Methods of information systems protection

UDC 004.056:654.026 **doi:** https://doi.org/10.20998/2522-9052.2021.4.15

О. Ю. Юдін[1], В. М. Сидоренко[2], С. О. Гнатюк[1,2], О. С. Верховець[1]

[1] Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації, Київ, Україна
[2] Національний авіаційний університет, Київ, Україна

МОДЕЛЬ РОЗРАХУНКУ КІЛЬКІСНОГО КРИТЕРІЮ ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

Анотація. Предмет статті – методи та моделі оцінки критичності галузевих інформаційно-телекомунікаційних систем (ІТС). **Мета даної статті** – провести аналіз існуючих методів та моделей оцінки критичності та використовуючи його результати запропонувати функціональну модель розрахунку кількісного критерію оцінки захищеності ІТС. **Результати.** На основі відомого методу аналізу ієрархій запропоновано функціональну модель розрахунку кількісного критерію оцінки захищеності ІТС, яка за рахунок обробки експертних оцінок, дозволяє отримати кількісний показник захищеності ІТС. Це дає можливість спростити процедуру підбору експертів, уникнути специфіки обробки експертних даних, а також здійснити оцінювання ІТС в умовах обмежених обсягів статистики. **Висновки.** Проведене дослідження показало, що розроблена модель розрахунку кількісного критерію оцінки захищеності ІТС, використовуючи попарні порівняння, дозволяє експертам сконцентрувати увагу на проблемі. Крім того, запропонована модель має вбудований критерій якості роботи експерта та дає можливість перейти від якісної оцінки у вигляді упорядкованого ряду буквено-числових комбінацій, до кількісної оцінки у вигляді відношення базового профілю захищеності до профілю захищеності визначеного експертом.

Ключові слова: інформаційно-телекомунікаційні системи; критична інфраструктура; критерій оцінки захищеності; функціональний профіль захищеності.

Вступ

Світові тенденції до збільшення кількості та підвищення складності кібератак зумовили актуалізацію питання захисту галузевих ІТС, зокрема, галузевих, які є критично важливими для функціонування суспільства, соціально-економічного розвитку держави та забезпечення інформаційної складової національної безпеки.

З урахуванням потреб національної безпеки і необхідності запровадження системного підходу до розв'язання проблеми захисту критичної інфраструктури, на загальнодержавному рівні, створення системи захисту такої інфраструктури є одним із пріоритетів у реформуванні сектору оборони і безпеки України [1]. При цьому, основними проблемами, які потребують розв'язання, є: відсутність єдиних критеріїв та методології віднесення ІТС об'єктів інфраструктури до критичної інфраструктури; відсутність єдиної методології оцінювання загроз безпеці ІТС об'єктів критичної інфраструктури.

Необхідно зазначити, що Законом України «Про основні засади забезпечення кібербезпеки України» [2] визначено необхідність формування переліку об'єктів критичної інформаційної інфраструктури та необхідність розробки критеріїв і порядку віднесення об'єктів до об'єктів критичної інфраструктури, а Указом Президента України №96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [3] передбачено, що кіберзахист критичної інфраструктури має полягати, насамперед, у визначенні критеріїв віднесення інформаційних (автоматизованих), телекомунікаційних, інформаційно-телекомунікаційних систем до критичної інформаційної інфраструктури.

Таким чином, нормативно-правовими актами України задекларовано необхідність розробки єдиних критеріїв і методології віднесення ІТС об'єктів інфраструктури до критичної інфраструктури. При цьому доцільно зазначити, що використання якісних оцінок пов'язане зі складністю їх порівнювання та відтворювання. Насамперед, це обумовлено складністю підбору експертів і специфікою обробки експертних даних. Зазначені обмеження свідчать про наявність важливого наукового завдання щодо визначення критеріїв віднесення ІТС до критичної інформаційної інфраструктури.

Мета даної статті – провести аналіз існуючих методів та моделей оцінки критичності та використовуючи його результати запропонувати функціональну модель розрахунку кількісного критерію оцінки захищеності ІТС.

1. Аналіз існуючих досліджень

З метою вибору оптимального методу розрахунку кількісного критерію оцінки захищеності ІТС здійснимо аналіз існуючих методів прийняття рішень.

Методи теорії прийняття рішень застосовуються при відсутності повної інформації про об'єкт дослідження (ІТС). В загальному випадку методи прийняття рішень можна класифікувати по змісту та типу отримуваної експертної інформації [4-6]. Така класифікація наведена в табл. 1 [5].

З наведених чотирьох груп перші три відносяться до методів прийняття рішень в умовах визначеності і тільки четверта до методів прийняття рішень в умовах невизначеності.

Таблиця 1 – **Класифікація методів прийняття рішень по змісту та типу експертної інформації**

№ з/п	Зміст інформації	Тип інформації	Метод прийняття рішень
1	Експертна інформація не вимагається		1. Метод домінування 2. Метод на основі глобальних критеріїв
2	Інформація про перевагу на множині критеріїв	1. Якісна інформація 2. Кількісна оцінка переваги критеріїв 3. Кількісна інформації про заміщення	1. Лексикографічне упорядкування 2. Порівняння різниць критеріальних оцінок 3. Методи згортки на ієрархії критеріїв 4. Методи «ефективність-вартість» 5. Методи «порогів» 6. Методи ідеальної точки 7. Методи кривих байдужості 8. Методи теорії цінності
3	Інформація про перевагу альтернатів	Оцінка переваги парних порівнянь	1. Методи математичного програмування 2. Лінійна та нелінійна згортки при інтерактивному способі визначення її параметрів
4	Інформація про переваги на множині критеріїв та про наслідки альтернатив	1. Відсутність інформації про переваги 2. Кількісна інформація про наслідки 3. Якісна інформація про переваги та кількісна про наслідки	1. Методи з дискретизацією невизначеності 2. Стохастичне домінування 3. Методи прийняття рішень в умовах ризику та невизначеності на основі глобальних критеріїв 3. Метод аналізу ієрархій 4. Метод вирішальних матриць 5. Методи теорії нечітких множин 6. Метод практичного прийняття рішень 4. Методи кривих байдужості для прийняття рішень в умовах ризику та невизначеності 7. Методи дерев рішень 8. Декомпозиційні методи теорії очікуваної корисності

З четвертої групи найбільш перспективними [5] є такі методи: теорії очікуваної корисності; аналізу ієрархій; теорії нечітких множин.

Методи теорії очікуваної корисності полягають в тому, що кожна можлива дія, породжує наслідки, які характеризуються визначеним набором властивостей, факторів або показників. Обирається та альтернатива, наслідки якої є найбільш кращими. Таким чином, при застосуванні цього методу необхідно отримати кількісні оцінки всіх можливих результатів, які є наслідками процесів прийняття рішень та в подальшому, на підставі цих оцінок, обрати найкращій результат. В загальному випадку метод складається з п'яти етапів [6]:

1. Попередній аналіз. На цьому етапі визначаються можливі варіанти дій, які можливо виконати в процесі рішення.

2. Структурний аналіз. Структуризація проблеми на якісному рівні. Будується дерево рішень. Дерево рішень має два типи вершин: вершини – рішення та вершини – випадки. В вершинах-рішеннях вибір залежить від експерта, а в вершинах-випадках експерт може передбачати вибір з деякою ймовірністю.

3. Аналіз невизначеностей. На цьому етапі приймається рішення встановлення значень ймовірності для тих гілок на дереві рішень, які починаються з вершини-випадку. При цьому всі отримані значення ймовірностей підлягають перевірці на наявність узгодженості.

4. Аналіз корисності. На цьому етапі необхідно отримати кількісні оцінки корисностей наслідків результатів пов'язаних з реалізацією того чи іншого шляху на дереві рішень.

5. Процедури оптимізації. Оптимальна стратегія дій може бути найдена за допомогою розрахунків максимізації очікуваної корисності на всьому просторі можливих результатів.

Перевагою методу є можливість находження оптимального рішення в умовах ризику.

В той же час необхідно зазначати, що методи теорії очікуваної корисності мають недоліки, а саме:

- велика трудомісткість пов'язана зі збором інформації про переваги та ймовірнісні розподіли, що відносяться до наслідків [7];
- необхідність залучення аналітиків;
- відсутність механізмів перевірки суджень експертів (осіб приймаючих рішення).

Також, до недоліків згідно [8, 9] необхідно віднести те, що:

- людина не структурує проблеми холістично, як це передбачає теорія очікуваної корисності;
- людина не обробляє інформацію, особливо ймовірності, у відповідності до принципів очікуваної корисності;
- теорія очікуваної корисності погано передбачає поведінку людей, коли їх ставлять перед вибором в ході лабораторних випробувань.

Метод аналізу ієрархій (MAI) є математичним інструментом системного підходу до складних проблем прийняття рішень та реалізує процедуру синтезу пріоритетів, що обраховуються на підставі суб'єктивних суджень експертів. MAI дозволяє експерту знайти такий варіант рішення завдання (альтернативу), який найкращим чином узгоджується з його розумінням суті проблеми та вимогами до її рішення. В загальному випадку MAI складається з п'яти етапів [10]:

1) побудова якісної моделі проблеми , що включає мету, альтернативні варіанти досягнення мети та критерії для оцінки якості альтернатив. Модель викладається у вигляді ієрархії;

2) визначення пріоритетів всіх елементів ієрархії з використанням методу парних порівнянь. Формується матриця попарних порівнянь;

3) синтез глобальних пріоритетів альтернатив та отримання вектору пріоритетів;

4) перевірка суджень експертів на узгодженість шляхом оцінки ступеню узгодженості матриці попарних порівнянь;

5) отримання значення найкращої альтернативи та прийняття рішення.

Перевагами методу є [11]:

- використання попарних порівнянь, що дозволяє експерту сконцентрувати увагу на проблемі;
- додатковість вихідної матриці;
- наявність вербально-числової шкали;
- вбудований критерій якості роботи експерта – індексу узгодженості, який надає інформацію про порушення чисельної та транзитивної узгодженості суджень.

Слід зазначити, що МАІ не позбавлений недоліків [12-14], а саме:

- оцінки та порівняння більше дев'яти [13] або десяти [14] об'єктів (критеріїв, альтернатив). Зі збільшенням кількості об'єктів збільшується складність побудувати однорідної матриці попарних порівнянь. Також, обмеження викликані психологічними можливостями людини щодо порівняння та ранжирування великої кількості об'єктів;
- виникнення явища реверсу рангів, тобто зміни порядку раніше порівняних альтернатив при додаванні нових чи видалені існуючих;
- використання шкали відношень яка є ранговою шкалою кратною одиниці.

Методи теорії нечітких множин полягають у формалізації вхідних параметрів у вигляді вектору інтервальних значень (нечіткого інтервалу), а попадання в кожен інтервал характеризується деяким ступенем невизначеності. Межі можливих значень параметрів та області їх найбільш можливих значень визначаються на основі вихідних даних, досвіду та інтуїції. Таким чином основною характеристикою того чи іншого методу є функція приналежності параметру інтервалу [15]. Існує багато методів визначення функцій приналежності, наприклад - методи парних порівнянь, експертних оцінок, лінгвістичних термів з використанням статистичних даних, параметричні, інтервальної оцінки [16].

Можна виділити дві групи методів: прямі та непрямі [17]. Прямі методи полягають у тому, що безпосередньо експерт задає правила визначення функції приналежності, наприклад – методи засновані на ймовірнісній трактовці функції приналежності. Непрямі методи, полягають у тому, що значення функції приналежності обираються таким чином, щоб задовольнити заздалегідь сформульованим вимогам, наприклад – метод найбільших квадратів.

Перевагами методів нечітких множин є [18-21]:

- можливість достатньо об'єктивно проводити оцінку альтернатив за окремими критеріями;
- можливість включати в аналіз якісні змінні, оперувати нечіткими вхідними даними та лінгвістичними критеріями.

В той же час зазначені методи мають і недоліки, а саме [17; 22-23]:

- існує суб'єктивність в виборі функцій приналежності та формуванні правил нечіткого вводу і тому вид функції суттєво залежить від наявних відомостей та характеру задачі;
- необхідність представлення інформації про взаємозв'язок критеріїв;
- кожен метод має свої обмеження та особливості і користувач повинний знати сферу застосування кожного з методів;
- більшість методів нечітких множин показує слабку стійкість результатів відносно вихідних даних.

Найбільшу стійкість мають методи основані на правилах.

З урахуванням зазначеного вбачається за доцільне для розрахунку кількісного критерію оцінки захищеності застосувати метод аналізу ієрархій.

2. Основна частина дослідження

Модель розрахунку кількісного критерію оцінювання захищеності. Модель розрахунку кількісного критерію оцінки захищеності ІТС з використанням методу аналізу ієрархій дозволяє перейти від якісної оцінки у вигляді упорядкованого ряду буквено-числових комбінацій [24], що позначають рівні реалізованих послуг, до кількісної оцінки у вигляді відношення базового профілю захищеності до профілю захищеності визначеного експертом.

Вхідними даними для моделі є базовий ФПЗ [25] та відкоригований експертом ФПЗ. При цьому, НД ТЗІ 2.5-005-99, що визначає стандартні ФПЗ оброблюваної інформації від НСД, оперує вимогами щодо захисту певної інформації від певних загроз і відомих на сьогоднішній день функціональних послуг, що дозволяють протистояти даним загрозам і забезпечувати виконання вимог, які пред'являються. Враховуючи обмеження методу аналізу ієрархій щодо оцінки та порівняння не більше дев'яти або десяти критеріїв сформуємо групи критеріїв оцінки захищеності інформації (рис. 1). Як видно з рис. 1 найбільша група критеріїв другого рівня, критерії спостережності, може налічувати до 9 критеріїв. Інші групи, критеріїв всіх інших рівнів, налічують від чотирьох до п'яти критеріїв. Таким чином, для аналізу визначених критеріїв можна застосовувати метод аналізу ієрархій.

Блок-схема моделі розрахунку кількісного критерію оцінки захищеності ІТС на основі методу аналізу ієрархій наведена на рис. 2. Метод аналізу ієрархій для визначення співвідношення альтернатив (ФПЗБ та ФПЗЕ) відбувається в такій послідовності:

1. ***Будуються матриці попарних порівнянь для кожного рівня критеріїв*** (критерії захищеності – 1 рівень, критерії послуг безпеки – 2 рівень, критерії рівнів послуг безпеки – 3 рівень):

$$A = \left\| a_{ij} \right\|_{nxn}, \qquad (1)$$

де $a_{ij} = w_i / w_j$, w_i – «вага» i-го критерію, При цьому, $a_{ji} = 1/a_{ij}$, а $a_{ii} = 1$. Тобто, матриця є позитивною зворотно симетричною.

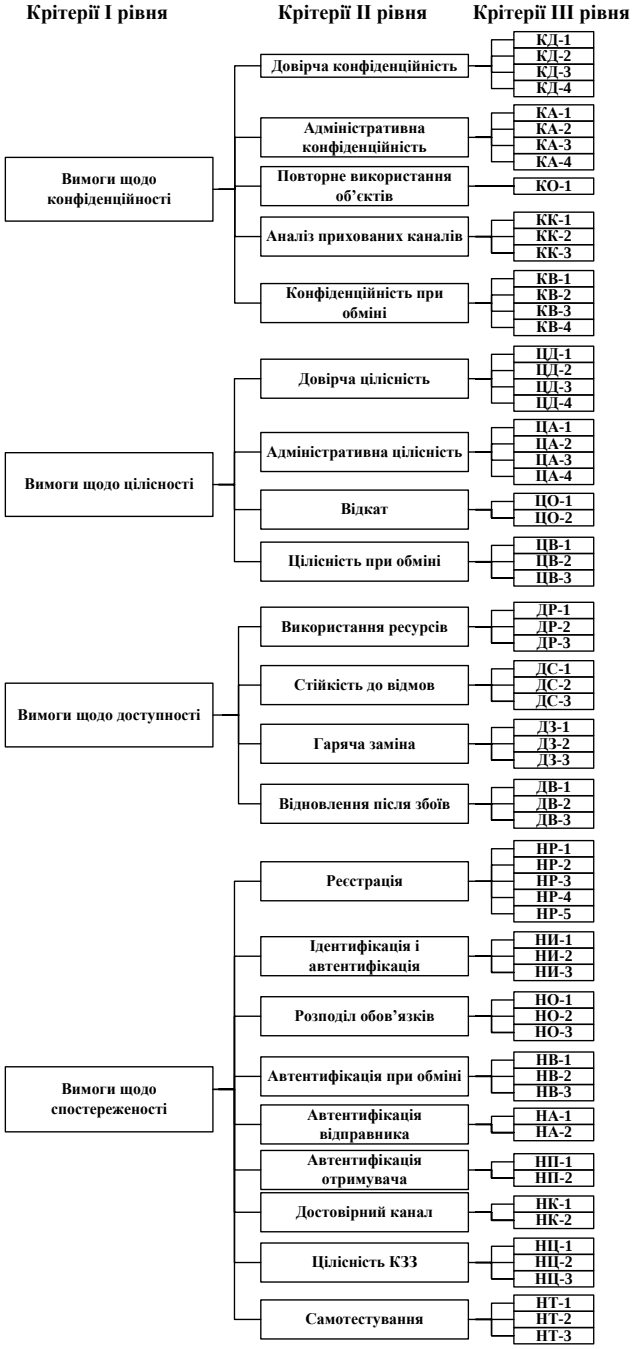

Рис. 1. Групи критеріїв оцінки захищеності інформації

Для визначення ваги будемо використовувати табл. 2 відносної важливості: Для критеріїв захищеності матриця порівнянь буде мати вигляд, наведений у табл. 3: Для критеріїв послуг безпеки складаються свої матриці попарних порівнянь. Всього до 4 матриць. Для критеріїв рівнів безпеки максимальна кількість матриць може скласти 22.

2. ***Здійснюється обчислення множини власних векторів матриці***, для чого для кожної строки матриці обчислюється середнє геометричне:

$$a_i = \sqrt[n]{a_{i1} \cdot a_{i2} \cdot a_{i3} \cdot a_{in}} = \sqrt[n]{\prod_{j=1}^{n} a_{ij}}, \qquad (2)$$

де n – розмірність матриці.

3. З***дійснюється нормалізація результатів***, результатом якої є нормалізований вектор пріоритетів:

$$\overline{a_i} = \frac{a_i}{\sum_{j=1}^{n} a_j}, \qquad (3)$$

4. ***Здійснюється перевірка узгодженості локальних пріоритетів***: Розрахунок найбільшого власного значення матриці здіснюється таким чином:

$$A_i = \sum_{i=1}^{n} a_{ij}, \qquad (4)$$

$$A_i' = A_i \overline{a_{ij}}, \qquad (5)$$

$$\lambda_{\max} = \sum_{i=1}^{n} A_i', \qquad (6)$$

Розрахунок індексу узгодженості:

$$J_p = \frac{\lambda_{\max} - m}{m-1}, \qquad (7)$$

де m – кількість елементів що порівнюються (розмір матриці).

Перевірка коректності індексу узгодженості здійснюється шляхом розрахунку відношення узгодженості АС за формулою:

$$A_c = \frac{J_p}{R_c}, \qquad (8)$$

де R_c – табличне значення (табл. 4).

У разі, якщо $A_c \geq 0{,}10$, то дані в матриці порівнянь підлягають перегляду та уточненню.

Таблиця 2 – **Шкала відносної важливості критеріїв**

Вербальна оцінка експерта	**Значення a_{ij}**
w_i абсолютно кращій за w_j	9
w_i набагато кращий за w_j	8
w_i значно кращий за w_j	7
w_i кращий за w_j	6
w_i суттєво переважає w_j	5
w_i переважає w_j	4
w_i дещо переважає w_j	3
w_i несуттєво переважає w_j	2
критерії рівноцінні	1
w_j несуттєво переважає w_i	1/2
w_j дещо переважає w_i	1/3
w_j переважає w_i	1/4
w_j суттєво переважає w_i	1/5
w_j кращій за w_i	1/6
w_j значно кращий за w_i	1/7
w_j набагато кращий за w_i	1/8
w_j абсолютно кращий за w_i	1/9

Таблиця 3 – **Матриця порівнянь для критеріїв захищеності**

	Конфіденційність	**Цілісність**	**Доступність**	**Спостереженість**
Конфіденційність	a_{11}	a_{12}	a_{13}	a_{14}
Цілісність	a_{21}	a_{22}	a_{23}	a_{24}
Доступність	a_{31}	a_{32}	a_{33}	a_{34}
Спостережність	a_{41}	a_{42}	a_{43}	a_{44}

Таблиця 4 – **Випадкові узгодженості для матриць порядку 2-9**

Розмір матриці (n)	2	3	4	5	6	7	8	9
Випадкова узгодженість (R_C)	0	0,58	0,9	1,12	1,24	1,32	1,41	1,45

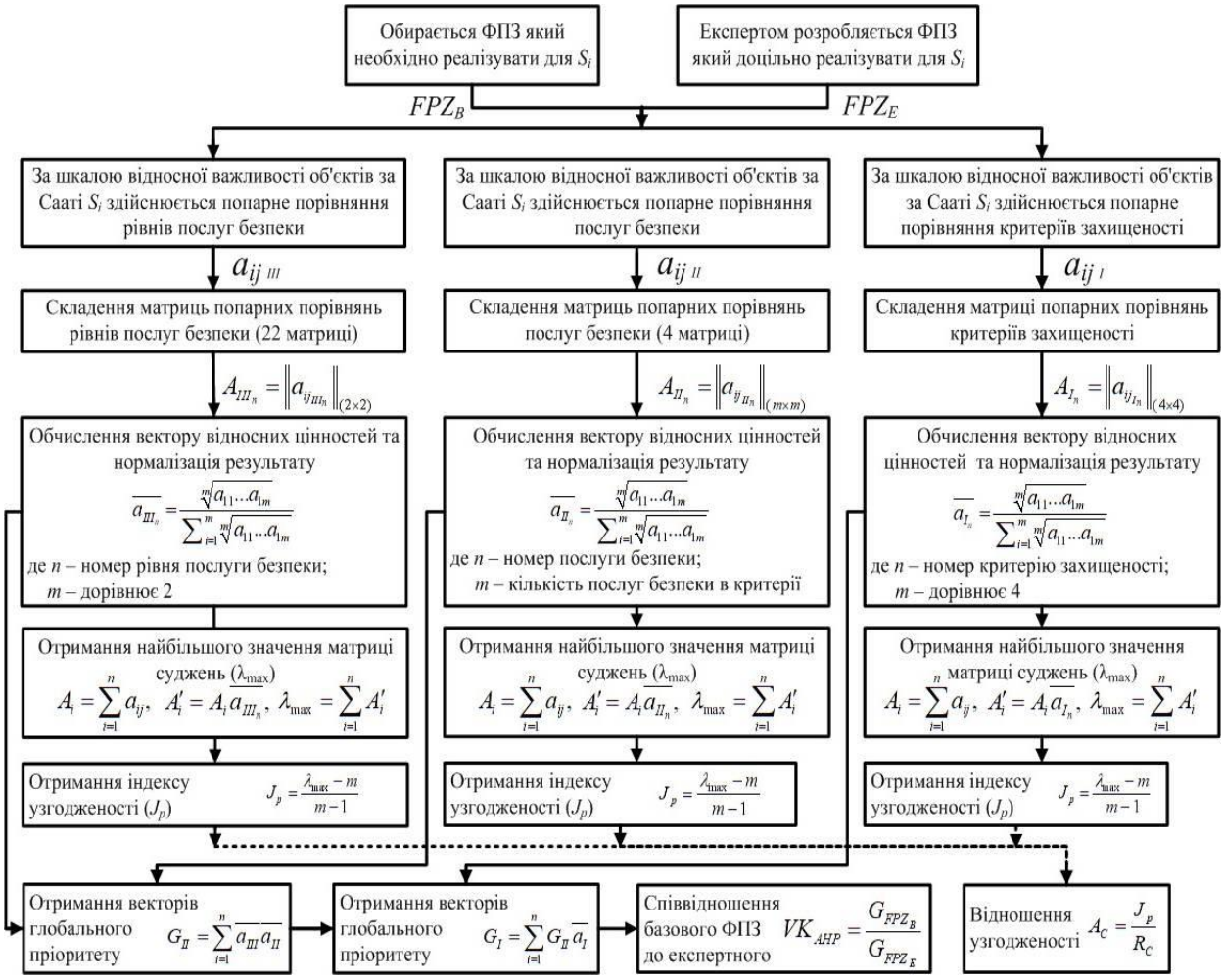

Рис. 2. Блок-схема методу розрахунку кількісного критерію оцінки захищеності ІТС

5. ***Розрахунок глобального пріоритету для критеріїв верхнього рівня***. Нормалізований вектор пріоритетів за кожним критерієм нижчого рівня перемножується на нормалізований вектор пріоритетів вищого рівня.

6. Добутки підсумовуються на вищому рівні.

$$G_i = \sum_{i=1}^{n} \overline{a_i}\,\overline{b_i}, \qquad (9)$$

де n – кількість критеріїв рівнів безпеки.

7. ***Визначення співвідношення альтернатив*** (ФПЗБ та ФПЗЕ).

Для кожного ФПЗ розраховується глобальний пріоритет за категоріями конфіденційності, цілісності, доступності та спостережності. Відношення цих глобальних пріоритетів, що характеризують кількісний критерій, можна представити у вигляді виразу:

$$VK_{AHP} = \frac{G_{FPZ_B}}{G_{FPZ_E}}, \qquad (10)$$

де G_{FPZ_B} – є табличним значенням ФПЗ для галузевої ІТС, а G_{FPZ_E} – є ФПЗ отриманий експертом за допомогою структурно-логічної моделі та структурно-функціонального методу формування ФПЗ галузевої ІТС.

Реалізація цієї моделі дозволяє перейти від якісних показників захищеності до кількісних.

Висновки

У представленій роботі, з метою вибору оптимального способу розрахунку кількісного критерію оцінювання захищеності ІТС, було проведено аналіз існуючих методів прийняття рішень.

Досліджені методи теорії очікуваної корисності, методи аналізу ієрархій та методи теорії нечітких множин.

Визначено, що з урахуванням основних переваг та недоліків зазначених методів, для розрахунку кількісного критерію оцінювання захищеності доцільним вбачається використання методу аналізу ієрархій.

Розроблено модель розрахунку кількісного критерію оцінювання захищеності ІТС, що базується на використанні методу аналізу ієрархій. Зазначена модель використовує попарні порівняння, що в свою чергу дозволяє експерту сконцентрувати увагу на проблемі.

Також, зазначена модель має вбудований критерій якості роботи експерта – індекс узгодженості, який надає інформацію про порушення чисельної та транзитивної узгодженості суджень.

Крім того, розроблена модель дозволяє перейти від якісної оцінки у вигляді упорядкованого ряду буквено-числових комбінацій, що позначають рівні реалізованих послуг, до кількісної оцінки у вигляді відношення базового профілю захищеності до профілю захищеності визначеного експертом.

У подальших роботах планується провести експериментальне дослідження розробленої моделі розрахунку кількісного критерію оцінювання захищеності ІТС.

Список літератури

1. С.О. Гнатюк, О.Ю. Юдін, В.М. Сидоренко, Я.П. Євченко «Метод формування функціонального профілю захищеності галузевих інформаційно-телекомунікаційних систем», Кібербезпека: освіта, наука, техніка. – 2021. – Т. 3. – № 11. – С. 166-182.
2. Україна. Закони. «Про основні засади забезпечення кібербезпеки України» : офіц. текст : [прийнятий Верховною Радою 5 жовтня 2017 р.]. К.: Відомості Верховної Ради України, 2017, № 45, ст.403.
3. Указ Президента України №96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України».
4. Козлов В.Н. Системный анализ, оптимизация и принятие решений: учебное пособие. – М: Проспект, 2012. – 176 с.
5. Сарапулова Т.В., Раевская Е.А., Пимонов А.Г. Многокритериальный выбор альтернатив на основе метода анализа иерархий: методические указания к лабораторной работе по дисциплине «Математические и инструментальные методы поддержки принятия решений» для магистрантов направления подготовки 09.04.03 «Прикладная информатика». – Кемерово: УИП КузГТУ, 2016. – 30 с.
6. Андрейчиков А.В., Андрейчикова О.Н. Анализ, синтез, планирование решений в экономике. – М.: Финансы и статистика, 2002. – 368 с.
7. Кини Р. Л., Райфа Х. Принятие решений при многих критериях: предпочтения и замещения: Пер. с англ./ Под ред. И. Р. Шахова. - М.: Радио и связь, 1981. – 560 с.
8. Paul J.H. Schoemaker. The Expected Utility Model: Its Variants, Purposes, Evidence and Limitations // Journal of Economic Literature, June 1982, v.XX, no.2, p.529-563.
9. Райфа Г. Анализ решений. Введение в проблему выбора в условиях неопределенности: Пер. с англ. – М.: Наука, 1977. – 408 с.
10. Саати Т. Принятие решений. Метод анализа иерархий: Пер. с англ./ Под ред. Р. Г. Вачнадзе. – М.: Радио и связь, 1993. – 278 с.
11. Тутыгин А.Г. Преимущества и недостатки метода анализа иерархий / Тутыгин А.Г., Коробов В.Б. // Известия Российского государственного педагогического университета имени А.И.Герцена. – СПб., 2010. – №122. – С.108-115.
12. Коробов В. Б. Некоторые проблемы применения экспертных методов на практике / В. Б. Коробов // Научный диалог. –Екатеринбург. – 2013. – № 3(15).– С. 94–108.
13. Миронова Н.А. Интеграция модификаций метода анализа иерархии для Систем поддержки принятия групповых решений / Н.А. Миронова // Радіоелектроніка, інформатика, управління. – Запоріжжя. – 2011. – № 2. – С. 47-54.
14. Емельянов С. В., Ларичев О. И. Многокритериальные методы принятия решений. – М.: Знание, 1985. 32 с.
15. Кофман А. Введение в теорию нечетких множеств: Пер. с англ. – М.: Радио и связь, 1982. – 432 с.
16. Борисов А. Н., Крумберг О. А., Федоров И. П. Принятие решений на основе нечетких моделей. – Рига: Зинатне, 1990. – 184 с.
17. А. Е. Кононюк. Дискретно-непрерывная математика. (Множества (нечеткие). – К.: Освіта України. 2012., – 452 с.
18. Нечеткие множества и теория возможностей. Последние достижения: Пер. с англ./ Под ред. Р. Р. Ягера – М.: Радио и связь, 1986. – 408 с.
19. Беллман Р., Заде Л. Принятие решений ів расплывчатых условиях // Вопросы анализа и процедуры принятия решений: Пер. с англ. – М.: Мир, 1976. – С. 172-175.
20. Орловский С. А. Проблемы принятия решений при нечеткой исходной информации. – М.: Наука, 1981. – 208 с.
21. Заде Л. Понятие лингвистической переменной и его применение к принятию приближенных решений: Пер. с англ. – М.: Мир, 1976. – 165 с.
22. Екологічна безпека №2/2013 (16) Структурные приоритеты экспертной системы экологического мониторинга В.П. Дмитриков, В.С. Бахарєв.
23. Еремин Н.А. Моделирование месторождений углеводородов Е 70 методами нечеткой логики. – М.: Наука, 1994. – 462 с.
24. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу // ДСТСЗІ СБ України. – 1999.

25. Юдін О.Ю. Аналіз вимог до елементів інформаційно-телекомунікаційних систем управління енергетичною інфраструктурою, які забезпечують кіберзахист / О.Ю.Юдін, С.Є. Гнатюк // Перспективні напрями захисту інформації. Третя всеукраїнська наук.-практ. конф., 02-06 вересня 2017 р.: тези доп. – Одеса: ОНАЗ, 2017.

Received (Надійшла) 19.10.2021
Accepted for publication (Прийнята до друку) 17.11.2021

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Юдін Олексій Юрійович – кандидат технічних наук, заступник начальника Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації, Київ, Україна;
Oleksii Yudin, PhD, Vice-Chief of the State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, Kyiv, Ukraine;
e-mail: alex@ukrdeftech.com.ua; ORCID ID: http://orcid.org/0000-0002-5710-0889

Сидоренко Вікторія Миколаївна – кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій, Національний авіаційний університет, Київ, Україна;
Viktoriia Sydorenko, PhD, Associate Professor, Associate Professor IT-Security Academic Department, National Aviation University, Kyiv, Ukraine;
e-mail: v.sydorenko@ukr.net; ORCID ID: http://orcid.org/0000-0002-5910-0837

Гнатюк Сергій Олександрович – доктор технічних наук, професор, заступник декана з наукової роботи Факультету кібербезпеки, комп'ютерної та програмної інженерії, Національний авіаційний університет, Київ, Україна;
Sergiy Gnatyuk, DSc, Professor, Vice-Dean for Research of the Faculty of Cybersecurity, Computer and Software Engineering, National Aviation University, Kyiv, Ukraine;
e-mail: s.gnatyuk@nau.edu.ua ; ORCID ID: http://orcid.org/0000-0003-4992-0564

Верховець Олексій Сергійович – заступник начальника науково-дослідного центру Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації, Київ, Україна;
Oleksii Verkhovets, Vice-Chief of the Research Center of the State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, Kyiv, Ukraine;
e-mail: o.s.verhts@gmail.com; ORCID ID: http://orcid.org/0000-0002-3897-106X

Модель расчета количественного критерия оценки защищенности информационно-телекоммуникационных систем критической инфраструктуры государства

А. Ю. Юдин, В. Н. Сидоренко, С. А. Гнатюк, А. С. Верховец

Аннотация. Предмет статьи – методы и модели оценки критичности отраслевых информационно-телекоммуникационных систем (ИТС). **Цель данной статьи** – провести анализ существующих методов и моделей оценки критичности и используя его результаты, предложить функциональную модель расчета количественного критерия оценки защищенности ИТС. **Результаты.** На основе известного метода анализа иерархий предложена функциональная модель расчета количественного критерия оценки защищенности ИТС, которая за счет обработки экспертных оценок позволяет получить количественный показатель защищенности ИТС. Это дает возможность упростить процедуру подбора экспертов, избежать специфики обработки экспертных данных, а также осуществить оценку ИТС в условиях ограниченных объемов статистики. **Выводы.** Проведенное исследование показало, что разработанная модель расчета количественного критерия оценки защищенности ИТС, используя попарность сравнений, позволяет экспертам сконцентрировать внимание на проблеме. Кроме того, предложенная модель имеет встроенный критерий качества работы эксперта и позволяет перейти от качественной оценки в виде упорядоченного ряда буквенно-числовых комбинаций, к количественной оценке в виде отношения базового профиля защищенности к профилю защищенности определенного экспертом.

Ключевые слова: информационно-телекоммуникационные системы; критическая инфраструктура; критерий оценки защищенности; функциональный профиль защищенности.

Model of the quantitative criterion calculation for security assessment of the information and telecommunications systems in the critical infrastructure of the state

Oleksii Yudin, Viktoriia Sydorenko, Sergiy Gnatyuk, Oleksii Verkhovets

Abstract. The subject of the article is methods and models for assessing the criticality of industry information and telecommunications systems (ITS). **The purpose of this article** is to analyze the existing methods and models of criticality assessment and use its results to propose a functional model for calculating the quantitative criterion for assessing the security of ITS. **Results.** Based on the known method of hierarchy analysis, a functional model for calculating the quantitative criterion for assessing ITS security is proposed, which, through the processing of expert assessments, allows to obtain a quantitative indicator of ITS security. This makes it possible to simplify the procedure for selecting experts, to avoid the specifics of processing expert data, as well as to assess ITS in a limited amount of statistics. **Conclusions.** The study showed that the developed model for calculating the quantitative criterion for assessing the security of ITS, using pairwise comparisons, allows experts to focus on the problem. In addition, the proposed model has a built-in quality criterion of the expert and allows to move from a qualitative assessment in the form of an ordered series of alphanumeric combinations, to a quantitative assessment in the form of the ratio of the basic security profile to the security profile defined by the expert.

Keywords: information and telecommunication systems; critical infrastructure; security assessment criterion; functional security profile.