УДК 519.9:004.681
DOI: 10.25140/2411-5363-2020-1(19)-114-123

Володимир Хорошко, Михайло Шелест, Юлія Ткач

БАГАТОКРИТЕРІАЛЬНА ОЦІНКА ЕФЕКТИВНОСТІ ПРОЄКТІВ ІЗ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Актуальність теми дослідження. *Багатокритеріальна оцінка ефективності проєктів є актуальним завданням у сфері кібербезпеки.*

Постановка проблеми. *Виникла нагальна потреба в різносторонньому та багатоаспектному оцінюванні ефективності проєктів із забезпечення кібербезпеки на різних етапах (при відборі проєктів, коли робота над ними ще не починалась, у процесі проведення робіт із виконання проєктів з метою оптимізації менеджменту та після виконання проєктів та коли дослідження завершені й можливо прослідкувати результати впровадження цих досліджень). Проте комплексна методика оцінки відсутня.*

Аналіз останніх досліджень і публікацій. *Зазвичай задачі оцінки та оптимізації об'єднують, вважаючи, що кінцева ціль полягає у зіставленні оцінок декількох альтернатив і вибір кращих із них. При такій постановці не розглядається випадок оцінки єдиного проєкту.*

Виділення недосліджених частин загальної проблеми. *Методику, яка дала б можливість отримання нормованої оцінки одного проєкту безвідносно до наявності (або відсутності) інших проєктів, нині не запропоновано.*

Постановка завдання. *Розроблена методика призначена для вирішення актуального завдання проведення системного аналізу й отримання багатосторонньої характеристики проєктів, підвищення достовірності висновків про наукову значущість результатів, про соціальну й економічну ефективність запланованих і виконаних робіт у кібербезпеці.*

Виклад основного матеріалу. *Задача оцінювання складних об'єктів і процесів передбачають зіставлення безлічі різних, зазвичай суперечливих властивостей, що дає підстави віднести ці задачі до класу багатокритеріальних. Вирішення багатокритеріальних задач є утрудненим унаслідок складності їх формулювання. Розроблена методика багатокритеріальної оцінки ефективності проєктів із забезпечення кібербезпеки дає можливість проведення системного аналізу й отримання багатокритеріальної характеристики проєкту, підвищення достовірності висновків отриманих результатів про соціальну та економічну ефективність запланованих і виконуваних робіт у галузі інформаційної безпеки. За допомогою запропонованої методики вирішуються завдання формування системи критеріїв та показників ефективності забезпечення кібербезпеки; побудови формалізованої аналітичної і якісної оцінки забезпечення кібербезпеки за сукупністю критеріїв якості; візуалізованого представлення оцінки проєкту. У перспективі припускається використовувати отримані результати для оцінки ефективності проєктів в інших предметних галузях. Методика неприйнятна в тих випадках, коли якісні показники принципово не зводяться до кількісних (числових) величин і не можуть бути виміряні за існуючими шкалами. Методику не можна використовувати без додаткової модифікації, якщо є такі критерії, які можуть приймати тільки дискретні (цілочисельні) значення.*

Висновки відповідно до статті. *Розроблену методику при деякій модифікації можна застосовувати у різних галузях, зокрема у сфері кібербезпеки, як на етапі відбору проєктів, так і в процесі проведення робіт з виконання проєктів, а також після виконання проєктів.*

Ключові слова: *кібербезпека; багатокритеріальна оцінка; ефективність проєктів.*
Рис.: 1. Табл.: 5. Бібл.: 11.

Актуальність теми дослідження. Завдання оцінювання ефективності забезпечення кібербезпеки – важлива проблема, від успішного вирішення якої залежить достовірність висновків про захищеність об'єкта, про економічність і фізичну ефективність робіт, що заплановані та виконані.

Постановка проблеми. Комплексна оцінка ефективності проєктів із забезпечення кібербезпеки сприятиме вирішенню актуального завдання проведення системного аналізу й отримання багатосторонньої характеристики проєктів, підвищення достовірності висновків про наукову значущість результатів, про соціальну й економічну ефективність запланованих і виконаних робіт у кібербезпеці.

Аналіз останніх досліджень і публікацій. Задача оцінювання складних об'єктів і процесів передбачають зіставлення безлічі різних, зазвичай суперечливих властивостей, що дає підстави віднести ці задачі до класу багатокритеріальних [1; 2]. Відомо, що вирішення багатокритеріальних задач є утрудненим унаслідок складності їх формулювання.

Для створення високоякісної збалансованості програми із забезпечення кібербезпеки зазвичай використовується метод експертних оцінок. До процесу оцінювання долучаються найбільш кваліфіковані вітчизняні й закордонні експерти. Участь закордонних експертів не завжди використовується, оскільки питання, пов'язані із забезпеченням кібербезпеки, мають певний рівень секретності.

Формування програми починається з підготовки та оголошення конкурсу про можливість участі в дослідженнях. За цими заявкам визначається кількість учасників, а також наукові й технічні галузі знань, за якими необхідно створювати експертні комісії.

Комісія обговорює сильні і слабкі сторони проєктів, обсяг розглянутих задач і ранжує проєкти згідно із запропонованими критеріями на підставі консенсусу. Комісія може також рекомендувати проєкти, які найкраще задовольняють цілям програми.

У монографії [3] розглянуто загальний випадок розробки технології підтримки прийняття рішень, коли потрібно вибрати альтернативу з множини неоднорідних альтернатив, для яких не можна сформувати єдину множину кількісних критеріїв оцінки. У цьому випадку задачі вирішуються методами, заснованими на ієрархічному цільовому оцінюванні альтернатив, без залучення критеріального аналізу. Водночас є великий клас задач прийняття рішень, коли для оцінки альтернатив можна залучити кількісні (або ті, що зводяться до них) критерії, які допускають операції в нормалізованому критеріальному просторі. Для таких задач застосовна теорія багатокритеріальної оцінки й оптимізації.

При формалізації рішення багатокритеріальних задач можна керуватися різними принципами. Концепція Чарнза-Купера [4] заснована на принципі «ближче до ідеальної (утопічною) точки». Різновид цієї концепції – метод TOPSIS (Technique for Preference by Similarity to the Ideal Solution) – метод наближення до ідеального розв'язання [5]. Загальний недолік методів, заснованих на цьому принципі, – громіздкість і можливість порушення обмежень. Цих недоліків позбавлений принцип «подалі від обмежень» [1].

У процесі дослідження багатокритеріальних задач особа, що приймає рішення (ОПР), керується своїм набором індивідуальних переваг, який формально відбивається деякою функцією корисності (цінності) в критеріальному просторі [6] або, іншими словами, схемою компромісів, скалярною згорткою векторного критерію [1]. Можливі різні апроксимації функції корисності. Найбільш поширений метод простого адитивного зважування (SAW (Simple Additive Weightiny) [7]. Однак слід мати на увазі, що це лише лінійне наближення критеріальної функції і в ситуаціях, що відрізняються від базової, яке може призводити до істотних спотворень. А найголовніше - лінеаризація критеріальної функції не дозволяє вирішувати багатокритеріальну задачу формально, без безпосередньої участі ОПР.

Для зменшення впливу суб'єктивності передбачається використовувати формалізований апарат скалярної згортки критеріїв на основі концепції нелінійної схеми компромісів [1].

Адекватні методи дослідження багатокритеріальних задач використовують залучення в тому чи іншому вигляді фахівця (експерта), що є компетентним в цій предметній галузі [3; 8]. У роботі експертні методи використовуються тільки для визначення розмірності і якісного складу вектора критерію, а також для кількісної оцінки значень частинних критеріїв (кардинальні оцінки).

Виділення недосліджених частин загальної проблеми. Незважаючи на численні дослідження в напрямі методик прийняття рішень та оцінювання ефективності, досі не запропоновано комплексну методику багатокритеріальної оцінки ефективності проєктів, зокрема в галузі кібербезпеки.

Мета статті. Головною метою роботи є розробка комплексної методики багатокритеріальної оцінки ефективності проєктів із забезпечення кібербезпеки.

Виклад основного матеріалу. Зазвичай задачі оцінки та оптимізації об'єднують, вважаючи, що кінцева мета полягає в зіставленні оцінок декількох альтернатив і вибір кращих із них. При такій постановці не розглядається випадок оцінки єдиного проєкту. Відмінна риса запропонованої методики – можливість отримання нормованої оцінки одного проєкту, безвідносно до наявності (або відсутності) інших проєктів.

Ефективність проєктів оцінюється в трьох випадках:

1. При відборі проєктів, коли робота над ними ще не починалась.
2. У процесі проведення робіт із виконання проєктів з метою оптимізації менеджменту.
3. Після виконання проєктів, коли дослідження завершені й можливо прослідкувати результати впровадження цих досліджень.

Розроблену методику при деякій модифікації можна застосовувати в усіх згаданих випадках, але в деякій роботі ми зосередимо увагу на оцінці ефективності виконаних проєктів із забезпечення кібербезпеки.

За допомогою запропонованої методики розв'язуються такі задачі:

- формування системи критеріїв та показників ефективності забезпечення кібербезпеки;
- розробка формалізованої аналітичної і якісної оцінки забезпечення кібербезпеки за сукупністю критеріїв якості (при цьому базовою є така постановка задачі: дано – об'єкт оцінки, ефективність захисту якого характеризуються x-мірним вектором критеріїв $y = \{y_k\}^s{}_{k=1}$, потрібно знайти узагальнену аналітичну оцінку ефективності (якості) захищеності об'єкту $Y(y)$ і його якісну оцінку;
- візуалізоване представлення оцінки проєкту.

Для аналізу ефективності проєктів із забезпечення кібербезпеки нами розроблені форми подання комплексної інформації організаціями-виконавцями. Крім того, за бажанням експерта в їх розпорядження надаються технічні завдання, звіти, календарні плани та інші необхідні матеріали й документи по проєкту, що оцінюється. Для процедури експертизи проєктів у галузі кібербезпеки й отримання відповідей експертів розроблена типова форма – анкета. Форми та анкети – це рамочні документи, у кожному конкретному випадку показники можуть модифікуватись, виключатись або додаватися. Усе залежить від об'єкта, експертиза захищеності якого проводиться.

Можливості розробленої методики дозволяють здійснювати комплексну оцінку ефективності проєктів при кількості показників якостей від одиниць до декількох десятків.

Методика неприйнятна в тих випадках, коли якісні показники принципово не зводяться до кількісних (числових) величин і не можуть бути виміряні за наявними шкалами. Методику не можна використовувати без додаткової модифікації, якщо є такі критерії, які можуть приймати тільки дискретні (цілочисельні) значення.

Поставлені задачі розв'язуються багатокритеріальним методом з отриманням вихідних даних шляхом експертних оцінок. Експертна інформація для формування системи критеріїв та для оцінки частинних критеріїв ефективності проєктів із забезпечення кібербезпеки формується шляхом анкетного опитування за оціночними шкалами. Масив даних використовується як вихідний матеріал для розрахунку аналітичних оцінок якості, а також для побудови графічного образу ефективності проєкту й отримання якісних характеристик. Багатокритеріальна оцінка здійснюється як за традиційною нелінійною схемою компромісів [2; 4; 5], так і методом вкладених скалярних згорток векторного критерію [9]. В останньому випадку проєкти аналізуються і оцінюється за агрегованими критеріями, що робить аналіз випуклим та контрастним.

Оцінка ефективності проєкту починається з формування групи організаторів експертизи, в чиї обов'язки входить:

– вибір фахівців-експертів;
– розробка (і за необхідності узгодження з експертами) переліку критеріїв та показників ефективності;
– складання опитувальних листків (форм-анкет);
– проведення опитування експертів;
– аналіз і обробка інформації, отриманої від експертів;
– отримання і візуалізація оцінок за окремими (частинними) критеріями, групами критеріїв (агрегованих оцінок) і повною сукупністю критеріїв (узагальнена аналітична оцінка);
– отримання якісних характеристик проєкту.

Як експерти залучаються висококваліфіковані фахівці в галузі, що розглядається. Кількість експертів обумовлюється складністю задачі, яка розв'язується.

Організатори експертизи роблять попередній список критеріїв, який дозволяє оцінити якість проєкту забезпечення кібербезпеки.

Критерії структуруються за групами:

1. Загальні критерії.
2. Критерії науково-технічного розвитку.

3. Фінансово-економічні критерії.
4. Соціальні критерії.
5. Критерії забезпечення завдань оборони й безпеки.
6. Екологічні критерії.

Після консультації з експертами організатори експертизи включають у кожну групу конкретні критерії. Якщо всі експерти з отриманим списком згодні, і не вносять доповнень, то на цьому цей етап закінчується.

Якщо ж експерти вносять у початковий список додаткові критерії або мають сумнів щодо вже внесених, то відбувається етап ранжування критеріїв.

Щоб виявити дійсно значущі частинні критерії, експертам пред'являють (кожному окремо) складений ними первинний список. Їм пропонується вивчити список і вибрати з нього найбільш важливі, на думку експерта, частинні критерії, проранжувавши їх за важливістю. Критерії, які отримали найменшу суму рангів, виділяються в остаточний список. Кількість виділених критеріїв залежить від багатоаспектності проєкту (зазвичай їх буває від двох до семи в кожній групі). Необхідно, щоб різниця між кількістю голосів, відданих найменш важливому з виділених критеріїв і найбільш важливому з перерахованих, була щонайбільшою. Для агрегування може бути використаний також метод Кондорсе [3].

Виділені показники в усіх групах являють собою вихідну систему частинних критеріїв, з яких формується узагальнений критерій якості оцінюваного проєкту.

Експертам (кожному окремо) надається розроблена форма-анкета. У ній у складі рубрик за групами критеріїв перераховуються частинні критерії, виділені на попередньому етапі. Критеріям зіставляється неперервна шкала, розділена на 10 інтервалів. Цифра 0 на шкалі відповідає поняттю «ніякої цінності», цифра 10 – «максимальна цінність». Експерта просять оцінити вплив кожного з частинних критеріїв на ефективність проєкту й визначити для кожного критерію відповідну точку на шкалі.

Аналіз процесів прийняття рішень показав, що при оцінці об'єктів за шкалою балів експерти керуються так званою фундаментальною шкалою [3; 7] (табл. 1). У термінах теорії нечітких множин фундаментальна шкала являє собою функцію належності, за допомогою якої здійснюється перехід від лінгвістичної змінної (задовільна якість, висока якість і т. ін.) до кількісних оцінок (відповідно 5,5; 7,0) за шкалою балів, тобто перехід від нечітких якісних градації до чисел і навпаки.

Таблиця 1

Таблиця переходу від нечітких якісних градації до чисел і навпаки

Категорія якості	**Фундаментальна шкала f**	**Перетворена нормована фундаментальна шкала y_0, Y_0, Φ_0**
Неприйнятне	0-3	1,0-0,7
Низьке	3-5	0,7-0,5
Задовільне	5-6	0,5-0,4
Добре	6-8	0,4-0,2
Високе	8-10	0,2-0,0

Після заповнення експертами анкети повертаються до організаторів експертизи й обробляється. Масив отриманих від експертів даних – це сукупність чисел f_{ik}, що являють собою оцінку, дану f-м експертом k-му критерієм за шкалою анкети, j∈ $[1, m]$, m – кількість експертів. Розраховується усереднена оцінка, дана колективом експертів за кожним критерієм:

$$f_k = \frac{1}{m}\sum_{j=1}^{m} f_{jk},\ k\in[1,s], \quad (1)$$

де s – кількість критеріїв. Оцінки f_k – досить об'єктивна, якщо кількість експертів велика та склад їх досить однорідний (у складніших випадках застосовують методику обробки експертних оцінок з урахуванням коефіцієнтів компетентності експертів) [1; 2; 6].

При розгляданні експертами деяких критеріїв можливий випадок, коли вони вагаються з оцінкою і у відповідній графі ставлять прочерк. Тоді при розрахунку оцінки за формулою (1) замість величини m використовується число m_k, $m_k \le m$ що дорівнює

реальній кількості експертів, які брали участь в оцінці критеріїв. Нормовані оцінки за мінімізованими частинними критеріями отримуються з (1) за формулою:

$$y_{ok} = 1 - 0{,}1f_k,\ 0 \leq y_{ok} < 1,\ k \in [1,s]. \quad (2)$$

Символ «0» тут і далі відмічається нормована оцінка. Нормованим мінімізованим критеріям зіставляються перетворена нормована фундаментальна шкала (табл. 1). Сукупність нормованих критеріїв y_{ok} є вихідною для аналітичної багатокритеріальної оцінки проєкту відповідно до концепції нелінійної схеми компромісів [1; 6].

Для різнобічної характеристики оцінюваних проєктів використовується два види методів багатокритеріальної оцінки – це традиційний і агрегований.

Узагальнена аналітична оцінка проєкту щодо забезпечення кібербезпеки традиційним методом із використанням скалярної згортки по нелінійній схемі компромісів [1] здійснюється за формулою:

$$Y(y_0) = \sum_{k=1}^{s} (1 - y_{ok})^{-1}. \quad (3)$$

У задачі аналізу абсолютна величина $Y(y_0)$ ще нічого не говорить про те, наскільки відповідає завданню або не відповідає цей проєкт.

Для відповіді на це питання розв'язуємо задачу переходу від чисельної оцінки $Y(y_0)$ до лінгвістичної категорії «добре – неприйнятне».

Насамперед нормуємо аналітичну оцінку так, щоб при неприйнятних проєктах, нормована оцінка $Y(y_0)$ наближалася до оцінки одиниці, а при хороших до нуля:

$$Y_0(y_0) = \frac{Y(y_0)}{Y_{max}}, \quad (4)$$

де Y_{max} – гранично погана аналітична оцінка для проєкту, що розглядається.

Для визначення величини Y_{max} скористаємося принципом солідарної відповідальності. У застосуванні до нашої задачі він полягає в наступному.

В інтервалі неприйнятних оцінок (0,7-1,0) перетвореної нормованої фундаментальної шкали вибираємо деяку величину y_{0max}, яку реально може досягти будь-який із нормованих частинних критеріїв при неприйнятно поганій якості за даним критерієм. Відзначимо, що цю величину потрібно підібрати так, щоб правильно оцінювалися тестові приклади (налаштування вирішального правила).

Відповідно до принципу солідарності відповідальності, якщо який-небудь нормований критерій досяг величини y_{0max}, то і решті нормованим критеріям приписується можливість досягнення такого ж значення. Якщо це так, то величина Y_{max} можна визначити за формулою:

$$Y_{max} = S(1 - y_{omax})^{-1}$$

Нормована аналітична оцінка проєкту Y_0 також вимірюється за перетвореною нормованою фундаментальною шкалою (табл. 1), яка в термінах теорії нечітких множин являє собою функцію належності. З її допомогою виконується перехід від числа Y_0 до відповідної якісної градації .

Інформативність оцінок проєкту за допомогою агрегованого методу може бути підвищена за рахунок об'єднання частинних критеріїв у групи й формування агрегованих критеріїв за методом вкладених скалярних згорток [9].

Оцінки за агрегованими критеріями обчислюються відповідно до формули:

$$\varphi_i = \sum_{j=1}^{J} \left(1 - y_{oij}\right)^{-1},\ i \in [1, I], \quad (5)$$

де φ_i – це оцінки за агрегованими критеріями; y_{oij} – нормовані оцінки за окремими критеріями; I – кількість груп; J_i – кількість вихідних частинних критеріїв у цій групі.

Узагальнена нормована оцінка за агрегованими критеріями визначається за формулою:

$$\Phi = \sum_{i=1}^{I} \frac{1}{1 - \varphi_{0i}}, \quad (6)$$

якщо агреговані оцінки нормовані за формулою:

$$\varphi_{oi}=\frac{\varphi_i}{B_i},\ i\in[1,I].$$

У цій формулі $B_i = J_i\,(1-y_{omax})^{-1}$ є неприйнятно погана оцінка φ_{omax} агрегованого критерію φ_{oi} в кожній групі. Причому $\varphi_{omax} = y_{omax}$.

Отримана аналітична оцінка нормується за формулою:

$$\Phi_o = \frac{\Phi}{\Phi_{max}}, \quad (7)$$

це Φ_{max}=I $(1-y_{omax})^{-1}$ – неприйнятно погана величина оцінки Φ_o.

Нормована аналітична оцінка проєкту за агрегованими критеріями Φ_o також вимірюється за перетвореною нормованою фундаментальною шкалою (табл. 1), і на підставі цього виміру виходить якісна характеристика проєкту. Зазвичай оцінки Φ_o та Y_o наближені один до одного, але за наявності значних «викидів» нормованих частинних критеріїв оцінка Φ_o більша.

Оцінки за вектором критеріїв якості графічно представляються у вигляді «профілю проєкту». Вихідною інформацією для його побудови слугує сукупність нормованих критеріїв y_{ok}. Профіль дозволяє створювати цілісний образ проєкту, що оцінюється, щодо забезпечення кібербезпеки, що може виявитися вельми корисним, наприклад, при експрес-оцінках.

Програмне забезпечення для оцінки кібербезпеки об’єкта складається з 4 блоків:

1. Інформаційні дані про проєкт забезпечення кібербезпеки.
2. Організація процедури експертизи проєкту.
3. Обробка результатів експертизи проєкту.
4. Висновок і візуалізація результатів оцінки проєкту.

Управління програмою виконується ПЕОМ і складається із введення даних і команд на виконання розрахункових процедур у відповідні інформаційні поля.

Блок «Інформаційні дані про проєкт забезпечення кібербезпеки» містить:

- поля для введення назви проєкту, найменування організації-виконавця, дані про терміни виконання проєкту та обсяги фінансування;
- типову форму (анкету) представлення інформації, заповнену виконавцями проєкту.
- технічне завдання, звіт та інші відомості про проєкт.

Блок «Організації процедури експертизи проєкту» включає:

- список фахівців-експертів і відомості про них;
- анкету для проведення експертизи.

Блок «Обробки результатів експертизи проєкту» накопичує відповіді експертів, формує масив даних для подальшої обробки, визначає розмірність вектора частинних критеріїв, кількість груп критеріїв, кількість критеріїв у групах, а також виконує на основі формул розрахунок різних категорій оцінок ефективності проєкту.

Блок «Висновок і візуалізація результатів оцінки проєкту» здійснює видачу результатів розрахунку різних категорій оцінок ефективності проєкту, а також будують «профіль проєкту».

За допомогою запропонованої методики був проведений системний аналіз та отримано багатокритерійну оцінку кібербезпеки ситуаційного центру одного з міністерств України [10; 11].

У процесі консультацій з експертами визначено чотири групи з раніше перелічених критеріїв (I = 4), що включають 20 критеріїв (S = 20) оцінки цього проєкту оцінки кібербезпеки – загальні, наукового розвитку, економічні та соціальні. Чотири провідні фахівці в галузі інформаційної безпеки (m = 4) заповнили анкету (табл. 2).

Таблиця 2

Анкета експертів

№ критерію	Критерії оцінки якості проєкту	К-ть балів за 10-бальною шкалою
1. Загальні критерії		
	Ясність і чіткість формування цілей проєкту	Оцінка експерта
1	Міра відповідності проєкту поставленим цілям	
2	Ступінь повноти реалізації проєкту	
3	Ступінь інтеграції проєкту в Національну програму кібербезпеки	
4	Ступінь сприяння підвищенню престижу організації	
2. Критерії наукового розвитку		
5	Ступінь новизни у виконаній роботі	Оцінка експерта
6	Міра оригінальності та новизни поставлених цілей і отриманих результатів	
7	Міра сприяння розвитку методів та засобів забезпечення кібербезпеки	
8	Міра сприяння результатів проєкту появи нових методів забезпечення кібербезпеки	
9	Частина досліджень у проєкті, які виконані на світовому рівні	
10	Заходи сприяння розвитку знань про механізми забезпечення кібербезпеки	
11	Вплив проєкту на перспективу розвиток методів забезпечення кібербезпеки	
12	Міра висвітлення робіт із кібербезпеки в науковій літературі	
13	Міра популяризації та поширення знань про кібербезпеки	
14	Можливість використання результатів роботи при підготовці й перепідготовці фахівців із кібербезпеки	
3. Економічні критерії		
15	Рівень впровадженості результатів розробки в практику	Оцінка експерта
16	Рівень повноти передачі розроблених методів для застосування на критично важливих об’єктах	
17	Сприяння в залученні матеріальних ресурсів	
4. Соціальні критерії		
18	Вплив результатів розробки на Національну програму кібербезпеки	Оцінка експерта
19	Рівень можливості використання отриманих результатів при підготовці та перепідготовці фахівців із кібербезпеки	

Відповіді експертів зведені в табл. 3. Лівий стовпчик таблиці відповідає порядковому номеру критерію, відповідно тому номеру, який цей критерій має в анкеті. Нормовані значення частинних критеріїв отримані за формулою (1) і (2). Узагальнена аналітична оцінка проєкту класичним методом, обчислена за формулами (3) та (4). Розрахунок ефективності проєкту за агрегованими критеріями виконано за формулами (5) та (7).

Таблиця 3

Оцінки експертів

№ критерію	Оцінки експертів			
	1-й експерт	2-й експерт	3-й експерт	4-й експерт
1.	9	10	10	10
2.	9	10	10	10
3.	6	8	9	10
4.	-	8	6	9
5.	8	10	9	9
6.	7	10	10	9
7.	7	10	9	9
8.	9	8	9	10
9.	7	9	10	9
10.	-	9	8	9
11.	10	8	8	10
12.	8	10	9	9
13.	7	8	7	8
14.	8	7	8	8
15.	9	6	8	8
16.	8	8	9	7
17.	8	7	6	5
18.	9	9	10	4
19.	8	7	8	-
20.	9	8	7	4

Отримано чотири види результатів:

1) аналітична нормована оцінка проєкту із забезпечення кібербезпеки ситуаційного центру традиційним методом;

2) якісна оцінка проєкту із забезпечення кібербезпеки ситуативного центру традиційним методом за перетвореною нормованою фундаментальною шкалою;

3) аналітична нормована оцінка проєкту із забезпечення кібербезпеки ситуаційного центру агрегованих методом;

4) якісна оцінка проєкту із забезпечення кібербезпеки ситуаційного центру агрегованих методом за перетвореною нормованою фундаментальною шкалою.

Результати розрахунку ефективності проєкту із забезпечення кібербезпеки ситуаційного центру традиційним методом наведені в табл. 4, агрегованим – у табл. 5.

Таблиця 4

Результати розрахунку ефективності проєкту із забезпечення кібербезпеки ситуаційного центру традиційним методом

№ критерію	Значення y_o нормованих оцінок за частинним критерієм
1.	0,025
2.	0,025
3.	0,175
4.	0,267
5.	0,100
6.	0,100
7.	0,125
8.	0,100
9.	0,125
10.	0,133
11.	0,100
12.	0,100
13.	0,250
14.	0,225
15.	0,225
16.	0,200
17.	0,350
18.	0,200
19.	0,233
20.	0,300

Таблиця 5

Результати розрахунку ефективності проєкту із забезпечення кібербезпеки ситуаційного центру агрегованим методом

№ експерта	1	2	3	4
Значення φ_o нормованих агрегованих оцінок	0,287	0,295	0,337	0,342

Графічні результати представлені «профілем проєкту» (рис. 1). На рис. 1 по осі абсцис відкладені номери частинних критеріїв відповідно до лівого стовпчика анкети.

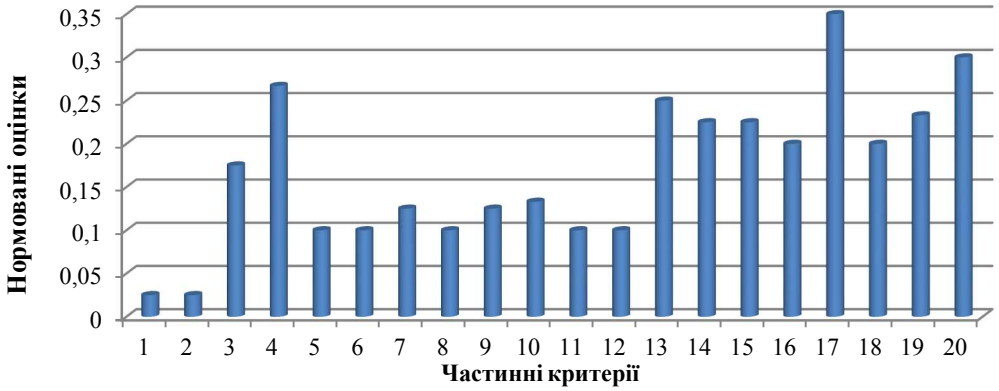

Рис. 1. Графічні результати за «профілем проєкту»

Висновки відповідно до статті. Комплексна методика багатокритеріальної оцінки ефективності проєктів із забезпечення кібербезпеки дає можливість проведення системного аналізу й отримання багатокритеріальної характеристики проєкту, підвищення достовірності висновків отриманих результатів про соціальну та економічну ефективність запланованих і виконуваних робіт у галузі інформаційної безпеки. У перспективі припускається використовувати отримані результати для оцінки ефективності проєктів в інших предметних галузях.

Список використаних джерел

1. Воронин А. Н. Многокритериальный синтез динамических систем. Київ: Наукова думка, 1992. 160 с.
2. Жуковский В. И., Молоствов В. С. Многокритериальное принятие решений в условиях неопределенности. Москва: МНИИПУ, 2008. 192 с.
3. Тоценко В. Г. Методы и системы поддержки принятия решений: Алгоритмический аспект. Київ: Наукова думка, 2002. 382 с.
4. Кузьменко Г. Е., Плиш В. Е. Функциональная архитектура интегрированой системи поддержки принятия решений в условиях ситуационных центров. Математические машины и системы. 1997. № 1. С. 56–63.
5. Тарасов В. А., Герасимов Б. М., Левин И. А., Корнейчук В. А. Интеллектуальные системы поддержки принятия решений: теория, синтез, эффективность. Киев: МАКНС, 2007. 336 с.
6. Фишберн П. Теория полезности для принятия решений. Москва: Наука, 1978. 352 с.
7. Saaty T. L. Decision Making for Leaders. Pittsburgh: RWS Publications, 2000. 240 p.
8. Орловский С. А. Проблемы принятия решений при нечеткой исходной информации. Москва: Наука, 1981. 208 с.
9. Руа Б. Проблемы и методы принятия решений в задачах с многими целевыми функциями. *Вопросы анализа принятия решения.* Москва: Мир, 1976. 380 с.
10. Морозов А. А., Ященко В. А. Ситуационные центры. Информационные технологии будущего (Новая информационная технология). Киев: Интертехнодрук, 2008. 332 с.
11. Морозов А. А., Кузьменко Г. Е. Построение сценариев развития событий –основа функционирования информационно-аналитических систем типа «ситуационные центры». *Системи підтримки прийняття рішень. Теорія і практика*. 2005. № 3. С. 42–44.

References

1. Voronyn, A. N. (1992). *Mnogokriterialnyi sintez dynamicheskikh sistem [Multicriteria synthesis of dynamical systems]*. Kyiv: Naukova dumka [in Russian].
2. Zhukovskyi, V. I. (2008). *Mnogokriterialnoe priniatie reshenii v usloviiakh neopredelennosti [Multi-criteria decision making under uncertainty*]. Moscow: MNIIPU [in Russian].
3. Totsenko, V. H. (2002). *Metody i sistemy podderzhki priniatiia reshenii: Algoritmicheskii aspekt [Decision-making methods and systems: Algorithmic aspect*]. Kyiv: Naukova dumka [in Russian].
4. Kuzmenko, G. E. (1997). Funktsionalnaia arkhitektura integrirovanoi sistemy podderzhki priniatiia reshenii v usloviiakh situatsionnykh tsentrov [Functional architecture of an integrated decision support system in situational centers]. *Matematicheskie mashiny i sistemy – Mathematical Machines and Systems*, 1, 56–63 [in Russian].
5. Tarasov, V. A., Herasymov, B. M., Levyn, I. A., & Korneichuk, V. A. (2005). *Intellektualnye sistemy podderzhki priniatiia reshenii: teoriia, sintez, effektivnost [Intelligent decision support systems: theory, synthesis, efficiency]*. Kyiv: MAKNS [in Russian].
6. Fyshbern, P. (1978). *Teoriia poleznosti dlia priniatiia reshenii [Theory of utility for decision making]*. Moscow: Nauka [in Russian].
7. *Saaty,* T. L. (2000). *Decision Making for Leaders*. Pittsburgh: RWS Publications [in English].
8. Orlovskyi, S. A. (1981). *Problemy pryniatyia reshenyi pry nechetkoi yskhodnoi ynformatsyy [Decision-making problems with fuzzy initial information*]. Moscow: Nauka [in Russian].
9. Rua, B. (1976). Problemy y metody pryniatyia reshenyi v zadachakh s mnohymy tselevymi funktsyiamy [Problems and decision-making methods in tasks with many objective functions]. *Voprosy analyza pryniatyia reshenyia. – Decision Analysis Issues.* Moscow: Mir [in Russian].
10. Morozov, A. A. & Yashchenko, V. A. (2008). *Situatsionnye tsentry. Informatsionnye tekhnologii budushcheho (Novaia informatsionnaia tekhnologia) [Situational centers. Information Technologies of the Future (New Information Technology*)]. Kyev: Intertekhnodruk [in Russian].

11. Morozov, A. A., Kuzmenko, H. E. (2005). Postroenye stsenariev razvitiia sobytii – osnova funktsionirovaniia informatsionno-analiticheskykh sistem tipa «situatsionnye tsentry» [Building scenarios for the development of events - the basis for the functioning of information-analytical systems such as «situational centers»]. *Sistemy pidtrymky priniattia rishen. Teoriia i praktyka – Decision support systems. Theory and Practice,* 3, 42–44 [in Russian].

UDC 519.9:004.681

Volodymyr Khoroshko, Mykhailo Shelest, Yuliia Tkach

MULTI-CRITERIA ASSESSMENT OF THE PROJECT EFFICIENCY OF CYBER SECURITY PROVISIONS

Urgency of the research. *Multicriteria assessment of project effectiveness is an urgent challenge in cybersecurity.*

Target setting. *There is an urgent need for a multifaceted and multidimensional assessment of the effectiveness of cybersecurity projects at various stages (when selecting projects where work has not begun on them, in the course of project implementation work to optimize management and after project implementation, and when studies are completed and possible to track the results of these studies). However, there is no comprehensive assessment methodology.*

Actual scientific researches and issues analysis. *Typically, evaluation and optimization tasks combine, believing that the ultimate goal is to map the estimates of several alternatives and choose the best ones. Such a statement does not consider the case of evaluation of a single project.*

Uninvestigated parts of general matters defining. *A methodology that would allow a standardized estimate of one project to be obtained regardless of the presence (or absence) of other projects has not yet been proposed.*

The research objective. *The developed methodology is intended for solving the urgent task of carrying out systematic analysis and obtaining the multilateral characterization of projects, increasing the reliability of conclusions about the scientific significance of the results, about the social and economic efficiency of planned and executed works in cybersecurity.*

The statement of basic materials. *Tasks for evaluating complex objects and processes involve a juxtaposition of many different, usually contradictory properties, which gives reason to attribute these tasks to the class of multicriteria. Solving multicriteria problems is difficult due to the complexity of their formulation. The developed methodology of multicriteria assessment of the effectiveness of cybersecurity projects enables the systematic analysis and obtaining of multicriteria characteristics of the project, enhancing the reliability of the results obtained on the social and economic efficiency of the planned and performed work in the field of information security. The proposed methodology addresses the challenges of developing a system of criteria and performance indicators for cybersecurity; building a formalized analytical and qualitative assessment of cybersecurity on the set of quality criteria; visualized presentation of project evaluation. In the long term, it is expected to use the results obtained to evaluate the effectiveness of projects in other subject areas. The technique is unacceptable in cases where qualitative indicators are not essentially reduced to quantitative (numerical) values and cannot be measured on existing scales. The technique cannot be used without further modification if there are criteria that can accept only discrete (integer) values.*

Conclusions. *The developed methodology with some modification can be applied in various fields, in particular in the field of cybersecurity, both at the stage of project selection and in the process of carrying out project implementation works, as well as after the implementation of projects.*

Keywords: *cybersecurity; multicriteria assessment; project effectiveness; information security.*

Fig.: 1. Table: 5. References: 11.

Хорошко Володимир Олексійович – доктор технічних наук, професор кафедри безпеки інформаційних технологій, Національний авіаційний університет (просп. Космонавта Комарова, 1, м. Київ, 03058, Україна).
Khoroshko Volodymyr – Doctor of Technical Sciences, Professor of Department of Information Technology Security, National Aviation University (1 Cosmonaut Komarov Av., 03058 Kyiv, Ukraine).
E-mail: professor_va@ukr.net
ORCID: http://orcid.org/0000-0001-6213-7086

Шелест Михайло Євгенович – доктор технічних наук, професор кафедри кібербезпеки та математичного моделювання, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Shelest Mykhailo – Doctor of Technical Sciences, Professor of Department of Cybersecurity and Mathematical Modeling, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
E-mail: mishel3141@gmail.com

ORCID: http://orcid.org/0000-0001-7110-4876

Ткач Юлія Миколаївна – доктор педагогічних наук, доцент, завідувач, професор кафедри кібербезпеки та математичного моделювання, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Tkach Yulia – Doctor of Pedagogical Sciences, Associate Professor, Head, Professor of Department of Cybersecurity and Mathematical Modeling, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
E-mail: tkachym79@gmail.com
ORCID: http://orcid.org/0000-0002-8565-0525

Хорошко В., Шелест М., Ткач Ю. Багатокритеріальна оцінка ефективності проєктів із забезпечення кібербезпеки. *Технічні науки та технології*. 2020. № 1 (19). С. 114-123.