцінки ризиків ІБ;
2) встановити взаємозв'язок між ними;
3) визначити набір методів для якісної оцінки ризиків для початкового бачення картини слабких сторін підприємства та внутрішніх і зовнішніх загроз;
4) визначити набір методів для кількісної оцінки ризиків ІБ для уточнення ступеня загального ризику для активів підприємства, а саме статистичний метод та метод експертних оцінок;
5) згенерувати сценарій за допомогою статистичного моделювання.

3.2. Структура та алгоритм моделі захисту інформації на засадах ризик-орієнтованої технологій

Змістова лінія моделі акцентує увагу на проведення якісної та кількісної оцінки ризику ІБ. На рисунку 2 представлено алгоритм процесу управління ризиками ІБ для малого та середнього бізнесу.

ISSN 2663 - 4023

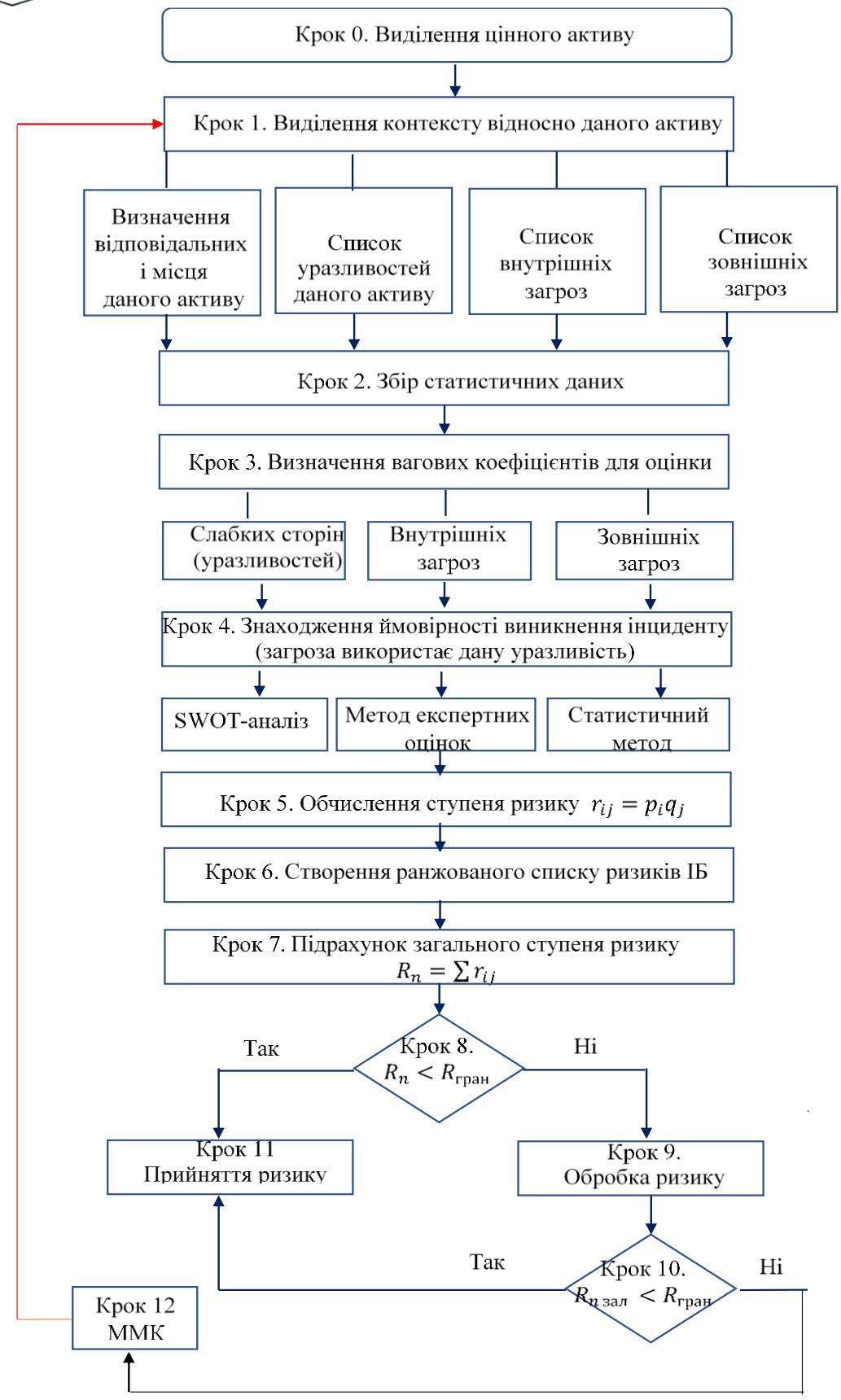


Рис. 2. Алгоритм моделі захисту інформації на засадах ризик-орієнтованої технологій

Опишемо процес управління ризиками ІБ для малого та середнього бізнесу за кроками.

Крок 0. Виділити цінний ресурс

Крок 1. Описати контекст відносно даного інформаційного ресурсу. Для ефективного забезпечення цього кроку, ми скористалися технологією формування множини пар «загроза – уразливість», описано у дослідженні [12].

Крок 2. Зібрати статистичні дані. Оформити, як приклад, наступним чином (таблиці 3-4).

Таблиця 3

Опис статистичних даних

Актив	Ідентифікація активу	Загрози	Уразливості
ПК №1 типу Б (ПК бухгалтерії з корпусу 1)	*Рівні забезпечення*: • Конфіденційність: середній (22000 у. о.) • Цілісність: середній (15200 у. о.) • Доступність: середній (34800 у. о.) *Максимальний час недоступності*: з 2:00 до 3:00. *Власник:* Шило В. С. *Місце знаходження*: м. Київ, вул. Хрещатик, 1 *Категорія:* Комп'ютерна техніка (КТ) *Цінність:* • 120000 у. о. – вартість • 22000 + 15200 + 34800 = 72000 – максимальний збиток при порушенні усіх рівнів забезпечення Сума: 192000 у. о.	*Загроза:* Проникнення шкідливого ПО *Джерело загрози:* Антропогенне *Тип загрози*: Внутрішня *Порушення властивостей:* К, Ц, Д	Відсутність антивірусного ПО, відсутність розмежування прав доступу до інформаційних ресурсів
		Загроза: Фізичне пошкодження *Джерело загрози:* Антропогенне, стихійне, техногенне *Тип загрози:* Внутрішня, зовнішня *Порушення властивостей:* Ц, Д	Ненадійні корпуси приладів, відсутність політики використання службових пристроїв
		Загроза: Відключення електроживлення *Джерело загрози:* Антропогенне, стихійне, техногенне *Тип загрози:* Внутрішня, зовнішня *Порушення властивостей:* Ц, Д	Відсутність аварійних генераторів

Таблиця 4

Шкала оцінювання рівня впливу (рівня забезпечення)

Якісна оцінка впливу	Значення шкали	Збиток (у. о.)
Низький	1	[0 – 15000)
Середній	2	[15000-40000)
Високий	3	40000>

Крок 3. Визначити вагові коефіцієнти для оцінки слабких сторін (уразливості), внутрішніх та зовнішніх загроз.

Крок 4. Знайти ймовірності виникнення інциденту (загроза використає дану уразливість).

Для отримання цілісної карти відносно ризиків ІБ на початковому етапі провести SWOT-аналіз. Як зразок, представлено у вигляді наступних таблиць 5-6.

Таблиця 5

Вихідна матриця SWOT-аналізу

Сильні сторони	**Слабкі сторони**
Перевірені процеси по підбору кваліфікованих працівників	Відсутність достатньої кількості інженерів
Наявність стратегії технологічного розвитку інфраструктури	Ненадійний підрядник, відповідальний за юридичні послуги
Конкурентно спроможні тарифи	Відсутність власних спеціалістів з інформаційної безпеки
Територіально вигідне положення в межах країни	Відсутність достатньої кількості персоналу служби підтримки
Можливості	**Загрози**
Надання франшизи для інтернет-провайдерів в інших областях	Нестабільна економічна ситуація в країні
Створення штату маркетологів та стратегії маркетингового розвитку	Агресивна маркетингова політика конкурентів
Створення сучасного графічного інтерфейсу для клієнтів	Можливі кібератаки, спонсоровані зацікавленими сторонами
Створення власного штату спеціалістів з інформаційної безпеки	

Процес проведення SWOT-аналізу ризиків ІБ представлено у дослідженні [8].

На останньому етапі відбувається підсумок всіх результатів та формування висновку аналізу у вигляді SWOT–матриці, в якій описується як застосувати сильні та слабкі сторони фірми для реалізації можливостей та уникненню загроз (результат на перетині відповідного рядка та стовпця).

Таблиця 6

SWOT-матриця стратегічних рішень

	Можливості (O)	Загрози (T)
Сильні сторони (S)	Переглянути рівень доступності клієнтських інтерфейсів та обновити його (S1-O3)	Використовуючи перевірені процеси найму працівників, набрати штати ІБ та маркетологів (S1-T2)
Слабкі сторони (W)	Регулярно проводити оцінку ефективності персоналу, добирати працівників в галузях, що не справляються через відсутність ресурсів (W1-O4)	Тримати провідні позиції на ринку надання інтернет з'єднання, впроваджуючи нові розробки для протистояння конкурентам в сфері телекомунікацій (W3-T3)

Для обчислення кількісної оцінки ризику ІБ застосувати статистичний метод. В Excel за допомогою вбудованих функцій знаходимо вибіркове середнє та середнє квадратичне відхилення. Зразок проведення статистичного методу представлено у дослідженні [13].

Для уточнення даних провести обчислення кількісного ризику ІБ за допомогою експертного методу. Проведення експертного методу описано у дослідженні [14].

Пропонуємо приклад обробки експертних даних для визначення:

- компетентність експертів і узагальнену оцінку об'єктів;
- узагальнене ранжування об'єктів;
- узгодженість оцінок експертів;

якщо дано $O=\{O_1,O_2,O_3,O_4,O_5,O_6\}-$ множина оцінювальних об'єктів;

$E=\{E_1,E_2,E_3,E_4,E_5\}-$ множина експертів;

$$A=(a)_{4x5}=\begin{pmatrix}1 & 2 & 3,5 & 3 & 4\\ 2,5 & 2 & 1,5 & 2 & 1\\ 2,5 & 2 & 3 & 1 & 2\\ 4 & 3,5 & 3,5 & 4 & 1\end{pmatrix}$$ – матриця оцінок об'єктів експертами.

І) Для розрахунку коефіцієнтів компетентності експертів (С) і узагальненої оцінки об'єктів (В) використаємо формули:

$$B\vec{x}=\lambda_B\vec{x}, C\vec{k}=\lambda_C\vec{k}, \sum_{i=1}^{n}x_i=1, \sum_{j=1}^{m}k_j=1,$$

n – об'єкти, m – експерти, $B=A\cdot A^T, C=A^T\cdot A, \vec{x}, \vec{k}$ – власні вектори матриць B і C відповідно, які відповідають власним числам λ_B, λ_C.

$$B=A\cdot A^T=\begin{pmatrix}1 & 2 & 3,5 & 3 & 4\\ 2,5 & 2 & 1,5 & 2 & 1\\ 2,5 & 2 & 3 & 1 & 2\\ 4 & 3,5 & 3,5 & 4 & 1\end{pmatrix}\cdot\begin{pmatrix}1 & 2,5 & 2,5 & 4\\ 2 & 2 & 2 & 3,5\\ 3,5 & 1,5 & 3 & 3,5\\ 3 & 2 & 1 & 4\\ 4 & 1 & 2 & 1\end{pmatrix}=$$

$$=\begin{pmatrix}42,25 & 21,75 & 28 & 39,25\\ 21,75 & 17,5 & 18,75 & 31,25\\ 28 & 18,75 & 24,25 & 33,5\\ 39,25 & 31,25 & 33,5 & 57,5\end{pmatrix}$$

$$C=A^T\cdot A=\begin{pmatrix}1 & 2,5 & 2,5 & 4\\ 2 & 2 & 2 & 3,5\\ 3,5 & 1,5 & 3 & 3,5\\ 3 & 2 & 1 & 4\\ 4 & 1 & 2 & 1\end{pmatrix}\cdot\begin{pmatrix}1 & 2 & 3,5 & 3 & 4\\ 2,5 & 2 & 1,5 & 2 & 1\\ 2,5 & 2 & 3 & 1 & 2\\ 4 & 3,5 & 3,5 & 4 & 1\end{pmatrix}=$$

ISSN 2663 - 4023

$$= \begin{pmatrix} 29,5 & 26 & 28,75 & 26,5 & 15,5 \\ 26 & 24,25 & 28,25 & 26 & 17,5 \\ 28,75 & 28,25 & 35,75 & 30,5 & 25 \\ 26,5 & 26 & 30,5 & 30 & 20 \\ 15,5 & 17,5 & 25 & 20 & 22 \end{pmatrix}$$

Для знаходження власних векторів матриць B і C скористаємося наближеним методом

$B = \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \dots & \dots & \dots \\ b_{n1} & \dots & b_{nn} \end{pmatrix}, \vec{y} = \begin{pmatrix} \sqrt[n]{b_{11} \cdot b_{12} \cdot \dots \cdot b_{1n}} \\ \dots \\ \sqrt[n]{b_{n1} \cdot b_{n2} \cdot \dots \cdot b_{nn}} \end{pmatrix}, \vec{x} = \begin{pmatrix} \frac{y_1}{\sum y_i} \\ \dots \\ \frac{y_n}{\sum y_i} \end{pmatrix}$ – нормований власний вектор.

Отже,

- коефіцієнти узагальненої оцінки об’єктів (B)

$$\vec{y} = \begin{pmatrix} 31,7 \\ 21,73 \\ 25,56 \\ 39,21 \end{pmatrix}, \qquad \vec{x} = \begin{pmatrix} 0,268 \\ 0,184 \\ 0,216 \\ 0,332 \end{pmatrix}$$

- коефіцієнти компетентності експертів (C)

$$\vec{y} = \begin{pmatrix} 24,63 \\ 24,08 \\ 29,45 \\ 26,31 \\ 19,72 \end{pmatrix}, \qquad \vec{k} = \begin{pmatrix} 0,198 \\ 0,194 \\ 0,237 \\ 0,212 \\ 0,159 \end{pmatrix}$$

2) Розрахунок узагальненого ранжування.

Побудуємо матриці ранжування експертів методом порівняння

$$y_{ik}^{j} = \begin{cases} 1, & x_{ij} \le x_{kj}; \\ 0, & x_{ij} > x_{kj} \end{cases}$$

$$y^1 = \begin{array}{c} \\ O_1 \\ O_2 \\ O_3 \\ O_4 \end{array} \begin{array}{c} \begin{array}{cccc} O_1 & O_2 & O_3 & O_4 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array}, \qquad y^2 = \begin{array}{c} \\ O_1 \\ O_2 \\ O_3 \\ O_4 \end{array} \begin{array}{c} \begin{array}{cccc} O_1 & O_2 & O_3 & O_4 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array},$$

$$y^3 = \begin{array}{c} \\ O_1 \\ O_2 \\ O_3 \\ O_4 \end{array} \begin{array}{c} \begin{array}{cccc} O_1 & O_2 & O_3 & O_4 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix} \end{array}, \qquad y^4 = \begin{array}{c} \\ O_1 \\ O_2 \\ O_3 \\ O_4 \end{array} \begin{array}{c} \begin{array}{cccc} O_1 & O_2 & O_3 & O_4 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array},$$

$$y^5 = \begin{array}{c} \\ O_1 \\ O_2 \\ O_3 \\ O_4 \end{array} \begin{array}{c} \begin{array}{cccc} O_1 & O_2 & O_3 & O_4 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \end{array}$$

Узагальнене ранжування отримаємо за формулою

$$y_{ik} = \begin{cases} 1, & a_{ik} \geq \dfrac{m}{2}; \\ 0, & a_{ik} < \dfrac{m}{2} \end{cases}, \quad \text{де } a_{ik} = \sum_{j=1}^{m} y_{ik}^{j}$$

$$y = \begin{array}{c} \\ O_1 \\ O_2 \\ O_3 \\ O_4 \end{array} \begin{array}{c} \begin{array}{cccc} O_1 & O_2 & O_3 & O_4 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array}, \qquad \text{отже } O_2 = O_3 > O_1 > O_4$$

Зауваження:

1. Якщо враховувати компетентність експертів k_j, то $y_{ik} = \begin{cases} 1, & b_{ik} \geq \dfrac{1}{2}; \\ 0, & b_{ik} < \dfrac{1}{2} \end{cases}$, де

$$b_{ik} = \sum_{j=1}^{m} k_j y_{ik}^{j}$$

2. Якщо відомі ймовірності $p_1, p_2, ..., p_d$ проявів тієї чи ситуації, то

$$y_{ik} = \begin{cases} 1, & c_{ik} \geq \dfrac{1}{2}; \\ 0, & c_{ik} < \dfrac{1}{2} \end{cases}, \quad \text{де } c_{ik} = \sum_{j=1,s=1}^{m,d} k_j \cdot p_s \cdot y_{ik}^{js}$$

3) Розрахунок дисперсійного коефіцієнта конкордації експертів (коефіцієнт узгодженості)

$$W = \frac{12 \cdot S}{m^2 \left(n^3 - n\right) - m \cdot \sum_{j=1}^{m} T_j},$$

де

$T_j = \sum_{k=1}^{H_j} \left(h_k^3 - h_k\right)$ - показник зв'язних рангів в j-ранжуванні,

H_j – число груп рівних рангів в j-ранжуванні,

h_k – число рівних рангів у k-групі при j-ранжуванні,

$S = \sum_{i=1}^{n} \left(r_i - \bar{r}\right)^2$ –дисперсія,

ISSN 2663 - 4023

$\bar{r} = \frac{1}{n}\sum_{i=1}^{n} r_i$ – вибіркове середнє.

	E_1	E_2	E_3	E_4	E_5	r_i	$\bar{r}$	$\left(r_i - \bar{r}\right)^2$	S
O_1	1	2	3,5	3	4	13,5	12,25	1,5625	29,25
O_2	2,5	2	1,5	2	1	9		10,5625	
O_3	2,5	2	3	1	2	10,5		3,0625	
O_1	4	3,5	3,5	4	1	16		14,0625	
H_j	1	1	1	0	1				
h_k	2	3	2	0	2				
T_j	6	24	6	0	6				

$$W = \frac{12 \cdot 29,25}{5^2\left(4^3 - 4\right) - 5 \cdot 42} = \frac{351}{1500 - 210} = \frac{351}{1290} \approx 0,272 .$$

Статистичну значущість коефіцієнта конкордації перевіримо за допомогою критерія Пірсона (χ^2–критерій).

$$\chi^2_{\text{сп}} = m(n-1)W = 5 \cdot 3 \cdot 0,272 = 4,08$$
$$\chi^2_{\text{кр}} = \chi^2_{\text{кр}}(\alpha; n-1) = \chi^2_{\text{кр}}(0,1; 3) = 6,251$$

H_0: узгодження ранжування експертами не є значущим.

H_1: узгодження ранжування експертами є значущим.

Оскільки $\chi^2_{\text{сп}} < \chi^2_{\text{кр}}$, то приймається гіпотеза H_0, ранжування експертами не є узгодженим. Пропонується обговорити результати експерименту, у протилежному випадку розформувати експертну групу.

Крок 5. Обчислити ступінь ризику $r_{ij} = p_i q_j$.

Крок 6. Створити ранжований список ризиків ІБ.

Пропонуємо здійснити це у такому вигляді, як представлено у таблиці 7.

Таблиця 7

Ранжований список ризиків

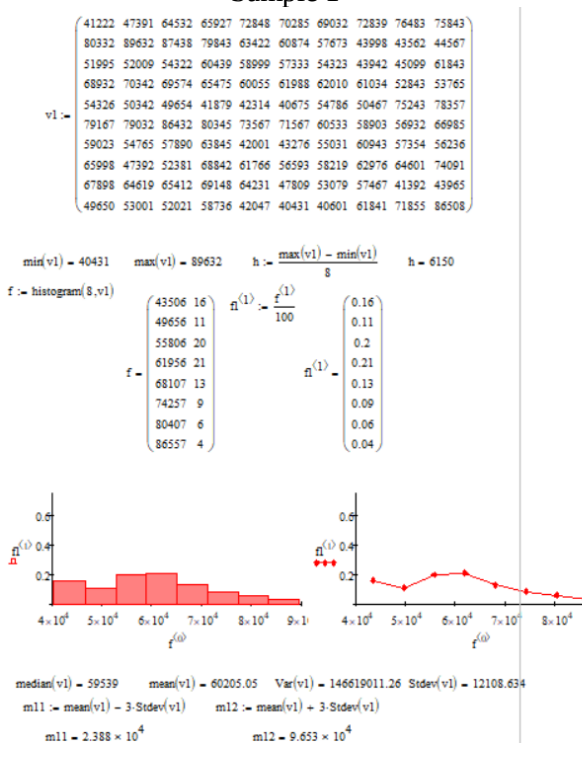
Актив	Загроза	Уразливість	Ймовірність реалізації	Рівень ризику
ПК №1 типу Б (персональні комп'ютери бухгалтерії з корпусу 1)	Загроза: Проникнення шкідливого ПО Джерело загрози: Антропогенне Тип загрози: Внутрішня Порушення властивостей: К, Ц, Д	Відсутність антивірусного ПО, відсутність розмежування прав доступу до інформаційних ресурсів	0.8 (висока)	0.8 * (22000 + 15200 + 34800) = 57600 у. е. (високий)
База даних	Загроза: Помилка в роботі бази Джерело загрози: Антропогенне, техногенне Тип загрози: Внутрішня Порушення властивостей: Ц, Д	Відсутність регламенту технічного обслуговування, використання застарілого ПЗ	0.6 (середня)	0.6 * (25000 + 41000) = 39600 у. е. (середній)

Сайт компанії	Загроза: Помилка в роботі серверу Джерело загрози: Антропогенне, техногенне Тип загрози: Внутрішня Порушення властивостей: Ц, Д	Відсутність регламенту проведення технічного обслуговування	0.5 (низька)	0.5 * (16000 + 18800) = 25400 у. е. (середній)

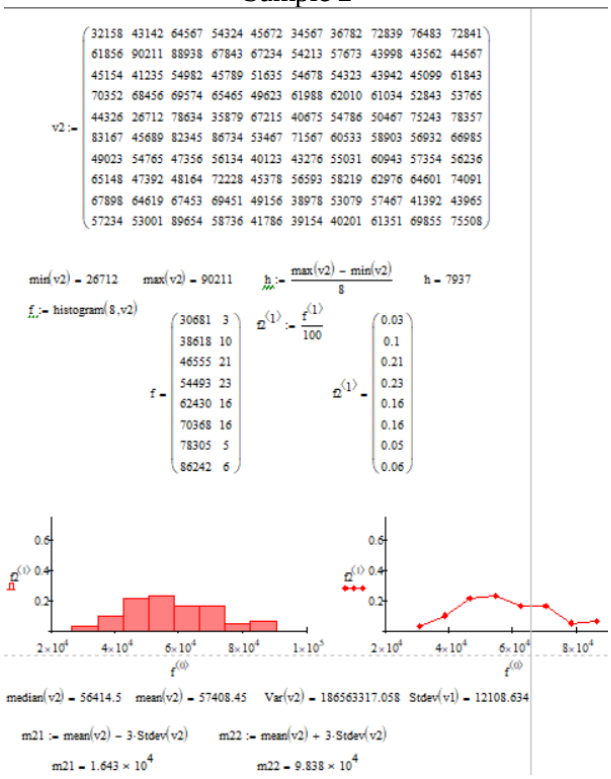
Крок 7. Підрахувати загального ступень ризику $R_n = \sum r_{ij}$ для кожного інформаційного ресурсу
Крок 8. Порівняти емпіричний ступень ризику зі ступенем критичним, який визначено в організації.
Якщо $R_n < R_{\text{гран}}$, то крок 11, у протилежному випадку – крок 9
Крок 9. Обробити емпіричний ступень ризику та обчислити залишковий ризик $R_{\text{залишк}}$
Крок 10. Порівняти залишковий ступень ризику зі ступенем критичним.
Якщо $R_n < R_{\text{гран}}$, то крок 11, у протилежному випадку – крок 12
Крок 11. Прийняти ризик
Крок 12. Згенерувати сценарій інцидентів за допомогою методу Монте-Карло.

При використанні статистичних методів використовують гіпотези про найбільш ймовірні закони розподілу випадкових величин, у нашому випадку – інцидентів у сфері ІБ. Є очевидним, враховуючи те, що нанесення збитків після інциденту по класифікації «низька», «середня», «висока» мають великі порядки розбіжності, є очевидним, що випадкова величина у такому вигляді не є розподіленою по нормальному закону. Тому ми пропонуємо усереднити оцінку збитків і, враховуючи результати дослідження [13], застосувати метод Монте-Карло для імітації інциденту. Було вибрано три вибірки інцидентів за 100 днів кожного року і здійснена статистична обробка за допомогою MathCad (Рис. 3).

Sample 1



Sample 2



Sample 3

ISSN 2663 - 4023

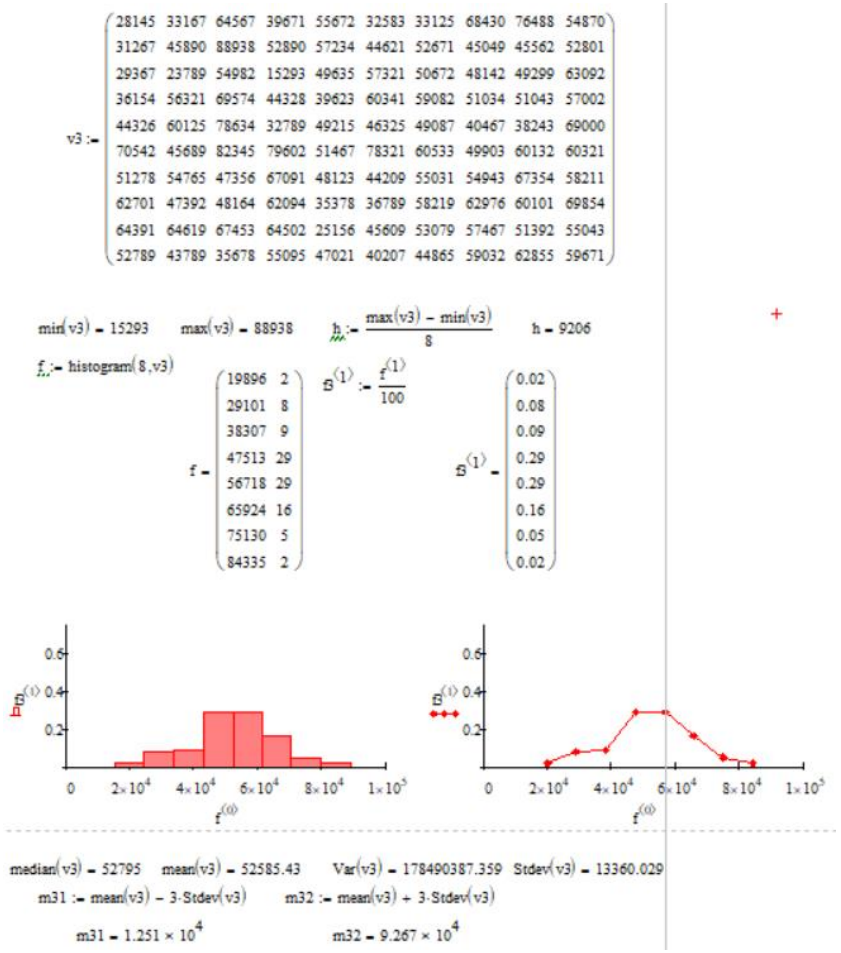
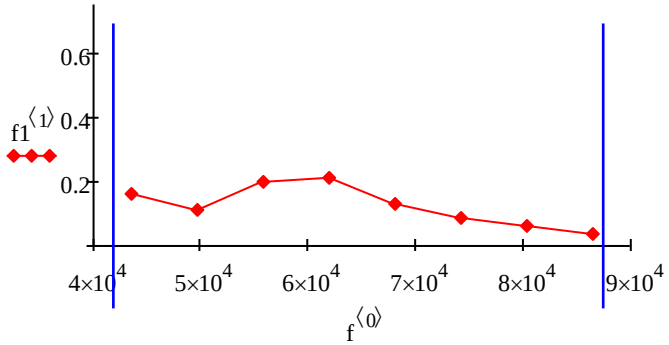


Рис. 3 Статистична обробка даних в MathCad

На основі правила трьох сігм $\bar{x} - 3\sigma \leq X \leq \bar{x} + 3\sigma$ для кожної вибірки знаходимо інтервал, на основі якого здійснюємо прогнозування щодо інцидентів у майбутньому (Рис. 4).



.

ISSN 2663 - 4023

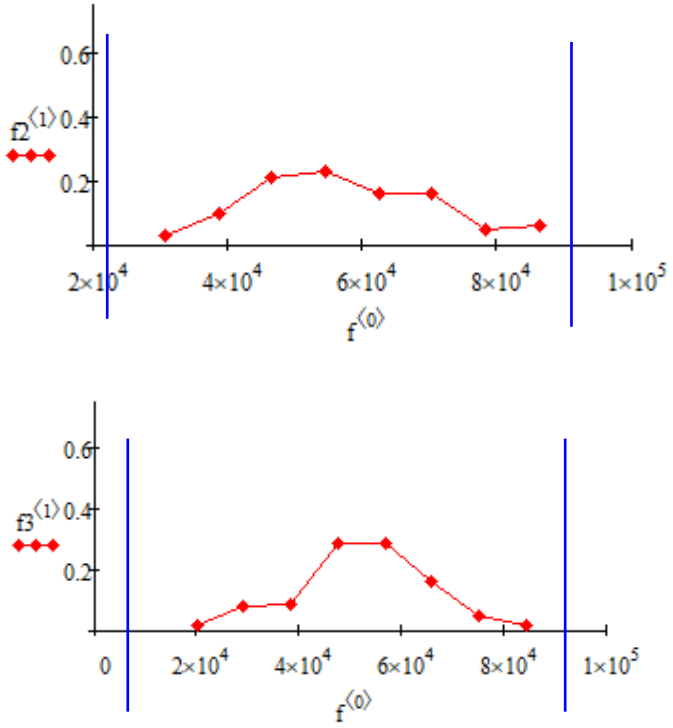


Рис. 4 Прогнозовані інтервали

Найбільшу ймовірність (приблизно 0,3) інцидентів відбувається близько 60000 в день. Практично достовірна подія, якщо в день відбувається від 40000 до 100000 інцидентів (Рис. 5).

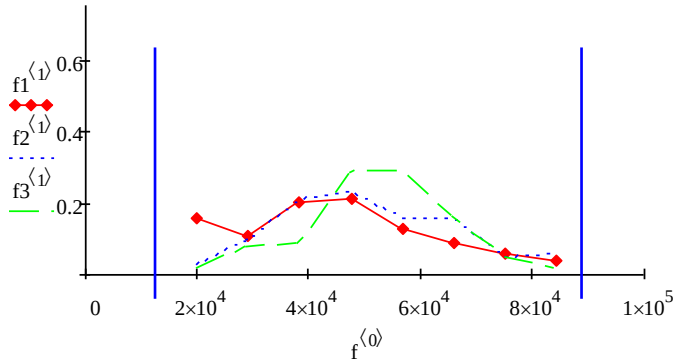


Рис. 5 Загальний інтервал

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Обробка, передача та захист інформації пов'язані з ризиками, які необхідно враховувати, оцінювати та керувати для успішної роботи організації, і такий процес має носити безперервний характер. Тому процес аналізу ризиків ІБ є одним з ключових етапів побудови системи управління інформаційної безпеки на будь-якому підприємстві. Подальші напрямки наукової роботи будуть спрямовані на дослідження законів розподілу випадкових величин в теорії ризиків ІБ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Shepherd, M. (2019). *30 Surprising Small Business Cyber Security Statistics (2021) - Fundera Ledger*. Fundera: Compare Your Best Small Business Loan and Credit Card Options. https://www.fundera.com/resources/small-business-cyber-security-statistics

2 Catteddu, D., & Hogben, G. (2009). *Cloud Computing: Benefits, risks and recommendations for information security*. ENISA.

3 Alali, M., Almogren, A., Hassan, M. M., Rassan, I. A. L., Bhuiyan, M. Z. A. (2018). Improving risk assessment model of cyber security using fuzzy logic inference system. *Computers & Security*, *74*, 323–339. https://doi.org/10.1016/j.cose.2017.09.011

4 Shin, J., Son, H., Heo, G. (2017). Cyber Security Risk Evaluation of a Nuclear I&C Using BN and ET. *Nuclear Engineering and Technology*, *49*(3), 517–524. https://doi.org/10.1016/j.net.2016.11.004

5 Савельєва, Т. В., Панаско, О. М., Пригодюк, О. М. (2018). Аналіз методів і засобів для реалізації ризик-орієнтованого підходу в контексті забезпечення інформаційної безпеки підприємства. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, *1*(1), 81–89. https://doi.org/10.24025/2306-4412.1.2018.153279

6 Архипов, О., Муратов, О., Бровко, В. (2019). *Основи теорії ризиків: навчальний посібник*. НА СБ України.

7 Ахметов, Б., Корченко, А., Архипов, А., & Казмирчук, С. (2018). *Построение систем анализа и оценивания рисков информационной безопасности. Теория и практические решения*. редакционно-издательский отдел КГУТИ им. Ш. Есенова. https://er.nau.edu.ua/handle/NAU/40479?locale=uk

8 Shevchenko, H., Shevchenko, S., Zhdanova, Yu., Spasiteleva, S., Negodenko, O. Information Security Risk Analysis SWOT. *Cybersecurity Providing in Information and Telecommunication Systems, 2923*, 309-317.

9 *Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки* (ДСТУ ISO/IEC 27005:2019). (2019).

10 *Положення, Постанова №95 от 28.09.2017, Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України*. (б. д.). Законодавство України - Законодательство Украины. http://search.ligazakon.ua/l_doc2.nsf/link1/PB17146.html

11 Stephenson, P. R. (2004). A formal model for information risk analysis using colored petri nets. У *Proceedings of the Fifth Workshop and Tutorial on Practical Use of Coloured Petri Nets and the CPN Tools* (с. 167–184). DAIMI PB - 570 / Kurt Jensen (Ed.).

12 Невойт, Я. В. (2016). *Метод оцінювання стану захищеності інформаційних ресурсів на основі дослідження джерел загроз інформаційній безпеції* [Дис. канд. техн. наук, ДУТ]. http://www.dut.edu.ua/uploads/p_1539_26349739.pdf

13 Шевченко, С., Жданова, Ю., Спасітєлєва, С., Адамович, О. (2017). Статистична обробка експериментальних даних як одна з форм науково-дослідної роботи студентів спеціальності «Кібербезпека». *Сучасний захист інформації, 2*(30), 95-103.

14 Бурячок, В. Л., Толубко, В. Б., Хорошко, В. О., Толюпа, С. В. (2015). *Інформаційна та кібербезпека: соціотехнічний аспект : підручник*. ДУТ.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (14), 2021
ISSN 2663 - 4023

Yuliia D. Zhdanova
PhD, Associate Professor, Associate Professor of the Department of Information and Cyber Security Professor Vladimir Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID: 0000-0002-9277-4972
y.zhdanova@kubg.edu.ua

Svitlana M. Shevchenko
PhD, Associate Professor, Associate Professor of the Department of Information and Cyber Security Professor Vladimir Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID: 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

Kateryna V. Kravchuk
master of the Faculty of Information Technology and Management
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID: 0000-0002-3589-8784
kvkravchuk.fitu20@kubg.edu.ua

INFORMATION PROTECTION MODEL BASED ON INFORMATION SECURITY RISK ASSESSMENT FOR SMALL AND MEDIUM-SIZED BUSINESS

Abstract. This study focuses on the protection of information resources on the basis of risk-oriented approach for small and medium-sized businesses with an emphasis on risk assessment of information security (IS). The analysis of scientific sources allowed to characterize the essence of the risk-oriented approach and to formulate the main provisions for creating a model of information protection based on this technology. The content line of the model focuses on conducting qualitative and quantitative IS risk assessment, namely, SWOT-analysis, statistical method, expert assessment method and Monte Carlo method. The step-by-step procedure of carrying out the stages of analysis and implementation of these methods for IS risk assessment is described. In order to obtain a comprehensive map of IS risks at the initial stage, it is proposed to conduct a SWOT analysis, in particular to identify business weaknesses and external and internal threats. Use a statistical method to quantify IS risk if there are sufficient analytical reports. Otherwise, implement the method of expert assessments. The final step is to generate a script using the Monte Carlo method. To effectively describe the context of each information resource, use the technology of forming multiple pairs "threat - vulnerability".
The relevance and possibilities of using this model as a methodology of information for small and medium businesses are substantiated.

Keywords: information security (IS) risks; SWOT analysis; statistical methods; method of expert assessments; Monte Carlo method; threats; vulnerabilities; information protection model.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 Shepherd, M. (2019). *30 Surprising Small Business Cyber Security Statistics (2021) - Fundera Ledger*. Fundera: Compare Your Best Small Business Loan and Credit Card Options. https://www.fundera.com/resources/small-business-cyber-security-statistics

2 Catteddu, D., & Hogben, G. (2009). *Cloud Computing: Benefits, risks and recommendations for information security*. ENISA.

3 Alali, M., Almogren, A., Hassan, M. M., Rassan, I. A. L., Bhuiyan, M. Z. A. (2018). Improving risk assessment model of cyber security using fuzzy logic inference system. *Computers & Security*, *74*, 323–339. https://doi.org/10.1016/j.cose.2017.09.011

4 Shin, J., Son, H., Heo, G. (2017). Cyber Security Risk Evaluation of a Nuclear I&C Using BN and ET. *Nuclear Engineering and Technology*, *49*(3), 517–524. https://doi.org/10.1016/j.net.2016.11.004

5 Savelieva, T. V., Panasko, O. M., Pryhodiuk, O. M. (2018). Analiz metodiv i zasobiv dlia realizatsii ryzyk-oriientovanoho pidkhodu v konteksti zabezpechennia informatsiinoi bezpeky pidpryiemstva. *Visnyk*

Cherkaskoho derzhavnoho tekhnolohichnoho universytetu. Seriia: Tekhnichni nauky, *1*(1), 81–89. https://doi.org/10.24025/2306-4412.1.2018.153279

6 Arkhypov, O., Muratov, O., Brovko, V. (2019). *Osnovy teorii ryzykiv: navchalnyi posibnyk*. NA SB Ukrainy.

7 Akhmetov, B., Korchenko, A., Arkhypov, A., & Kazmyrchuk, S. (2018). Postroenye system analyza y otsenyvanyia ryskov ynformatsyonnoi bezopasnosty. Teoryia y praktycheskye reshenyia. redaktsyonno-yzdatelskyi otdel KHUTY ym. Sh. Esenova. https://er.nau.edu.ua/handle/NAU/40479?locale=uk

8 Shevchenko, H., Shevchenko, S., Zhdanova, Yu., Spasiteleva, S., Negodenko, O. Information Security Risk Analysis SWOT. *Cybersecurity Providing in Information and Telecommunication Systems, 2923*, 309-317.

9 *Informatsiini tekhnolohii. Metody zakhystu. Upravlinnia ryzykamy informatsiinoi bezpeky* (DSTU ISO/IEC 27005:2019). (2019).

10 *Polozhennia, Postanova №95 ot 28.09.2017, Pro zatverdzhennia Polozhennia pro orhanizatsiiu zakhodiv iz zabezpechennia informatsiinoi bezpeky v bankivskii systemi Ukrainy.* Zakonodavstvo Ukrainy - Zakonodatelstvo Ukrayny. http://search.ligazakon.ua/l_doc2.nsf/link1/PB17146.html

11 Stephenson, P. R. (2004). A formal model for information risk analysis using colored petri nets. У *Proceedings of the Fifth Workshop and Tutorial on Practical Use of Coloured Petri Nets and the CPN Tools* (с. 167–184). DAIMI PB - 570 / Kurt Jensen (Ed.).

12 Nevoit, Ya. V. (2016*). Metod otsiniuvannia stanu zakhyshchenosti informatsiinykh resursiv na osnovi doslidzhennia dzherel zahroz informatsiinii bezpetsii* [Dys. kand. tekhn. nauk, DUT]. http://www.dut.edu.ua/uploads/p_1539_26349739.pdf

13 Shevchenko, S., Zhdanova, Yu., Spasitielieva, S., Adamovych, O. (2017). Statystychna obrobka eksperymentalnykh danykh yak odna z form naukovo-doslidnoi roboty studentiv spetsialnosti «Kiberbezpeka». *Suchasnyi zakhyst informatsii, 2*(30), 95-103.

14 Buriachok, V. L., Tolubko, V. B., Khoroshko, V. O., Toliupa, S. V. (2015). *Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt : pidruchnyk*. DUT.