АВТОМАТИЗОВАНИЙ АНАЛІЗ СТРАТЕГІЙ ІНВЕСТУВАННЯ В ІНФОРМАЦІЙНУ БЕЗПЕКУ НА ОСНОВІ ЕКСПЕРТНИХ ІМОВІРНІСНИХ ОЦІНОК

Кравченко Владислав Романович
здобувач вищої освіти ОС "Магістр",
Харківський національний економічний університет імені Семена Кузнеця
Харків, Україна,

Солодовник Ганна Валеріївна
к.т.н, доцент,
доцент кафедри кібербезпеки та інформаційних технологій
Харківський національний економічний університет імені Семена Кузнеця
Харків, Україна,

Актуальність. Сьогодні підприємства України працюють в умовах підвищеної турбулентності зовнішнього середовища. Глобалізація економіки зумовлює значний конкурентний тиск, відтік трудових ресурсів та руйнація інфраструктури значно знижують виробничі потужності, цифровізація бізнес-процесів та війна в сфері цифрових технологій спричиняють зростання інформаційних ризиків для організацій різних типів. Можливість спотворення та знищення інформаційних ресурсів є одним з багатьох чинників, які призводять до паралічу функціонування або навіть знищення підприємства. Тому у фінансовій та організаційно-управлінській сферах будь-якої установи питання інвестицій у заходи з підвищення інформаційного захисту складають значну частку.

Сучасні атаки стають більш цілеспрямованими, автоматизованими та економічно вмотивованими, що збільшує ймовірність успішних компрометацій навіть у компаніях із базовими засобами захисту. Водночас поширення використання хмарних сервісів, мобільних застосунків та віддалених робочих середовищ у бізнесі призводять до значного розширення сфер, які охоплюють такі атаки. Кім того економічні наслідки інцидентів інформаційної безпеки стають все відчутнішими: порушення доступності сервісів, втрата даних, фінансові збитки, зниження репутаційної довіри та можливі штрафи за недотримання вимог регуляторів. Значення інформаційної безпеки у конкурентному середовищі значно зростає через те, що компанії, які демонструють високий рівень захищеності, здобувають переваги у співпраці з партнерами, інвесторами та клієнтами. Таким чином, інвестиції у підвищення рівня захисту є не лише технічним, а й стратегічним управлінським рішенням.

Наведені факти обумовлюють актуальність розробки програмного інструментарію підтримки прийняття рішень щодо інвестицій у підвищення рівня інформаційного захисту, які наразі набувають сенсу не лише технічних, а й стратегічних управлінських рішень.

Метою роботи є розробка застосунку вибору стратегії інвестування в інформаційну безпеку підприємства в умовах невизначеності. Об'єктом є процес прийняття управлінських рішень щодо інвестування в систему інформаційної безпеки підприємства. Предметом – методи, моделі та програмні засоби вибору оптимальної стратегії інвестування в інформаційну безпеку підприємства в умовах невизначеності.

Аналіз інформаційних джерел. Через значну актуальність питання визначення найкращої стратегії захисту в інформаційних системах є предметом багатьох вітчизняних та закордонних науковців. В досліджені [1], яке розглядає питання захисту інформаційних ресурсів з позиції ризик-орієнтованого підходу, для кількісної оцінки ризику інформаційної безпеки (ІБ) застосовано статистичний метод, а метод експертних оцінок використано лише як альтернативний. Поєднання статистичних та експертних оцінок в [2] використано для оцінювання ризиків ІБ. З експертних методів застосовано метод попарних порівнянь з подальшим визначенням узгодженості думок експертів. Програмна реалізація запропонованих моделей розроблена у середовищі електронних таблиць.

Метод попарних порівнянь та аналізу ієрархій використовуються в багатьох дослідженнях іноземних колег. Так у [3] метод аналізу ієрархій та багатокритеріальний аналіз є інструментом визначення пріоритетів для заходів інформаційної безпеки університету. Експертні оцінювання використовуються для визначення ваг критеріїв оцінювання альтернатив стратегії захисту інформаційних ресурсів. Класичним прикладом застосування методу рейтингів є дослідження [4], в якому визначається оптимальний розподіл бюджету на підвищення рівня безпеки інформаційної системи організації на підставі розрахунку критеріїв та підкритеріїв оцінювання альтернативних пропозицій розподілу бюджету. В роботі [5] проведено огляд застосувань методів багатокритеріального прийняття рішень щодо безпеки в інформаційних системах з наголосом на те, що такі методи спираються на суб'єктивні експертні судження в питаннях зважування критеріїв та вибору найкращої альтернативи рішення.

Аналіз інформаційних джерел виявив недостатню увагу до експертних методів у сфері кількісного аналізу інформаційних ризиків. Слід визнати, що перевагою статистичних методів є їх об'єктивність та наукова обґрунтованість завдяки використанню математичного апарату, але ці методи потребують достатньої кількості статистичних даних. Проте під час вирішення проблеми формування стратегії захисту інформації часто вникає ситуація відсутності достовірної та повної інформації, що породжує умови невизначеності. Основними причинами виникнення такої ситуації є значна турбулентність зовнішнього середовища та динамічність і складність об'єктів інформатизації. Іншою причиною є фінансова та технічна обмеженість щодо збору та обробки повної інформації, так званий економічно-оптимальний півень невизначеності. Тому в деяких ситуаціях кращим варіантом є застосування евристичних методів, які спираються на використання персональних якостей конкретних людей та передбачають використання творчого мислення у процесі розробки рішення, а

також надають можливості генерації нових ідей, використання яких підвищує ефективність управлінських рішень. Окремою групою евристичних методів є методи експертного оцінювання. Спираючись на проведений аналіз за методологічний інструментарій вирішення проблеми вибору стратегії інвестування в інформаційну безпеку підприємства в умовах невизначеності слід обрати метод Дельфі, який належить до групи методів колективних експертних оцінювань.

Основним недоліком експертних оцінок є їх високий рівень суб'єктивності, внаслідок чого відсутня впевненість у достовірності отриманих результатів. Крім того можливим є виникнення негативних процесів таких як упередженість експертів, вплив авторитету, значна зашумленість тривіальними ідеями, феномен зрушення оцінок в бік підвищення їх ризикованості. Нівелювати зазначені негативні риси дозволяє метод Дельфі [6], який передбачає проведення кількох турів анонімних опитувань достатньої кількості експертів за умови їх ознайомлення з оцінками та коментарями колег без зазначення авторства. Аналіз даних аналітичною групою передбачає обчислення: середньогрупової самооцінки, як середньоарифметичного всіх самооцінок; простої оцінки, як середньоарифметичного від усіх оцінок; середньозваженої оцінки, як суми добутків оцінок та самооцінок, поділеної на суму всіх самооцінок; медіани; довірчого інтервалу, ліва границя якого обчислюється як сума мінімальної оцінки та квартилі, а права – як різниця між максимальною оцінкою та квартилю. Ступінь погодженості експертних думок за використання цього метода визначається розміром довірчого інтервалу, а остаточна оцінка – медіаною. Укрупнена блок схема проведення опитування методом Дельфі наведена на рисунку 1.

В даній роботі завдання було сформульовано наступним чином. Компанія розглядає питання підвищення ефективності власної системи захисту інформації. Відомі розміри можливих збитків за наявного рівня захисту у разі реалізації значних загроз та активних атак на інформаційні ресурси (несприятливий стан). За умови впровадження заходів із удосконалення системи захисту компанія не зазнає фінансових втрат у цьому сценарії. Якщо ж рівень загроз є низьким (сприятливий стан), то за поточного рівня захисту очікувані збитки є незначними. Необхідно прийняти обґрунтоване управлінське рішення щодо доцільності інвестування в заходи підвищення рівня інформаційної безпеки компанії з урахуванням вартості модернізації системи захисту інформації.

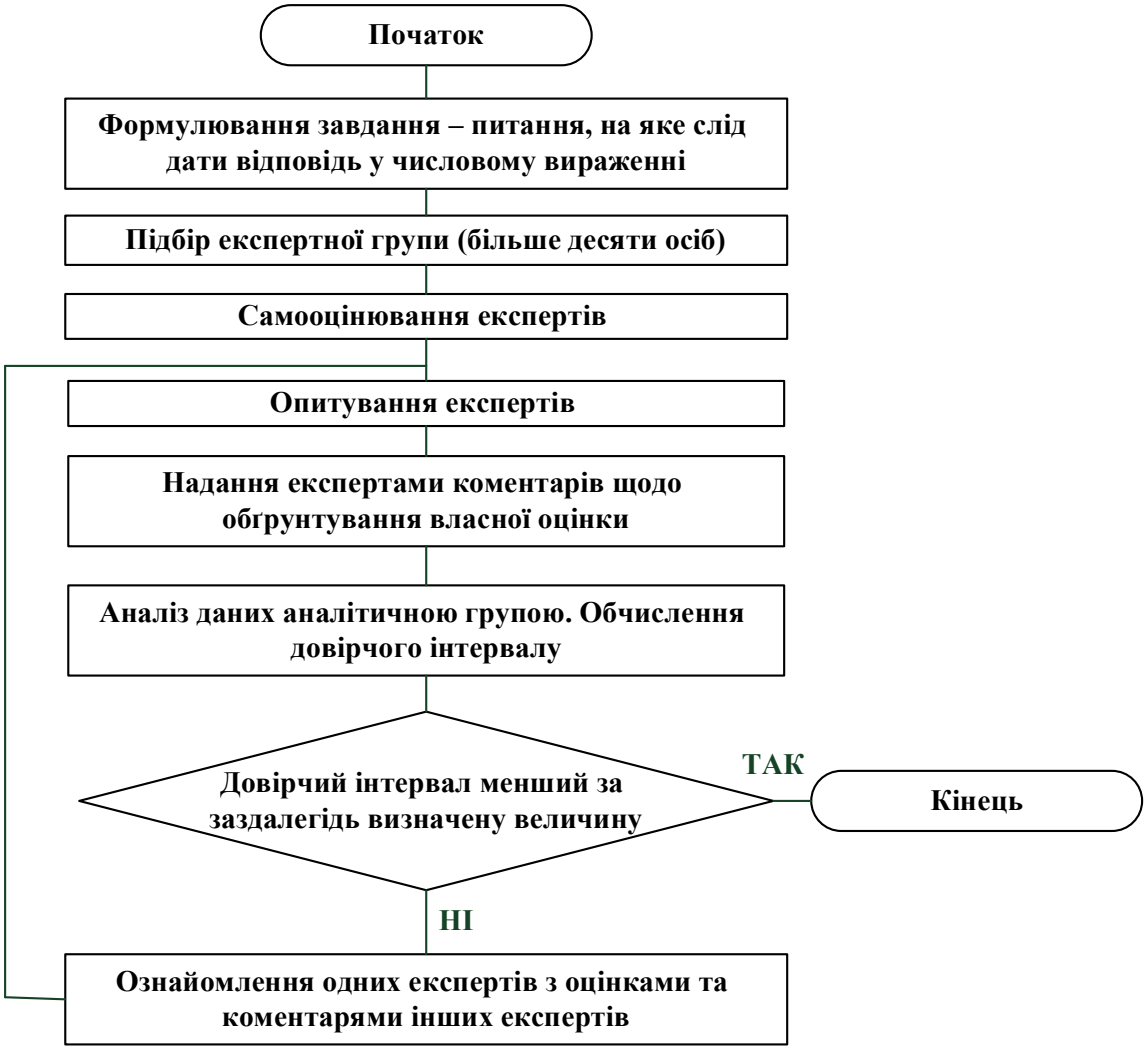

Рисунок 1. Блок-схема алгоритму методу Дельфі
Джерело: власна розробка авторів

Використання експертних методів для розв'язання цієї задачі є обґрунтованим з огляду на специфіку інформаційної безпеки та характер наявних даних. Динамічність кіберзагроз робить статистичні дані неактуальними стосовно рівня та структури ризиків. Особливості параметрів, які впливають на інформаційні ризики, такі як вмотивованість зловмисників, складність архітектури, швидкість реагування, є якісними й не підлягають кількісному вимірюванню. Під час розробки управлінського рішення щодо інвестування у систему захисту інформації слід враховувати компетентні оцінки спеціалістів, які мають практичний досвід роботи із системами безпеки, технологіями захисту та аналізом інцидентів для точнішого визначення очікуваного рівня ризику. Тому оцінка ймовірності появи значних атак потребує залучення фахівців, які глибоко розуміють поточні тенденції, особливості інфраструктури об'єкта автоматизації та потенційні вектори атак. В цій ситуації експертні методи і, зокрема метод експертного опитування Делфі, дозволяє формалізувати суб'єктивні судження фахівців і перетворити їх на узгоджені кількісні оцінки.

Проблема оцінювання рівня загроз та ймовірності настання сприятливого чи несприятливого стану інформаційного середовища належить до класу слабоструктурованих задач, для яких відсутні точні статистичні дані або їх обсяг є недостатнім для застосування класичних імовірнісно-статистичних підходів. Тому розв'язання сформульованої задачі передбачає визначення ймовірності сприятливого стану методом Дельфі та визначення найкращої стратегії за значенням середньо ймовірного рівня втрат.

Програмними засобами автоматизації розв'язання обрані засоби вільного програмного забезпечення: мова програмування Python та середовище розробки Visual Studio Code. З економічної точки зору використання вільного програмного забезпечення дозволяє суттєво знизити витрати на придбання ліцензійного програмного забезпечення. Доступ до вихідного коду такого забезпечення дає можливість отримувати допомогу від глобальної IT-спільноти, сприяє підвищенню рівня безпеки завдяки прозорості через проведення аудиту та оцінки безпеки незалежним експертам.

Робота застосунку представлена екранними формами: на рисунку 2 наведено екрану форму введення початкових даних та проміжних результатів другого туру проведення експертних опитувань методом Дельфі, на рисунку 3 – графічне зображення результатів розрахунків. Вихідними даними роботи застосунку є автоматично сформований у текстовому вигляді висновок за задачею: яку стратегію інвестування слід обрати. Вхідними даними моделі є: розміри можливих збитків за наявного рівня захисту у разі реалізації несприятливого сценарію атак на інформаційну систему; розміри можливих збитків за наявного рівня захисту у разі реалізації сприятливого сценарію атак на інформаційну систему; вартість модернізації системи захисту інформації. Параметром є кількість експертів, які приймають участь у опитуванні.

На початку роботи кожен експерт надає самооцінку, яка відбиває його суб'єктивну оцінку власного рівня досвіду та ознайомленості із запропонованою проблемою. На підставі цих даних розраховується середньогрупова самооцінка. Під час відбору експертів можуть враховуватися абсолютна (відношення кількості правильно проведених експертиз до їх загальної кількості) та відносна (відношення абсолютної ефективності до середньої абсолютної ефективності групи експертів) ефективності діяльності експертів, на підставі яких можна розрахувати вагові коефіцієнти компетентності.

Кожен етап опитувань завершується розрахунком простої оцінки, середньозваженої оцінки, медіани та довірчого інтервалу, які складають проміжні результати. На підставі розміру довірчого інтервалу суб'єкт прийняття рішень здійснює вибір щодо проведення наступного туру експертних опитувань.

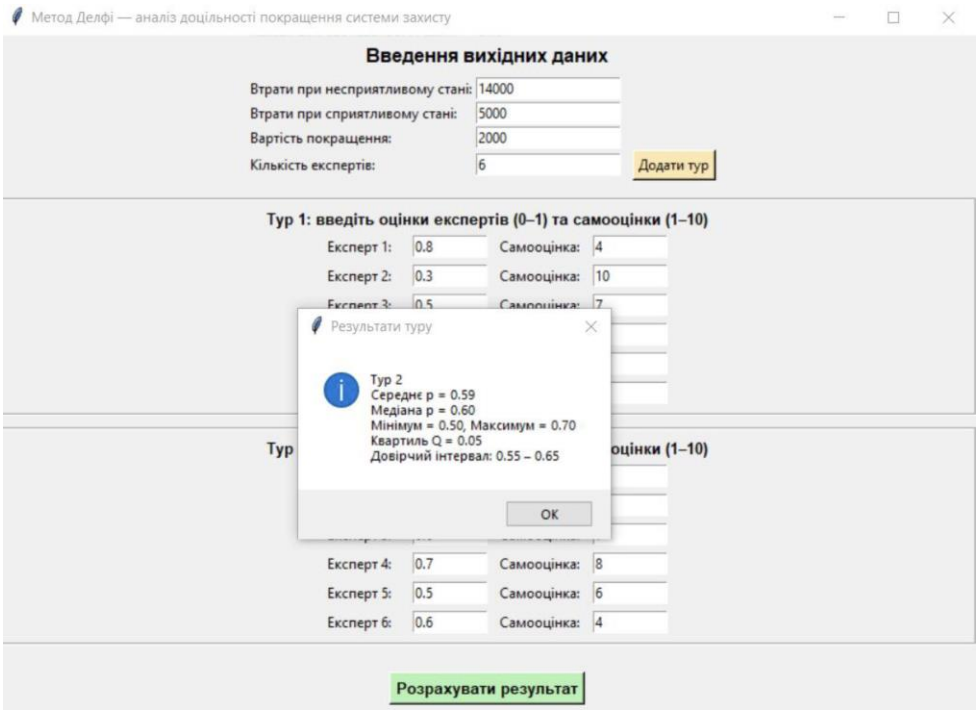

Рисунок 2. Екрана форма введення початкових даних
Джерело: власна розробка авторів

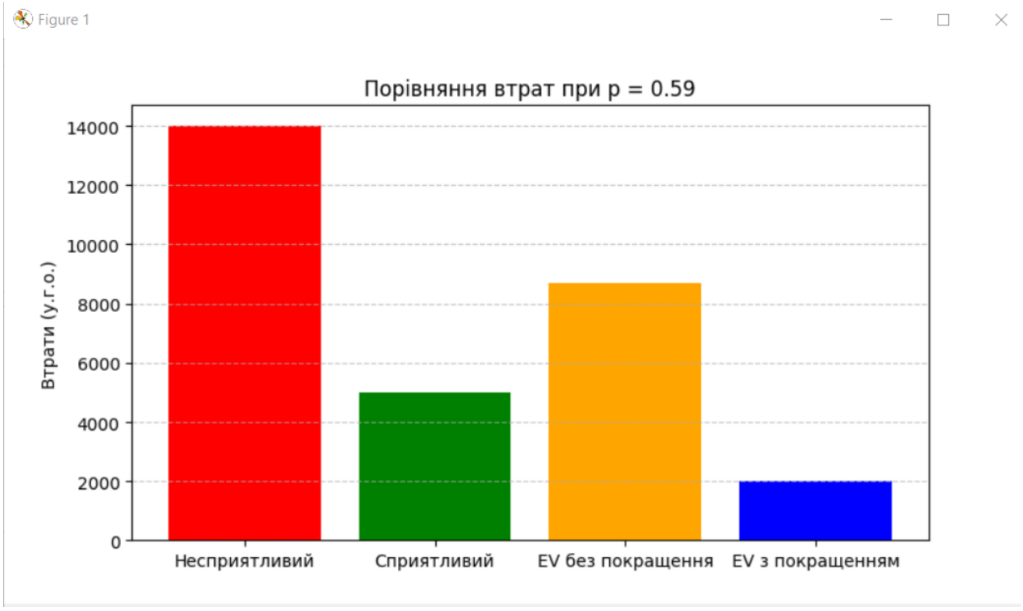

Рисунок 3. Екрана форма результатів роботи застосунку
Джерело: власна розробка авторів

Ітерації опитування припиняються за виконання однієї з умов: розмір довірчого інтервалу задовольняє суб'єкт прийняття рішень, тоді робота програми передбачає розрахунок очікуваних втрат як середнє значення втрат зважене за ймовірностями настання сприятливого та несприятливого станів, які визначили експерти на останньому турі опитування, або розмір довірчого інтервалу збільшується (залишається незмінним) відносно попереднього туру, в цьому випадку слід переглянути формулювання завдання опитування або склад експертної групи.

Висновки. Огляд інформаційних джерел та аналіз задачі підвищення ефективності системи захисту інформації дозволив визначити актуальність створення застосунку вибору стратегії інвестування в інформаційну безпеку підприємства в умовах невизначеності. Практичне значення автоматизації розв'язання задачі в запропонованій постановці полягає в тому, що вона дозволяє здійснити формалізований аналіз ризиків і визначити раціональну стратегію поведінки організації в умовах невизначеності. Подальший розвиток роботи полягає у: додаванні кількості сценаріїв атак до параметрів моделі; доопрацюванні інтерфейсу з метою отримання коментарів від експертів та надання їм можливості ознайомлення з коментарями колег; розробці моделі розрахунку вагових коефіцієнтів компетентності експертів на підставі абсолютної та відносної ефективності їх діяльності з подальшою інтеграцію автоматизації такої моделі до створеного у роботі застосунку.

Список літератури

1. Шевченко С. Модель захисту інформації на основі оцінки ризиків інформаційної безпеки для малого та середнього бізнесу // *Комп'ютерна безпека*. 2021. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/321/269

2. Дзюба Л.Ф. Оцінювання ризиків інформаційної безпеки з використанням методів математичної статистики // *Вісник Львівського державного університету безпеки життєдіяльності*. 2022. URL: https://journal.ldubgd.edu.ua/index.php/Visnuk/article/view/2470

3. Cabrera J.S., Reyes A.R.L., Lasco C.A. Multicriteria Decision Analysis on Information Security Policy: A Prioritization Approach // *Advances in Technology Innovation*. 2021. Т. 6, № 1. С. 31–38. URL: https://ojs.imeti.org/index.php/AITI/article/view/5476

4. Bodin L., та ін. Evaluating Information Security Investments Using the Analytic Hierarchy Process // *Communications of the ACM*. URL: https://cacm.acm.org/research/evaluating-information-security-investments-sing-the-analytic-hierarchy-process

5. Madanchian M., та ін. Applications of Multi-Criteria Decision Making in Information Systems for Strategic and Operational Decisions // *Computers*. 2025. Т. 14, № 6. Стаття 208. URL: https://www.mdpi.com/2073-431X/14/6/208

6. Nugraha Y., та ін. An Adaptive Wideband Delphi Method to Study State Cyber Defence Requirements. 2015. URL: https://www.cs.ox.ac.uk/files/7462/IEEE_TETC_Nugraha_Cyber%20Defence%20Requirements.pdf