DOI: https://doi.org/10.17721/ISTS.2020.1.9-15
УДК 519.816

ВИЗНАЧЕННЯ ПРІОРИТЕТНОСТІ ЗАХОДІВ КІБЕРБЕЗПЕКИ ПРИ НЕПОВНИХ ЕКСПЕРТНИХ РАНЖУВАННЯХ

Гнатієнко Григорій[1]
orcid.org/0000-0002-0465-5018

Тмєнова Наталія[2]
orcid.org/0000-0003-1088-9547

[1] Україна, м. Київ, Київський національний університет імені Тараса Шевченка, g.gna5@ukr.net
[2] Україна, м. Київ, Київський національний університет імені Тараса Шевченка, tmyenovox@gmail.com

Історія статті:
Надійшла до редакції
13.01.2020
Прийнято
23.01.2020

Ключові слова:
організаційна система; інформаційна безпека; метрика; відстань; медіана; групове упорядкування об’єктів; неповне експертне ранжування.

Анотація. Якісне функціонування системи інформаційної безпеки та вирішення проблем, що виникають при захисті інформації, наразі є актуальним напрямом в різних сферах людської життєдіяльності. Успішний кіберзахист полягає у створенні та реалізації багаторівневої системи заходів, які охоплюють різні аспекти, що мають комплексно взаємодіяти та взаємодоповнювати один одного. Ці заходи мають різний характер, і їх пріоритетність з точки зору різних служб організації може суттєво відрізнятися, тому розробку послідовності виконання заходів кібербезпеки логічно формалізувати у класі задач групового вибору. В роботі пропонується гнучкий математичний апарат для моделювання задач інформаційної безпеки та адекватного застосування аналізу думок колективу експертів на практиці. Описано підхід до знаходження результуючого ранжування пріоритетності заходів як розв’язку задачі багатокритеріальної оптимізації, де послідовність виконання заходів може передбачати взаємодію виконавців і вимагати регламентування послідовності дій усіх елементів та підсистем організаційної системи. Такий підхід дозволяє об'єднати різні за складом та пріоритетністю заходи інформаційної безпеки, запропоновані експертами різних підрозділів; знаходити компромісне рішення для різнорідної групи експертів; не порушувати задані переваги жодного експерта при обчисленні компромісного ранжування заходів кібербезпеки. Запропонований підхід може бути корисним при розробці заходів забезпечення належного рівня кібербезпеки та сприятливим при розробці і впровадженні процедур швидкого реагування на загрози, а також бути незамінним при комплексній побудові системи безпеки організації або її удосконаленні та містити елементи навчання, узгодження, координації, комплексності учасників експертної групи, які є керівниками підрозділів єдиної організаційної системи.

Abstract. High-quality functioning of the information security system and solving problems that arise in the information protection, is currently a topical trend in various areas of human life. Successful cyber protection consist in creating and implementing a multi-level system of measures that cover various aspects with complex interact and complement each other. These measures have a different nature, and their priorities may differ significantly in terms of different services of the organization, so it is logical to formalize the sequence of cybersecurity implementation in a class of group choice tasks. The paper proposes a flexible mathematical apparatus for modeling information security problems and adequate application of the opinion analysis of experts’ team in practice. The approach to finding the resultant ranking of measures priority is described as a solution to the problem of multicriteria optimization, where the sequence of measures implementation may involve the interaction of performers and require regulation of the actions sequence of all elements and subsystems of the organizational system. This approach allows to combine different information security measures proposed by the experts of various departments; to find a compromise solution for a diverse group of experts; not to violate any expert's preferences under calculating the compromise ranking of cyber security measures. The proposed approach can be useful in developing appropriate cybersecurity measures and favorable in developing and implementing of rapid response procedures to threats, as well as it can be indispensable in the overall building or improving organization security system and it can contain elements of training, coordination, and complexity of expert team members, who are the heads of units of a single organizational system.

1. ВСТУП

Важливість проблеми підвищення рівня інформаційної безпеки зростає разом із інтенсивним розвитком інформаційних технологій та посиленням конкуренції у сучасному світі. Забезпечення функціонування безпекової складової будь-якої сучасної інформаційної системи є актуальною у міждержавних відносинах, у будь-якій галузі народного господарства, у різноманітних напрямках людської життєдіяльності тощо. Вирішення проблем, що виникають при захисті інформації, є досить складним процесом, який базується на системному підході, що застосовується при створенні комплексної системи захисту інформації. Якість функціонування системи інформаційної безпеки залежить від якості функціонування елементів системи, тому моделювання інтегрального рівня безпеки інформаційної системи є актуальним напрямком досліджень.

Наявність значної кількості способів негативного впливу на системи інформаційної безпеки потребує вдосконалення заходів кібербезпеки. Успішний кіберзахист полягає у створенні та реалізації багаторівневої системи заходів, які охоплюють такі основні аспекти: організаційний, персонал організації, комп'ютери, локальні мережі, програмне забезпечення, бази даних та різноманітні сховища даних, які слід комплексно убезпечити. Для вдалого захисту від загроз усі ці аспекти кіберзахисту мають комплексно взаємодіяти та взаємодоповнювати один одного.

2. АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Оцінка захищеності системи потрібна для створення механізму та умов оперативного реагування на загрози інформаційній безпеці та прояви негативних тенденцій функціонування системи. Для цього слід застосовувати комплекс заходів та протидій. Найбільш розповсюдженими методиками в галузі захищеності інформаційних систем є три основних метода захищеності системи: формальний, статистичний та класифікаційний [1, 2]. Перспективним підходом є підвищення об'єктивності і комплексності оцінки засобів захисту інформації на базі формалізації експертних даних.

Задачі групового (колективного, колегіального, демократичного) упорядкування об'єктів дозволяють моделювати практичні ситуації у різних предметних областях. Особливістю загальноприйнятих постановок таких задач є зафіксована для усіх членів експертної групи множина об'єктів, що у багатьох випадках суттєво знижує якість експертизи. Наразі існують дослідження, в яких допускається можливість задання неповних ранжувань у задачах колективного ранжування [3], але алгебраїчні методи обчислення медіани до таких задач на сьогодні ще не застосовувалися.

Заходи щодо інформаційної безпеки мають різнопланновий характер, і їх пріоритетність, з точки зору різних служб організації, може суттєво відрізнятися. Тому розробку послідовності виконання цих заходів логічно формалізувати у класі задач групового вибору, орієнтованого на визначення кількох рівноцінних розв'язків або упорядкування кількох виділених чи усіх заданих альтернатив [4]. Гнучкий підхід до упорядкування об'єктів, коли кожен експерт може пропонувати часткове упорядкування вибраної ним підмножини з усієї множини альтернатив, та пошук повного результуючого ранжування об'єктів алгебраїчними методами дослідниками не пропонувалися. Адже при цьому з'являється можливість враховувати ситуацію, коли деякі експерти можуть не знати про особливості функціонування окремих елементів з множини заходів безпеки, що стосуються загальної проблеми інформаційної безпеки усієї організаційної системи.

3. МЕТА ДОСЛІДЖЕННЯ

У дослідженні пропонується гнучкий математичний апарат для моделювання задач інформаційної безпеки та адекватного застосування аналізу думок колективу експертів на практиці. Мета дослідження вимагає розробки алгоритму визначення пріоритетності заходів інформаційної безпеки та забезпечення незалежності визначення та задання індивідуальних переваг експертів для успішного застосування комплексних заходів безпеки. Зокрема, експерт не повинен залежати від множини заходів, які можуть бути ним пропоновані для розв'язання деякої загальної проблеми. Це дозволяє апріорно підвищити професійність групового розв'язку, оскільки експерти мають можливість робити свої судження у межах своєї високої професійності на

множині критеріїв, де вони є безсумнівними спеціалістами, а не у жорстких рамках визначення пріоритетів на усій множині заходів безпеки, заданої для усіх членів експертної групи.

4. ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

На сьогодні традиційно виділяються такі види безпеки: економічна, юридична, фізична та інформаційна. Водночас до інформаційних загроз традиційно відносяться такі:
– розголошення конфіденційної інформації;
– витік конфіденційної інформації через технічні засоби;
– несанкціонований доступ до охоронюваних відомостей;
– знищення або несанкціоновані зміни інформації;
– блокування або руйнування технічних засобів прийому, передачі, обробки та зберігання інформації.

Усі зазначені вище аспекти інформаційної безпеки можуть належати до зони відповідальності різних служб та підрозділів організації. Тому природно, що керівники таких підрозділів не можуть бути однаково компетентними у всіх питаннях безпеки. Комплексність є одним із основних принципів організації та функціонування системи інформаційної безпеки. Складність побудови політики комплексної інформаційної безпеки обумовлена тим, що інформаційна безпека досягається комплексом організаційних, технічних та інших заходів.

Слід зазначити, що часто саме послідовність виконання кроків при прийнятті рішення є найсуттєвішим чинником як захисту, так і забезпечення надійності та усунення загроз.

Нехай розв'язується задача визначення послідовності впровадження заходів інформаційної безпеки деякої складної системи. Для цього різними підрозділами здійснюється підготовка та обґрунтування рішень щодо послідовності або пріоритетності заходів комплексної безпеки великої та багатопрофільної організації. Нехай колективом експертів задано k часткових порядків (неповних ранжувань) $R^i, i = 1,...,k.$

Представники різних підрозділів та служб, які входять до експертної групи, у межах своєї компетенції та уявлення про важливість заходів надають індивідуальні (частково впорядковані) пропозиції щодо послідовності запропонованих ними заходів. Серед членів експертної групи часто не співпадають множина запропонованих заходів, компетентність, інтереси, пріоритети, акценти, аспекти, уявлення про ідеалізацію моделі тощо. Тому на першому етапі розв'язання задачі слід використовувати підхід, що ґрунтується на об'єднанні множин та на введенні додаткових евристик.

Для оцінки загроз інформаційній безпеці традиційно застосовуються теорія надійності, математична статистика, теорія ймовірності, експертні технології прийняття рішень. У свою чергу, методи обробки експертної інформації поділяються на три основні групи: статистичні методи, методи шкалювання та алгебраїчні методи [5].

Для розв'язання задачі, яку сформульовано у цій роботі, найбільш прийнятним є алгебраїчний підхід. Суть алгебраїчних методів полягає в тому, що на множині допустимих оцінок задається відстань і результуюча оцінка визначається як така, відстань якої до оцінок експертів за певним вибраним критерієм є мінімальною.

При такій постановці задачі проблематика полягає у тому, що у задачах колективного ранжування об'єктів, як правило, розглядаються ситуації, коли експерти задають індивідуальні ранжування у фіксованому просторі із заданою кількістю об'єктів. При класичному алгебраїчному підході кожен експерт має задати свої переваги на множині усіх без виключення об'єктів, а результуюче (компромісне, колективне, групове, агреговане, інтегроване, інтегральне тощо) ранжування відшукується на множині усіх можливих ранжувань заданої множини об'єктів. Знайдене таким чином результуюче ранжування вважається узагальненою думкою групи експертів, які беруть участь у розв'язанні задачі лінійного (повного) упорядкування заданої множини об'єктів.

Для розробки комплексної системи взаємодії між елементами системи будемо застосовувати формалізм бінарних відношень, який зручно виражати орієнтованим графом або у вигляді матриці попарних порівнянь. При наявності значної кількості об'єктів порівняння, у нашому випадку – заходів безпеки, побудова такої матриці є трудомістким процесом. Тому на практиці для зменшення трудових витрат експертів нерідко крім процедури попарних порівнянь об'єктів застосовуються множинні порівняння. Результати множинних порівнянь складаються, як правило, з повних відношень, заданих між 3-5 об'єктами. Але досягнення повноти, непротирічливості, транзитивності, узгодженості тощо та задоволення вимог щодо цих показників повною мірою вимагає великих зусиль та витрат часу від експертів. Для

розв'язання задачі створення комплексу заходів безпеки будемо використовувати неповні ранжування – такі упорядкування об'єктів, кількість яких є більшою п'яти, але залишається меншою від усієї множини об'єктів, які слід упорядкувати.

Неповним ранжуванням $R^{(н)}$ множини A назвемо таке ранжування, у якому не для усіх n об'єктів множини A визначено відношення порядку. При цьому $A_i \subset A, \forall i = 1,...,k,$ відношення включення є строгим. Тобто в множині A існує хоча б один об'єкт, якого немає у підмножині $A_i, i = 1,...,k.$

На практиці часто виникають ситуації, коли експерти не в змозі здійснити достовірне ранжування об'єктів з усієї множини. Вимагати від них виконання цієї задачі означає свідомо створювати заздалегідь недостовірні початкові дані. Тому у цій роботі пропонується розглядати ситуації, коли кожен з k експертів має можливість установити частковий порядок на тій підмножині $A_i, i \in I = \{1,...,k\},$ множини об'єктів $A,\ A_i \subset A,\ i \in I,$ де він є компетентним, та які входять до його сфери впливу чи відповідальності. Тобто, задача починається з того, що k експертів задають часткові порядки $R^i = \{a_{j_1} \succ a_{j_2} \succ ... \succ a_{j_{ki}}\},$ $i \in I = \{1,...,k\},\quad k_i < k, i \in I,$ на вибраних ними підмножинах об'єктів $A_i \subset A, i \in I.$ Необхідно знайти деяке результуюче (агреговане, колективне) упорядкування n задач $R^* = (a_{i_1},...,a_{i_n}),$ $i_j \in I = \{1,...,n\},\ j \in I,$ яке побудоване за логікою, що характеризує процеси функціонування та забезпечення захисту деякої інформаційної системи. Упорядкування побудоване на основі індивідуальних упорядкувань задач, які виконуються k елементами системи $R^i = (a_{1_i},...,a_{n_i}),\ i \in J = \{1,...,k\},$ де $n_i -$ кількість задач в індивідуальному упорядкуванні, які виконуються $i -$ м елементом системи, $i \in J.$

На першому етапі розв'язання задачі здійснюється об'єднання підмножин заданих експертами заходів безпеки у єдину множину $A,$ до якої входять усі запропоновані експертами заходи $a_i \in A, i = 1,...,n,$

$$A = \bigcup_{i=1}^{k} A_i. \qquad (1)$$

Зрозуміло, що при цьому допускаються різні варіанти співвідношень між підмножинами: $A_{i_1} \cup A_{i_2} = \varnothing,\quad A_{i_1} \cup A_{i_2} \neq \varnothing,\quad A_{i_1} = A_{i_2},$ $i_1, i_2 \in J.$

Множина усіх заданих експертами заходів безпеки виду (1) є областю допустимих розв'язків для визначення результуючого ранжування заходів безпеки організації $R^*.$

Для визначення відстаней між ранжуваннями об'єктів використовують:

– метрику Кука неспівпадання рангів об'єктів у індивідуальних ранжуваннях

$$d(R^j, R^l) = \sum_{i \in I} \left| r_i^j - r_i^l \right|, \qquad (2)$$

де r_i^l – ранг i-го об'єкта у ранжуванні l-го експерта $R^l, l \in L,\ 1 \le r_i^l \le n,$

– метрику Хемінга

$$d(B^j, B^l) = 0{,}5 \sum_{i \in I} \sum_{s \in I} \left| b_{is}^j - b_{is}^l \right|, \qquad (3)$$

де $B^l = (b_{is}^l),\ l \in L,\ i, s \in I, -$ матриці попарних порівнянь (МПП), що відповідають ранжуванням $R^l, l \in L.$

Інколи для задач визначення результуючого ранжування використовується евклідова метрика.

Найпоширенішим методом знаходження результуючого ранжування об'єктів вважається обчислення медіани заданих ранжувань. Позначимо множину усіх можливих ранжувань n об'єктів через Ω^R, а множину МПП, які відповідають усім можливим ранжуванням n об'єктів – через Ω^B. Множину заданих експертами ранжувань будемо позначати через R^A, а множину відповідних їм МПП – через R^B. Для випадку, який розглядається у цій роботі, потужність множин R^A та R^B однакова: $\left|R^A\right| = \left|R^B\right| = n,\qquad R^l \in R^A,\ B^l \in R^B, l \in L.$ Зрозуміло, що $R^A \subset \Omega^R,\ R^B \subset \Omega^B.$ У загальному випадку потужність множини $\left|\Omega^B\right| = 2^{n(n-1)/2}.$ Але для методу, який описується у цій роботі, будемо вважати, що $\left|\Omega^R\right| = \left|\Omega^B\right| = n!,$ оскільки нас не цікавлять нетранзитивні елементи простору розв'язків $\Omega^B.$

Для метрики Кука (метрика неспівпадання рангів

об’єктів) виду (2) при використанні утилітарного критерію обчислюється медіана Кука-Сейфорда [4, 5]:

$$R^{CS} \in \Omega^{CS} = Arg \min_{R \in \Omega^R} \sum_{l \in L} d\left(R, R^l\right). \quad (4)$$

При використанні егалітарного критерію обчислюється ГВ-медіана (компроміс) [5]:

$$R^{ГВ} \in \Omega^{ГВ} = Arg \min_{R \in \Omega^R} \max_{l \in L} d\left(R, R^l\right). \quad (5)$$

Для метрики Хемінга (3) при використанні утилітарного критерію обчислюється медіана Кемені-Снелла:

$$R^{KC} \in \Omega^{KC} = Arg \min_{B \in \Omega^B} \sum_{l \in L} d\left(B, B^l\right). \quad (6)$$

При використанні егалітарного критерію обчислюється ВГ-медіана (компроміс) [4]:

$$R^{ВГ} \in \Omega^{ВГ} = Arg \min_{B \in \Omega^B} \max_{l \in L} d\left(B, B^l\right). \quad (7)$$

Крім того, в таких задачах можуть враховуватися коефіцієнти компетентності експертів: $\rho_1, ..., \rho_k$ (у нашому випадку: керівники підрозділів, відповідальних за впровадження заходів інформаційної безпеки, кожен – у зоні своєї відповідальності).

Методи визначення медіан виду (4)-(7) та їх особливості розглядаються у монографії [3].

Критеріальні функції, які застосовуються для визначення медіан (4)-(7), пов’язані з відстанями від заданих експертами ранжувань до обчислених розв’язків задачі. Тому ознакою ефективності одержаного розв’язку задачі слугують мінімальні значення критеріїв (4)-(7) для відповідних постановок задачі. Очевидно, що розв’язки, які не доставляють мінімумів зазначеним критеріям, є неефективними – вони домінуються розв’язками, які доставляють мінімум критеріям виду (4)-(7).

Для формалізації задачі побудови системи заходів щодо підвищення якості кібербезпеки можуть бути застосовані різні класи задач. Зокрема, перспективним є формалізація задачі розробки системи комплексної кібербезпеки у класі задач визначення нестрогого колективного ранжування: тобто, пошук результуючого ранжування може здійснюватися також у просторі нестрогих ранжувань. Такий підхід обґрунтовується тим, що деякі заходи безпеки мають виконуватися паралельно або навіть відбуватися одночасно. Тому логічно формалізувати поставлену задачу у класі обчислення розв’язку як нестрогого колективного ранжування [4, 6] (досконалі квазіпорядки [7], упорядкування [8], квазісерії [9], ранжування зі зв’язками [10], квазіпорядки [11], кластеризовані ранжування [12]).

Класичні методи теорії вибору (Кондорсе, Борда, Сімпсона, Копленда, Нансона, альтернативних голосів, відносної більшості тощо) також можуть бути обмежено застосовані при визначенні результуючого ранжування. Таке застосування описано, наприклад, в монографії [4]. Але при цьому слід враховувати недостатню обґрунтованість таких методів з точки зору теорії вимірювання. Для описаних вище задач більш прийнятними є алгебраїчні методи [4, 5].

Для обчислення медіан виду (4)-(7) може бути запропонована така схема.

Перш за все застосовується процедура об’єднання усіх заданих експертами об’єктів у єдину множину.

В результаті для кожного експерта маємо множину об’єктів, яка характеризується таким чином:

n_i – заданих ним у ранжуванні $R^i, i = 1,...,k,$ які будуть складати визначену частину відстаней;

$(n - n_i) = \nu_i$ – незаданих експертом у ранжуванні $R^i, i = 1,...,k,$ які складають ймовірнісну частину відстаней.

Після цього здійснюється генерування опорного ранжування $R^{*(0)}$ випадковим чином, тобто генеруванням перестановки n елементів.

На наступному етапі виникає необхідність визначити відстані від заданих експертами ранжувань до опорного ранжування за такими правилами:

– відстань від заданих експертами ранжувань $R^i, i = 1,...,k,$ до опорного ранжування $R^{*(0)}$ складається з двох складових: визначеної частини та ймовірнісної;

– ймовірнісна частина від заданого експертом ранжування $R^i, i = 1,...,k,$ до будь-якого опорного ранжування завжди дорівнює $\nu_i, i = 1,...,k,$ (для метрики Кука) (або $\nu_i \cdot (\nu_i - 1)/2, i = 1,...,k,$ – для метрики Хемінга);

– визначена частина дорівнює кількості інверсій між визначеними підмножинами перестановок: згенерованої опорної та заданої експертом $R^i, i = 1,...,k.$

Тобто в опорному ранжуванні кожного разу виділяємо n_i заданих і-м експертом об'єктів у ранжуванні R^i, і визначаємо кількість інверсій у перестановці об'єктів, відстань Хемінга (3) та відстань Кука (2).

Зрозуміло, що відстань від опорного ранжування $R^{*(0)}$ до кожного заданого експертом $R^i, i=1,...,k,$ дорівнює сумі ймовірнісної та визначеної частини.

Зважаючи на зазначений підхід, можна знайти результуючі ранжування виду (4)-(7), застосовуючи, наприклад, генетичний алгоритм [13] або евристичний алгоритм [14], розроблені для зазначених класів задач.

5. ВИСНОВКИ

В роботі запропоновано модель комплексного підходу до побудови системи кіберзахисту деякої складної організаційної системи. Також описано підхід до знаходження результуючого ранжування пріоритетності заходів як розв'язку задачі багатокритеріальної оптимізації. Послідовність виконання заходів може передбачати взаємодію виконавців і вимагати регламентування послідовності дій усіх елементів та підсистем організаційної системи.

Такий підхід дозволяє визначити результуючий комплекс заходів у вигляді медіани Кемені-Снелла, ГВ-медіани, медіани Кука-Сейфорда або ВГ-медіани. Запропонований підхід дозволяє:

– об'єднати різні за складом та пріоритетністю заходи інформаційної безпеки, запропоновані експертами різних підрозділів;

– знаходити компромісне рішення для різнорідної групи експертів;

– не порушувати задані переваги жодного експерта при обчисленні компромісного ранжування заходів кібербезпеки.

6. ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Запропонований у роботі підхід може:

– бути корисним при розробці заходів забезпечення належного рівня кібербезпеки;

– сприятливим при розробці та впровадженні процедур швидкого реагування на загрози;

– бути використаний для розв'язання задачі доповнення даних;

– за необхідністю, містити елементи навчання, узгодження, координації, комплексності учасників експертної групи, які є керівниками підрозділів єдиної організаційної системи;

– відігравати позитивну роль при формалізації та подальшій оптимізації бізнес-процесів організації при аналізі результатів розв'язання описаної задачі;

– бути незамінним при комплексній побудові системи безпеки організації або її удосконаленні.

7. СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] А.Г. Оксиюк, Я.В. Шестак, "Анализ современных методик и методов проведения оценки защищенности информационных систем", *Наукові записки Українського науково-дослідного інституту зв'язку*, №4, с.17-23, 2015.

[2] А.Г. Оксиюк, Я.В. Шестак, О.Д. Огбу, "Построение безопасной ифраструктуры как необходимость выживания", *Вісник Національного технічного університету «ХПІ». Збірник наукових праць. Серія: Механіко-технологічні системи та комплекси*, №50, с.112-117, 2016.

[3] А.Г. Додонов, Д.В. Ландэ, В.В. Цыганок, О.В. Андрейчук, С.В. Каденко, А.Н. Гайворонская, *Распознавание информационных операций*, Киев: ООО «Инжиниринг», 2017, 282 с.

[4] Г.М. Гнатієнко, В.Є. Снитюк, *Експертні технології прийняття рішень: монографія*, К.: ТОВ «Маклаут», 2008, 444с.

[5] О.Ф. Волошин, С.О. Мащенко, *Теорія прийняття рішень: навчальний посібник*, К.: Видавничо-поліграфічний центр "Київський університет", 2006, 304 с.

[6] И. М. Макаров, Т. М. Виноградская, А. А. Рубчинский, В. В. Соколов, *Теория выбора и принятия решений,* М.: Наука, 1982, 330 с.

[7] Ю.А. Шрейдер, *Равенство, сходство, порядок,* М.: Наука, 1971, 256 с.

[8] Дж. Кемени, Дж. Снелл, *Кибернетическое моделирование: некоторые приложения*, М.: Советское радио, 1972, 192 с.

[9] Б.Г. Миркин, *Проблема группового выбора*, М.: Наука, 1973, 256 с.

[10] М. Холлендер, Д. Вулф, *Непараметрические методы статистики*, М.: Финансы и статистика, 1983, 518 с.

[11] О.Ф. Волошин, Г.М. Гнатієнко, В.І. Кудін, *Послідовний аналіз варіантів. Технології та застосування*, К.: Стилос, 2013, 304 с.

[12] А.И. Орлов, *Методы принятия управленческих решений: учебник*, М.: КНОРУС, 2018, 286 с.

[13] Hnatiienko H.M., Kruglov A.I. "Definition of a compromise ranking on the set of individual rankings using the genetic

algorithm", *Міжнародний науковий симпозіум «ІНТЕЛЕКТУАЛЬНІ РІШЕННЯ». Обчислювальний інтелект (результати, проблеми, перспективи): праці міжнар. наук.-практ. конф.*, Ужгород, Україна, 15-20 квітня, 2019, с.63-64.

[14] Hnatiienko H.M., Hnatiienko V.H. "Heuristic algorithm for determining compromise rankings on a set of individual expert rankings", *INTELLIGENT SOLUTIONS. Decision Making Theory: Proceedings of the International School-Seminar*, Uzhhorod, Ukraine, April 15-20, 2019, pp.53-54.

Гнатієнко Григорій Миколайович, *кандидат технічних наук, здобув вищу освіту в Київському державному університеті ім. Т.Г. Шевченка в 1984 році, працює заступником декана факультету інформаційних технологій Київського національного університету імені Тараса Шевченка. Сфера наукових інтересів – обробка експертної інформації, інформаційні технології.*

Тмєнова Наталія Пилипівна*, кандидат фізико-математичних наук, здобула вищу освіту в Київському університеті імені Тараса Шевченка в 1999 році, працює доцентом кафедри інтелектуальних технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка. Сфера наукових інтересів – технології обробки природномовної інформації, інформаційні технології.*