

УДК 004.056.5::629.7.08 (045)

СЕРГІЙ ГНАТЮК,
ВІКТОРІЯ СИДОРЕНКО,
ВАСИЛЬ КІНЗЕРЯВИЙ

МЕТОД ІДЕНТИФІКАЦІЇ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ В АВІАЦІЙНІЙ ГАЛУЗІ

Останнім часом у світі спостерігається тенденція до збільшення кількості надзвичайних подій різного роду. Щодня світові ЗМІ повідомляють про природні та техногенні катастрофи, збройні конфлікти, терористичні акти, важкі злочини, акти піратства, вчинені як злочинними організаціями, так і окремими особами. Все частіше в результаті таких подій жертвами стає велика кількість людей та завдається шкода життєво важливим для існування держав системам, об'єктам і ресурсам. Серед останніх особливої уваги потребує галузь цивільної авіації, так як існує необхідність у забезпеченні безперервної комунікації та взаємодії між наземними системами і повітряними суднами. Більшість провідних держав світу стали приділяти значну увагу методам і засобам ідентифікації, систематизації та забезпечення безпеки об'єктів критичної інфраструктури, втрата або порушення нормального функціонування яких призведе до суттєвих або навіть непоправних негативних наслідків для національної безпеки держави. Проте, за результатами проведеного аналізу встановлено, що існуючі підходи до виявлення та ідентифікації об'єктів інфраструктури не є системними та чітко формалізованими, орієнтовані лише на певні галузі інфраструктури та не враховують повної множини параметрів і особливостей критичної інфраструктури особливо її інформаційної складової. З огляду на це, у цій роботі розроблено метод ідентифікації об'єктів критичної інформаційної інфраструктури, який дає можливість визначити елементи критичної інфраструктури, їх взаємовплив та вплив на функціональні операції критичної авіаційної інформаційної системи. Цей метод, а також розроблений на його основі програмний застосунок, можуть використовуватись на практиці для ідентифікації об'єктів критичної інформаційної інфраструктури різних галузей.

Ключові слова: критична інфраструктура, критична інформаційна інфраструктура, ідентифікація об'єктів критичної інформаційної інфраструктури, критичні авіаційні інформаційні системи, цивільна авіація.

Вступ. Сучасне суспільство повністю залежить від інформаційно-комунікаційних систем і мереж, відмова яких може призвести до хаосу, значних фінансових збитків та навіть масової загибелі людей. Щоправда, переважна частина людства схильна приймати найважливіші сервіси (зокрема, їх якість) як належне до тих пір, поки щось або хтось не порушить їх роботу. Для визначення і узагальнення найважливіших та найуразливіших активів держави порівняно нещодавно до міжнародного законодавства було введено термін критична інфраструктура (КІ) [1] - [2]. Поняття КІ почали активно вживати у другій половині 90-х років минулого сторіччя здебільшого відносно розподілених великомасштабних інформаційних систем (центрів обробки даних, об'єднаних комунікаційних мереж) [3].

Аналіз останніх досліджень і публікацій. Що стосується підходів до ідентифікації об'єктів критичної інформаційної інфраструктури (КІІ), з огляду на роботи [4] - [6], на сьогодні в розвинених державах світу відомо незначну кількість методів і моделей, що можуть забезпечити керівникам відповідних ланок управління можливість приймати обґрунтоване і правильне рішення щодо віднесення об'єктів до КІІ. Дослідження вітчизняної нормативної бази, в [1], [7] свідчить, що галузь захисту КІІ нашої держави перебуває на початковому етапі формування. Хоча чинним вітчизняним законодавством й визначено окремі об'єкти соціально-економічної сфери України, надзвичайні події на яких можуть призвести до суспільно небезпечних наслідків, проте вони не складають єдину систему [8]. Відповідно до [9] в Україні на сьогодні триває розробка

пропозицій щодо формування переліку інформаційно-телекомунікаційних систем об'єктів КІ держави, проте, поки що, без особливих результатів. У роботі [10] проведено багатокритеріальний аналіз підходів до виявлення критично важливих об'єктів інфраструктури для оцінювання їх можливостей щодо виявлення та ідентифікації найбільш важливих об'єктів КІ. Для цього було використано такі базові критерії: чіткість формалізації, простота реалізації, гнучкість та універсальність, точність, оперативність, інформаційна складова та об'єктивність. Проведений аналіз підходів показав, що найбільш вдалим (з точки зору застосування для КІ) є імітаційне моделювання та підходи, які як і багато інших базуються на теорії графів. Крім того, широко використовуються знання теорії самоорганізованих мереж А. Барабаші та ідентифікація об'єктів КІ на основі категоріювання – деякі аспекти цих підходів теж можуть бути використані для об'єктів КІ. Проте, варто також зазначити, що загальні підходи до виявлення та ідентифікації найбільш важливих об'єктів КІ в основному орієнтовані на економічні, екологічні, техногенні та інші системи безпеки держави, та не враховують повної множини параметрів і особливостей КІ, а саме її інформаційної складової.

Постановка завдання. Серед галузей КІ особливого захисту потребує цивільна авіація (ЦА), де відповідно до керівних документів у цій галузі (зокрема [11]), необхідно ідентифікувати і захищати критичні авіаційні інформаційні системи (КАІС). Адже очевидно, що несанкціоноване втручання у роботу авіатранспортної системи може призвести до значних економічних збитків, людських жертв і руйнування загальнодержавної інфраструктури. Отже, забезпечення захисту авіаційних систем є загальнообов'язковим для кожної держави, яка є і хоче залишатись частиною міжнародної авіаційної спільноти. Проте, необмежена кількість об'єктів і параметрів систем, які постійно варіюються, та важко прогнозована поведінка об'єктів з великою кількістю взаємозв'язків є основними причинами труднощів виявлення об'єктів КІ держави (зокрема в авіаційній галузі). Зважаючи на це, **метою роботи** є розробка і дослідження ефективного методу ідентифікації об'єктів КІ в авіаційній галузі.

Виклад основного матеріалу дослідження. Запропонований метод ідентифікації об'єктів КІ в авіаційній галузі (див. рис. 1) реалізується в такі етапи: 1) формування елементів КІ; 2) формування можливих чинників впливу на елемент КІ; 3) визначення ступеню пошкодження та ваги впливу чинника на елемент КІ; 4) формування функцій впливу елементів КІ; 5) графоаналітичне відображення функціональних процесів системи КІ; 6) оцінювання якості функціонування системи КІ.

Вхідні дані методу: 1) структурно-функціональні схеми аналізованої системи; 2) інформація про елементи інфраструктури та їх функціональні операції аналізованої системи; 3) докладний опис всіх можливих чинників та їх параметрів, які можуть впливати на функціонування системи.

Вихідні дані: 1) множина ідентифікованих елементів інфраструктури; 2) множина чинників впливу на елемент інфраструктури та опис їх параметрів; 3) таблиці ступенів пошкодження елементів інфраструктури для кожного чинника впливу; 4) таблиці ваг впливу елементів інфраструктури для кожного чинника впливу; 5) перелік пар елементів інфраструктури для яких встановлено відношення впливу та їх розраховане значення функції впливу; 6) граф функціонального процесу системи КІ; 7) матриця впливу елементів інфраструктури на їх функціональні операції та перелік ранжованих за порядком важливості елементів інфраструктури системи КІ.

Розглянемо детально кожен з етапів реалізації запропонованого методу. Процедура формування елементів КІ реалізується на рівні системи (при $l=2$ згідно (8) в [12]) і стосується лише елементів інформаційної інфраструктури (ЕІ), які повністю відображають структуру обраного рівня деталізації. Метод ідентифікації об'єктів КІ реалізується для певної системи, визначеної (1) в [12] множини

$$\mathbf{S} = \left\{ \bigcup_{i=1}^n S_i \right\} = \{S_1, S_2, \dots, S_n\}, S_i \subseteq \mathbf{S}, (i = \overline{1, n})$$

системи КІ, n – загальна кількість зазначених систем).

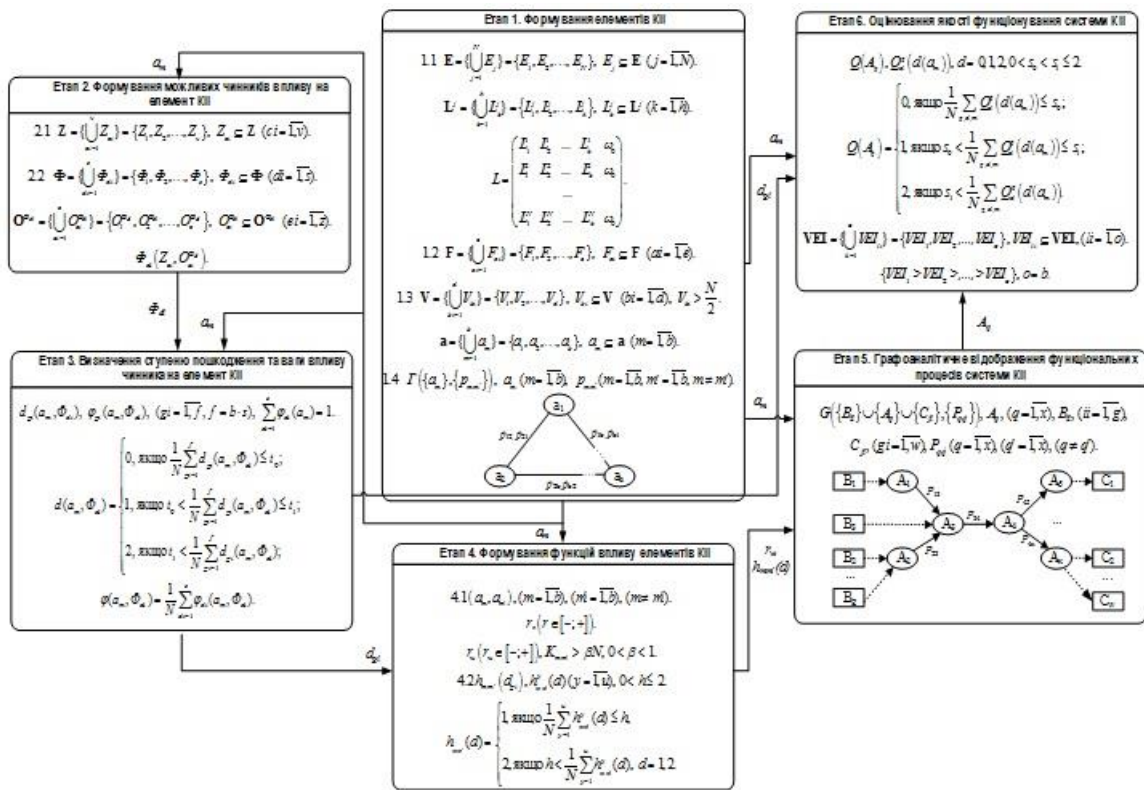


Рисунок 1 – Схема реалізації методу ідентифікації об’єктів КП авіаційної галузі

Етап 1. Формування елементів КП

Крок 1.1. Формування можливих ЕП. Для формування можливих ЕП певної системи S_i ,

кожен експерт з множини \mathbf{E} ($\mathbf{E} = \{\bigcup_{j=1}^N E_j\} = \{E_1, E_2, \dots, E_N\}$, $E_j \subseteq \overline{\mathbf{E}}$ ($j = \overline{1, N}$) – експерти у галузі

КП, N – загальна кількість експертів), формує всі можливі ЕП ($\mathbf{L}^j = \{\bigcup_{k=1}^h L_k^j\} = \{L_1^j, L_2^j, \dots, L_h^j\}$,

$L_k^j \subseteq \mathbf{L}^j$ ($k = \overline{1, h}$) – можливі ЕП сформовані j -м експертом, h – кількість елементів, які характеризують систему S_i). У результаті виконання кроку 1.1 формується матриця (1), у якій відображені всі можливі елементи КП певної системи S_i . Сформовані ЕП $\{L_1^j, L_2^j, \dots, L_h^j\}$ можуть мати різну довжину, тому згідно описаному в [13] – [14] підходу, вони доповнюються пустим елементом ω_0 таким чином, щоб всі рядки матриці L мали однакову довжину.

$$L = \begin{pmatrix} L_1^1 & L_2^1 & \dots & L_k^1 & \omega_0 \\ L_1^2 & L_2^2 & \dots & L_k^2 & \omega_0 \\ \dots & \dots & \dots & \dots & \dots \\ L_1^N & L_2^N & \dots & L_k^N & \omega_0 \end{pmatrix}. \tag{1}$$

Наприклад, для системи S_{SNS} – супутникові навігаційні системи (СНС) [15], при $N = 3$, сформуємо матрицю можливих ЕП згідно (1):

$$L = \begin{pmatrix} L_1^1 & L_2^1 & L_3^1 & L_4^1 & L_5^1 \\ L_1^2 & L_2^2 & L_3^2 & L_4^2 & \omega_0 \\ L_1^3 & L_2^3 & L_3^3 & L_4^3 & L_5^3 \end{pmatrix},$$

де L_1^1 – штучні супутники Землі (ШСЗ);

L_2^1 – контрольна станція;

L_3^1 – додаткова станція;

L_4^1 – станція спостереження;

L_5^1 – приймачі; L_1^2 – ШСЗ;

L_2^2 – контрольно-спостережна станція;

L_3^2 – додаткові станції; L_4^2 – приймачі;

L_1^3 – ШСЗ; L_2^3 – контрольно-спостережна станція;

L_3^3 – додаткові станції; L_4^3 – SPS-приймачі;

L_5^3 – PPS-приймачі (згідно [15] - [16]).

Крок 1.2. Виділення унікальних ЕП. Для виділення унікальних ЕП з отриманих можливих

L_k^j виділяємо відповідну множину \mathbf{F} ($\mathbf{F} = \{\bigcup_{ai=1}^e F_{ai}\} = \{F_1, F_2, \dots, F_e\}$, $F_{ai} \subseteq \mathbf{F}$ ($ai = \overline{1, e}$) – унікальні ЕП, e – кількість унікальних ЕП).

Наприклад, для системи S_{SNS} множина унікальних ЕП при $e = 8$, згідно [15] - [16], дорівнює: $\mathbf{F}_{\text{SNS}} = \{\bigcup_{ai=1}^8 F_{ai}\} = \{F_1, F_2, \dots, F_8\}$, де F_1 – ШСЗ, F_2 – контрольна станція, F_3 – додаткова станція, F_4 – станція спостереження, F_5 – приймачі; F_6 – контрольно-спостережна станція F_7 – SPS-приймачі, F_8 – PPS-приймачі.

Крок 1.3. Узгодження ЕП. Формування узгоджених ЕП з отриманих унікальних ЕП F_{ai} здійснюється за допомогою встановлення співпадіння елементів F_{ai} у матриці L у вигляді

множини \mathbf{V} ($\mathbf{V} = \{\bigcup_{bi=1}^d V_{bi}\} = \{V_1, V_2, \dots, V_d\}$, $V_{bi} \subseteq \mathbf{V}$ ($bi = \overline{1, d}$) – співпадіння елементів F_{ai} у матриці L , d – кількість співпадінь відповідного F_{ai} у матриці L).

Узгодження множини ЕП відбувається згідно з виразом: $V_{bi} > \frac{N}{2}$, отримані значення d та їх відповідні ЕП, пропонується

для затвердження у якості узгодженої множини елементів КІІ: $\mathbf{a} = \{\bigcup_{m=1}^b a_m\} = \{a_1, a_2, \dots, a_b\}$, де

$a_m \subseteq \mathbf{a}$ ($m = \overline{1, b}$) – елементи КІІ, які повністю відображають структуру системи КІІ, b – загальна кількість зазначених елементів.

Наприклад, для системи S_{SNS} множина співпадінь елементів F_{ai} у матриці L , при $N = 3$,

$d = 8$, згідно [15] - [16], дорівнює: $\mathbf{V}_{\text{SNS}} = \{\bigcup_{bi=1}^8 V_{bi}\} = \{V_1, V_2, \dots, V_8\} = \{3, 1, 3, 1, 2, 2, 1, 1\}$, а узгоджена

множина ЕП, згідно з виразом: $V_{bi} > \frac{N}{2}$, при $b = 4$, має вигляд: $\mathbf{a}_{\text{SNS}} = \{\bigcup_{m=1}^4 a_m\} = \{a_1, a_2, \dots, a_4\}$, де a_1

– ШСЗ, a_2 – контрольно-спостережна станція, a_3 – додаткова станція, a_4 – приймачі.

Крок 1.4. Формування графу відображення ідентифікованих елементів КІІ. Графоаналітичне відображення ідентифікованих ЕП представлено неорієнтованим графом (2):

$$\Gamma(\{a_m\}, \{p_{mm'}\}), \quad (2)$$

де вершини a_m ($m = \overline{1, b}$) відповідають ідентифікованим елементам КІІ, а ребра $p_{mm'}$ – зв'язкам між елементами a_m , де ($m = \overline{1, b}, m' = \overline{1, b}, m \neq m'$) (див. рис. 2).

Наприклад, при $b = 4$, згідно (2), вершинами графу $\Gamma \in a_1$ – ШСЗ, a_2 – контрольно-спостережна станція, a_3 – додаткова станція, a_4 – приймачі, а зв'язками між цими елементами є ребра: $p_{12}, p_{21}, p_{13}, p_{31}, p_{14}, p_{41}, p_{23}, p_{32}, p_{24}, p_{42}, p_{34}, p_{43}$ (див. рис. 3).

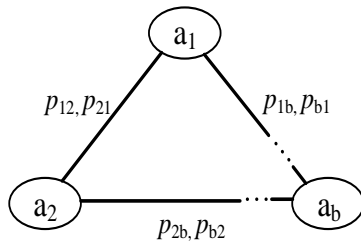


Рисунок 2 – Графоаналітичне відображення ідентифікованих a_m

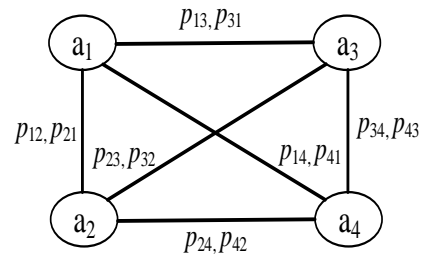


Рисунок 3 – Графоаналітичне відображення ідентифікованих a_m при $b = 4$ для S_{SNS}

Етап 2. Формування можливих чинників впливу на елемент КІІ

Крок 2.1. Формування множини зон впливу. На цьому кроці формується відповідна множина зон впливу $Z = \{\bigcup_{ci=1}^v Z_{ci}\} = \{Z_1, Z_2, \dots, Z_v\}$, де $Z_{ci} \subseteq Z$ ($ci = \overline{1, v}$) – зони впливу на ЕП, v – загальна кількість зон впливу, яка задовольняє наступній умові: в кожену зону Z_{ci} потрапляє один елемент КІІ a_m (може бути введено множину зон, які є частинами території розташування системи КІІ).

Наприклад, для системи S_{SNS} , при $v = 2$, згідно [15], множина зон впливу має такий вигляд:
 $Z_{SNS} = \{\bigcup_{ci=1}^2 Z_i\} = \{Z_1, Z_2\}$, де Z_1 – космічна або орбітальна зона, Z_2 – наземна зона управління та контролю.

Крок 2.2. Формування чинників впливу на елемент КІІ. Для формування можливих чинників впливу введемо відповідну множину $\Phi = \{\bigcup_{di=1}^s \Phi_{di}\} = \{\Phi_1, \Phi_2, \dots, \Phi_s\}$, де $\Phi_{di} \subseteq \Phi$ ($di = \overline{1, s}$) – чинники впливу на ЕП a_m , S – загальна кількість зазначених чинників впливу. Кожен чинник Φ_{di} для певної зони Z_{ci} може бути представлений у вигляді множини параметрів $O^{\Phi_{di}} = \{\bigcup_{ei=1}^z O_{ei}^{\Phi_{di}}\} = \{O_1^{\Phi_{di}}, O_2^{\Phi_{di}}, \dots, O_z^{\Phi_{di}}\}$, де $O_{ei}^{\Phi_{di}} \subseteq O^{\Phi_{di}}$ ($ei = \overline{1, z}$) – параметри чинників впливу Φ_{di} на ЕП a_m , Z – загальна кількість параметрів чинника Φ_{di} , що формується на основі експертних знань та може описуватись текстовим повідомленням чи містити кількісні показники. У результаті виконання перерахованих операцій формується множина можливих чинників впливу Φ_{di} , у якій кожен чинник є набором $\Phi_{di}(Z_{ci}, O_{ei}^{\Phi_{di}})$.

Наприклад, для S_{SNS} , при $s = 7$, згідно [17] - [18] множину чинників впливу можна представити у такому вигляді $\Phi_{SNS} = \{\bigcup_{di=1}^7 \Phi_{di}\} = \{\Phi_1, \Phi_2, \dots, \Phi_7\}$, де Φ_1 – геометричний чинник (geometric dilution of precision, GDOP), який свідчить про стан впливу похибок псевдо дальності (останнє характеризує міру віддаленості споживача від GPS – супутника) показань годин на точність обчислення координат; Φ_2 – горизонтальний чинник (horizontal dilution of precision, HDOP), який показує ступінь впливу точності визначення горизонталі на похибку обчислення координат; Φ_3 – відносний чинник (relative dilution of precision, RDOP), безрозмірний показник, який описує вплив на точність визначення координат похибки псевдо дальності; Φ_4 – часовий чинник (time dilution of precision, TDOP), дорівнює чиннику зниження

точності, нормалізованому на період 60 с; Φ_5 – вертикальний чинник (vertical dilution of precision, VDOP), описує ступінь впливу похибки показників годин на точність координат; Φ_6 – чинник положення (position dilution of precision, PDOP), який показує ступінь впливу похибки у вертикальній площині на точність визначення координат; Φ_7 – чинник комунікації (communication dilution of precision, CDOP), що показує значення записів мережевих з’єднань згідно бази даних NLS-KDD [19]. Кожен запис зазначеної бази складається з 42 полів: 41 поле описує параметри мережевого трафіку, останнє поле може приймати значення, що свідчить про відсутність атаки (normal) або значення найменування типу атаки, які розділяються на 4 основних класи – відмова в обслуговуванні (DoS), несанкціоноване отримання прав доступу незареєстрованим користувачем (R2L), несанкціоноване підвищення привілеїв зареєстрованим користувачем (U2R) та сканування портів (Probe).

Як приклад для чинника Φ_7 , представимо множину параметрів чинника впливу, при $z = 5$, в наступному вигляді: $\mathbf{O}^{\Phi_7} = \{\bigcup_{ei=1}^5 O_{ei}^{\Phi_7}\} = \{O_1^{\Phi_7}, O_2^{\Phi_7}, \dots, O_5^{\Phi_7}\}$, де $O_1^{\Phi_7}$ – базові параметри; $O_2^{\Phi_7}$ – параметри контенту; $O_3^{\Phi_7}$ – часові параметри; $O_4^{\Phi_7}$ – апаратні параметри; $O_5^{\Phi_7}$ – параметр присутності/відсутності атаки. Після чого сформуємо для чинника Φ_7 можливі набори параметрів: $\Phi_7(Z_1, O_1^{\Phi_7}, O_2^{\Phi_7}, O_3^{\Phi_7}, O_4^{\Phi_7}, O_5^{\Phi_7})$; $\Phi_7(Z_2, O_1^{\Phi_7}, O_2^{\Phi_7}, O_3^{\Phi_7}, O_4^{\Phi_7}, O_5^{\Phi_7})$.

Етап 3. Визначення ступеню пошкодження та ваги впливу чинника на елемент КІІ

Для кожного визначеного чинника впливу Φ_{di} та елемента КІІ a_m , згідно з [13], фіксуються значення двох величин $d_{gi}(a_m, \Phi_{di})$ та $\varphi_{gi}(a_m, \Phi_{di})$ – ступінь пошкодження елемента a_m та ваги впливу чинника Φ_{di} на ЕІІ відповідно, де $gi = \overline{1, f}$, $f = b \cdot s$. Для оцінювання ступеню пошкоджень елементів $d_{gi}(a_m, \Phi_{di})$ використовується лінгвістична шкала, що відображена наступним чином: *Damage absent* – “0” (ЕІІ не піддався впливу або вплив був незначний); *Middle damage* – “1” (вплив на ЕІІ визвав значне пошкодження обладнання); *Complete failure* – “2” (вплив на ЕІІ привів до повного руйнування). Точні значення лінгвістичних змінних *Damage absent*, *Middle damage*, *Complete failure* встановлюється для кожної системи КІІ індивідуально.

Далі кожен експерт E_j визначає $d_{gi}(a_m, \Phi_{di})$ та $\varphi_{gi}(a_m, \Phi_{di})$ для всіх елементів a_m та всіх чинників Φ_{di} . До того ж, для будь-якого ЕІІ a_m має виконуватись умова $\sum_{di=1}^s \varphi_{di}(a_m) = 1$. Після цього відбувається обробка даних, отриманих від усіх експертів E_j , у якості узгоджених оцінок ступеню пошкодження ЕІІ $d_{gi}(a_m, \Phi_{di})$ і ваги впливу $\varphi_{gi}(a_m, \Phi_{di})$ на елементи КІІ приймаються значення відповідно до (3):

$$d(a_m, \Phi_{di}) = \begin{cases} 0, & \text{якщо } \frac{1}{N} \sum_{gi=1}^f d_{gi}(a_m, \Phi_{di}) \leq t_0; \\ 1, & \text{якщо } t_0 < \frac{1}{N} \sum_{gi=1}^f d_{gi}(a_m, \Phi_{di}) \leq t_1; \\ 2, & \text{якщо } t_1 < \frac{1}{N} \sum_{gi=1}^f d_{gi}(a_m, \Phi_{di}); \end{cases} \quad (3)$$

$$\varphi(a_m, \Phi_{di}) = \frac{1}{N} \sum_{di=1}^s \varphi_{di}(a_m, \Phi_{di}).$$

де значення порогових величин t_0, t_1 задовольняють умові $0 < t_0 < t_1 \leq 2$ і встановлюються заздалегідь та можуть переглядатися в залежності від системи КІІ.

Наприклад, для системи S_{SNS} , при $b = 4$ та $s = 7$, згідно [15] та [18] відповідно, узгоджені експертами згідно з (3) значення величин ступеню пошкодження та ваги впливу зазначені в табл. 1 (значення порогових величин $t_0 = 1$ та $t_1 = 1,5$).

Таблиця 1 – Приклад значень ступеню пошкодження і ваги впливу на елементи КП

	Φ_1		Φ_2		Φ_3		Φ_4		Φ_5		Φ_6		Φ_7	
	d_1	φ_1	d_2	φ_2	d_3	φ_3	d_4	φ_4	d_5	φ_5	d_6	φ_6	d_7	φ_7
a_1	1	0,2	1	0,1	0	0,1	1	0,1	1	0,2	0	0	2	0,3
a_2	1	0,2	1	0,2	1	0,2	1	0,2	1	0	1	0	1	0,2
a_3	1	0,1	0	0,1	0	0,1	0	0,1	0	0,1	1	0,1	1	0,4
a_4	1	0,2	0	0,1	0	0,1	0	0,1	0	0,1	0	0,1	1	0,3

Етап 4. Формування функцій впливу елементів КП

Крок 4.1. Визначення відношень впливу між елементами КП. На цьому кроці визначаються і узгоджуються існування відношень впливу між елементами КП за наступним правилом: два елементи КП a_m та $a_{m'}$ ($m = \overline{1, b}, m' = \overline{1, b}, m \neq m'$) пов'язані відношенням впливу, якщо пошкодження елемента a_m викликає пошкодження елемента $a_{m'}$. Отже, для кожної можливої пари елементів КП $(a_m, a_{m'})$ кожен експерт E_j вказує значення відношення впливу r наступним чином ($r \in [-; +]$): якщо вплив має місце, то ставиться "+", якщо ні – "-". Далі відбувається обробка даних отриманих від кожного E_j , де значення $K_{mm'}$ дорівнює кількості "+" у рядку, що відповідає парі $(a_m, a_{m'})$, а значення r_w – узгоджена оцінка, приймає значення "+", якщо у відповідному рядку виконується нерівність: $K_{mm'} > \beta N$, "-" – якщо не виконується. Значення величини $0 < \beta < 1$ встановлюється заздалегідь та може переглядатися в залежності від системи КП.

Наприклад, для системи S_{SNS} , при $b = 4$, згідно з [15], формуються можливі пари ЕП та оцінюється вплив між цими елементами. Оброблені значення відображені в табл. 2 (значення величини $\beta = 0,5$), де сірим кольором позначені пари, для яких встановлено відношення впливу.

Таблиця 2 – Відношення впливу між елементами КП

Пара $(a_m, a_{m'})$	Результат			Кількість "+" $(K_{mm'})$	Узгоджена оцінка (r_w)
	1	2	3		
(a_1, a_2)	+	+	+	3	+
(a_1, a_3)	-	-	+	1	-
(a_1, a_4)	+	-	+	2	+
(a_2, a_1)	+	+	+	3	+
(a_2, a_3)	+	+	+	3	+
(a_2, a_4)	+	-	+	2	+
(a_3, a_1)	-	-	-	0	-
(a_3, a_2)	-	-	-	0	-
(a_3, a_4)	+	+	+	3	+
(a_4, a_1)	-	+	-	1	-
(a_4, a_2)	+	-	-	1	-
(a_4, a_3)	+	-	-	1	-

Крок 4.2. Визначення функцій взаємовпливу між парами елементів КП. Для визначення величини впливу пошкоджених елементів на інші елементи КП, на основі підходу запропонованого у [13], кожен експерт E_j фіксує значення функції впливу – $h_{mm'}(d_{gi})$. Визначення останньої здійснюється наступним чином: для пар ЕП $(a_m, a_{m'})$, для яких на кроці 4.1 встановлено відношення впливу $r_w = “+”$, необхідно вказати значення $h_{mm'}$, яке показує ступінь впливу на елемент $a_{m'}$, при пошкодженні елемента a_m (визначення $h_{mm'}$ проводиться відносно двох рівнів ступеня впливу *Middle damage* – “1”, та *Complete failure* – “2”). Далі отримані від всіх експертів E_j дані обробляються – в якості узгоджених оцінок функції впливу $h_{mm'}^y(d)$ для пари $(a_m, a_{m'})$ приймаються значення відповідно до (4), де $y = \overline{1, u}$. Гранична величина τ задовольняє умові $0 < \tau \leq 2$, встановлюється заздалегідь та може переглядатися у залежності від системи КП.

$$h_{mm'}(d) = \begin{cases} 1, & \text{якщо } \frac{1}{N} \sum_{y=1}^u h_{mm'}^y(d) \leq \tau, \\ 2, & \text{якщо } \tau < \frac{1}{N} \sum_{y=1}^u h_{mm'}^y(d), \quad d = 1, 2. \end{cases} \quad (4)$$

Наприклад, для системи S_{SNS} та сформованих пар, для яких встановлено відношення впливу (див. табл. 2), визначимо значення функції впливу та відобразимо їх в табл. 3 ($\tau = 1$).

Таблиця 3 – Оцінювання функцій впливу

Пара $(a_m, a_{m'})$	Результат			Узгоджена оцінка $(h_{mm'}^y(d))$
	1	2	3	
(a_1, a_2)	$h_{12}^1(1) = 2,$ $h_{12}^1(2) = 2$	$h_{12}^2(1) = 1,$ $h_{12}^2(2) = 2$	$h_{12}^3(1) = 2,$ $h_{12}^3(2) = 2$	$h_{12}^y(1) = 2,$ $h_{12}^y(2) = 2$
(a_1, a_4)	$h_{13}^1(1) = 1,$ $h_{13}^1(2) = 1$	$h_{13}^2(1) = 1,$ $h_{13}^2(2) = 2$	$h_{13}^3(1) = 1,$ $h_{13}^3(2) = 2$	$h_{13}^y(1) = 1,$ $h_{13}^y(2) = 2$
(a_2, a_1)	$h_{21}^1(1) = 0,$ $h_{21}^1(2) = 2$	$h_{21}^2(1) = 1,$ $h_{21}^2(2) = 1$	$h_{21}^3(1) = 0,$ $h_{21}^3(2) = 2$	$h_{21}^y(1) = 1,$ $h_{21}^y(2) = 2$
(a_2, a_3)	$h_{23}^1(1) = 1,$ $h_{23}^1(2) = 1$	$h_{23}^2(1) = 1,$ $h_{23}^2(2) = 1$	$h_{23}^3(1) = 1,$ $h_{23}^3(2) = 1$	$h_{23}^y(1) = 1,$ $h_{23}^y(2) = 1$
(a_2, a_4)	$h_{24}^1(1) = 1,$ $h_{24}^1(2) = 2$	$h_{24}^2(1) = 1,$ $h_{24}^2(2) = 2$	$h_{24}^3(1) = 1,$ $h_{24}^3(2) = 2$	$h_{24}^y(1) = 1,$ $h_{24}^y(2) = 2$
(a_3, a_4)	$h_{34}^1(1) = 1,$ $h_{34}^1(2) = 1$	$h_{34}^2(1) = 1,$ $h_{34}^2(2) = 1$	$h_{34}^3(1) = 1,$ $h_{34}^3(2) = 2$	$h_{34}^y(1) = 1,$ $h_{34}^y(2) = 1$

Етап 5. Графоаналітичне відображення функціональних процесів системи КП

Відображення функціональних процесів системи КП на основі підходу, описаного в [14], можна представити орієнтованим ациклічним графом (5):

$$G(\{B_{ii}\} \cup \{A_q\} \cup \{C_{ji}\}, \{P_{qq'}\}), \quad (5)$$

де вершини $A_q, (q = \overline{1, x})$ – функціональні операції, які виконує один ЕП a_m (X – загальна кількість функціональних операцій), вершини $B_{ii} (ii = \overline{1, g})$ та $C_{ji} (gi = \overline{1, w})$ вхідні та вихідні дані операцій систем відповідно (відносно даної системи, де g – загальна кількість вхідних даних, w – загальна кількість вихідних даних), а ребра $P_{qq'}$ – зв'язки між операціями $A_q, A_{q'}$, де $q = \overline{1, x}, q' = \overline{1, x}, q \neq q'$.

Наявність в графі орієнтованого ребра $P_{qq'}$, яке йде з вершини A_q до вершини $A_{q'}$, означає, що спочатку виконується операція A_q , а потім $A_{q'}$. Ребро, що йде з B_i в A_q , назване вхідним для даної системи, символізує, що на вхід операції A_q надходять дані, які є результатом виконання операції B_i . У свою чергу, ребро, що йде з A_q в C_{ji} , назване вихідним для даної системи, символізує, що на вхід операції C_{ji} надходять дані, які є результатом виконання операції A_q (див. рис. 4).

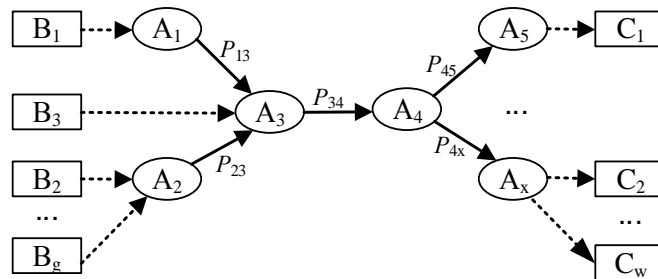


Рисунок 4 – Графоаналітичне відображення функціональних процесів системи КІІ

Таке представлення дозволяє відобразити у зручному вигляді формалізований опис функціональних етапів операцій та зв'язків між ними, а також відповідні вхідні та вихідні дані. Наприклад, для досліджуваної системи, згідно [16], при $x = 4$, $g = 2$, $w = 2$, відобразимо схему функціонального процесу за допомогою графу (5), в якому вершини A_q відповідають функціональним операціям (A_1 – супутниковий сегмент, A_2 – сегмент контролю та спостереження, A_3 – додатковий сегмент, A_4 – сегмент користувача), вершини B_1, B_2, C_1, C_2 – відповідають вхідним та вихідним даним операцій A_q , а ребра $P_{12}, P_{14}, P_{21}, P_{23}, P_{24}, P_{34}$ – зв'язкам між елементами $A_q, A_{q'}$, встановленими на кроці 4.1, (див. рис. 5).

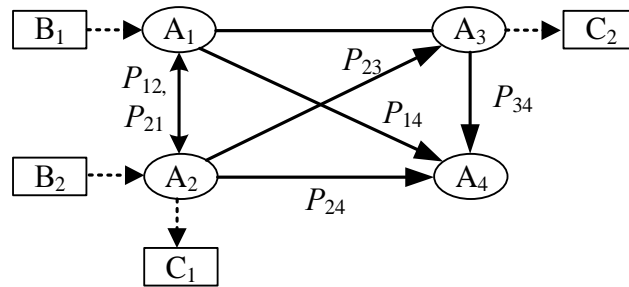


Рисунок 5 – Графоаналітичне відображення функціональних процесів системи S_{SNS}

Етап 6. Оцінювання якості функціонування системи КІІ

Наслідком впливу на ЕІІ може бути зниження якості виконання функціональних операцій. Для оцінювання значення якості виконання функціональних операцій $Q(A_q)$ вводиться така лінгвістична шкала: *Normal* – “0” (операція виконується у відповідності з функціональним регламентом); *Deviation* – “1” (операція виконується, але спостерігаються суттєві відхилення від функціонального регламенту); *Interruption* – “2” (операція не виконується).

Матриця впливу $Q_d^q(d(a_m))$ відображає виконання функціональної операції A_q за умови, що ЕІІ a_m має відповідне пошкодження $d(a_m)$ та формується послідовно кожним експертом E_j для всіх ЕІІ та їх відповідних операцій, де верхній індекс виразу Q_d^q відповідає номеру операції, а нижній значенню пошкодження $d \in \{0,1,2\}$.

Далі відбувається обробка даних, отриманих від кожного експерта E_j , у якості узгодженої оцінки виконання функціональної операції приймається значення згідно (6), де порогові значення s_0, s_1 задовольняють умові $0 < s_0 < s_1 \leq 2$ (встановлюються керівником відповідної галузі інфраструктури та експертами заздалегідь і можуть переглядатися в залежності від системи КІІ).

$$Q(A_q) = \begin{cases} 0, \text{ якщо } \frac{1}{N_{q,d,m}} \sum Q_d^q(d(a_m)) \leq s_0; \\ 1, \text{ якщо } s_0 < \frac{1}{N_{q,d,m}} \sum Q_d^q(d(a_m)) \leq s_1; \\ 2, \text{ якщо } s_1 < \frac{1}{N_{q,d,m}} \sum Q_d^q(d(a_m)). \end{cases} \quad (6)$$

Ранжування узгоджених за всіма E_j якостей функціонування системи КІІ відбувається шляхом порівняння кількісних значень отриманих в матриці впливу. Сума кількісних показників якості $Q(A_q)$, одержаних для одного ЕІ a_m , порівнюється з сумою кількісних показників якості $Q(A_q)$, одержаних для інших ЕІ та ранжується наступним чином: $\{VEI_1 > VEI_2 > \dots > VEI_o\}$, де множина $VEI = \{\bigcup_{li=1}^o VEI_{li}\} = \{VEI_1, VEI_2, \dots, VEI_o\}$, $VEI_{li} \subseteq VEI$, $(li = \overline{1, o})$ – ранжовані за порядком важливості для системи ЕІ, o – номер за порядком ранжованих ЕІ відносно суми показників якості (слід зазначити, що кількість $o = b$).

Наприклад, для системи S_{SNS} згідно (6), побудуємо узгоджену матрицю впливу всіх ЕІ на всі функціональні операції системи, відображену у табл. 4 (значення величин $q_0 = 0,5, q_1 = 1,5$).

Таблиця 4 – Матриця впливу елементів КІІ на функціональні операції

Операція (A_q)	Шкала ступенів пошкодження елементів a_m		
	$d(a_1)=0$	$d(a_1)=1$	$d(a_1)=2$
A_1	0	2	2
A_2	0	1	2
A_3	0	1	2
A_4	0	1	1
	$d(a_2)=0$	$d(a_2)=1$	$d(a_2)=2$
A_1	0	1	2
A_2	0	2	2
A_3	0	1	2
A_4	0	1	1
	$d(a_3)=0$	$d(a_3)=1$	$d(a_3)=2$
A_1	0	0	1
A_2	0	0	1
A_3	0	1	2
A_4	0	1	2
	$d(a_4)=0$	$d(a_4)=1$	$d(a_4)=2$
A_1	0	0	1
A_2	0	1	1
A_3	0	0	1
A_4	0	1	2

Наприклад, для системи S_{SNS} , згідно табл. 4, при $b=o=4$, множина ранжованих за порядком важливості для системи ЕП має вигляд: $VEI_{SNS} = \{a_1, a_2, a_3, a_4\}$, де a_1 – ШСЗ, a_2 – контрольно-спостережна станція, a_3 – додаткова станція, a_4 – приймачі.

Для експериментального дослідження розроблено спеціальний програмний застосунок (див. рис. 6), який дає змогу ідентифікувати об’єкти КІ певної галузі та визначити їх вплив на функціональні операції.

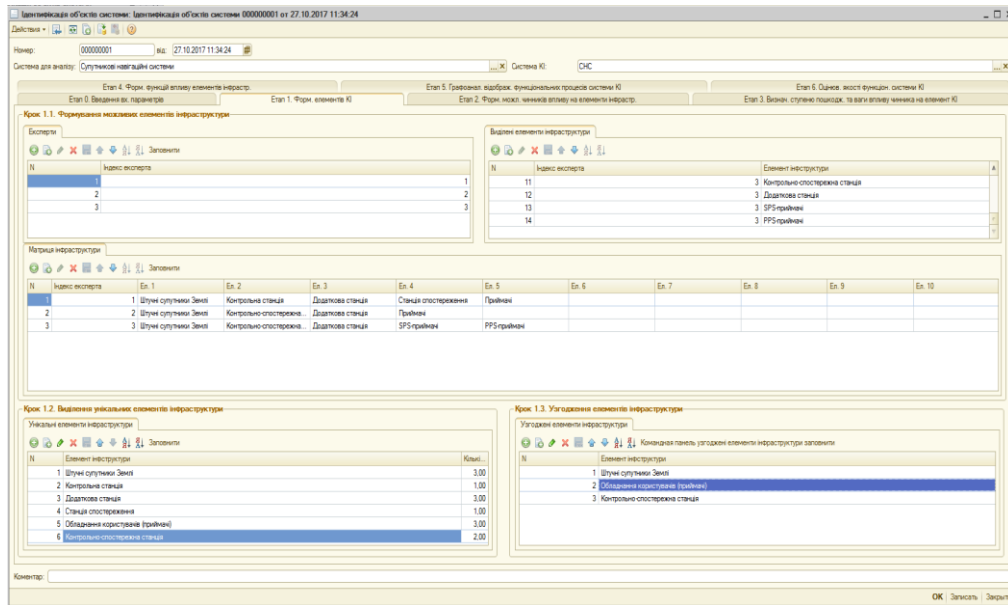


Рисунок 6 – Фрагмент вікна розробленого програмного застосунку

Для оцінювання адекватності запропонованого методу проводилась перевірка його реагування на зміну вхідних даних. Для досліджуваної системи S_{SNS} змінювалась (зменшувалась та збільшувалась) кількість ЕП та елементів КІ.

Таблиця 5 – Результати експериментального дослідження методу ідентифікації об’єктів КІ

Експеримент 1		Експеримент 2																																																																																																									
$a_{SNS} = \{\bigcup_{i=1}^3 a_i\} = \{a_1, a_2, a_3\}$		$a_{SNS} = \{\bigcup_{i=1}^6 a_i\} = \{a_1, a_2, \dots, a_6\}$																																																																																																									
$\Phi_{SNS} = \{\bigcup_{di=1}^7 \Phi_{di}\} = \{\Phi_1, \Phi_2, \dots, \Phi_7\}$																																																																																																											
<table border="1"> <thead> <tr> <th></th> <th>Φ_1</th> <th>Φ_2</th> <th>Φ_3</th> <th>Φ_4</th> <th>Φ_5</th> <th>Φ_6</th> <th>Φ_7</th> </tr> </thead> <tbody> <tr> <th>d_1</th> <td>φ_1</td> <td>d_2</td> <td>φ_2</td> <td>d_3</td> <td>φ_3</td> <td>d_4</td> <td>φ_4</td> </tr> <tr> <th>a_1</th> <td>1</td> <td>0,2</td> <td>1</td> <td>0,1</td> <td>0</td> <td>0,1</td> <td>1</td> </tr> <tr> <th>a_2</th> <td>1</td> <td>0,2</td> <td>1</td> <td>0,2</td> <td>1</td> <td>0,2</td> <td>1</td> </tr> <tr> <th>a_3</th> <td>1</td> <td>0,2</td> <td>0</td> <td>0,1</td> <td>0</td> <td>0,1</td> <td>0</td> </tr> </tbody> </table>			Φ_1	Φ_2	Φ_3	Φ_4	Φ_5	Φ_6	Φ_7	d_1	φ_1	d_2	φ_2	d_3	φ_3	d_4	φ_4	a_1	1	0,2	1	0,1	0	0,1	1	a_2	1	0,2	1	0,2	1	0,2	1	a_3	1	0,2	0	0,1	0	0,1	0	<table border="1"> <thead> <tr> <th></th> <th>Φ_1</th> <th>Φ_2</th> <th>Φ_3</th> <th>Φ_4</th> <th>Φ_5</th> <th>Φ_6</th> <th>Φ_7</th> </tr> </thead> <tbody> <tr> <th>d_1</th> <td>φ_1</td> <td>d_2</td> <td>φ_2</td> <td>d_3</td> <td>φ_3</td> <td>d_4</td> <td>φ_4</td> </tr> <tr> <th>a_1</th> <td>1</td> <td>0,2</td> <td>1</td> <td>0,1</td> <td>0</td> <td>0,1</td> <td>1</td> </tr> <tr> <th>a_2</th> <td>1</td> <td>0,2</td> <td>1</td> <td>0,2</td> <td>1</td> <td>0,2</td> <td>1</td> </tr> <tr> <th>a_3</th> <td>1</td> <td>0,1</td> <td>0</td> <td>0,1</td> <td>0</td> <td>0,1</td> <td>0</td> </tr> <tr> <th>a_4</th> <td>1</td> <td>0,2</td> <td>1</td> <td>0,2</td> <td>1</td> <td>0,2</td> <td>1</td> </tr> <tr> <th>a_5</th> <td>1</td> <td>0,1</td> <td>0</td> <td>0,1</td> <td>1</td> <td>0,1</td> <td>0</td> </tr> <tr> <th>a_6</th> <td>1</td> <td>0,2</td> <td>0</td> <td>0,1</td> <td>0</td> <td>0,1</td> <td>0</td> </tr> </tbody> </table>			Φ_1	Φ_2	Φ_3	Φ_4	Φ_5	Φ_6	Φ_7	d_1	φ_1	d_2	φ_2	d_3	φ_3	d_4	φ_4	a_1	1	0,2	1	0,1	0	0,1	1	a_2	1	0,2	1	0,2	1	0,2	1	a_3	1	0,1	0	0,1	0	0,1	0	a_4	1	0,2	1	0,2	1	0,2	1	a_5	1	0,1	0	0,1	1	0,1	0	a_6	1	0,2	0	0,1	0	0,1	0
	Φ_1	Φ_2	Φ_3	Φ_4	Φ_5	Φ_6	Φ_7																																																																																																				
d_1	φ_1	d_2	φ_2	d_3	φ_3	d_4	φ_4																																																																																																				
a_1	1	0,2	1	0,1	0	0,1	1																																																																																																				
a_2	1	0,2	1	0,2	1	0,2	1																																																																																																				
a_3	1	0,2	0	0,1	0	0,1	0																																																																																																				
	Φ_1	Φ_2	Φ_3	Φ_4	Φ_5	Φ_6	Φ_7																																																																																																				
d_1	φ_1	d_2	φ_2	d_3	φ_3	d_4	φ_4																																																																																																				
a_1	1	0,2	1	0,1	0	0,1	1																																																																																																				
a_2	1	0,2	1	0,2	1	0,2	1																																																																																																				
a_3	1	0,1	0	0,1	0	0,1	0																																																																																																				
a_4	1	0,2	1	0,2	1	0,2	1																																																																																																				
a_5	1	0,1	0	0,1	1	0,1	0																																																																																																				
a_6	1	0,2	0	0,1	0	0,1	0																																																																																																				

Продовження таблиці 5

Пара $(a_m, a_{m'})$	Результат			Узгоджена оцінка $(h_{m'}^y(d))$
	1	2	3	
(a_1, a_2)	$h_{12}^1(1)=2, h_{12}^1(2)=2$	$h_{12}^2(1)=1, h_{12}^2(2)=2$	$h_{12}^3(1)=2, h_{12}^3(2)=2$	$h_{12}^y(1)=2, h_{12}^y(2)=2$
(a_1, a_3)	$h_{13}^1(1)=1, h_{13}^1(2)=1$	$h_{13}^2(1)=1, h_{13}^2(2)=2$	$h_{13}^3(1)=1, h_{13}^3(2)=2$	$h_{13}^y(1)=1, h_{13}^y(2)=2$
(a_2, a_1)	$h_{21}^1(1)=0, h_{21}^1(2)=2$	$h_{21}^2(1)=1, h_{21}^2(2)=1$	$h_{21}^3(1)=0, h_{21}^3(2)=2$	$h_{21}^y(1)=1, h_{21}^y(2)=2$
(a_2, a_3)	$h_{23}^1(1)=1, h_{23}^1(2)=2$	$h_{23}^2(1)=1, h_{23}^2(2)=1$	$h_{23}^3(1)=1, h_{23}^3(2)=2$	$h_{23}^y(1)=1, h_{23}^y(2)=2$

Пара $(a_m, a_{m'})$	Результат			Узгоджена оцінка $(h_{m'}^y(d))$
	1	2	3	
(a_1, a_2)	$h_{12}^1(1)=2, h_{12}^1(2)=2$	$h_{12}^2(1)=1, h_{12}^2(2)=2$	$h_{12}^3(1)=2, h_{12}^3(2)=2$	$h_{12}^y(1)=2, h_{12}^y(2)=2$
(a_1, a_3)	$h_{13}^1(1)=2, h_{13}^1(2)=2$	$h_{13}^2(1)=2, h_{13}^2(2)=2$	$h_{13}^3(1)=2, h_{13}^3(2)=2$	$h_{13}^y(1)=2, h_{13}^y(2)=2$
(a_1, a_4)	$h_{14}^1(1)=1, h_{14}^1(2)=2$	$h_{14}^2(1)=1, h_{14}^2(2)=2$	$h_{14}^3(1)=1, h_{14}^3(2)=2$	$h_{14}^y(1)=1, h_{14}^y(2)=2$
(a_1, a_5)	$h_{15}^1(1)=2, h_{15}^1(2)=2$	$h_{15}^2(1)=2, h_{15}^2(2)=2$	$h_{15}^3(1)=2, h_{15}^3(2)=2$	$h_{15}^y(1)=2, h_{15}^y(2)=2$

Операція	Шкала ступенів пошкодження елементів a_m		
	$d(a_1)=0$	$d(a_1)=1$	$d(a_1)=2$
A_1	0	1	2
A_2	0	1	2
A_3	0	1	1
	$d(a_2)=0$	$d(a_2)=1$	$d(a_2)=2$
A_4	0	1	1
A_2	0	2	2
A_3	0	1	2

Операція	Шкала ступенів пошкодження елементів a_m		
	$d(a_1)=0$	$d(a_1)=1$	$d(a_1)=2$
A_1	0	1	2
A_2	0	1	2
A_3	0	1	1
A_4	0	1	2
A_5	0	1	1
A_6	0	1	1
	$d(a_2)=0$	$d(a_2)=1$	$d(a_2)=2$
A_1	0	1	2
A_2	0	2	2
A_3	0	1	2

$VEI_{SNS} = \{a_2, a_1, a_3\}$

$VEI_{SNS} = \{a_2, a_4, a_1, a_5, a_6, a_3\}$

Як видно з табл. 5 зміна вхідних даних призвела до відповідної зміни вихідних даних (множин ідентифікованих елементів КІІ; таблиць ступенів пошкодження та ваг впливу елементів КІІ для кожного чинника впливу; перелік пар елементів КІІ для яких встановлено відношення впливу та їх обраховані значення функції впливу; граfi функціональних процесів систем КІІ; матриці впливу елементів КІІ на їх функціональні операції та перелік ранжованих за порядком важливості елементів КІІ), що свідчить про коректну роботу розробленого методу.

Висновки. Таким чином, у статті розроблено метод ідентифікації, який за рахунок графоаналітичного відображення елементів критичної інфраструктури і їх функціональних процесів, формування можливих чинників і функцій впливу, а також матриці впливу елементів інфраструктури на функціональні операції, дає можливість визначити (ідентифікувати) елементи галузі критичної інфраструктури, їх взаємовплив та вплив на функціональні операції критичної авіаційної інформаційної системи. Крім того, розроблено програмний застосунок, який може бути використаний для ідентифікації об'єктів КІІ різних галузей.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

- [1] С. Гнатюк, М. Рябий, та В. Лядовська, “Визначення критичної інформаційної інфраструктури та її захист: аналіз підходів”, *Зв'язок*, №4, с. 3-7, 2014.
- [2] A. Wenger, V. Mauer, and M. Cavelti, ”International critical information infrastructure protection handbook 2008-2009”, *Center for Security Studies*, ETH Zurich, 2009.
- [3] С. Гнатюк, та В. Лядовська, ”Критерії визначення елементів критичної інфраструктури держави”, на *XXIII всеукр. наук.-практ. конф. Інноваційний потенціал світової науки – XXI сторіччя*. Запоріжжя, с. 55-57, 2013.
- [4] Green paper on a European programme for critical infrastructure protection (COM/2005/576 final). [Online]. Available: http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf. Accessed on: Sept. 03, 2017.
- [5] R. Mattioli, and C. Levy-Bencheton, “Methodologies for the identification of Critical Information Infrastructure assets and services”, *ENISA Report*, 2014.
- [6] А. Кондратьев, ”Современные тенденции в исследовании критической инфраструктуры в зарубежных странах”, *Зарубежное военное обозрение*, № 1, с. 19-30, 2012.
- [7] В. Сидоренко, М. Александер, та А. Наджі, “Сучасні підходи до визначення та ідентифікації критичної інформаційної інфраструктури”, на *Наук.-практ. конф. Актуальні питання забезпечення кібернетичної безпеки та захисту інформації*, м. Київ, 2016, с.134-137.
- [8] О. Довгань, ”Критична інфраструктура як об’єкт захисту від кібернетичних атак”, на *Наук.-практ. конф. Інформаційна безпека: виклики і загрози сучасності*. Київ, 2013, с. 17-20.
- [9] Кабінет міністрів України. (2016, Серп. 23). *Постанова № 563 про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави*. [Електронний ресурс]. Доступно: <http://zakon3.rada.gov.ua/laws/show/563-2016-%D0%BF>. Дата звернення: Лип. 12, 2017.
- [10] С. Гнатюк, В. Сидоренко, та О. Дуксенко, “Сучасні підходи до виявлення та ідентифікації найбільш важливих об’єктів критичної інфраструктури”, *Безпека інформації*, т. 21, № 3, с. 269-275, 2015.
doi: 10.18372/2225-5036.21.9690.
- [11] International Civil Aviation Organization. *Doc 8973 ICAO. Aviation Security Manual*, 2014.
- [12] С. Гнатюк, В. Сидоренко, та Н. Сейлова, ”Універсальна модель даних для формування переліку об’єктів критичної інформаційної інфраструктури держави”, *Безпека інформації*, т. 23, № 2, с. 80-91, 2017.
doi: 10.18372/2225-5036.23.11823.
- [13] В. Шершаков, Э. Трахтенгерц, и Д. Камаев, *Сетецентрические методы компьютерной поддержки управления ликвидацией последствий чрезвычайных ситуаций*. Москва, Российская Федерация: URSS, 2015.
- [14] А. Андреев, Д. Камаев, и Э. Трахтенгерц, “Экспертное прогнозирование последствий повреждения систем жизнеобеспечения”, *Управление Большими Системами*, вып. 25, с. 243-293, 2009.
- [15] Ю. Соловьев, *Системы спутниковой навигации*. Москва, Российская Федерация: Эко-Трендз, 2000.
- [16] О. Голуб, та С. Шеремет, “Спутникові системи навігації на транспорті», *Електронний підручник*”. [Електронний ресурс]. Доступно: http://www.shevchenkove.org.ua/person_syte. Дата звернення: Верес. 03, 2017.
- [17] І. Сновидов, “Фактори, що впливають на точність промірювань”, *Вісник держгідрографії*, № 1 (48), с. 4-6, 2015.
- [18] Я. Максименко, “Дослідження службових параметрів наземних та бортових приймачів з використанням системи GPS”. [Електронний ресурс]. Доступно: http://kivra.kpi.ua/wp-content/uploads/file/work/2015/Maksimenko/Maksimenko_PZ.pdf. Дата звернення: Верес. 03, 2017.

- [19] M. Tavallae, E. Bagheri, W. Lu, and A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set", in *Submitted to Second IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA)*, Ottawa, 2009, pp. 1-6.
doi: 10.1109/CISDA.2009.5356528.

Стаття надійшла до редакції 09 вересня 2017 року.

REFERENCES

- [1] S. Gnatyuk, M. Ryabiy, and V. Lyadovskaya, "Definition of critical information infrastructure and its protection: analysis of approaches", *Communication*, no. 4, pp. 3-7, 2014.
- [2] A. Wenger, V. Mauer, and M. Cavelt, "International critical information infrastructure protection handbook 2008-2009", *Center for Security Studies*, ETH Zurich, 2009.
- [3] S. Gnatyuk, and V. Lyadovskaya, "Criteria for determining the elements of the critical infrastructure of the state", in *Proc. XXIII Ukr. sci. and prac. conf. Innovative potential of world science – XXI century*", Zaporizhzhia, pp. 55-57, 2013.
- [4] Green paper on a European programme for critical infrastructure protection (COM/2005/576 final). [Online]. Available: http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf. Accessed on: Sept. 03, 2017.
- [5] R. Mattioli, and C. Levy-Bencheton, "Methodologies for the identification of Critical Information Infrastructure assets and services", *ENISA Report*, 2014.
- [6] A. Kondratiev, "Modern trends in the study of critical infrastructure in foreign countries", *Foreign Military Review*, no. 1, pp. 19-30, 2012.
- [7] V. Sydorenko, M. Alexander, and A. Naji, "Modern approaches to the definition and identification of critical information infrastructure", in *Proc. Sci. and prac. conf. Current issues of cyber security and information security*, Kyiv, 2016, pp.134-137.
- [8] O. Dovgan, "Critical infrastructure as an object of protection against cyber attacks", *Proc. Sci. and prac. conf. Information security: the challenges and threats of our time*, Kyiv, 2013, pp. 17-20.
- [9] Cabinet of Ministers of Ukraine. (2016, Aug. 23). Resolution № 563 on approval of the procedure for the formation of the list of information and telecommunication systems of critical infrastructure objects of the state. [Online]. Available: <http://zakon3.rada.gov.ua/laws/show/563-2016-%D0%BF>. Accessed on: July 12, 2017.
- [10] S. Gnatyuk, V. Sydorenko, and O. Duksenko, "Modern approaches to critical infrastructure objects detection and identification", *Information security*, vol. 21, no. 3, pp. 269-275, 2015.
doi: 10.18372/2225-5036.21.9690.
- [11] International Civil Aviation Organization. *Doc 8973 ICAO. Aviation Security Manual*, 2014.
- [12] S. Gnatyuk, V. Sydorenko, and N. Seilova, "Universal data model for the formation of the critical information infrastructure of the state objects list", *Information security*, vol. 23, no. 2, pp. 80-91, 2017.
doi: 10.18372/2225-5036.23.11823.
- [13] V. Shershakov, E. Trahtengerts, and D. Kamaev, *Network-centric methods of computer support for the management of emergency response*. Moscow, Russia: URSS, 2015.
- [14] A. Andreev, D. Kamaev, and E. Trahtengerts, "Expert forecasting of the consequences of damage to life support systems", *Management of large systems*, iss. 25, pp. 243-293, 2009.
- [15] Y. Soloviev, *Satellite navigation systems*, Moscow, Russia: Eco-Trendz, 2000.
- [16] O. Golub, and S. Sheremet, "Satellite navigation systems in transport". [Online]. Available: http://www.shevchenkove.org.ua/person_syte. Accessed on: Sept. 03, 2017.
- [17] I. Snovidov, "Factors affecting measurement accuracy", *Bulletin of the state hydrography*, no. 1 (48), pp. 4-6, 2015.
- [18] Y. Maksimenko, "Investigation of the parameters of ground and on board receivers using the GPS system". [Online]. Available: http://kivra.kpi.ua/wp-content/uploads/file/work/2015/Maksimenko/Maksimenko_PZ.pdf. Accessed on: Sept. 03, 2017.
- [19] M. Tavallae, E. Bagheri, W. Lu, and A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set", in *IEEE Symposium on Computational Intelligence for Security and Defense Applications*, Ottawa, 2009, pp. 1-6.
doi: 10.1109/CISDA.2009.5356528.

СЕРГЕЙ ГНАТЮК,
ВИКТОРИЯ СИДОРЕНКО,
ВАСИЛИЙ КИНЗЕРЯВЫЙ

МЕТОД ИДЕНТИФИКАЦИИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В АВИАЦИОННОЙ ОТРАСЛИ

В последнее время в мире наблюдается тенденция к увеличению количества чрезвычайных событий различного рода. Ежедневно мировые СМИ сообщают о природных и техногенных катастрофах, вооруженных конфликтах, террористических актах, тяжких преступлениях, актах пиратства, совершенных как преступными организациями, так и отдельными лицами. Все чаще в результате таких событий жертвами становятся большое количество людей и наносится вред жизненно важным для существования государств системам, объектам и ресурсам. Среди последних особого внимания требует отрасль гражданской авиации, так как существует необходимость в обеспечении непрерывной коммуникации и взаимодействии между наземными системами и воздушными судами. Большинство ведущих государств мира стали уделять значительное внимание методам и средствам идентификации, систематизации и обеспечения безопасности объектов критической инфраструктуры, потеря или нарушение нормального функционирования которых приведет к существенным или даже непоправимым негативным последствиям для национальной безопасности государства. Однако, по результатам проведенного анализа установлено, что существующие подходы к выявлению и идентификации объектов инфраструктуры не являются системными и четко формализованными, ориентированные только на определенные области инфраструктуры и не учитывают полного множества параметров и особенностей критической инфраструктуры особенно ее информационной составляющей. Беря во внимание это, в работе разработан метод идентификации объектов критической информационной инфраструктуры, который дает возможность определить элементы критической инфраструктуры, их взаимовлияние и влияние на функциональные операции критической авиационной информационной системы. Этот метод, а также разработанное на его основе программное обеспечение, могут использоваться на практике для идентификации объектов критической информационной инфраструктуры различных отраслей.

Ключевые слова: критическая инфраструктура, критическая информационная инфраструктура, идентификация объектов критической информационной инфраструктуры, критические авиационные информационные системы, гражданская авиация.

SERHII HNATIUK,
VIKTORIA SYDORENKO,
VASYL KINZERIAVYI

METHOD OF OBJECT IDENTIFICATION OF CRITICAL INFORMATION INFRASTRUCTURE IN AVIATION INDUSTRY

In recent times all over the world the number of different emergency situations was increased. Every day mass media informs about natural and man-caused disasters, weapon conflicts, acts of terrorism, global crimes, acts of piracy that were committed by both crime organizations and single offenders. Increasingly frequently as a result of these events many people fall a victim and also state critical importance systems and resources can be damaged. According that, civil aviation industry requires special attention, just as there is need for continuous communication and interconnection between ground-based and aircrafts systems. Most of the world's leading states began to devote considerable attention to the methods and means of identifying, systematizing and securing critical infrastructure objects. Loss or operational breakdown of these objects can cause significant or irreparably damage for national security of the state. However, according to the analysis, the existing approaches to identifying and identifying infrastructure objects are not systemic and clearly formalized, are oriented only to certain sectors of the infrastructure and do not take into account the full range of parameters and features of the critical infrastructure, especially its information

component. In view of this, in this work a method of object identification of critical information infrastructure is developed, which gives ability to determine the critical infrastructure elements, their mutual influence and influence on functional operations of the critical aviation information system. This method, as well as a software application developed on its basis, can be used for identification the objects of critical information infrastructure in different industries.

Keywords: critical infrastructure, critical information infrastructure, critical aviation information systems, object identification of critical information infrastructure, civil aviation.

Сергій Олександрович Гнатюк, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій, Національний авіаційний університет, Київ, Україна.

E-mail: S.Gnatyuk@nau.edu.ua.

Вікторія Миколаївна Сидоренко, асистент кафедри безпеки інформаційних технологій, Національний авіаційний університет, Київ, Україна.

E-mail: v.sydorenko@ukr.net.

Василь Миколайович Кінзерявий, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій, Національний авіаційний університет, Київ, Україна.

E-mail: V.Kinzeryavyu@gmail.com.

Сергей Александрович Гнатюк, кандидат технических наук, доцент, доцент кафедры безопасности информационных технологий, Национальный авиационный университет, Киев, Украина.

Виктория Николаевна Сидоренко, ассистент кафедры безопасности информационных технологий, Национальный авиационный университет, Киев, Украина.

Василий Николаевич Кинзерявий, кандидат технических наук, доцент, доцент кафедры безопасности информационных технологий, Национальный авиационный университет, Киев, Украина.

Serhii Hnatiuk, candidate of technical sciences, associate professor, associate professor of IT-security academic department, National Aviation University, Kyiv, Ukraine.

Viktoriia Sydorenko, assistant of IT-security academic department, National Aviation University, Kyiv, Ukraine.

Vasyl Kinzeriavyyi, candidate of technical sciences, associate professor, associate professor of IT-security academic department, National Aviation University, Kyiv, Ukraine.

УДК 004.056.53:621.391

ГОР ЯКОВІВ

ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА, КОНЦЕПТУАЛЬНА МОДЕЛЬ КІБЕРПРОСТОРУ І КІБЕРБЕЗПЕКА

Семантичні невизначеності між базовими поняттями у галузі кібербезпеки значно звужують діапазон і знижують результативність наукових досліджень щодо методів аналізу і прогнозування, наприклад, АРТ кібератак або розробки комплексів захисту на основі формальних моделей доказу їх ефективності. Напрямок можливого подолання проблеми – розробка концептуальної моделі кіберпростору і кібербезпеки, що дозволяє знижувати рівень можливих невизначень при описі різноманітних складних ситуацій у кіберпросторі завдяки застосуванню спеціальних інструментів термінологічної, графічної і математичної формалізації. Початок досліджень – обране твердження: фізичну основу кіберпростору складають інформаційно-телекомунікаційні системи (ІТС). Аналіз інформаційних процесів

© І. Яковів, 2017