КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.25.330343
УДК 004.94:519.21

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

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

Спасітєлєва Світлана Олексіївна
кандидат фізико-математичних наук, доцент,
доцент кафедри інформаційної та кібернетичної
безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0003-4993-6355
s.spasitielieva@kubg.edu.ua

Сокульский Олег Євгенович
кандидат технічних наук, доцент,
доцент кафедри інформаційних систем та технологій
Національний технічний університет України «Київський
політехнічний інститут імені Ігоря Сікорського», Київ, Україна
ORCID ID: 0000-0003-3853-9928
mortimer@ukr.net

ПРИЙНЯТТЯ РІШЕНЬ НА ОСНОВІ ЛІНІЙНОЇ ОПТИМІЗАЦІЇ У ПРОЦЕСІ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. Інформаційна безпека є критично важливою галуззю, в якій необхідно враховувати безліч різних факторів та обмежень для забезпечення надійного захисту даних та інфраструктури. Одним з основних завдань у цій галузі є оптимальний розподіл обмежених ресурсів між різними заходами захисту, що потребує застосування математичних методів для пошуку оптимальних рішень. У даній статті розглянуто застосування методів лінійного програмування для вирішення проблем, пов'язаних з оптимізацією витрат на заходи щодо зниження ризиків інформаційної безпеки. Здійснено огляд наукових джерел щодо прикладного аспекту застосування методів лінійного програмування у процесі управління ризиками інформаційної безпеки. Покроково описано процес побудови моделі на основі задачі лінійного програмування, починаючи з формалізації задачі, вибору цільової функції та обмежень і закінчуючи отриманням оптимального розв'язку з його аналізом та інтерпретацією. Модель у вигляді задачі лінійного програмування дозволяє оптимізувати загальні витрати на забезпечення інформаційної безпеки, зважаючи на вибраний напрям оптимізації й з урахуванням заданих обмежень на ресурси бюджетні, часові, технічні та інші. Представлено використання лінійної оптимізації на основі SWOT-аналізу ризиків інформаційної безпеки, що дозволяє організаціям систематизувати та конкретизувати процес управління ризиками, спрямовуючи обмежені ресурси на найбільш критичні області та забезпечуючи оптимальний захист даних та інформаційних систем. Отримані результати показують, що використання методів лінійного програмування дозволяє досягти значної

оптимізації витрат на інформаційну безпеку, забезпечуючи високий рівень захисту. Серед перспективних напрямів для подальших опрацювань запропонована багатокритеріальна оптимізація та динамічне планування з урахуванням часових змін ризиків і витрат. Дане дослідження можливо використати як наочний приклад міжпредметних зв'язків дисциплін спеціальності 125 Кібербезпека та захист інформації у навчальній діяльності студентів цієї спеціальності.

Ключові слова: прийняття рішень; інформаційна безпека; ризики інформаційної безпеки; управління ризиками інформаційної безпеки; лінійна оптимізація.

ВСТУП

Постановка проблеми. У сучасному світі інформаційні технології відіграють першорядну роль у забезпеченні стабільного функціонування організацій різного виду діяльності. З розвитком цифрових технологій та збільшенням обсягів оброблюваних даних зростає значущість забезпечення інформаційної безпеки. Підвищення степеня загроз інформаційній безпеці може спричинити значні фінансові втрати, витік конфіденційних даних, репутаційні ризики та інші негативні наслідки. В умовах постійного зростання кількості кібератак та збільшення їх складності, завдання оцінки ризиків інформаційної безпеки з метою управління ними стає критично важливим.

Розрізняють якісні (SWOT-аналіз, PEST-аналіз, SNW-аналіз) та кількісні (математичні, ймовірнісні та статистичні) групи методів оцінки ризиків інформаційної безпеки. Традиційним та найбільш поширеним методом якісно-кількісного аналізу ризиків в інформаційних та кібернетичних системах є метод експертних оцінок. Але він часто не дозволяє повною мірою врахувати безліч факторів, що впливають на ризики, а кількісна оцінка ризику, що ґрунтується на експертних висновках фахівців, нерідко є суб'єктивною.

У зв'язку з цим виникає потреба у використанні більш точних та об'єктивних підходів для кількісної оцінки ризиків та прийняття обґрунтованих управлінських рішень. У цьому контексті методи кількісного аналізу, такі як лінійне програмування, є перспективним інструментом для більш точного та об'єктивного прийняття рішень у процесі управління інформаційними ризиками.

Лінійне програмування є одним з ефективних методів математичної оптимізації, який знаходить широке застосування у різних галузях людської діяльності, таких як економіка, фінанси, виробництво та логістика. Його основні переваги включають можливість точної формалізації задачі, використання обчислювальних алгоритмів знаходження оптимальних рішень і гнучкість у відповідності до різних обмежень і параметрів. Лінійне програмування як метод оптимізації дозволяє знаходити оптимальні рішення в умовах обмежених ресурсів. Його застосування у галузі інформаційної безпеки відкриває нові можливості для побудови моделей, які можуть допомогти організаціям ефективно управляти ризиками, мінімізуючи потенційні збитки та оптимізуючи використання доступних ресурсів.

Аналіз останніх досліджень і публікацій. Розробка та вдосконалення різних заходів у сфері захисту інформації ґрунтується, перш за все, на методах, методиках, моделях, алгоритмах, які надаються різними розділами математики [1] – [11]. Важливу роль тут відіграють методи математичного програмування.

Від початку розвитку математичного програмування з кінця 30-х років XX ст. як самостійного наукового напрямку лінійне програмування розвинулося не тільки як спеціальний розділ математичного [12], а й як потужний прикладний оптимізаційний

інструмент [13]. Останнім часом методи лінійного програмування впевнено застосовуються для моделювання економічної, інформаційної та кібербезпеки організацій [14] – [16]. Також виявилося, що методи кількісного оцінювання ризиків інформаційної безпеки можуть бути інтегровані з методами лінійного програмування [17] – [19]. Оптимізаційні моделі, зокрема моделі лінійного програмування, використовуються в процесі управління ризиками інформаційної безпеки [20] – [22]. Отже, застосування методів лінійного програмування в галузі інформаційної безпеки відкриває нові можливості для побудови моделей, які можуть допомогти організаціям ефективно управляти ризиками, оптимізуючи використання доступних ресурсів та мінімізуючи потенційні збитки.

Метою статті є дослідження можливості застосування методів лінійного програмування для оптимізації ризиків інформаційної безпеки. Основні завдання дослідження включають розробку математичної моделі оптимізації ризиків, проведення аналізу на основі тестового прикладу та оцінку ефективності запропонованого підходу.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Лінійне програмування (часто використовують також назву лінійна оптимізація) є найбільш розвинутою частиною математичного програмування — напряму математики, що розроблює теорію та методи розв’язування оптимізаційних задач для функцій багатьох змінних з обмеженнями на область зміни змінних. Лінійне програмування розглядає методи розв’язування важливої для практики задачі відшукання максимуму (мінімуму) лінійної функції від багатьох змінних за наявності обмежень на область зміни цих змінних у вигляді лінійних рівнянь і/або нерівностей [23].

Математична модель задачі лінійного програмування (ЗЛП) в загальному вигляді включає в себе:

- змінні $x_j, j = \overline{1,n}$, значення яких треба визначити, зазвичай записують як вектор $\vec{X} = (x_1, x_2, \dots, x_n)$;
- обмеження, що накладаються на змінні $x_j, j = \overline{1,n}$, і утворюють область G в n-вимірному евклідовому просторі, яка визначається системою лінійних нерівностей або рівнянь:

$$\sum_{j=1}^{n} a_{ij} x_j \{\leq, =, \geq\} b_i, i = \overline{1,m}$$

- цільову функцію (критерій оптимальності) — лінійну функцію від змінних $x_j, j = \overline{1,n}$, яку необхідно оптимізувати:

$$Z = \sum_{j=1}^{n} c_j x_j \to \max_{X \in G}(\min) .$$

Коефіцієнти a_{ij}, b_i, c_j обмежень та цільової функції — задані сталі величини.

До обмежень приєднують:

- умову невід’ємності змінних:

$$x_j \geq 0, j = \overline{1,n}.$$

За потреби обмеження можуть бути доповнені умовою цілочисельності.

Вектор $\vec{X} = (x_1, x_2, \dots, x_n)$, що задовольняє всі обмеження задачі та умову невід’ємності змінних, називають допустимим розв’язком або допустимим планом

задачі лінійного програмування. Допустимий розв'язок $\vec{X}^* = (x_1^*, x_2^*, \ldots, x_n^*)$, який надає найбільшого або найменшого значення цільовій функції, називається оптимальним розв'язком або оптимальним планом задачі лінійного програмування. Розв'язок ЗЛП складається з оптимального плану і значення цільової функції на цьому плані.

У випадку сумісності системи обмежень результат її розв'язання утворює опуклу область допустимих розв'язків (многогранник розв'язків) G, що разом з геометричною інтерпретацією цільової функції як гіперплощини в n-вимірному просторі дає можливість знайти таку кутову точку многогранника розв'язків, у якій лінійна цільова функція досягає свого оптимального значення.

У випадку 2-вимірного простору використовується графічний метод розв'язування ЗЛП, який дає наочне представлення сутності ЗЛП: після знаходження області допустимих розв'язків будують лінію рівня цільової функції, яку переміщують за градієнтом цільової функції у випадку максимізації, або проти — у випадку мінімізації. В результаті буде знайдена кутова точка, яка визначатиме оптимальний розв'язок ЗЛП, або встановлено необмеженість цільової функції в області допустимих розв'язків.

Одним з найпоширеніших та ефективніших методів розв'язування задач лінійного програмування є симплекс-метод, запропонований американським математиком Дж. Данцигом в 1947 р. Він використовує ітераційний процес для переміщення по вершинах області допустимих розв'язків у напрямку покращення значення цільової функції доки не буде знайдено оптимальний розв'язок.

Завдяки простій постановці і наявності універсальних методів розв'язування ЗЛП знайшла широке застосування в управлінні об'єктами та плануванні процесів у різних видах людської діяльності.

Лінійне програмування надає потужні інструменти для аналізу та оптимізації, що робить його цінним методом для вирішення широкого кола завдань у різних галузях, наприклад, в економіці й фінансах — для оптимізації портфелів інвестицій, розподілу ресурсів та управління запасами; в промисловості і логістиці — для оптимізації виробничих процесів, для оптимізації перевезень; в інформаційній безпеці — для управління ризиками, оптимізації розподілу ресурсів для забезпечення безпеки, планування та управління безпекою.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Методика оптимізації ризиків інформаційної безпеки за допомогою лінійного програмування

Процес оптимізації ризиків інформаційної безпеки в інформаційній системі організації за допомогою лінійного програмування містить наступні кроки (табл. 1):

Таблиця 1

Процес оптимізації ризиків інформаційної безпеки за допомогою лінійного програмування

№	Крок	Зміст кроку
1	Визначення та класифікація ризиків інформаційної безпеки	Ідентифікація та класифікація можливих ризиків інформаційної безпеки, що містить – ідентифікацію загроз як потенційних інцидентів, що можуть негативно вплинути на інформаційну систему (наприклад, витоки даних, внутрішні загрози, атаки зловмисників); – оцінку уразливостей, тобто пошук слабких місць системи, що можуть бути використані загрозами (наприклад, у місцях зберігання та обробки інформації).
2	Збір даних та обґрунтування параметрів моделі	Необхідно зібрати та проаналізувати наступні дані для визначення параметрів моделі: – ймовірності виникнення ризиків: можуть бути оцінені на основі статистичних даних та експертних оцінок; – очікувані збитки: оцінка можливого фінансового або іншого збитку від реалізації кожного ризику; – витрати на заходи для зниження ризиків: можуть включати витрати на впровадження технологій, навчання персоналу та інші заходи; – наслідки виникнення ризиків: можуть бути оцінені у грошовому еквіваленті, що включає прямі та непрямі втрати; – доступні ресурси: технічні, бюджет, час та інші обмеження.
3	Побудова моделі	Для оптимізації ризиків використовується лінійна модель, яка дозволяє мінімізувати загальний ризик інформаційної безпеки системи за певних обмежень. У моделі використовуються: – змінні, що презентують заходи щодо зниження ризиків; – критерій оптимальності у вигляді цільової функції, що напрямлена на мінімізацію загального ризику або збитків; – обмеження: бюджетні, ресурсні, вимоги до безпеки.
4	Розв’язування задачі лінійного програмування	З використанням зібраних даних і сформульованої моделі задача лінійного програмування розв’язується за допомогою універсального алгоритму симплекс-методу. Це дозволяє визначити оптимальні заходи для зниження ризиків інформаційної безпеки в інформаційній системі організації при заданих обмеженнях.
5	Аналіз та інтерпретація отриманих результатів	Розв’язок ЗЛП складається з – оптимальних значень змінних, що вказують, які заходи щодо зниження ризиків мають бути реалізовані та в якому обсязі; – оптимального значення цільової функції, що вказує на очікуваний мінімізований загальний ризик як на мінімальний збиток після реалізації оптимальних заходів.
6	Реалізація отриманих результатів	На підставі отриманих результатів здійснюються практичні висновки та рекомендації, а саме вказується: – які заходи щодо зниження ризиків є пріоритетними; – як найефективніше розподілити доступні ресурси для мінімізації ризиків. – які слід зробити конкретні кроки для реалізації запропонованих заходів щодо зниження ризиків.
7	Оцінка та коригування моделі	Після реалізації запропонованих заходів та аналізу їх ефективності модель може бути скоригована для покращення оцінки та управління ризиками у майбутньому. Для цього проводиться – оцінка ефективності фактично реалізованих заходів; – актуалізація даних про нові загрози, уразливості та зміни доступних ресурсів; – перегляд цільової функції та обмежень для адаптації моделі до умов, що змінюються, та нових вимог безпеки.

Модель оцінки ризиків інформаційної безпеки на основі лінійного програмування

Приведемо одну з можливих моделей на основі лінійного програмування, яка дозволить знизити ризики інформаційної безпеки.

Припустимо, що організація хоче оцінити та мінімізувати ризики інформаційної безпеки для своєї IT-інфраструктури. В даній IT-інфраструктурі ідентифіковано n типів ризиків. Для зниження ризиків проводяться m видів заходів з безпеки. Витрати на проведення одного заходу $v_i, i = \overline{1,m}$. Одноразове застосування заходу i до ризику j потребує використання технічних ресурсів $t_{i,j}, i = \overline{1,m}$, робочого часу $l_{i,j}, i = \overline{1,m}$, витрат $v_{i,j}, i = \overline{1,m}$ і знижує величину ризику j на $r_{i,j}, i = \overline{1,m}$. Відомо, що загальний обсяг технічних ресурсів обмежений відповідно F одиницями, загальний фонд робочого часу становить L людино-годин, обсяг виділених коштів з бюджету на заходи для зниження ризику складає B. Треба визначити, які заходи та скільки разів необхідно провести, щоб отримати загальне максимальне зниження ризиків.

Для простоти розглянемо випадок наявності одного ризику, тобто $n = 1$.

Якщо позначити через $x_j, j = \overline{1,n}$, змінні, що презентують заходи щодо зниження ймовірності виникнення ризику, то модель у вигляді ЗЛП виглядає так:

Цільова функція:

$$Z = r_1 x_1 + r_2 x_2 \to \max$$

Обмеження:

за ресурсом

$$t_1 x_1 + t_2 x_2 \le F;$$

за робочим часом

$$l_1 x_1 + l_2 x_2 \le L;$$

за бюджетом

$$v_1 x_1 + v_2 x_2 \le B.$$

Умова невід'ємності змінних:

$$x_j \ge 0, j = \overline{1,n}.$$

Проілюструємо отриманий результат на змістовному прикладі.

Нехай в IT-інфраструктурі невеликої організації виявлено потенційний ризик, викликаний загрозою несанкціонованого доступу до даних. Для зниження ризику проводяться 2 види заходів з безпеки: впровадження нових IT-технологій і навчання персоналу. Одноразове застосування кожного заходу потребує технічного ресурсу, робочого часу, грошових витрат і знижує ризик на відповідну величину. Дані наведені в табл. 2. Треба визначити, які заходи та скільки разів необхідно провести, щоб отримати загальне максимальне зниження ризику.

Таблиця 2

	Впровадження нових IT-технологій	**Навчання персоналу**	**Загальний обсяг**
Технічний ресурс (одиниць)	$t_1 = 2$	$t_2 = 5$	F=28
Трудомісткість (людино-годин)	$l_1 = 1{,}5$	$l_2 = 2$	L =12
Обсяг виділених коштів з бюджету (тис. умовних грошових одиниць)	$v_1 = 6$	$v_2 = 2$	B =30
Зниження ризику (тис. умовних грошових одиниць)	$r_1 = 3{,}5$	$r_2 = 1{,}5$	

ISSN 2663 - 4023

Якщо позначити через x_1, x_2 змінні, що демонструють заходи щодо зниження ймовірності виникнення ризику, то модель у вигляді ЗЛП виглядає так:

$$Z = 3{,}5x_1 + 1{,}5x_2 \to \max$$
$$\begin{cases} 2x_1 + 5x_2 \le 28; \\ 1{,}5x_1 + 2x_2 \le 12; \\ 6x_1 + 2x_2 \le 30; \end{cases}$$
$$x_1, x_2 \ge 0.$$

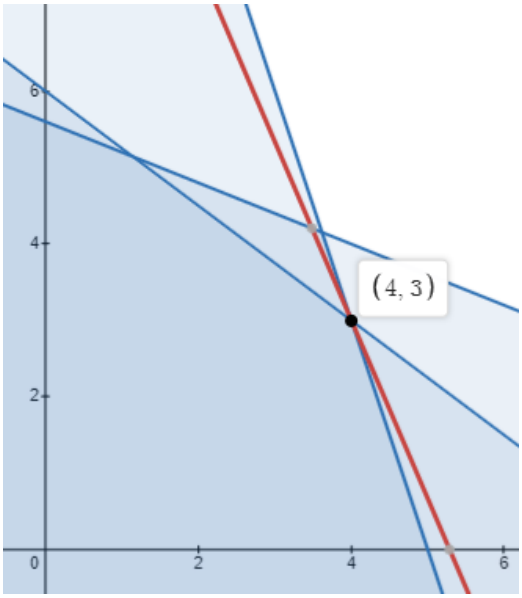

Рис. 1. Графічний метод

Розв'язуючи ЗЛП графічним (рис. 1) або симплекс-методом, отримуємо оптимальний план $\vec{X}^* = (4{,}3)$, на якому $Z = 14 + 4{,}5 = 18{,}5$.

Отже, щоб отримати максимальне зниження ризику від несанкціонованого доступу до даних, треба провести 4 заходи з впровадження нових IT-технологій і 3 заходи з навчання персоналу, на що організація може розподілити 18,5 тис. умовних грошових одиниць, що нижче загального обсягу виділених коштів з бюджету в 30 тис. умовних грошових одиниць.

Варіанти практичного застосування моделі оптимізації ризиків інформаційної безпеки за допомогою лінійного програмування

Модель оптимізації ризиків інформаційної безпеки на основі лінійного програмування може бути корисною для організацій будь-якого розміру та типу діяльності. Зазначимо кілька можливих практичних застосувань цієї моделі.

1. Оптимізація розподілу бюджету на заходи щодо зниження ризиків.

Організації часто стикаються з обмеженими ресурсами при плануванні заходів щодо забезпечення інформаційної безпеки. Модель лінійного програмування дозволяє оптимізувати розподіл бюджету так, щоб максимізувати загальний рівень захисту за певних обмежень на витрати.

Наприклад, компанія може використати модель лінійного програмування для вирішення питання щодо впровадження конкретних заходів (покращення системи

моніторингу, навчання співробітників безпеки, оновлення програмного забезпечення, тощо) для мінімізації загальних ризиків з урахуванням обмеженого бюджету.

2. Вибір оптимальних стратегій управління ризиками.

Модель лінійного програмування може бути застосована для аналізу різних концепцій управління ризиками, а саме:

- оптимальному вибору між внутрішніми та зовнішніми заходами захисту;
- наданню переваг заходам з управління ризиками в залежності від їхньої дієвості та витрат.

Наприклад, банк може використати модель лінійного програмування для визначення оптимальної комбінації технічних та організаційних заходів захисту банківських даних, мінімізуючи можливі фінансові втрати від кібератак.

3. Планування та оцінка нових проєктів або технологій.

При впровадженні в організації нових проєктів або технологій виникають нові ризики інформаційної безпеки. Модель лінійного програмування може допомогти після попередньої оцінки ризиків розробити оптимальні стратегії щодо зниження цих ризиків.

Наприклад, технологічна компанія може використати модель лінійного програмування для планування необхідних заходів для управління потенційними ризиками, пов’язаних із запуском нового хмарного сервісу.

4. Підтримка прийняття управлінських рішень.

Модель оптимізації ризиків інформаційної безпеки за допомогою лінійного програмування надає кількісні дані, які може використовувати керівництво організації для прийняття обґрунтованих управлінських рішень. Це допомагає об’єктивно оцінити переваги та витрати за різними схемами управління ризиками.

Наприклад, керівництво корпорації може використати модель лінійного програмування для аналізу можливих стратегій захисту конфіденційної інформації клієнтів, що допомагає зробити обґрунтований вибір на користь оптимального рівня інвестицій у інформаційну безпеку.

Отже, застосування моделі оптимізації ризиків інформаційної безпеки на основі лінійного програмування дозволяє організаціям ефективно управляти та мінімізувати ризики, пов’язані з безпекою даних та інформаційних систем. Цей підхід сприяє підвищенню рівня захисту інформації, оптимізації витрат та забезпеченню конкурентоспроможності на ринку.

Проведення лінійної оптимізації на основі SWOT-аналізу ризиків інформаційної безпеки

Корисним напрямком застосування лінійного програмування до інформаційної безпеки є проведення лінійної оптимізації на основі SWOT-аналізу ризиків інформаційної безпеки [25], [26]. SWOT-аналіз — це дослідницька процедура, яка дозволяє виявити в інформаційної безпеці організації

- сильні сторони (Strength) — внутрішні переваги, що сприяють захисту даних;
- слабкі сторони (Weakness) — внутрішні загрози, уразливості та недоліки, що існують в системі безпеки;
- можливості (Opportunities) — зовнішні фактори і можливості, що можуть покращити інформаційну безпеку;
- загрози (Threats) — зовнішні фактори, що можуть негативно вплинути на безпеку даних.

За результатами SWOT-аналізу:

1) визначається актуальний напрям оптимізації ризиків інформаційної безпеки, який може бути, зокрема, зорієнтований на:
   – мінімізацію витрат на заходи з управління ризиками з урахуванням сильних і слабких сторін;
   – мінімізацію ризиків з урахуванням можливостей і загроз;
   – максимізацію рівня захисту даних з урахуванням бюджетних обмежень;
2) визначаються змінні (витрати на заходи безпеки, на зниження рівня ризиків, на ресурси тощо) і параметри лінійної моделі;
3) вводяться обмеження на змінні за бюджетом, за ресурсами, за рівнем безпеки;
4) будується модель оптимізації як ЗЛП, яка розв'язується методами лінійного програмування.

Аналіз та інтерпретація результатів лінійної оптимізації на основі SWOT-аналізу ризиків інформаційної безпеки проводиться зважаючи на потреби і бізнес-цілі організації. Це дозволяє порівнювати рівні витрат на зниження ризиків інформаційної безпеки при різних сценаріях; прогнозувати зміни в оцінках ризиків при зміні параметрів; приймати обґрунтовані управлінські рішення щодо зниження ризиків.

Як приклад розглянемо віртуальну організацію «Інтернет-провайдер» [25], яка після SWOT-аналізу ризиків ІБ виявила, що сильною стороною є висококваліфікований персонал, слабкою — відсутність системи аварійного електропостачання, можливістю є закупка нового обладнання, а загрозою — витік інформації. На основі цього SWOT-аналізу можна побудувати модель у вигляді задачі лінійного програмування для оптимізації витрат на заходи щодо зниження ризиків. При цьому модель буде враховувати витрати на оновлення обладнання та навчання персоналу.

Таким чином, використання лінійної оптимізації на основі SWOT-аналізу ризиків інформаційної безпеки дозволяє організаціям систематизувати та конкретизувати процес управління ризиками, спрямовуючи ресурси на найбільш критичні області та забезпечуючи оптимальний захист даних та інформаційних систем.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У ході дослідження було продемонстровано ефективне використання методів лінійної оптимізації для мінімізації загальних витрат на заходи для зниження ризиків інформаційної безпеки. Побудована модель дозволяє оптимально розподілити ресурси серед різних заходів захисту, забезпечуючи відповідність всім заданим обмеженням та максимізуючи ефективність захисту при обмеженому бюджеті. Крім того, використання методів лінійного програмування дозволяє вирішувати проблему оптимального розподілу ресурсів з урахуванням великої кількості факторів.

Побудована модель може бути адаптована під різні обмеження і можливості, що дозволяє отримати зручний інструмент для прийняття рішень щодо управління ризиками інформаційної безпеки. При правильно підібраних параметрах моделі отримуємо оптимальне рішення, яке відповідає реальним потребам і можливостям організації.

Підсумовуючи, відзначимо серед переваг лінійної оптимізації ризиків інформаційної безпеки ефективність, точність, високу адаптивність, прозорість у процесі прийняття рішень, раціональний розподіл ресурсів при мінімальних затратах. Серед

недоліків звернемо увагу на обмеженість лінійної моделі, яка не враховує складні залежності, невизначеність, потребує точних даних.

З огляду на перераховані переваги і недоліки підкреслимо, що лінійна оптимізація, з одного боку, дає потужний інструмент для управління ризиками інформаційної безпеки, а з іншого боку — потребує уважного ставлення до особливостей кожної конкретної задачі.

Серед можливих напрямків подальших досліджень відзначимо можливість введення в модель лінійної оптимізації не лише витрати, але й інші метрики (наприклад, час впливу, практичність впровадження). У результаті така багатокритеріальна оптимізація дозволить отримати комплексні управлінські рішення у сфері інформаційної безпеки, які враховують не тільки витрати, а й інші важливі показники.

Включення в модель часових параметрів, тобто змін в часі ризиків і витрат на заходи щодо їх зниження, дозволить отримати довгострокові рішення для управління інформаційною безпекою.

Відзначені напрямки розширюють застосування лінійного програмування для управління ризиками інформаційної безпеки і можуть дозволити організаціям ефективніше розподіляти свої ресурси в умовах мінливого цифрового середовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Шевченко, С. М., Жданова, Ю. Д., Спасітєлєва, С.О., Негоденко, О. В., Мазур, Н. П., & Кравчук, К. В. (2019). Математичні методи в кібербезпеці: фрактали та їх застосування в інформаційній та кібернетичній безпеці. *Кібербезпека: освіта, наука, техніка, 1(5),* 31–39.
2. Шевченко, С. М., Жданова, Ю. Д., Складанний, П. М., & Спасітєлєва, С. О. (2021). Математичні методи в кібербезпеці: графи та їх застосування в інформаційній та кібернетичній безпеці. *Кібербезпека: освіта, наука, техніка, 1(13),* 133–144.
3. Шевченко, С. М., Складанний, П. М., Негоденко, О. В., & Негоденко, В. П. (2022). Дослідження прикладних аспектів теорії конфліктів у системах безпеки. *Кібербезпека: освіта, наука, техніка, 2(18),* 150–162.
4. Shevchenko, S., Shevchenko, H., Zhdanova, Y., Spasiteleva, S., & Negodenko, O. (2023) Conflict Analysis in the Information Security System: Subject – Subject. *CEUR Workshop Proceedings. 3421*, 56–66.
5. Шевченко, С. М., Жданова, Ю. Д., & Спасітєлєва, С. О. (2023) Математичні методи в кібербезпеці: теорія катастроф. *Кібербезпека: освіта, наука, техніка, 3(19)*, 165–175.
6. Шевченко, С. М., Жданова, Ю. Д., Складанний, П. М., & Бойко, С. В. (2023) Теоретико-ігровий підхід до моделювання конфліктів у системах інформаційної безпеки. *Кібербезпека: освіта, наука, техніка, 2(22),* 168–178.
7. Шевченко, С. М., Жданова, Ю. Д., Спасітєлєва, С. О., Складанний, П. М., & Негоденко, В. П. (2024). Математичні методи в кібербезпеці: кластерний аналіз та його застосування в інформаційній та кібернетичній безпеці. *Кібербезпека: освіта, наука, техніка, 3(23)*, 258–273.
8. Korniyenko, B., Galata, L., Ladieva, L. (2019). Mathematical Model of Threats Resistance in the Critical Information Resources Protection System. *CEUR Workshop Proceedings, 2577,* 281–291.
9. Лисенко, Н. О., Мазуренко, В. Б., Федорович, А. І., Астахов, Д. С., & Стаценко, В. І. (2021) Огляд математичних методів у системах виявлення та попередження кіберзагроз. *Актуальні проблеми автоматизації та інформаційних технологій, 2021(25),* 91–102. http://dx.doi.org/10.15421/432110
10. Khoroshko, V., Brailovskyi, M., Khokhlachova, Y., & Vyshnevska, N. S. (2023) Mathematical Models And Algorithms For Determining Time Decision-Making In The Cyber Defense System. *Scientific and Practical Cyber Security Journal (SPCSJ), 7(3),* 11–16.
11. Sobchuk, V., Barabash, O., Musienko, A., Tsyganivska, I., & Kurylko, O. (2023) Mathematical Model of Cyber Risks Management Based on the Expansion of Piecewise Continuous Analytical Approximation Functions of Cyber Attacks in the Fourier Series. *Axioms, 12(10).*
12. Lieberman, G. J., & Hillier, F. S. (2010). *Introduction to Operations Research.*
13. Bazaraa, M. S., Jarvis, J. J., & Sherali, H. D. (2010). *Linear Programming and Network Flows – 4th ed.* Wiley.

14. Jain, S., & Mukhopadhyay, A. (2023). Optimization of Investments in Cybersecurity: A Linear Programming Approach. *WISP 2023 Proceedings 8.*
15. Enayaty-Ahangar, F., Albert, L. A., & DuBois, E. (2020). A survey of optimization models and methods for cyberinfrastructure security. *IISE Transactions, 53(2),* 182–198.
16. Hong, Y., Vaidya, J., Rizzo, N., & Liu, Q., (2016). Privacy Preserving Linear Programming. https://doi.org/10.48550/arXiv.1610.02339
17. Talabis, M., & Martin, J. (2012). *Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis.* Newnes.
18. Chinemeze, A. K., Mbam, B. C. E. (2019). Impact of Risk Management on Software Projects in Nigeria Using Linear Programming. *American Journal of Engineering Research (AJER), 8(7),* 186–192.
19. Feng, N., Wang, H. J., & Li, M. (2021). A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. *Reliability Engineering & System Safety, 256,* 57–73. https://doi.org/10.1016/j.ins.2013.02.036
20. White, J. (2014). *Security Risk Assessment*. https://www.perlego.com/book/1830498/security-risk-assessment-managing-physical-and-operational-security-pdf
21. Ridley, D., Llaugel, F., Daniels, I., & Khan, A. (2022). Study on Linear Programming in Risk Management. *Novel Research Aspects in Mathematical and Computer Science, 1,* 151–161
22. Mohammed, A. R, & Kassem, S. S. (2020). Product Mix Optimization Scenarios: A Case Study for Decision Support Using Linear Programming Approach. *International Conference on Innovative Trends in Communication and Computer Engineering (ITCE), 50–55.* https://doi.org/10.1109/ITCE48509.2020.9047758
23. Мартиненко, М. А., Нещадим, О. М., & Сафонов, В. М. (2010). *Математичне програмування: Підручник.* К.: НУХТ.
24. Шевченко, С. М., Жданова, Ю. Д., Спасітєлєва, С. О., & Складанний, П. М. (2020). Проведення SWOT-аналізу оцінювання інформаційних ризиків як засіб формування практичних навичок студентів спеціальності 125 Кібербезпека. *Кібербезпека: освіта, наука, техніка, 2(10),* 158–168.
25. Shevchenko, H., Shevchenko, S., Zhdanova, Yu., Spasiteleva, S., & Negodenko, O. (2021). Information Security Risk Analysis SWOT. *CEUR Workshop Proceedings, 2923,* 309–317.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023

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

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

Svitlana Spasiteleva
PhD, Associate Professor,
Associate Professor of the Department of Information and Cyber Security
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0003-4993-6355
s.spasitielieva@kubg.edu.ua

Oleg Sokulsky
PhD, Associate Professor,
Associate Professor of the Department of Information Systems and Technologies
National Technical University of Ukraine "Kyiv Polytechnic
Institute named after Igor Sikorsky", Kyiv, Ukraine
ORCID ID: 0000-0003-3853-9928
mortimer@ukr.net

DECISION-MAKING ON THE BASE OF LINEAR OPTIMIZATION IN THE PROCESS OF MANAGEMENT OF INFORMATION SECURITY RISKS

Abstract. Information security is a critical field in which many different factors and constraints must be taken into account to ensure that data and infrastructure are protected. One of the main challenges in this area is the optimal allocation of limited resources between different security measures, which requires the use of mathematical methods to find optimal solutions. This article discusses the use of linear programming methods to solve problems related to optimizing the costs of information security risk reduction measures. The article reviews scientific sources on the applied aspect of linear programming for risk assessment and information security risk management. The article shows the process of building a model based on a linear programming problem, starting with the formalization of the problem, selection of the objective function and constraints, and ending with obtaining an optimal solution with its analysis and interpretation. The model in the form of a linear programming problem allows optimizing the total costs of information security, taking into account the chosen direction of optimization and given the given constraints on resources—budget, time, technical and other. The article presents the use of linear optimization based on the SWOT analysis of information security risks, which allows organizations to systemize and specify the risk management process, directing limited resources to the most critical areas and ensuring optimal protection of data and information systems. The obtained results show that the use of linear programming methods allows to achieve a significant optimization of information security costs, providing a high level of protection. Among the promising directions for further research are multi-criteria optimization and dynamic planning with consideration of time changes in risks and costs. This study can be used as an illustrative example of intersubject connections of the disciplines of the specialty 125 Cybersecurity and information protection in the educational activities of students of this specialty.

Keywords: decision-making; information security; information security risks; information security risk management; linear optimization.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Shevchenko, S., Zhdanova, Yu., Spasiteleva, S., Negodenko, O., Mazur, N., Kravchuk, K. (2019). Mathematical Methods in Cybersecurity: Fractals and their Applications in Information And Cyber Security. *Cybersecurity: education, science, technique, 1(5),* 31–39.
2. Shevchenko, S., Zhdanova, Yu., Skladannyi, P., Spasiteleva, S., (2021). Mathematical Methods in Cibersecurity: Graphs and their Application in Information and Cybernetic Security. *Cybersecurity: education, science, technique, 1(13),* 133–144.
3. Shevchenko, S., Skladannyi, P., Negodenko, O., Negodenko, V. (2022). Study of applied aspects of conflict theory in security systems. *Cybersecurity: education, science, technique, 2(18),* 150–162.
4. Shevchenko, S., Shevchenko, H., Zhdanova, Y., Spasiteleva, S., & Negodenko, O. (2023). Conflict Analysis in the Information Security System: Subject – Subject. *CEUR Workshop Proceedings*, *3421.* 56–66.
5. Shevchenko, S., Zhdanova, Yu., & Spasiteleva, S. (2023) Mathematical Methods in Cybersecurity: Catastrophe Theory. C*ybersecurity: education, science, technique*, *3(19),* 165–175.
6. Shevchenko, S., Zhdanova, Yu., Skladannyi, P., & Boiko, S. (2023) Game Theoretical Approach to the Modeling Of Conflicts in Information Security Systems. *Cybersecurity: education, science, technique, 2(22),* 168–178.
7. Shevchenko, S., Zhdanova, Yu., Spasiteleva, S., Mazur, N., Skladannyi, P., & Negodenko, V. (2024). Mathematical Methods in Cyber Security: Cluster Analysis And its Application in Information and Cybernetic Security *Cybersecurity: education, science, technique, 3(23),* 258–273.
8. Korniyenko, B., Galata, L., Ladieva, L. (2019). Mathematical Model of Threats Resistance in the Critical Information Resources Protection System. *CEUR Workshop Proceedings, 2577,* 281–291.
9. Lysenko, N. O., Mazurenko, V. B., Fedorovych, A. I., Astakhov, D. S., Statsenko, V. I. (2021). Review of Mathematical Methods in Cyber Threat Detection and Prevention Systems. *Actual problems of automation and information technologies*, *2021(25),* 91–102. http://dx.doi.org/10.15421/432110
10. Khoroshko, V., Brailovskyi, M., Khokhlachova, Y., Vyshnevska, N. S. (2023). Mathematical Models And Algorithms For Determining Time Decision-Making In The Cyber Defense System. *Scientific and Practical Cyber Security Journal (SPCSJ), 7(3),* 11–16.
11. Sobchuk, V., Barabash, O., Musienko, A., Tsyganivska, I., & Kurylko, O. (2023) Mathematical Model of Cyber Risks Management Based on the Expansion of Piecewise Continuous Analytical Approximation Functions of Cyber Attacks in the Fourier Series. *Axioms, 12(10).*
12. Lieberman, G. J., & Hillier, F. S. (2010). *Introduction to Operations Research*.
13. Bazaraa, M. S., Jarvis, J. J., & Sherali, H. D. (2010). *Linear Programming and Network Flows – 4th ed.* Wiley.
14. Jain, S., & Mukhopadhyay, A. (2023). Optimization of Investments in Cybersecurity: A Linear Programming Approach. *WISP 2023 Proceedings 8.*
15. Enayaty-Ahangar, F., Albert, L. A., & DuBois, E. (2020). A survey of optimization models and methods for cyberinfrastructure security. *IISE Transactions, 53(2),* 182–198.
16. Hong, Y., Vaidya, J., Rizzo, N., & Liu, Q., (2016). Privacy Preserving Linear Programming. https://doi.org/10.48550/arXiv.1610.02339
17. Talabis, M., & Martin, J. (2012). *Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis.* Newnes.
18. Chinemeze, A. K., Mbam, B. C. E. (2019). Impact of Risk Management on Software Projects in Nigeria Using Linear Programming. *American Journal of Engineering Research (AJER), 8(7),* 186–192.
19. Feng, N., Wang, H. J., & Li, M. (2021). A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. *Reliability Engineering & System Safety, 256,* 57–73. https://doi.org/10.1016/j.ins.2013.02.036
20. White, J. (2014). *Security Risk Assessment*. https://www.perlego.com/book/1830498/security-risk-assessment-managing-physical-and-operational-security-pdf
21. Ridley, D., Llaugel, F., Daniels, I., & Khan, A. (2022). Study on Linear Programming in Risk Management. *Novel Research Aspects in Mathematical and Computer Science, 1,* 151–161

22. Mohammed, A. R, & Kassem, S. S. (2020). Product Mix Optimization Scenarios: A Case Study for Decision Support Using Linear Programming Approach. *International Conference on Innovative Trends in Communication and Computer Engineering (ITCE), 50–55.* https://doi.org/10.1109/ITCE48509.2020.9047758
23. Martynenko, M. A., Neshchadym, O. M., & Safonov, V. M. (2010). *Mathematical programming: Textbook.* K.: NUHT.
24. Shevchenko, S., Zhdanova, Yu., Spasiteleva, S., Skladannyi, P., (2020). Conducting a SWOT-analysis of information risk Assessment as a means of formation of practical skills of students specialty 125 Cybersecurity. *Cybersecurity: education, science, technique*, *2(10),* 158–168.
25. Shevchenko, H., Shevchenko, S., Zhdanova, Yu., Spasiteleva, S., & Negodenko, O. (2021). Information Security Risk Analysis SWOT. *CEUR Workshop Proceedings, 2923,* 309–317.