КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (16), 2022
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2022.16.618
УДК 004.056:654.026

Гнатюк Сергій Олександрович
д.т.н., професор, заступник декана факультету кібербезпеки, комп'ютерної та програмної інженерії
Національний авіаційний університет, Київ, Україна
ORCID ID: 0000-0003-4992-0564
s.gnatyuk@nau.edu.ua,

Юдін Олексій Юрійович
к.т.н., заступник начальника
Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації, Київ, Україна
ORCID ID: 0000-0002-4730-1463
alex@ukrdeftech.com.ua,

Сидоренко Вікторія Миколаївна
к.т.н., доцент, доцент кафедри безпеки інформаційних технологій
Національний авіаційний університет, Київ, Україна
ORCID ID: 0000-0002-5910-0837
v.sydorenko@ukr.net,

Смірнова Тетяна Віталіївна
к.т.н., доцент, доцент кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет, Кропивницький, Україна
ORCID ID: 0000-0001-5093-1581
sm.tetyana@gmail.com

Жаксигулова Даурія Дарибаївна
докторант PhD
Східноказахстанський технічний університет ім. Д. Серікбаєва, Усть-Каменогорськ, Казахстан
ORCID: 0000-0003-0646-2823
dauriya.dzh@gmail.com

ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ МОДЕЛІ РОЗРАХУНКУ КІЛЬКІСНОГО КРИТЕРІЮ ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

Анотація. Світові тенденції до збільшення кількості та підвищення складності кібератак зумовили актуалізацію питання захисту інформаційно-телекомунікаційних систем (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. Таким чином, виникає необхідність розробки методів та моделей віднесення ІТС до критичної інфраструктури для забезпечення національної безпеки України. У роботі досліджено модель розрахунку кількісного критерію оцінювання захищеності ІТС на основі методу аналізу ієрархій, що дозволило за рахунок обробки експертних оцінок отримати кількісний показник захищеності ІТС. Це дало можливість спростити процедуру підбору експертів, уникнути специфіки обробки експертних даних, а також здійснити оцінювання ІТС в умовах обмежених обсягів статистики. Розроблена модель дозволяє перейти від якісного оцінювання у вигляді упорядкованого ряду буквено-числових комбінацій, що позначають рівні реалізованих послуг, до кількісного оцінювання у вигляді відношення функціональних профілів захищеності. Крім того, розроблено спеціалізоване програмне забезпечення, яке реалізує досліджувану модель, що дозволило провести експериментальне дослідження і верифікацію зазначеної моделі на прикладі ІТС Національної

© С.О. Гнатюк, О.Ю. Юдін, В.М. Сидоренко, Т.В. Смірнова, Д. Д. Жаксигулова 2022

системи конфіденційного зв'язку. У подальших дослідженнях авторами планується дослідити модель розрахунку кількісного критерію оцінювання захищеності ІТС в інших галузях критичної інфраструктури (енергетики, транспорту тощо).

Ключові слова: інформаційно-телекомунікаційна система, критична інфраструктура, об'єкт критичної інфраструктури, кібербезпека, критерій оцінювання захищеності, функціональний профіль захищеності.

ВСТУП

Світові тенденції до збільшення кількості та підвищення складності кібератак зумовили актуалізацію питання захисту галузевих інформаційно-телекомунікаційних систем (ІТС), зокрема, таких, які є критично важливими для функціонування суспільства, соціально-економічного розвитку держави та забезпечення інформаційної складової національної безпеки [1]. 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 будь-якої держави (зокрема й України [2]). При цьому, основними проблемами, які потребують вирішення, 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 тощо. Необхідно зазначити, що Законом України «Про основні засади забезпечення кібербезпеки України» [3] визначено необхідність формування переліку об'єктів критичної інформаційної інфраструктури та необхідність розробки критеріїв і порядку віднесення об'єктів до об'єктів критичної інфраструктури, а відповідним Указом Президента України [4] передбачено, що кіберзахист критичної інфраструктури має полягати, насамперед, у визначенні критеріїв віднесення інформаційних (автоматизованих), телекомунікаційних, ІТС до критичної інформаційної інфраструктури. Крім того, наприкінці 2021 року було прийнято базовий у цій галузі закон [5] (ведення в дію якого відбудеться 15 червня 2022 року), що визначає правові та організаційні засади створення та функціювання національної системи захисту критичної інфраструктури.

Таким чином, зазначеними нормативно-правовими актами України задекларовано необхідність розробки єдиних критеріїв і методології віднесення ІТС об'єктів інфраструктури до критичної інфраструктури держави. При цьому доцільно зазначити, що використання якісних (замість кількісних) 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.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

З метою вибору оптимального методу розрахунку кількісного критерію оцінювання захищеності ІТС у роботі [2] було здійснено аналіз існуючих методів прийняття рішень. Визначено, що в загальному випадку методи прийняття рішень можна класифікувати за змістом та типом отримуваної експертної інформації [6-8]. Крім того досліджені методи відносяться до методів прийняття рішень в умовах визначеності та в умовах

ISSN 2663 - 4023

невизначеності (нечіткості). Відповідно до [2], найбільш перспективними на думку авторів, є наступні методи:

1. Методи теорії очікуваної корисності полягають в тому, що кожна можлива дія, породжує наслідки, які характеризуються визначеним набором властивостей, чинників 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 найкращий результат [2, 8].

2. Метод аналізу ієрархій є математичним інструментом системного підходу до складних проблем прийняття рішень та реалізує процедуру синтезу пріоритетів, що обраховуються на підставі суб'єктивних суджень експертів. Метод аналізу ієрархій дозволяє експерту знайти такий варіант рішення завдання, який найкращим чином узгоджується з його розумінням суті проблеми та вимогами до її рішення.

3. 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 [9]. Існує багато сучасних методів визначення функцій приналежності, наприклад – методи попарних порівнянь, експертних оцінок, лінгвістичних термів з використанням статистичних даних, параметричні, інтервальної оцінки тощо [10].

Проведений у роботі аналіз показав, що найбільшу ефективність мають методи основані на правилах. З урахуванням переваг та недоліків зазначених методів, було вирішено для розрахунку кількісного критерію оцінки захищеності застосувати метод аналізу ієрархій. Крім того, у зазначеній роботі [2] авторами було запропоновано модель розрахунку кількісного критерію оцінювання захищеності ІТС критичної інфраструктури держави. Проте, у цій роботі наведено лише теоретичне обґрунтування зазначеної моделі без експериментального дослідження в певній галузі критичної інфраструктури. З огляду на це, *Метою цієї роботи* статті є експериментальне дослідження моделі розрахунку кількісного критерію оцінки захищеності ІТС.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Запропонована модель з використанням методу аналізу ієрархій дозволяє перейти від якісного оцінювання у вигляді упорядкованого ряду буквено-числових комбінацій [11], що позначають рівні реалізованих послуг, до кількісного оцінювання у вигляді відношення базового профілю захищеності до профілю захищеності визначеного експертом. Вхідними даними для моделі є базовий функціональний профіль захищеності (ФПЗ) [12] (він же ФПЗБ) та відкоригований експертом ФПЗ (ФПЗЕ). При цьому, НД ТЗІ 2.5-005-99, що визначає стандартні ФПЗ оброблюваної інформації від несанкціонованого доступу, оперує вимогами щодо захисту певної інформації від певних загроз і відомих на сьогодні функціональних послуг, що дозволяють протистояти цим загрозам і забезпечувати виконання вимог, які пред'являються. Блок-схема зазначеної моделі розрахунку кількісного критерію оцінювання захищеності ІТС на основі методу аналізу ієрархій, наведена на рис. 1 [2].

ISSN 2663 - 4023

Метод аналізу ієрархій для визначення співвідношення альтернатив (ФПЗБ та ФПЗЕ) реалізується у наступній 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):

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

де $a_{ij} = w_i / w_j$, w_i – «вага» i-того критерію.

При цьому, $a_{ji} = 1/a_{ij}$, $a_{ii} = 1$. Тобто, матриця є позитивною, зворотно симетричною.

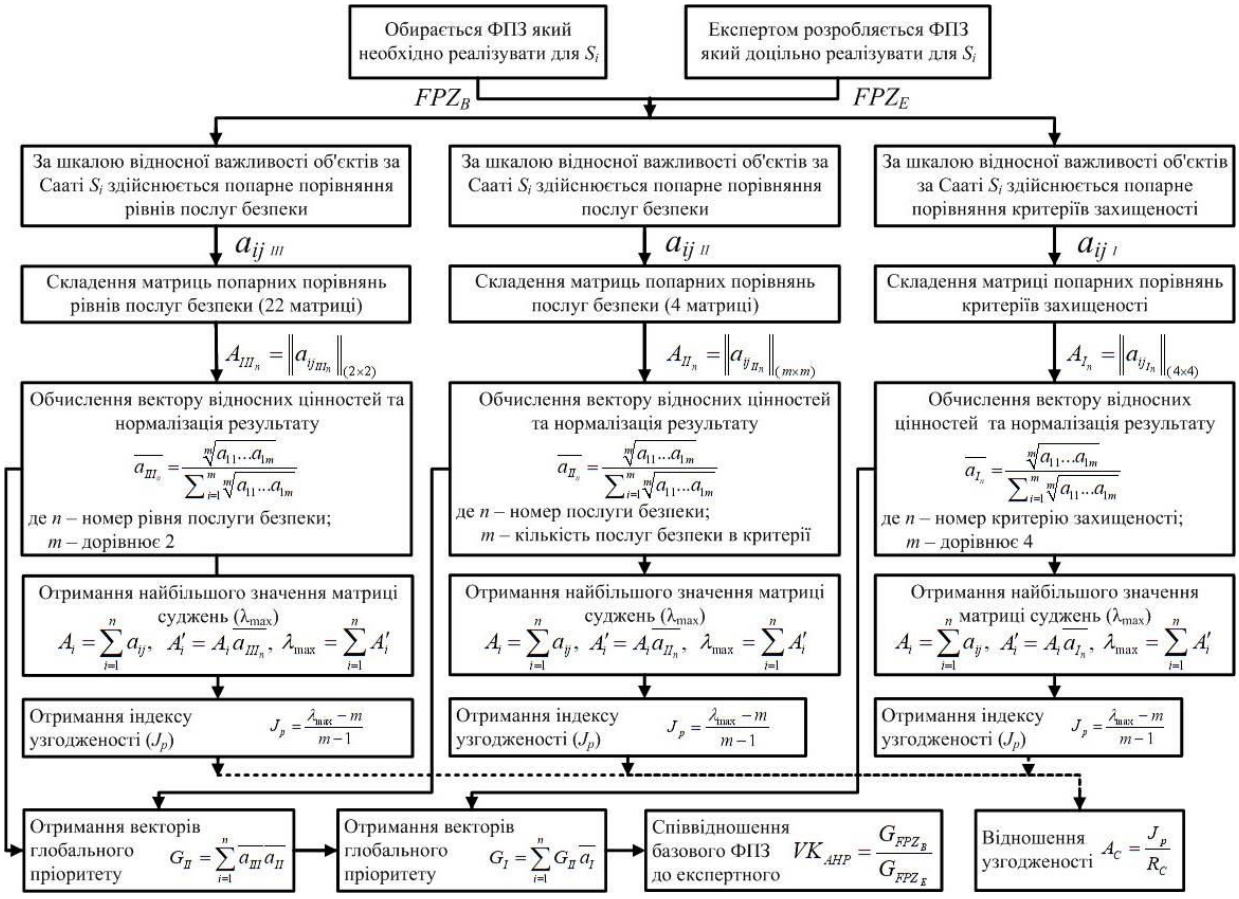

Рис. 1. Блок-схема досліджуваної моделі

Для визначення ваги будемо використовувати наступну таблицю (табл. 1) відносної важливості:

Таблиця 1

Шкала відносної важливості критеріїв

Вербальна оцінка експерта	Значення a_{ij}
w_i абсолютно кращий 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

ISSN 2663 - 4023

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 кращий 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

Для критеріїв захищеності матриця порівнянь буде мати вигляд, наведений у табл. 2:

Таблиця 2

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}
Спостереженість	a_{41}	a_{42}	a_{43}	a_{44}

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:

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

де n – розмірність матриці.

3. Здійснюється нормалізація результатів, результатом якої є нормалізований вектор пріоритетів:

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

4. Здійснюється перевірка узгодженості локальних пріоритетів:

Розрахунок найбільшого власного значення матриці:

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

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

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

Розрахунок індексу узгодженості:

$$J_p = \frac{\lambda_{\max} - m}{m-1}, \tag{7}$$

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

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

$$A_c = \frac{J_p}{R_c}, \tag{8}$$

де R_c – табличне значення (табл. 3).

Таблиця 3

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

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

5. Розрахунок глобального пріоритету для критеріїв верхнього рівня.

Нормалізований вектор пріоритетів за кожним критерієм нижчого рівня перемножується на нормалізований вектор пріоритетів вищого рівня. Добутки підсумовуються на вищому рівні.

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

де n – кількість критеріїв рівнів безпеки.

6. Визначення співвідношення альтернатив (ФПЗБ та ФПЗЕ).

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

$$VK_{AHP} = \frac{G_{FPZ_B}}{G_{FPZ_E}}, \tag{10}$$

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.

ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ

У більшості держав світу інформаційно-телекомунікаційна галузь займає одне з перших місць за критичністю після енергетики та транспорту [13]. З урахуванням цього експериментальна перевірка розроблених у роботі положень була здійснена на прикладі

ІТС Національної системи конфіденційного зв'язку (НСКЗ). З метою перевірки моделі розрахунку кількісного критерію побудовані матриці попарних порівнянь для кожного рівня критеріїв.

Для критеріїв захищеності (згідно [12]) матриця порівнянь буде мати такий вигляд (табл. 3):

Таблиця 3

Матриця порівнянь для критеріїв захищеності

	Конфіденційність	Цілісність	Доступність	Спостереженість
Конфіденційність	*1*	a_{12}	a_{13}	a_{14}
Цілісність	a_{21}	*1*	a_{23}	a_{24}
Доступність	a_{31}	a_{32}	*1*	a_{34}
Спостереженість	a_{41}	a_{42}	a_{43}	*1*

Для критеріїв послуг безпеки (згідно [12]) матриці порівнянь будуть мати вигляд, представлений у табл.4-7.

Матриця критеріїв конфіденційності представлена в табл. 4, де КД – довірча конфіденційність; КА – адміністративна конфіденційність; КО – повторне використання об'єктів; КК – аналіз прихованих каналів; КВ- конфіденційність при обміні.

Таблиця 4

Матриця критеріїв конфіденційності

	КД	КА	КО	КК	КВ
КД	*1*	a_{12}	a_{13}	a_{14}	a_{15}
КА	a_{21}	*1*	a_{23}	a_{24}	a_{25}
КО	a_{31}	a_{32}	*1*	a_{34}	a_{35}
КК	a_{41}	a_{42}	a_{43}	*1*	a_{45}
КВ	a_{51}	a_{52}	a_{53}	a_{54}	*1*

Матриця критеріїв цілісності представлена в табл. 5

Таблиця 5

Матриця критеріїв цілісності

	Довірча цілісність	Адміністративна цілісність	Відкат	Цілісність при обміні
Довірча цілісність	*1*	a_{12}	a_{13}	a_{14}
Адміністративна цілісність	a_{21}	*1*	a_{23}	a_{24}
Відкат	a_{31}	a_{32}	*1*	a_{34}
Цілісність при обміні	a_{41}	a_{42}	a_{43}	*1*

Матриця критеріїв доступності представлена в табл. 6.

Таблиця 6

Матриця критеріїв доступності

	Використання ресурсів	Стійкість до відмов	Гаряча заміна	Відновлення після збоїв
Використання ресурсів	*1*	a_{12}	a_{13}	a_{14}
Стійкість до відмов	a_{21}	*1*	a_{23}	a_{24}
Гаряча заміна	a_{31}	a_{32}	*1*	a_{34}
Відновлення після збоїв	a_{41}	a_{42}	a_{43}	*1*

Матриця критеріїв спостереженості представлена в табл. 7, де НР – реєстрація; НИ – ідентифікація і автентифікація; НО – розподіл обов'язків, НВ – автентифікація при обміні; НА – автентифікація відправника; НП – автентифікація отримувача; НК – достовірний канал; НЦ – цілісність КЗЗ; НТ – самотестування.

Таблиця 7

Матриця критеріїв спостереженості

	НР	НИ	НО	НВ	НА	НП	НК	НЦ	НТ
НР	*1*	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	a_{17}	a_{18}	a_{19}
НИ	a_{21}	*1*	a_{23}	a_{24}	a_{25}	a_{26}	a_{27}	a_{28}	a_{29}
НО	a_{31}	a_{32}	*1*	a_{34}	a_{35}	a_{36}	a_{37}	a_{38}	a_{39}
НВ	a_{41}	a_{42}	a_{43}	*1*	a_{45}	a_{46}	a_{47}	a_{48}	a_{49}
НА	a_{51}	a_{52}	a_{53}	a_{54}	*1*	a_{56}	a_{57}	a_{58}	a_{59}
НП	a_{61}	a_{62}	a_{63}	a_{64}	a_{65}	1	a_{67}	a_{68}	a_{69}
НК	a_{71}	a_{72}	a_{73}	a_{74}	a_{75}	a_{76}	1	a_{78}	a_{79}
НЦ	a_{81}	a_{82}	a_{83}	a_{84}	a_{85}	a_{86}	a_{87}	*1*	a_{89}
НТ	a_{91}	a_{92}	a_{93}	a_{94}	a_{95}	a_{96}	a_{97}	a_{98}	*1*

Для критеріїв рівнів безпеки, в нашому випадку, складаються всі 22 матриці порівнянь згідно табл. 8, де НР-1 – зовнішній аналіз; НР-2 – захищений журнал; НР-3 – сигналізація про небезпеку; НР-4 – детальна реєстрація; НР-5 – аналіз в реальному часі.

Таблиця 8

Матриця критеріїв рівнів безпеки

	НР-1	НР-2	НР-3	НР-4	НР-5
НР-1	*1*	a_{12}	a_{13}	a_{14}	a_{15}
НР-2	a_{21}	*1*	a_{23}	a_{24}	a_{25}
НР-3	a_{31}	a_{32}	*1*	a_{34}	a_{35}
НР-4	a_{41}	a_{42}	a_{43}	*1*	a_{45}
НР-5	a_{51}	a_{52}	a_{53}	a_{54}	*1*

При заповненні матриць використовується шкала, наведена в табл. 1. Обчислення множини власних векторів матриці здійснено за допомогою (2) та обчислюється, як середнє геометричне для кожної матриці. Обчислення здійснюється за допомогою розробленого авторами спеціалізованого програмного забезпечення (ПЗ) [14]. Нормалізацію результатів, підсумком якої є нормалізований вектор пріоритетів,

ISSN 2663 - 4023

здійснено за (3) за допомогою ПЗ [14]. Перевірка узгодженості локальних пріоритетів здійснена за (4-7) також за допомогою [14]. При цьому при виборі пріоритетів послуг доступності була допущена помилка (рис. 2).

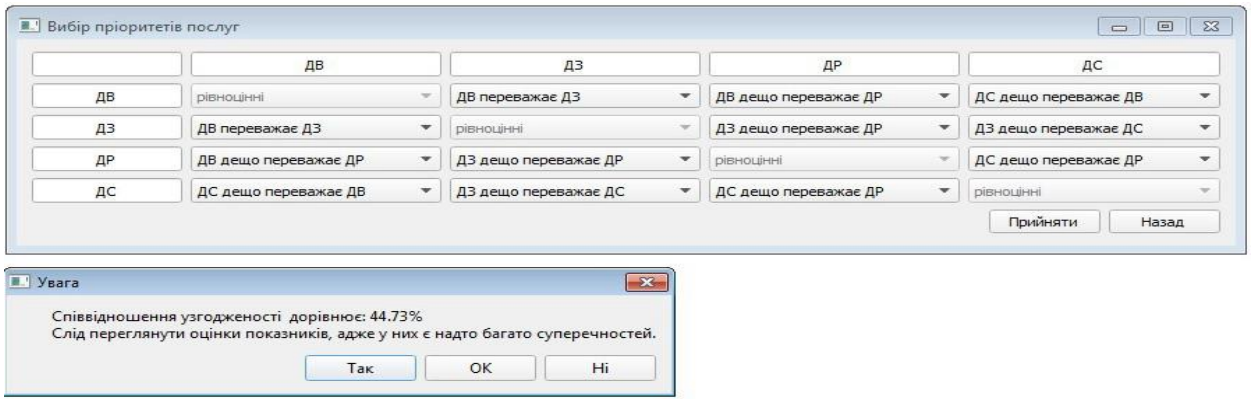

Рис. 2. Попередження про можливу помилку при виборі пріоритетів послуг доступності

За результатами аналізу помилки експертами були переглянуті пріоритети послуг доступності (рис. 3).

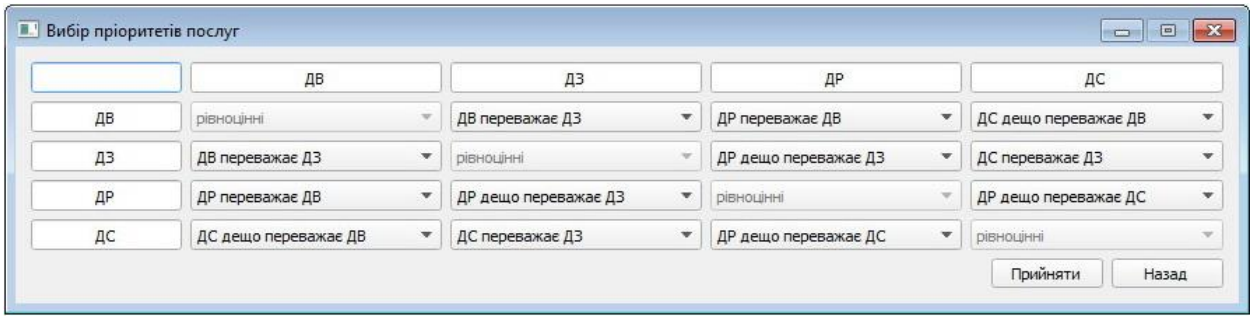

Рис. 3. Матриця критеріїв доступності

Розрахунок глобального пріоритету для критеріїв конфіденційності, цілісності, доступності та спостереженості здійснено за (9). Результат розрахунків співвідношення альтернатив (ФПЗБ та ФПЗЕ) наведений на рис. 4.

Рис. 4. Результат розрахунків співвідношення альтернатив

Як видно з рис. 4, показник важливості критеріїв конфіденційності, які реалізовані в НСКЗ, суттєво нижчий за показник, який доцільно досягти.

Відношення глобальних пріоритетів, що характеризують кількісний критерій захищеності, обраховується за (10). Значення цього критерію становить:

$$VK_{AHP} = \frac{0,417484}{0,582516} = 0,716691$$

Таким чином, з використанням моделі розрахунку кількісного критерію оцінювання захищеності ІТС отримано значення показників захищеності основних підсистем НСКЗ.

ВИСНОВКИ

Таким чином, в роботі досліджено модель розрахунку кількісного критерію оцінювання захищеності ІТС на основі методу аналізу ієрархій, що дозволило за рахунок обробки експертних оцінок отримати кількісний показник захищеності ІТС. Це дало можливість спростити процедуру підбору експертів, уникнути специфіки обробки експертних даних, а також здійснити оцінювання ІТС в умовах обмежених обсягів статистики. Розроблена модель дозволяє перейти від якісного оцінювання у вигляді упорядкованого ряду буквено-числових комбінацій, що позначають рівні реалізованих послуг, до кількісного оцінювання у вигляді відношення ФПЗБ до ФПЗЕ. Також, за допомогою запропонованої моделі сформований перелік складових НСКЗ, а саме: виділено 4 системи, 10 підсистем 1 рівня, 34 підсистеми 2 рівня та ідентифіковано 1036 складових елементів. Отримано значення кількісного критерію захищеності $VK_{AHP} = 0,716691$.

Крім того, розроблено спеціалізоване ПЗ, яке реалізує досліджувану модель, що дозволяє, використовуючи якісні показники (послуги безпеки), отримати кількісний показник у вигляді коефіцієнту, що характеризує співвідношення базового ФПЗ до запропонованого галузевим експертом; У подальших дослідженнях планується дослідити модель розрахунку кількісного критерію оцінювання захищеності ІТС в інших галузях критичної інфраструктури (енергетики, транспорту тощо).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Про основні засади забезпечення кібербезпеки України, Закон України № 2163-VIII (2021) (Україна). https://zakon.rada.gov.ua/laws/show/2163-19#Text

2 Юдін, О., Сидоренко, В., Гнатюк, С., Верховець, О. (2021). Модель розрахунку кількісного критерію оцінювання захищеності інформаційно-телекомунікаційних систем критичної інфраструктури держави. *Сучасні інформаційні системи*, *5*(4), 109–115.

3 Гнатюк, С., Юдін, О., Сидоренко, В., Євченко, Я. (2021). Метод формування функціонального профілю захищеності галузевих інформаційно-телекомунікаційних систем. *Кібербезпека: освіта, наука, техніка*, *3*(11), 166-182.

4 Про Стратегію кібербезпеки України, Рішення Ради національної безпеки і оборони України (2016) (Україна). https://zakon.rada.gov.ua/laws/show/n0003525-16#Text

5 Про критичну інфраструктуру, Закон України № 1882-IX (2021) (Україна). https://zakon.rada.gov.ua/laws/show/1882-20#Text

6 Sarkar, T., Salazar-Palma, M., Zhu, M., & Chen, H. (2021). Mathematical Principles Related to Modern System Analysis. У *Modern Characterization of Electromagnetic Systems and its Associated Metrology* (с. 1–20). IEEE. https://doi.org/10.1002/9781119076230.ch1

7 Guo, X., Gao, M., Zhang, M., Chen, Y., & Tseng, S.-P. (2020). Design and Implementation of Teaching Quality Assessment System based on Analytic Hierarchy Process Fuzzy Comprehensive Evaluation method. У *2020 8th International Conference on Orange Technology (ICOT)*. IEEE. https://doi.org/10.1109/icot51877.2020.9468778.

8 Sandoval-Alfaro, O. E., & Quintero-Meza, R. R. (2021). Application of Data Analytics Techniques for Decision Making in the Retrospective Stage of the Agile Scrum Methodology. У *2021 Mexican International Conference on Computer Science (ENC)*. IEEE. https://doi.org/10.1109/enc53357.2021.9534800.

9 *Введение в теорию нечетких множеств* (А. Кофман, Пер.). (1982). Радио и связь.

10 Ma, Z., Wang, S., Deng, X., & Jiang, W. (2018). An improved approach for adversarial decision making under uncertainty based on simultaneous game. У *2018 Chinese Control And Decision Conference (CCDC)*. IEEE. https://doi.org/10.1109/ccdc.2018.8407545.

11 Юдін, О., & Гнатюк, С. (2017). Аналіз вимог до елементів інформаційно-телекомуні-каційних систем управління енергетичною інфраструктурою, які забезпечують кіберзахист, Перспективні напрями захисту інформації. У *Третя всеукраїнська наук.-практ. конф.* ОНАЗ.

12 НД ТЗІ 2.5-004-99, Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, ДСТСЗІ СБ України, 1999.

13 Gnatyuk, S., Sydorenko, V., Polozhentsev, A., & Sotnichenko, Y. (2020). Experimental Cybersecurity Level Determination in the Civil Aviation Critical Infrastructure. У *2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)*. IEEE. https://doi.org/10.1109/picst51311.2020.9467987.

14 Свідоцтво про реєстрацію авторського права на твір № 9 від 14 липня 2018 р., UA.ЄАБА.18013-01 34 01, Державна служба інтелектуальної власності України, «Програмне забезпечення розрахунку коефіцієнту критичності інформаційно-телекомунікаційних систем».

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (16), 2022
ISSN 2663 - 4023

Sergiy O. Gnatyuk
DSc, Professor, Vice-Dean of the Faculty of Cybersecurity, Computer and Software Engineering
National Aviation University, Kyiv, Ukraine
ORCID ID: 0000-0003-4992-0564
s.gnatyuk@nau.edu.ua

Oleksiy Yu. Yudin
PhD, Vice-Chair of the Institute
State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, Kyiv, Ukraine
ORCID ID: 0000-0002-4730-1463
alex@ukrdeftech.com.ua

Viktoriia M. Sydorenko
PhD, Associate Professor, Associate Professor of IT-Security Academic Department
National Aviation University, Kyiv, Ukraine
ORCID ID: 0000-0002-5910-0837
v.sydorenko@ukr.net

Tetiana V. Smirnova
PhD, Associate Professor, Associate Professor of Academic Department of Cybersecurity and Software
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID: 0000-0001-5093-1581
sm.tetyana@gmail.com

Dauriya D. Zhaksigulova
PhD Student
D. Serikbayev East Kazakhstan Technical University, Ust`-Kamenogorsk, Kazakhstan
ORCID ID: 0000-0003-0646-2823
dauriya.dzh@gmail.com

EXPERIMENTAL STUDY OF THE MODEL FOR CALCULATING THE QUANTITATIVE CRITERIA FOR ASSESSING THE SECURITY LEVEL OF INFORMATION AND TELECOMMUNICATION SYSTEMS IN CRITICAL INFRASTRUCTURE OF THE STATE

Abstract. Global trends in the number and complexity of cyber-attacks have led to the information and telecommunications systems (ITS) protection, in particular, industry, which are critical to society, socio-economic development and information component of national security. Given the needs of national security and the need to introduce a systematic approach to solving the problem of critical infrastructure protection, at the national level, creating a system of protection of such infrastructure is one of the priorities in reforming the defense and security sector of Ukraine. Thus, there is a need to develop methods and models for classifying ITS as a critical infrastructure to ensure Ukraine's national security. The paper studies the model of calculating the quantitative criterion for assessing the security of ITS based on the method of hierarchy analysis, which allowed the processing of expert assessments to obtain a quantitative indicator of ITS security. This made 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. The developed model allows to move from qualitative assessment in the form of an ordered series of alphanumeric combinations denoting the levels of implemented services, to quantitative assessment in the form of the ratio of functional security profiles. In addition, specialized software has been developed that implements the studied model, which allowed to conduct experimental research and verification of this model on the example of ITS of the National Confidential Communications System. In further research, the authors plan to investigate the model for calculating the quantitative criterion for assessing the security of ITS in other areas of critical infrastructure (energy, transport etc.).

Keywords: information and telecommunication system, critical infrastructure, critical infrastructure object, cybersecurity, security assessment criterion, functional security profile.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy, Zakon Ukrainy № 2163-VIII (2021) (Ukraina). https://zakon.rada.gov.ua/laws/show/2163-19#Text

2 Iudin, O., Sydorenko, V., Hnatiuk, S., Verkhovets, O. (2021). Model rozrakhunku kilkisnoho kryteriiu otsiniuvannia zakhyshchenosti informatsiino-telekomunikatsiinykh system krytychnoi infrastruktury derzhavy. Suchasni informatsiini systemy, 5(4), 109–115.

3 Hnatiuk, S., Yudin, O., Sydorenko, V., Yevchenko, Ya. (2021). Metod formuvannia funktsionalnoho profiliu zakhyshchenosti haluzevykh informatsiino-telekomunikatsiinykh system. Kiberbezpeka: osvita, nauka, tekhnika, 3(11), 166-182.

4 Pro Stratehiiu kiberbezpeky Ukrainy, Rishennia Rady natsionalnoi bezpeky i oborony Ukrainy (2016) (Ukraina). https://zakon.rada.gov.ua/laws/show/n0003525-16#Text

5 Pro krytychnu infrastrukturu, Zakon Ukrainy № 1882-IX (2021) (Ukraina). https://zakon.rada.gov.ua/laws/show/1882-20#Text

6 Sarkar, T., Salazar-Palma, M., Zhu, M., Chen, H. (2021). Mathematical Principles Related to Modern System Analysis. In *Modern Characterization of Electromagnetic Systems and its Associated Metrology* (p. 1–20). IEEE. https://doi.org/10.1002/9781119076230.ch1

7 Guo, X., Gao, M., Zhang, M., Chen, Y., Tseng, S.-P. (2020). Design and Implementation of Teaching Quality Assessment System based on Analytic Hierarchy Process Fuzzy Comprehensive Evaluation method. In *2020 8th International Conference on Orange Technology (ICOT)*. IEEE. https://doi.org/10.1109/icot51877.2020.9468778.

8 Sandoval-Alfaro, O. E., Quintero-Meza, R. R. (2021). Application of Data Analytics Techniques for Decision Making in the Retrospective Stage of the Agile Scrum Methodology. In *2021 Mexican International Conference on Computer Science (ENC)*. IEEE. https://doi.org/10.1109/enc53357.2021.9534800.

9 *Vvedenye v teoryiu nechetkykh mnozhestv (A. Kofman, Per.). (1982). Radyo y sviaz*.

10 Ma, Z., Wang, S., Deng, X., & Jiang, W. (2018). An improved approach for adversarial decision making under uncertainty based on simultaneous game. In *2018 Chinese Control And Decision Conference (CCDC)*. IEEE. https://doi.org/10.1109/ccdc.2018.8407545.

11 Iudin, O., Hnatiuk, S. (2017). Analiz vymoh do elementiv informatsiino-telekomuni-katsiinykh system upravlinnia enerhetychnoiu infrastrukturoiu, yaki zabezpechuiut kiberzakhyst, Perspektyvni napriamy zakhystu informatsii. In *Tretia vseukrainska nauk.-prakt. konf.* ONAZ.

12 ND TZI 2.5-004-99, Kryterii otsinky zakhyshchenosti informatsii v kompiuternykh systemakh vid nesanktsionovanoho dostupu, DSTSZI SB Ukrainy, 1999.

13 Gnatyuk, S., Sydorenko, V., Polozhentsev, A., & Sotnichenko, Y. (2020). Experimental Cybersecurity Level Determination in the Civil Aviation Critical Infrastructure. In *2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)*. IEEE. https://doi.org/10.1109/picst51311.2020.9467987.

14 Svidotstvo pro reiestratsiiu avtorskoho prava na tvir № 9 vid 14 lypnia 2018 r., UA.IeABA.18013-01 34 01, Derzhavna sluzhba intelektualnoi vlasnosti Ukrainy, «Prohramne zabezpechennia rozrakhunku koefitsiientu krytychnosti informatsiino-telekomunikatsiinykh system».

(cc) BY-NC-SA

This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.