УДК 004.056.5:[621.391:658
DOI: 10.31673/2409-7292.2024.010009

**Біляєв Д. А., Мацько О. Й.,
Сампір О. М., Новікова І. В.**

МЕТОД БАГАТОКРИТЕРІАЛЬНОГО ВИБОРУ ОПТИМАЛЬНОГО ВАРІАНТА СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА

Розробка будь-якої складної технічної системи як правило пов'язується з вирішенням оптимізаційної задачі. У випадку проектування системи захисту інформації для інформаційно-комунікаційної системи підприємства – це пошук оптимального варіанта комплекту засобів захисту з усієї множини можливих. Як і всяка складна система, система захисту інформації інформаційно-комунікаційної системи підприємства характеризується множиною показників функціонування, які характеризують систему захисту з точки зору протидії: вторгненням зловмисників до системи; загрозам конфіденційності, цілісності та доступності інформації; шкідливим програмним засобам та ін. У статті розглядається метод багатокритеріального вибору оптимального варіанта системи захисту інформації для інформаційно-комунікаційної системи підприємства. Запропоновано 5 підходів щодо вибору архітектури складної системи. Підходи, що розглядаються проілюстровані на модельному прикладі вибору одного з чотирьох варіантів системи захисту інформації інформаційно-комунікаційної системи підприємства. Запропоновано простий та досить наглядний метод вибору оптимального варіанта системи захисту інформації для інформаційно-комунікаційної системи підприємства з множини можливих. Цей метод дозволяє розв'язувати задачу безпосередньо по сукупності показників якості без згортання критеріїв у комплексний показник. Перспективами розвитку запропонованого методу є його удосконалення з метою реалізації можливості надання переваги окремим критеріям.

Ключові слова: захист інформації, інформаційно-комунікаційна система, оптимальний варіант, багатокритеріальний вибір.

Вступ

Прогрес у нових інформаційно-комунікаційних технологіях розширює межі можливого та відкриває нові ринки для інноваційних продуктів і послуг інформаційно-комунікаційних технологій. Прийняття продуктів і систем інформаційно-комунікаційних технологій із властивостями безпеки залежить від впевненості споживачів і довіри ринку до функціональних можливостей безпеки, а також від того, чи відповідають заходи безпеки, застосовані до цих продуктів, внутрішнім вимогам безпеки. Така впевненість і довіра досягаються в першу чергу завдяки ретельному розвитку вимог безпеки, критеріїв перевірки, оцінювання та сертифікації.

Постановка проблеми

Розробка будь-якої складної технічної системи як правило пов'язується з вирішенням оптимізаційної задачі. У випадку проектування системи захисту інформації для інформаційно-комунікаційної системи підприємства – це пошук оптимального варіанта комплекту засобів захисту з усієї множини можливих. Як і всяка складна система, система захисту інформації інформаційно-комунікаційної системи підприємства характеризується множиною показників функціонування, які характеризують систему захисту з точки зору протидії: вторгненням зловмисників до системи; загрозам конфіденційності, цілісності та доступності інформації; шкідливим програмним засобам та ін.

Крім того, не маловажливою є також вартість комплекту засобів, які планується придбати та встановити підприємство. У загальному випадку такі критерії є достатньо суперечливими, тобто покращуючи один показник, ми неминуче погіршуємо інші показники. Тому виникає завдання визначення деякого компромісного варіанта системи, який у рівній мірі задовольнятиме усім вимогам (компроміс Парето). У такому випадку, як правило, результати за кожним окремим показником якості будуть дещо гіршими, ніж при однокритеріальній оптимізації за цим параметром.

Аналіз наукових джерел

Існує досить велика кількість методів багатокритеріального вибору оптимального (найкращого) варіанта системи з множини можливих.

У [1] проведено систематичний огляд стандарту ISO/IEC 15408 та його запровадження, спонукуючись до прийняття загальних критеріїв, які використовуються для оцінки та сертифікації безпеки інформаційно-комунікаційних технологій. На основі аналізу сучасних тенденцій оцінки кібербезпеки досліджено бар'єри впровадження загальних критеріїв. Крім того, автори діляться досвідом і уроками, отриманими під час оцінки кіберкритеріїв щодо розробки профілю захисту, який визначає вимоги безпеки з загальними критеріями.

У статті [2] 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.

В публікації [3] розроблено модель системи підтримки прийняття рішень для фінансування проектів для створення сприятливих умов розвитку центрів управління кібербезпекою об'єктів критичної інфраструктури. Модель передбачає методи та засоби активної протидії стороні що атакує. На відміну від існуючих підходів, модель заснована на вирішенні білінійної гри диференціальної якості з кількома термінальними поверхнями. У роботі був використаний метод дискретного наближення. Це дало змогу знайти рішення білінійної диференціальної гри якості із залежними рухами. Результати обчислювального експерименту в рамках програмної реалізації системи підтримки прийняття рішень у галузі фінансування проектів кібербезпеки, зокрема, у створенні та розвитку центрів управління кібербезпекою для критично важливих об'єктів інфраструктури описані. Розроблена система підтримки прийняття рішень дозволяє отримувати оптимальні стратегії фінансування із забезпечення кібербезпеки критично важливих об'єктів інфраструктури. В публікації [4] обговорюються відмінності між IoT та IT-системами, потреба в рішеннях безпеки IoT, а також висвітлюємо ключові компоненти, необхідні для архітектури системи безпеки мережі IoT. Досліджуються типи атак IoT, при цьому групуючи їх на основі групування їх критеріїв впливу.

У статті [5] запропоновано окремі показники оцінювання здатності (ефективності) функціонування системи захисту і кібербезпеки інформації в інформаційно-комунікаційних системах спеціального зв'язку. Ці показники становлять підґрунтя для подальшого обґрунтування методики оцінювання здатності (ефективності) функціонування системи захисту інформації і кібербезпеки інформації в інформаційно-комунікаційних системах спеціального зв'язку. У статті [6] отримана оцінка та категоризація даних на основі критеріїв оцінювання систем захисту, яка допоможе дослідникам кібербезпеки та страховій індустрії в їхніх зусиллях зрозуміти, вимірювати та керувати кіберризиками. Стаття [7] визначає фундаментальну термінологію та концепції, які використовуються в спільноті кібербезпеки і описує основні кроки для включення ризиків кібербезпеки в загальний процес управління ризиками, що є центральною відповідальністю служб захисту.

У [8] міститься огляд поточного стану аномалій і концепцій безпеки, пов'язаних з IoT, та пропонується вирішення багатокритеріальної задачі вибору засобів безпеки. Автори класифікують та аналізують найпоширеніші проблеми безпеки щодо багаторівневої архітектури Інтернету речей, включаючи підключення, зв'язок і протоколи керування. Розроблено систему критеріїв безпеки IoT, досліджуючи поточні атаки, загрози та передові рішення. Встановлено цілі безпеки, які слугуватимуть еталоном для оцінки відповідності рішення конкретним випадкам використання IoT. У статті [9] представлено результати дослідження компетенцій з кібербезпеки у сфері загроз державному кіберпростору та методів забезпечення безпеки та захисту даних. Важливим елементом дослідження було визначення

© Біляєв, Д. А., Мацько, О. Й., Сампір, О. М., & Новікова, І. В. (2024). Метод багатокритеріального вибору оптимального варіанта системи захисту інформації для інформаційно-комунікаційної системи підприємства. Сучасний захист інформації, 1(57), 77–82. https://doi.org/10.31673/2409-7292.2024.010009.

форм навчання, за допомогою яких можна досягти більшої ефективності підвищення компетенцій у сфері кібербезпеки. Результатом реалізації завдань дослідження стала розробка рекомендованих рішень, що сприяють покращенню людського фактору у сфері кібербезпеки.

Не зважаючи на досить велику кількість публікацій, методики вирішення багатокритеріальних задач оптимізації є неприйнятними в тих випадках, коли якісні показники систем захисту інформації принципово не зводяться до кількісних (числових) величин і не можуть бути виміряні за існуючими шкалами.

Метою даної статті є запропонувати новий метод багатокритеріальної оптимізації для вирішення задачі синтезу системи захисту інформації для інформаційно-комунікаційної системи підприємства.

Виклад основного матеріалу

Кожному варіантові структури системи відповідає точка у багатовимірному просторі, координатами якої є значення показників функціонування (рис. 1) [10].

Існує теоретичний підхід згідно якого простір нормується в одиничний гіперкуб таким чином, що за кожним показником функціонування рух від 0 до 1 відповідає зміні параметра від найгіршого значення до найкращого. Тоді точка з координатами {1, 1, ..., 1} завжди відповідає гіпотетичному об’єкту, який має найкращі з можливих значень за всіма показниками. Відстані від цієї вершини гіперкуба до точки, яка відповідає положенню конкретного об’єкта, буде відповідати віддаленості об’єкта від найкращого значення та являє собою величину, обернену рейтингу рішення (вибір найкращого варіанта об’єкта). Однак на практиці часто мають місце нерівнозначності різних параметрів системи для визначення рейтингу рішення. Тому при обчисленні відстаней необхідно урахувати ваги, які відповідають значимості показників функціонування.

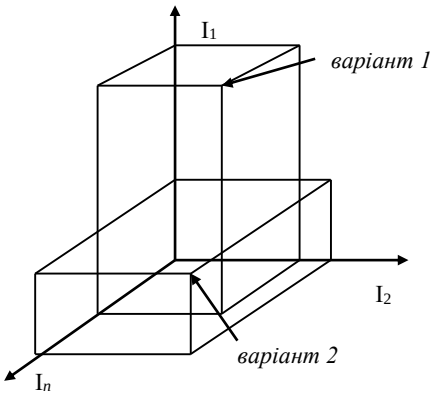

Рис. 1. Геометрична інтерпретація
множини варіантів системи

При виборі “архітектури” складної системи (I_1, I_2, ..., I_l) найбільш широко застосовуються наступні підходи [10].

А. Урахування одного чи декількох обмежень на відповідні показники функціонування

$$(I_1, I_2, ..., I_l): I_i > I_i^{зад}, \ i = \overline{1,l},$$

де $I_i^{зад}$, $i=\overline{1,l}$ – задані (граничні, допустимі) значення показників функціонування).

Б. Максимізація обраного показника

$$(I_1, I_2, ..., I_l): \max I_j.$$

В. Максимізація нормованої суми виважених показників

$$(I_1, I_2, ..., I_l): \max \sum_{i=1}^{l} \gamma_i I_i.$$

Г. Максимізація об’єму гіперкуба показників якості

$$(I_1, I_2, ..., I_l): \max \prod_{i=1}^{l} I_i.$$

Д. Максимізація площі багатокутника показників якості

$$(I_1, I_2, ..., I_l): \max S(I_1, I_2, ..., I_l),$$

де $S(I_1, I_2, ..., I_l)$ – площа багатокутника, побудованого у крузі одиничного радіуса.

Для побудови l-кутника необхідно круг одиничного радіуса поділити на l рівних частин. У полярній системі координат з центром O (центр круга) по осям I_j, $j=\overline{1,l}$ відкладаємо відповідні нормовані показники якості функціонування, а потім сполучаємо сусідні точки прямою лінією. У результаті отримуємо багатокутник, який відповідає одному варіанту багатокритеріального вибору (рис. 2).

Кожному можливому варіанту буде відповідати свій l-кутник. Перевага у запропонованому підході віддається варіантові з максимальною площею S_{max} l-кутника.

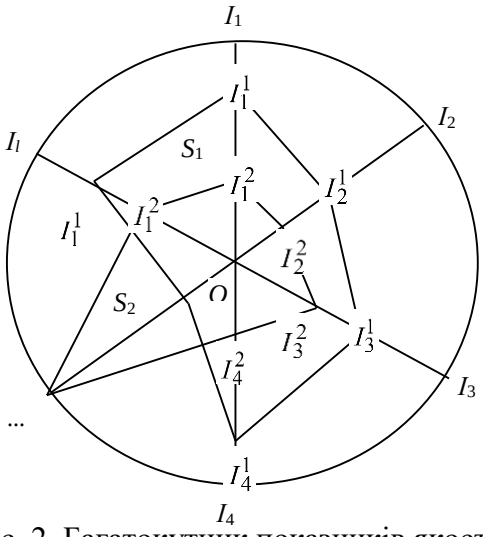

Рис. 2. Багатокутник показників якості

Підходи, що розглядаються проілюструємо на модельному прикладі вибору одного з чотирьох варіантів системи захисту інформації інформаційно-комунікаційної системи підприємства. Нормовані (приведені до 1, тобто визначені відносно своїх максимально можливих значень) показники функціонування системи наведені у таблиці.

Базуючись на множині критеріїв, наведених у [5] виберемо найкращий з варіантів системи з використанням розглянутих підходів А, Б, В, Г, Д (табл. 1).

Підхід А. Визначаємо варіант системи при $I_1^{зад}$=0,8. Встановленому обмеженню задовольняють одразу перший та третій варіанти. За даним критерієм варіанти рівнозначні. Однак можна рекомендувати варіант ІІ, у якого мінімальне значення одного з показників (0,6) більше мінімального значення показника (0,5) у четвертого варіанта.

Підхід Б. Виберемо варіант, при якому показник ефективності буде мати максимальне значення. Варіант II має значення показника 0,9 за трьома показниками і може вважатися переважаючим, оскільки всі інші варіанти мають меншу кількість максимальних значень показників.

Таблиця 1

Нормовані показники якості функціонування системи

Показники		Позначення показника	Варіант I	Варіант II	Варіант III	Варіант IV
Здатність системи протидіяти:	вторгненню зловмисника до системи	П1	0,9	0,6	0,8	0,5
	загрозам конфіденційності та/або цілісності інформації	П2	0,8	0,7	0,9	0,5
	загрозам доступності інформації	П3	0,8	0,6	0,8	0,7
	шкідливим програмним засобам	П4	0,6	0,8	0,5	0,8
	спробам зловмисника щодо вторгнення до системи	П5	0,9	0,7	0,3	0,9
	махінаціям	П6	0,6	0,9	0,2	0,8
	наявності відомих вразливостей	П7	0,7	0,8	0,4	0,6
	збору інформації зловмисником	П8	0,5	0,9	0,6	0,7
	зловмисній інформації	П9	0,3	0,8	0,8	0,5
Вартість системи		П10	0,2	0,9	0,7	0,3

Підхід В. У якості виважених коефіцієнтів обираємо (наприклад на основі методу експертних оцінок): γ_1=0,5; γ_2=0,3; γ_3=0,3; γ_4=0,2; γ_5=0,5; γ_6=0,4; γ_7=0,3; γ_8=0,2; γ_9=0,5; γ_{10}=0,8.

Обчислюємо для кожного варіанта адитивний показник функціонування

$$I_{\Sigma}^{I} = \sum_{i=1}^{10} \gamma_i I_i = 2{,}36;\ I_{\Sigma}^{II} = 3{,}1;\ I_{\Sigma}^{III} = 2{,}44;\ I_{\Sigma}^{IV} = 2{,}35.$$

У даному випадку найбільш ефективним є варіант II (I_{Σ}^{II}=3,1).

Підхід Г.

$$I_{\Pi}^{I} = \prod_{i=1}^{10} I_i = 0{,}00392;\ I_{\Pi}^{II} = 0{,}06584;\ I_{\Pi}^{III} = 0{,}00232;\ I_{\Pi}^{IV} = 0{,}00635.$$

У даному випадку також кращим є варіант II (I_{Π}^{II}=0,06584).

Підхід Д. Будуємо круг одиничного радіуса та ділимо його на 10 рівних частин (рис. 3). Відкладаємо по осям значення показників $П_1$, ... $П_{10}$, які відповідають кожному з чотирьох варіантів (табл. 1). Далі сполучаємо точки відповідних варіантів та отримуємо чотири багатокутника. Обчислюємо площі кожного багатокутника: S_{I}=1,1991; S_{II}=1,7428; S_{III}=0,1668; S_{IV}=1,2197.

При даному підході більш прийнятним є варіант II (S_{II} = 1,7428). Слід відзначити, що при усіх підходах варіант II виявляється кращим, що підтверджує можливість застосування різних підходів.

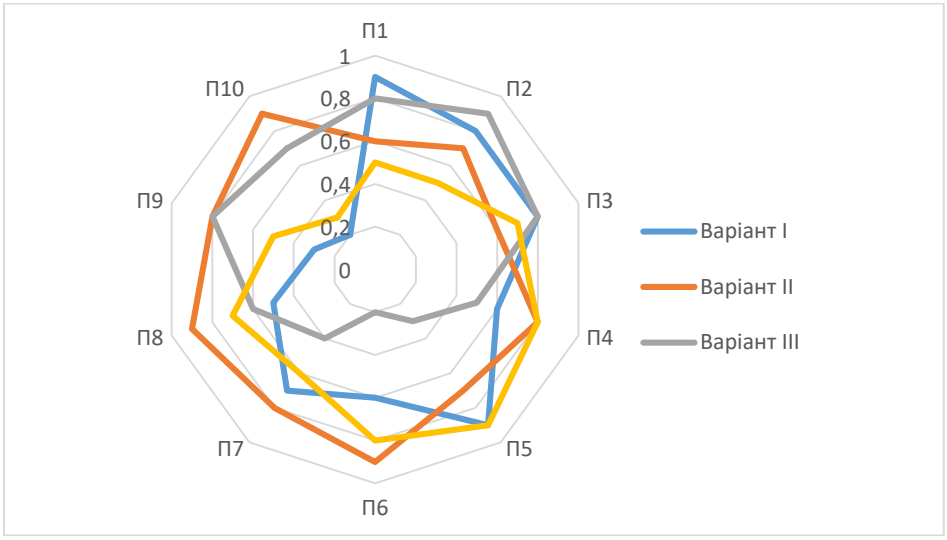

Рис. 3. Реалізація підходу Д до вибору оптимального варіанта системи захисту

Висновок

Таким чином, у статті запропоновано простий та досить наглядний метод вибору оптимального варіанта системи захисту інформації для інформаційно-комунікаційної системи підприємства з множини можливих. Цей метод дозволяє розв'язувати задачу безпосередньо по сукупності показників якості без згортання критеріїв у комплексний показник. Перспективами розвитку запропонованого методу є його удосконалення з метою реалізації можливості надання переваги окремим критеріям.

Перелік посилань

1. Sun, N. et al. Defining Security Requirements With the Common Criteria: Applications, Adoptions, and Challenges, in IEEE Access, vol. 10, pp. 44756-44777, 2022, doi: 10.1109/ACCESS.2022.3168716.

2. Хорошко, В., Шелест, М., Ткач, Ю. Багатокритеріальна оцінка ефективності проєктів із забезпечення кібербезпеки. Технічні науки та технології. 2020. № 1 (19). С. 114-123. DOI: 10.25140/2411-5363-2020-1(19)-114.

3. Гулак, Г. М., Лахно, В. А. Модель процесу інвестування в розвиток кібербезпеки для побудови системи підтримки прийняття рішень. Кібербезпека: освіта, наука, техніка, №2 (6), 2019. 154-163. DOI: 10.28925/2663-4023.2019.6.154163.

4. Hamza, A., Gharakheili, H. H., & Sivaraman, V. (2020). IoT Network Security: Requirements, Threats, and Countermeasures. ArXiv, abs/2008.09339.

5. Козубцов, І. М., Черноног, О. О., Козубцова, Л. М., Артемчук, М. В., Нещерет, І. Г. Вибір окремих показників оцінювання здатності функціонування системи захисту інформації і кібербезпеки інформації в інформаційно-комунікаційних системах спеціального зв'язку. Кібербезпека: освіта, наука, техніка, № 4 (16), 2022. 19-27. DOI 10.28925/2663-4023.2022.16.1927.

6. Cremer F, Sheehan B, Fortmann M, Kia AN, Mullins M, Murphy F, Materne S. Cyber risk and cybersecurity: a systematic review of data availability. Geneva Pap Risk Insur Issues Pract. 2022;47(3):698-736. doi: 10.1057/s41288-022-00266-6. Epub 2022 Feb 17. PMID: 35194352; PMCID: PMC8853293.

7. Borky, J. M., Bradley, T. H. Protecting Information with Cybersecurity. Effective Model-Based Systems Engineering. 2018 Sep 9:345–404. doi: 10.1007/978-3-319-95669-5_10. PMCID: PMC7122347.

8. Tariq, U.; Ahmed, I.; Bashir, A.K.; Shaukat, K. A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. Sensors 2023, 23, 4117. https://doi.org/10.3390/s23084117.

9. Szczepaniuk, E. K., Szczepaniuk, H. Analysis of cybersecurity competencies: Recommendations for telecommunications policy, Telecommunications Policy, Volume 46, Issue 3, 2022, 102282, ISSN 0308-5961, https://doi.org/10.1016/j.telpol.2021.102282.

10. Савченко, В. А., Машков, О. А., Кравченко, Ю. В., Власенко, Г. М. Метод багатокритеріального вибору оптимального варіанта системи радіонавігаційного забезпечення. Зб. наук. праць інституту проблем моделювання в енергетиці. Моделювання та інформаційні технології. – К.: ІПМЕ, 2003. – №22. – С.37–41.

Надійшла 30.01.2024