ISSN 2521-6643

Системи та технології

№ 2 (56/1) 2018

Системи та технології

(правонаступник наукового журналу "Вісник Академії митної служби України. Серія: "Технічні науки")

№ 2 (56/1)

Науковий журнал включено до Переліку наукових фахових видань України, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів з галузі "Технічні науки" (наказ Міністерства освіти і науки України від 04.04.2018 р. № 326, додаток 9)

Дніпро
Університет митної справи та фінансів
2018

УДК 62

Системи та технології
(правонаступник наукового журналу
“Вісник Академії митної служби України. Серія: “Технічні науки”)
Науковий журнал
Видається двічі на рік
Заснований у травні 1999 р.

Рекомендовано до друку та до поширення через мережу Інтернет вченою радою Університету митної справи та фінансів (протокол № 6 від 26.11.2018 р.)

DOI: https://doi.org/10.32836/2521-6643-2018-2-56
ISSN 2521-6643

Коректори: Л. І. Малигіна, О. О. Смирнова, І. В. Орищій
Комп’ютерна верстка: О. О. Іщенко, Т. Г. Пунтус

Свідоцтво про державну реєстрацію: серія КВ № 21857-11757ПР від 21.12.2015 р.
Тираж 300 прим. Замовлення № 63.

Адреса редакції та видавця: вул. Володимира Вернадського, 2/4, Дніпро, 49000
Тел.: (056) 756-05-05. Електронна адреса: redactor.umsf@gmail.com

Підписано до друку 30.12.2018. Формат 60×84/16. Папір офсетний.
Гарнітура Таймс. Ум. друк. арк. 15,00. Обл.-вид. арк. 13,33.

Засновник і видавець: Університет митної справи та фінансів
(Свідоцтво про видавничу діяльність ДК № 6198 від 24.05.2018 р.)

ЗМІСТ

CONTENTS

DOI: https://doi.org/10.32836/2521-6643-2018.2-56.1
УДК 629.7.014-519.064.5-022.332:621.311.25-047.36

Г. В. Фесенко, кандидат технічних наук, доцент кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського "Харківський авіаційний інститут"
І. М. Клюшніков, кандидат технічних наук, провідний науковий співробітник наукового центру Повітряних сил Харківського національного університету Повітряних сил ім. І. Кожедуба

ВИКОРИСТАННЯ АЛГОРИТМУ РОЗФАРБОВУВАННЯ ГРАФА ДЛЯ ВИЗНАЧЕННЯ ПОРЯДКУ ЗБИРАННЯ ДАНИХ РАДІАЦІЙНОГО МОНІТОРИНГУ З ТОЧОК "РАНДЕВУ" БЕЗПРОВОДНОЇ ЛІТАЛЬНОЇ МЕРЕЖІ

Присвячено використанню жадібного алгоритму розфарбовування графа для визначення кількості й порядку застосування БПЛА літакового типу (ЛБПЛА) для збирання інформації від точок "рандеву" літальної безпроводної мережі на основі БПЛА (БПЛА-БМ) під час післяаварійного моніторингу Запорізької АЕС (ЗАЕС). Запропонована спрощена схема розгортання БПЛА-БМ для організації передачі даних від постів контролю автоматизованої системи контролю радіаційної обстановки (АСКРО) до кризового центру під час післяаварійного моніторингу АЕС. Розроблено та описано схему розгортання підсистем БПЛА-БМ для організації передачі даних між чотирма постами контролю АСКРО ЗАЕС і точками "рандеву" у випадку пошкодження проводних каналів зв'язку. Використовуючи побудований на бітових операціях над матрицею суміжності жадібний алгоритм розфарбовування графа, визначено, що для збирання даних від чотирьох постів контролю АСКРО ЗАЕС необхідно використовувати три ЛБПЛА

Ключові слова: *безпілотний літальний апарат; алгоритм розфарбовування графа; атомна електростанція; безпровідна мережа; wi-fi; LoRaWAN; післяаварійний моніторинг; пост контролю; кризовий центр*.

Посвящено использованию жадного алгоритма раскраски графа для определения количества и порядка применения БПЛА самолетного типа (ЛБПЛА) для сбора информации от точек "рандеву" летающей беспроводной сети на основе БПЛА (БПЛА-БС) во время послеаварийного мониторинга Запорожской АЭС (ЗАЭС). Предложена упрощенная схема развертывания БПЛА-БС для организации передачи данных от постов контроля автоматизированной системы контроля радиационной обстановки (АСКРО) в кризисный центр в ходе послеаварийного мониторинга АЭС. Разработана и описана схема развертывания подсистем БПЛА-БС для организации передачи данных между четырьмя постами контроля АСКРО ЗАЭС и точками "рандеву" в случае повреждения проводных каналов связи. Используя построенный на битных операциях над матрицей смежности жадный алгоритм раскраски графа, определено, что для сбора данных от четырех постов контроля АСКРО ЗАЭС необходимо использовать три ЛБПЛА.

Ключевые слова: *беспилотный летательный аппарат; алгоритм раскраски графа; атомная электростанция; беспроводная сеть; Wi-Fi; LoRaWAN; послеаварийный мониторинг; пост контроля; кризисный центр*.

Wired networks, connecting monitoring stations (MS) of the automated radiation monitoring system (ARMS) to the crisis centre (CrS), can be damaged as a result of an NPP accident. To cope with the problem, an unmanned aerial vehicle (UAV)-enabled wireless network (UEWN), can be deployed. The aim of the paper is to develop an approach based on a graph coloring algorithm to determine the number of UAVs of an airplane-type and define the order of their use for gathering data from rendezvous points of a deployed UEWN during Zaporizhzhia NPP (ZNPP) post-accident monitoring missions. The existing graph coloring algorithms are analyzed and presented as a table. For later use, the greedy graph coloring algorithm based on bitwise operations on the adjacency matrix is selected. A simplified scheme of deployment of a UEWN for transmitting the data from the MS to the CrS during NPP post-accident monitoring missions was developed and described. Two segments within the UEWN were considered:

1) Wi-Fi segment, comprising the WiFi equipment of the MS, the onboard WiFi equipment of the UAVs of a multi-rotor type (MUAVs), and onboard WiFi equipment of the UAV of an airplane-type (AUAV); 2) LoRaWAN segment, comprising the LoRaWAN equipment of the AUAV and the LoRaWAN equipment of the CrS. A scheme of UEWN subsystems deployment for the organization of data transfer between four monitoring stations of ARMS for ZNPP and rendezvous points in case of loss of wired networks. Using the selected graph coloring algorithm, it has been determined that three AUAVs are required for gathering and transmitting the data from four MSs to the CrS. Further studies should focus on investigating the effect of the location of the automatic battery replacement stations and their features on the UEWN's functioning.

Key words: *unmanned aerial vehicle; graph coloring algorithm, nuclear power plant; wireless network; WiFi; LoRaWAN; post-accident monitoring; monitoring station; crisis centre.*

Постановка проблеми. Для здійснення безперервного контролю радіаційної обстановки (РО) на проммайданчику АЕС, у санітарно-захисній зоні та зоні спостереження в усіх режимах експлуатації АЕС в обсязі, достатньому для оперативного висновку про відповідність/невідповідність РО вимогам нормативних документів, що визначають заходи та порядок забезпечення радіаційної безпеки на АЕС, створюється автоматизована система контролю радіаційної обстановки (АСКРО). Використання АСКРО дозволяє підвищити рівень контролю радіаційних параметрів АЕС шляхом автоматизації процесів вимірювання, збиання, обробки, візуалізації, архівування та зберігання інформації про параметри РО. Основними елементами такої системи виступають пости контролю (ПК). Під час виникнення аварії на майданчику (надзвичайної ситуації (НС) на місцевому або регіональному рівні) або комунальної аварії (НС на регіональному або державному рівні) ПК мають забезпечувати зовнішній кризовий центр (КЦ) необхідною інформацією щодо РО за допомогою проводних каналів зв'язку. Однак такі канали можуть бути пошкоджені внаслідок аварій, що потребуватиме пошуку альтернативних шляхів передачі інформації до КЦ. Одним з них може бути розгортання безпроводної мережі на базі БПЛА (БПЛА-БМ) [1–3]. У разі створення такої мережі виникає необхідність організації збирання даних про РО від БПЛА, що є точками "рандеву" (ТР).

Аналіз останніх досліджень і публікацій. Уявімо, що ТР можуть передавати інформацію тільки в окремі часові інтервали. В цьому випадку найбільш цікавим є підхід, що запропонований у [4]. Він передбачає використання алгоритму розфарбовування графа для призначення БПЛА на відповідні точки у відповідні часові інтервали (у [4] такими точками виступають призначені для атаки бойовими БПЛА цілі, а інтервалами – часові інтервали доступності цілей для атаки). Проведений аналіз літератури [5–13] показує наявність великої кількості евристичних алгоритмів розфарбовування графа, які для більшої наочності ототожнені з джерелом їх описання і подані у вигляді таблиці 1.

Таблиця 1

Евристичні алгоритми розфарбовування графа

№ з/п	Суть евристичного алгоритму	Джерело
1	Жадібний алгоритм розфарбовування (Greedy-Colour)	[5]
2	Розфарбовування графа з обміном кольорами (Colour-with-Interchange)	[6]
3	Послідовне розфарбовування графа без упорядкування його вершин (Random-Sequential-Colour)	[6]
4	Розфарбовування з обміном кольорами з упорядкуванням вершин графа за спаданням їх ступенів (Largest-First-Interchange-Colour)	[6]
5	Послідовне розфарбовування з динамічним упорядкуванням вершин графа (Saturation-Colour)	[6]
6	Послідовне розфарбовування графа з упорядкуванням його вершин за спаданням їх ступенів (Largest-First-Colour)	[7]
7	Послідовне розфарбовування графа починаючи з вершин максимальних ступенів (Smallest-Last-Colour)	[8]
8	Розфарбовування з обміном кольорами без упорядкування вершин графа (Random-Sequential-Interchange-Colour)	[9]
9	Розфарбовування з обміном кольорами, починаючи з вершин максимальних ступенів графа (Smallest-Last-Interchange-Colour)	[10]
10	Жадібне розфарбовування графа, де його вершини упорядковуються таким чином, що в кожної є принаймні одна сусідня, пофарбована в попередній колір (Connected-Sequential-Colour)	[11]
11	Жадібне розфарбовування незалежних підмножин (Greedy Independent Sets-Colour).	[12]
12	Жадібний алгоритм розфарбовування графа, побудований на бітових операціях над матрицею суміжності	[13]

Для подальшого використання обрано жадібний алгоритм розфарбовування графа, побудований на бітових операціях над матрицею суміжності, оскільки він характеризується більшою простотою і швидкістю розрахунків [13].

Мета статті – розробка підходу на основі жадібного алгоритму розфарбовування графа щодо визначення кількості й порядку застосування БПЛА літакового типу (ЛБПЛА) для збираня інформації від точок "рандеву" безпроводної літальної мережі під час післяаварійного моніторингу Запорізької АЕС (ЗАЕС).

Завдання дослідження:

– запропонувати спрощену схему розгортання БПЛА-БМ для організації передачі інформації від постів контролю до кризового центру під час післяаварійного моніторингу АЕС;

– розробити й описати схему розгортання підсистем БПЛА-БМ для організації передачі даних між чотирма постами контролю АСКРО ЗАЕС і точками "рандеву" у випадку пошкодження проводних каналів зв'язку;

– використовуючи жадібний алгоритм розфарбовування графа, визначити кількість і порядок застосування ЛБПЛА для збирання даних від точок "рандеву" під час післяаварійного моніторингу ЗАЕС.

Виклад основного матеріалу. В процесі функціонування БПЛА-БМ здійснюється збирання, накопичення даних з ПК та подальша їх передача до КЦ.

Нехай маємо такий сценарій. Проводна мережа АСКРО АЕС, яка поєднує ПК безпосередньо з КЦ, була пошкоджена внаслідок аварії. З метою продовження постачання КЦ необхідними даними про РО від ПК розгортається БПЛА-БМ (рис. 1), що складається з n БПЛА мультироторного типу (МБПЛА1_R,…, МБПЛА$(n–1)_R$, МБПЛАn_{RG}) та одного БПЛА літакового типу (ЛБПЛА$_{RG}$).

МБПЛА1_R,…, МБПЛА$(n–1)_R$ працюють як ретранслятори.

МБПЛАn_{RG} може працювати:

– як шлюз для отримання та зберігання даних від МБПЛА$(n–1)_R$;

– як ретранслятор для передачі даних до ЛБПЛА $_{RG}$, виступаючи при цьому точкою "рандеву".

ЛБПЛА$_{RG}$ взаємодіє з МБПЛАn_{RG} у встановлений час свого режиму патрулювання і виконує функції:

– шлюзу для отримання та зберігання даних від МБПЛАn_{RG};

– ретранслятора для передачі даних до КЦ.

Використовуються такі технології зв'язку:

1) wi-fi (IEEE 802.11) для забезпечення каналу КЦ-БПЛА та каналу БПЛА-БПЛА;

2) енергоефективна мережа далекого радіуса дії Low-power Wide-area Network (LoRaWAN) для забезпечення каналу ЛБПЛА$_{RG}$–КЦ.

Таким чином, БПЛА-БМ складається з двох сегментів:

1) сегмента wi-fi, що включає обладнання Wi-Fi у ПК, обладнання Wi-Fi на борту МБПЛА та обладнання Wi-Fi на борту ЛБПЛА;

2) сегмент LoRaWAN, що включає обладнання LoRaWAN на борту ЛБПЛА та обладнання LoRaWAN у КЦ.

МБПЛА1$_R$,…, МБПЛА(n–1)$_R$, МБПЛАn_{RG} утворюють флот МБПЛА.

Для забезпечення безперебійної роботи БПЛА-БМ використовується мережа автоматичних обмінно-зарядних станцій: АОЗС1,…, АОЗСm.

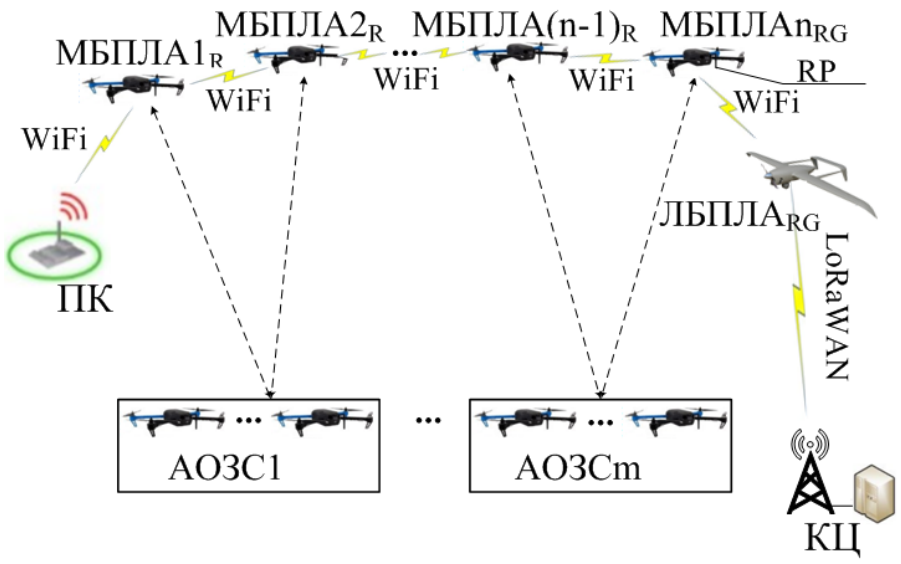


Рис. 1. Спрощена схема розгортання БПЛА-БМ
для організації передачі даних від посту контролю до кризового центру
під час післяаварійного моніторингу АЕС

Для забезпечення передачі даних про РО лише тільки від одного ПК у разі пошкодження проводного каналу ПК–КЦ достатньо розгортання у складі БПЛА-БМ лише однієї підсистеми на основі МБПЛА для організації

передачі даних від пошкодженого ПК до ТР і використання лише одного ЛБПЛА, для організації каналу wi-fi ТР–ЛБПЛА та LoRaWAN каналу ЛБПЛА–КЦ.

Однак під час аварії на АЕС можуть бути пошкоджені проводні канали зв'язку з більшою кількістю постів контролю. В цьому випадку схема розгортання БПЛА-БМ буде дещо складнішою. У загальному вигляді вона матиме у своєму складі:

– *m* підсистем на основі МБПЛА, які забезпечуватимуть передачу даних від пошкоджених постів контролю до відповідних точок "рандеву";

– *n* ЛБПЛА для обльоту точок "рандеву" з метою збирання даних про РО шляхом установлення каналу ТР–ЛБПЛА та подальшої їх передачі до КЦ за каналом ЛБПЛА–КЦ.

Розглянемо випадок (рис. 2), коли розгорнутий після аварії зовнішній КЦ Запорізької АЕС (ЗАЕС) (на рис. 2 не зображений) унаслідок пошкодження проводних ліній зв'язку втратив зв'язок з чотирма ПК (ПК9, ПК14, ПК15 та ПК16 [14]), що входять до складу АСКРО цієї станції. На рис. 2 зображено утворені на основі МБПЛА чотири підсистеми для передачі даних від пошкоджених постів контролю до відповідних точок "рандеву".

Рис. 2. Схема розгортання підсистем БПЛА-БМ на основі МБПЛА для організації передачі даних від постів контролю до точок "рандеву" під час післяаварійного моніторингу ЗАЕС

Надалі, щоб подати схему розгортання БПЛА-БМ у кінцевому варіанті, нам необхідно визначити скільки ЛБПЛА потрібно використати й у якій послідовності вони мають здійснювати обліт точок “рандеву” для отримання від них даних про РО.

Час початку та закінчення функціонування кожної підсистеми на основі МБПЛА залежить від:

– часу початку розгортання підсистеми;

– ємності акумуляторів МБПЛА;

– віддалення АОЗС, які здійснюють заміну акумуляторів БПЛА, від місця БПЛА в підсистемі.

Як уже було зазначено, наприкінці функціонування кожної підсистеми необхідно передавати накопичені дані на ЛБПЛА для їх подальшої передачі до КЦ. Час передачі даних (час функціонування каналу ТР–ЛБПЛА) визначається інтервалом:

$$T_{TPi} = \left(t_i^s; t_i^e\right), \tag{1}$$

де t_i^s – час початку функціонування *i*-ї ТР як ретранслятора даних на ЛБПЛА;

t_i^e – час закінчення функціонування *i*-ї ТР як ретранслятора даних на ЛБПЛА.

Під час функціонування системи, що розглядається, можуть виникати випадки, коли ці інтервали перетинаються, тобто виконується умова:

$$\left(t_i^s; t_i^e\right) \cap \left(t_j^s; t_j^e\right) \neq \varnothing; i, j \in \left(\overline{1,n}\right); i \neq j \tag{2}$$

За таких умов одного ЛБПЛА для забезпечення отримання та передачі даних від усіх точок “рандеву” не достатньо.

Для визначення кількості ЛБПЛА, необхідних для встановлення каналу зв’язку з кожною точкою “рандеву”, пропонується застосовувати жадібний алгоритм розфарбовування графа, побудований на бітових операціях над матрицею суміжності.

Візьмемо, що для передачі даних каналом ТР–ЛБПЛА необхідно витратити 4 хвилини. Часові інтервали передачі даних від відповідної точки

“рандеву” до ЛБПЛА подано в табл. 2. У ній показано пости контролю, з яких точки “рандеву” отримують дані.

Таблиця 2

Часові інтервали передачі даних від точок “рандеву” до ЛБПЛА

Пост контролю	Точка “рандеву”	Часовий інтервал передачі даних
ПК9	ТР4	[00.08; 00.13]
ПК14	ТР1	[00.10; 00.14]
ПК15	ТР3	[00.14; 00.19]
ПК16	ТР2	[00.12; 00.17]

Припустимо, що час, необхідний на переміщення ЛБПЛА між точками “рандеву” не враховується, оскільки вважається, що відстані між точками “рандеву” та швидкість ЛБПЛА дозволяють йому своєчасно прибувати в потрібну точку “рандеву” для отримання даних.

Розрахунки проведемо в такому порядку.

Спочатку побудуємо неорієнтований граф $G = (V, E)$ (рис. 3), де V – множина вершин (відповідають точкам “рандеву”); E – множина ребер між вершинами. Вершини мають ребра, якщо перетинаються часові інтервали передачі даних від точок “рандеву” до ЛБПЛА. Для наведених вихідних даних маємо:

$$V = \{1, 2, 3, 4\};$$

$$E = \{(1,2),(1,3),(1,4),(2,1),(2,3),(3,1),(3,2),(3,4),(4,1),(4,3)\}.$$

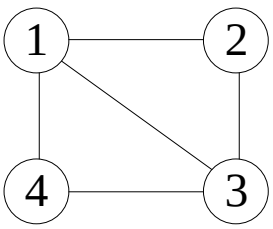


Рис. 3. Граф, що відповідає вихідним даним

Наступним кроком є побудова для графа G = (*V*, *E*) матриці суміжності A розміром $n \times n = 4$, для якої значення елемента a_{ij} відповідає наявності ребра з *i*-ї вершини графа до *j*-ї вершини графа, тобто $a_{ij} \in \{0,1\}$.

Будь-яка вершина суміжна із собою, тому на головній діагоналі розташовуються одиниці. Для графа, зображеного на рис. 3, матриця суміжності має вигляд

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

Далі, починаючи з першого рядка матриці суміжності A ($i = 1$), здійснюється пошук першої суміжної нефарбованої вершини, для якої $a_{1j} = 0$. Для матриці, що аналізується, всі елементи першого рядка дорівнюють одиниці. В такому випадку номер першого рядка додається до першої кольорової групи.

Далі проводиться подібна процедура для другого рядка ($i = 2$). У другому рядку суміжною нефарбованою вершиною є вершина з номером 4 ($a_{14} = 0; j = 4$).

Відповідно до алгоритму, беремо суму другого та четвертого рядків для отримання оновленого рядка матриці:

$$\begin{array}{cccc} 1 & 1 & 1 & 0 \\ \vee & & & \\ 1 & 0 & 1 & 1 \\ \hline 1 & 1 & 1 & 1 \end{array}$$

Усі елементи оновленого рядка a_{2j} матриці дорівнюють одиниці, тому вершини з номерами 2 та 4 додаються до третьої кольорової групи.

Наступним аналізується третій рядок ($i = 3$). Усі елементи третього рядка дорівнюють одиниці, тому вона додається до третьої кольорової групи.

Таким чином, для забезпечення збираня та передачі даних від ПК9, ПК14, ПК15, ПК16 необхідно три ЛБПЛА (ЛБПЛА$_{RG1}$, ЛБПЛА$_{RG2}$, ЛБПЛА$_{RG3}$) (рис. 4), які взаємодіють з відповідними точками “рандеву” (табл. 3).

Таблиця 3

Взаємодія ЛБПЛА з точками “рандеву”
для отримання даних від постів контролю

Пост контролю	Точка “рандеву”	ЛБПЛА
ПК9	ТР4	ЛБПЛА$_{RG1}$
ПК14	ТР1	ЛБПЛА$_{RG2}$
ПК15	ТР3	ЛБПЛА$_{RG1}$
ПК16	ТР2	ЛБПЛА$_{RG3}$

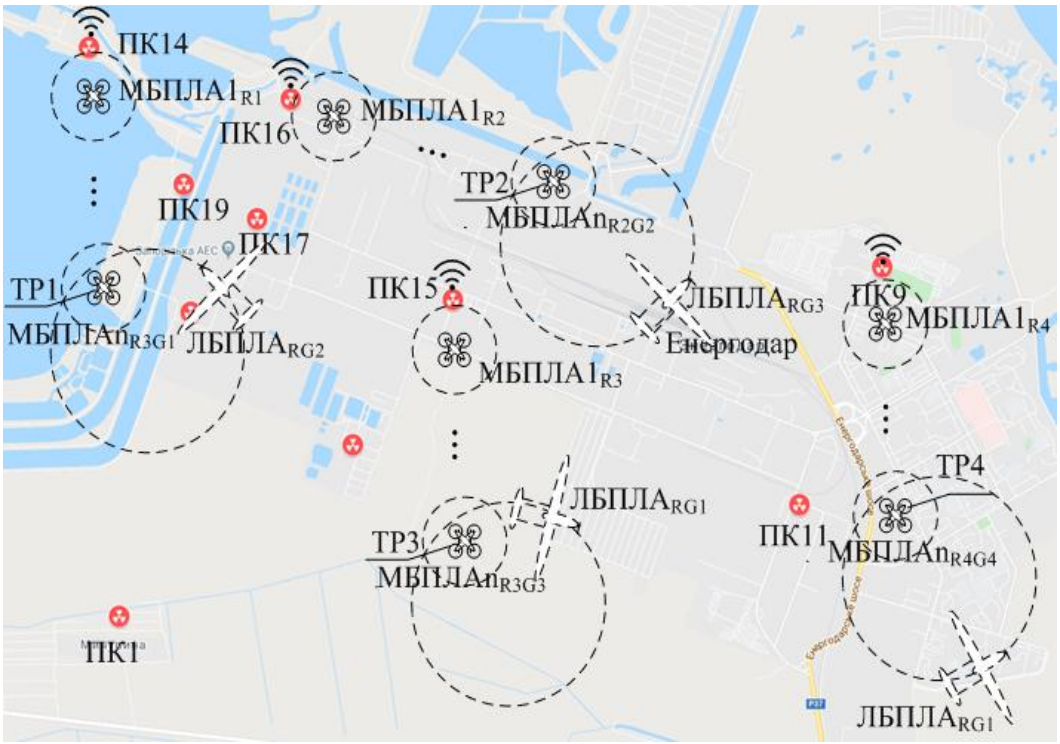


Рис. 4. Схема розгортання БПЛА-БМ для організації передачі даних
від постів контролю до кризового центру
під час післяаварійного моніторингу ЗАЕС із позначенням порядку взаємодії
БПЛА літакового типу з точками “рандеву”

Як видно з табл. 3, ЛБПЛА$_{RG1}$ використовується для збирання та передачі даних одразу від двох постів контролю (ПК9 та ПК15), для чого спочатку взаємодіє з ТР4, а потім з ТР3.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Проаналізовано й подано у вигляді таблиці наявні евристичні алгоритми розфарбовування графа. Для подальшого використання обрано жадібний алгоритм розфарбовування графа, побудований на бітових операціях над матрицею суміжності. Запропоновано спрощену схему розгортання БПЛА-БМ для організації передачі даних від постів контролю АСКРО до кризового центру під час післяаварійного моніторингу АЕС. Розроблено й описано схему розгортання підсистем БПЛА-БМ для організації передачі даних між чотирма постами контролю АСКРО ЗАЕС і точками "рандеву" у разі пошкодження проводних каналів зв'язку. Використовуючи обраний алгоритм розфарбовування графа, визначено, що для забезпечення збирання та передачі даних від ПК9, ПК14, ПК15, ПК16 необхідно три ЛБПЛА (ЛБПЛА$_{RG1}$, ЛБПЛА$_{RG2}$, ЛБПЛА$_{RG3}$). При цьому ЛБПЛА$_{RG1}$ використовується для збирання та передачі даних одразу від двох постів контролю (ПК9 та ПК15), для чого спочатку взаємодіє з ТР4, а потім з ТР3. ЛБПЛА$_{RG2}$ взаємодіє з ТР1, а ЛБПЛА$_{RG3}$ – з ТР2. Подальші дослідження доцільно зосередити на вивченні впливу місця розташування АОЗС та їх особливостей на час функціонування БПЛА-БМ.

Список використаних джерел:

1. Концепція побудови мобільних систем пост-аварійного моніторингу АЕС з використанням флоту квадрокоптерів / А. О. Саченко, В. В. Кочан, В. С. Харченко та ін. *Радіоелектронні комп'ютерні системи.* 2016. № 5 (79). С. 207–214.

2. Система послеаварийного мониторинга АЭС с использованием беспилотных летательных аппаратов: концепция, принципы построения / А. О. Саченко, В. В. Кочан, В. С. Харченко и др. *Ядерна та радіаційна безпека.* 2017. № 1 (73). С. 24–29.

3. An Internet of Drone-based multi-version post-severe accident monitoring system: structures and reliability / Fesenko H., Kharchenko V., Sachenko A. and oth. // *Dependable IoT for human and industry modeling, architecting, implementation*. Denmark, The Netherlands: River Publishers, 2018. P. 197–217.

4. *Моисеев В. С.* Групповое применение беспилотных летательных аппаратов: монография. Казань: Школа, 2017. 572 с.

5. Kučera L. The greedy coloring is a bad probabilistic algorithm. *Journal of Algorithms.* 1991. Vol. 12. 674–684.

6. Kosowski A., Manuszewski K. Classical coloring of graphs. *Contemporary Mathematics*. 2011. Vol. 352. P. 1–20.

7. Distributed largest-first algorithm for graph coloring / J. Hansen, M. Kubale, Ł. Kuszner, A. Nadolski. *Lecture Notes in Computer Science*. 2004. Vol. 3149. P. 804–811. DOI: 10.1007/978-3-540-27866-5.

8. *Matula D., Beck L.* Smallest-last ordering and clustering and graph coloring algorithms. *Journal of the ACM (JACM)*. 1983. Vol. 30. P. 135–145.

9. *Read R.* Graph theory and computing. USA, New York: Academic Press, 2014. 344 p.

10. *Matula D., Marble G., Isaacson J.* Graph coloring algorithms. *Graph Theory and Computing*. USA, New York: Academic Press, 2014. P. 109–122.

11. *Hertz A., Werra D.* Connected sequential colorings. *Annals of Discrete Mathematics*. 1989. Vol. 39. P. 51–59. DOI: 10.1016/S0167-5060(08)70297-8.

12. *Wu Q., Hao J.-K.* Coloring large graphs based on independent set. *Computers & OR*. 2012. Vol. 39. P. 283–290. DOI: 10.1016/j.cor.2011.04.002.

13. A fast greedy sequential heuristic for the vertex colouring problem based on bitwise operations / L. Komosko, M. Batsyn, P. Segundo, P. Pardalos. *Journal of Combinatorial Optimization*. 2016. Vol. 4. P. 1665–1677.

14. Вестрон. Автоматизированная система контроля радиационной обстановки ЗАЭС. Техническое задание. ТЗ – ВН. 702.410.34. Харьков, 2011. 124 с.

References:

1. Kochan V. V., Sachenko A. A., Kharchenko V. S., Yatskiv V. V., Chernyshov M. A., Bykovyi P. Ye., Roshchupkin O. Yu. and Koval V. S. (2016), *"Kontseptsiia pobudovy mobilnykh system post-avariinoho monitorynhu AES z vykorystanniam flotu kvadrokopteriv"* ["Concept of building of NPP post-emergency monitoring mobile systems using quadrocopter fleet"], Journal *Radioelektronni i komp'iuterni systemy* [Radioelectronic and Computer Systems], vol. 5(79), pp. 207–214 [Ukraine].

2. Kharchenko V. S., Jastrebeneckij M. A., Fesenko H. V., Sachenko A. A. and Kochan V. V. (2017), *"Sistema posleavarijnogo monitoringa AJeS s ispol'zovaniem bespilotnyh letatel'nyh apparatov: modeli nadezhnosti"* ["NPP post-accident monitoring system based on unmanned aircraft vehicle: Concept, design principles"], Journal *Yaderna ta radiatsiina bezpeka* [Nuclear and Radiation Safety], vol. 4 (76), pp. 50–55 [Ukraine].

3. Fesenko H., Kharchenko V., Sachenko A., Hiromoto R. and Kochan V. (2018), “An Internet of Drone-based multi-version post-severe accident monitoring system: structures and reliability”. Dependable IoT for Human and Industry Modeling, Architecting, Implementation, River Publishers, Denmark, The Netherlands, pp. 197–217.

4. Moiseev V. S. (2017), *Gruppovoye primeneniye bespilotnykh letatel'nykh apparatov* [Group use of unmanned aerial vehicles], Monograph, Kazan’, 572 p. [Russia].

5. Kučera L. (1991) “The greedy coloring is a bad probabilistic algorithm”. // Journal of Algorithm, vol. 12, pp. 674–684.

6. Kosowski A. and Manuszewski K. (2011), “Classical coloring of graphs”. Contemporary Mathema, vol. 352, pp. 1–20.

7. Hansen J., Kubale M., Kuszner Ł. and Nadolski A. (2004), “Distributed largest-first algorithm for graph coloring”. Lecture Notes in Computer Science, vol. 3149, pp. 804–811. DOI:10.1007/978-3-540-27866-5.

8. Matula D. and Beck L. (1983), “Smallest-last ordering and clustering and graph coloring algorithms”. Journal of the ACM (JACM), vol. 30, pp. 135–145.

9. Read R. (2014), *Graph theory and computing*, Academic Press, USA, New York, 344 p.

10. Matula D., Marble G. and Isaacson J. (2014), “Graph coloring algorithms”. Graph Theory and Computing, Academic Press, USA, New York, pp. 109–122.

11. Hertz A. and Werra D. (1989), “Connected Sequential Colorings”. Annals of Discrete Mathematics, vol. 39, pp. 51–59. DOI: 10.1016/S0167-5060(08)70297-8.

12. Wu Q. and Hao J.-K. (2012), “Coloring large graphs based on independent set”. Computers & OR, vol. 39, pp. 283–290. DOI: 10.1016/ j.cor.2011.04.002.

13. Komosko L., Batsyn M., Segundo P. and Pardalos P. (2016). “A fast greedy sequential heuristic for the vertex colouring problem based on bitwise operations”. Journal of Combinatorial Optimization, vol. 4, pp. 1665–1677.

14. Vestron. Avtomatizirovannaya sistema kontrolya radiatsionnoy obstanovki ZAES. Tehnicheskoe zadanie. TZ -–VN. 702.410.34 [Westron. Automat-ed system for Radiation situation monitoring. Technical Task. TZ – VN. 702.410.34] (2011). Kharkiv, 124 p. [Ukraine]

DOI: https://doi.org/10.32836/2521-6643-2018.2-56.2
УДК 004.519.217

С. О. Яремчук, кандидат технічних наук,
доцент кафедри судових енергетичних
установок і систем Дунайського інституту
Національного університету
"Одеська морська академія"

МЕТРИКИ НАДІЙНОСТІ НА ОСНОВІ ЗАЛЕЖНОСТЕЙ ДЕФЕКТНОСТІ ПРОГРАМНОГО КОДУ ВІД ЙОГО СКЛАДНОСТІ

У роботі виконано аналіз недоліків небагатьох наявних метрик надійності програмних систем та визначено необхідність розробки нових метрик надійності на основі оцінювання складності вихідного коду. На основі відомих метрик складності об'єкто-орієнтованого коду розроблено єдину комплексну оцінку складності. З її використанням запропоновано метрики надійності вихідного коду: співвідношення між дефектними та бездефектними модулями, імовірність виявлення дефектів у модулях, модульна щільність дефектів, локалізація та розподіл дефектів у коді. Запропоновано визначати розроблені метрики надійності для раніше розроблених і верифікованих систем або їх частин, для яких відомі метричні оцінки складності та кількість дефектів. Запропоновані метрики надійності можуть бути використані для планування ресурсів та виконання ефективної верифікації новоствореного коду нових ітерацій, частин, версій, функцій або нових систем конкретного розробника. Метрики надійності можуть бути розраховані для будь-яких систем, подібних до новорозробленої системи за функціональністю, оцінками складності, кваліфікацією розробників, рівнем процесів та методологією розробки.

Ключові слова: *програмна система; програмне забезпечення; надійність; дефект; відмова; вихідний код; складність; метрика.*

В работе выполнен анализ недостатков немногих существующих метрик надежности программных систем и установлена необходимость разработки новых метрик надежности на основе оценки сложности

исходного кода. На основе известных метрик сложности объектно-ориентированного кода разработана единая комплексная оценка сложности. С ее использованием предложены метрики надежности исходного кода: соотношение между дефектными и бездефектными модулями, вероятность обнаружения дефектов в модулях, модульная плотность дефектов, локализация и распределение дефектов в коде. Предложено рассчитывать метрики надежности для ранее разработанных и верифицированных систем или их частей, для которых известны метрические оценки сложности и количество дефектов. Предложенные метрики надежности могут быть использованы для планирования ресурсов и выполнения эффективной верификации вновь разработанного кода новых итераций, частей, версий, функций или новых систем конкретного разработчика. Метрики надежности могут быть рассчитаны для любых систем, подобных новой разработанной системе по функциональности, оценкам сложности, квалификации разработчиков, уровнем процессов и методологии разработки.

Ключевые слова: *программная система; программное обеспечение; надежность; дефект; отказ; исходный код; сложность; метрика.*

The work has analyzed the few existing metrics of the software systems reliability. Standard metrics have been found to have disadvantages. Existing metrics are not sufficient to assess the reliability in a timely manner during the development phase of software systems. It is determined that the complexity of the source code is a major cause of the errors.

The analysis of complexity types for software systems has been performed. It is established need of the additional development of new reliability metrics on the basis of the assessment of the source code complexity.

A study of existing complexity metrics has been conducted. Metrics were chosen that are most informative for reliability evaluation. Based on the selected object-oriented code complexity metrics, a single combined complexity assessment has been developed instead of twenty different scale estimates. This reduces the source data array by twenty times, significantly reduces the hardware load and the processing time. The practical use of the combined complexity assessment greatly simplifies the assessment, visualization and understanding of the properties of the system, as well as facilitates in-depth analysis of its reliability.

Using combined complexity assessment, code reliability metrics are proposed: the ratio between defective and defect-free modules, the probability of the

defects detection in modules, the modular density of defects, the localization and the distribution of defects in the code. The procedure for the designing and the analyzing reliability metrics is described. The proposed reliability metrics are calculated and rendered for various software systems based on their metric data.

The analysis of developed metrics was carried out. Directions of their practical using by specialists of software companies have been established. It is proposed to calculate reliability metrics for previously developed and verified systems or their parts, for which metric assessments of complexity and the defects number are known.

The proposed reliability metrics can be used to plan resources and perform the efficient verification of newly created code of new iterations, parts, versions, functions, or new systems for a particular developer. Reliability metrics can be calculated for any system similar to the newly developed system in terms of the functionality, complexity assessments, the developer qualification, the process level, and the development methodology.

Key words: *software system; software; reliability; defect; fault; source code; complexity; metric.*

Постановка проблеми. Наразі безліч програмних систем (software system, далі система) використовується підприємствами і фізичними особами для різноманітних потреб. Під програмною системою ми розуміємо сукупність взаємопов'язаних підсистем, класів, компонентів або модулів, які взаємодіють між собою з метою виконання вимог користувачів. Зростання потреб користувачів обумовлює підвищення складності систем. Динамічні зміни в предметних областях та законодавстві викликають необхідність змін та розширення функціональності систем. Це призводить до збільшення кількості дефектів в їхньому програмному коді та обумовлює зниження їхньої надійності. Невиявлені розробниками дефекти та їх усунення на етапі експлуатації значно підвищують витрати на супроводження систем. Дослідження, проведені компаніями TRW, Hewlett-Packard та IBM, переконливо доводять, що усунення дефектів на етапі експлуатації в 4–100 разів дорожче, ніж на етапі розробки. Згідно з оцінками Національного інституту стандартів та технологій США, внаслідок низької надійності систем економічні втрати лише цієї країни станолять щороку близько шістдесяти мільярдів доларів. Для підвищення надійності необхідно зменшити кількість не виявле-

них розробниками дефектів, що дозволить скоротити витрати на супроводження та знизити ризики катастрофічних втрат, техногенних аварій та людських жертв, обумовлених низькою надійністю систем. Надійність програмних систем оцінюється за допомогою метрик надійності, які описані в стандартах.

Аналіз стандартів щодо метрик надійності програмних систем. Відповідно до ISO/IEC 25010-2011 [1], під надійністю систем розумітимемо комплексу властивість, яка характеризує здатність системи правильно виконувати свої функції упродовж визначеного періоду часу. Згідно з ISO/IEC 9126 [2–4], основними показниками надійності на етапі розробки систем визначено *оцінки кількості дефектів, щільності дефектів та ступінь виявлення дефектів*. Згідно зі стандартами [5–6], під дефектом (defect, fault) розуміється програмна аномалія, некоректне визначення операції, процесу чи даних у програмному забезпеченні (ПЗ), що може викликати не відповідне до специфікації функціонування ПЗ або призвести до відмови. Дефекти виникають у ПЗ внаслідок помилок розробників. Їх визначення наведено в стандартизованих словниках термінів якості ПЗ [7–8].

Метрика "Оцінка кількості дефектів" (assessment of defects number) розраховується за допомогою моделі надійності. Зазвичай важко вибрати найбільш адекватну модель із великої кількості наявних моделей, що значно знижує точність оцінювання цієї метрики. Метрика "Щільність дефектів" (defect density) має суттєві недоліки. Вона не враховує складність вихідного програмного коду системи (source code, далі – код), а також рядки коментарів, порожні та системні рядки в коді, що призводить до перекручень значень цієї метрики. На наш погляд, не обсяг, а складність коду є першоджерелом помилок.

Окрім небагатьох стандартних показників надійності, розробникам необхідні показники кількості дефектних та бездефектних модулів, локалізації дефектів, розподілу дефектів у коді, ймовірності дефектів у модулях, модульної щільності дефектів. Стандарт [8] визначає модуль (компонент) програмних систем як окрему дискретну ідентифіковану структурну одиницю, яка може бути протестована окремо, без чіткого визначення її розмірів.

Своєчасне визначення показників надійності дозволяє розробникам заздалегідь розрахувати, залучити й використати ресурси розробки таким чином, щоб за визначений проміжок часу виявити й усунути якомога більше

дефектів. Для зменшення кількості невиявлених дефектів потрібно визначити показники надійності системи ще до початку виявлення та усунення дефектів. Але зазвичай ці показники стають відомими тільки після завершення цього процесу. На наш погляд, для подолання цієї суперечності необхідно оцінити показники надійності апріорно, до початку верифікації програмного коду систем на основі його складності, виходячи з того, що складність коду є першопричиною дефектів коду.

Згідно з прпцями багатьох дослідників складність, є супутньою властивістю програмних систем. Їхня складність характеризується великою кількістю різноманітних станів, процесів, складових та зв'язків між ними, використанням різних мов програмування і моделей розробки та виконанням великої кількості функцій для розвннєязання багатоцільових задач. Програмним системам властива *статична* складність, що описує зв'язність і структуру підсистем, *динамічна* складність, пов'язана з поведінкою системи у часі, *ієрархічна* складність, *структурна* складність, яка визначається кількістю ієрархічних рівнів, підсистем і компонентів системи, *алгоритмічна* складність, *цикломатична* складність, *обчислювальна* складність, яка оцінюється кількістю операцій для отримання результату і кількістю оброблюваних елементів, часова та просторова складність.

На підставі аналізу стандарту IEEE 1061 [9] зроблено висновок, що основним методом оцінювання складності програмного коду є розрахунок числових показників за відповідними метриками. Згідно з цим стандартом, метрика (metric) – це кількісна (або якісна) оцінка ступеня, в якому система відповідає заданим властивостям. У контексті нашого дослідження метрика складності (далі – метрика) – це математичний вираз числової оцінки одного або кількох аспектів складності програмного коду. Наразі багатьма науковцями та практиками програмної інженерії розроблено близько п'ятдесяти метрик складності. Вибір метрик залежить від систем програмування. За цією ознакою найбільш відомі та необхідні метрики оцінювання складності процедурно-орієнтованого та об'єктно-орієнтованого програмування, які описані в [10]. Метрика WMC (Weighted methods per class) визначає загальну складність методів класу. Метрика DIT (Depth of Inheritance tree) оцінює глибину дерева наслідування як найдовший шлях за ієрархією класів від класу-предка до класу-нащадка. Метрика NOC (Number of children) оцінює кількість класів-нащадків. Метрика CBO (Coupling between object classes) характеризує зчепленість між класами, тобто кількість класів, з якими

пов'язаний вихідний клас. Метрика RFC (Response for a class) визначає кількість методів (даного та інших класів), які викликає даний клас. Метрика LCOM (Lack of cohesion in Methods) визначає, наскільки методи класу не пов'язані між собою через змінні. Саме ці метрики ми використали у нашому дослідженні.

Після проведеного аналітичного огляду джерел [1–12] зроблено наступний висновок. Нині зусиллями дослідників та спеціалістів програмної інженерії розроблено велику кількість метрик оцінювання різноманітних властивостей коду. Однак немає метрик оцінювання дефектності коду залежно від його складності. Водночас складність коду, на наш погляд, є головною причиною помилок. Саме ця обставина обумовлює мету дослідження.

Мета даної статті – розробка та аналіз метрик надійності, які оцінюють дефектність програмного коду залежно від його складності.

Складність коду вимірюється за допомогою відомих метрик, значення яких підраховуються автоматично під час компіляції або інтерпретації програмного коду. Дефектність коду вимірюється як кількість виявлених дефектів у модулях. Значення метрик надійності розраховуються для раніше розроблених і верифікованих систем або їх частин, для яких відомі метричні оцінки складності та кількість дефектів. Розраховані метрики можуть бути використані для планування ресурсів та виконання ефективної верифікації новоствореного коду нових ітерацій, частин, версій, функцій або нових систем конкретного розробника. Метрики надійності можуть бути розраховані для будь-яких систем, подібних до новорозробленої системи за функціональністю, метричними оцінками складності, кваліфікацією розробників, рівнем процесів та методологією розробки.

Виклад основного матеріалу.

Аналіз складності коду та розробка єдиної комплексної оцінки складності. Набори даних систем зі сховища [13] містять числові метричні оцінки складності окремих модулів коду за двадцятьма метриками. Це оцінки обчислювальної складності, складності структури, зв'язності, зчеплення, розмірів модуля та ін. Набори даних містять також інформації про відсутність або наявність кількості дефектів у кожному модулі, що було виявлено в процесі верифікації. Структуру даних можна описати таким вектором метрик (vector of metrics, VM)

$$VM = \begin{Bmatrix} module\_name, wmc, dit, noc, cbo, rfc, lcom, ca, ce, npm, lcom3, loc, \\ dam, moa, mfa, cam, ic, cbm, amc, max\_cc, avg\_cc, bug \end{Bmatrix}.$$

Для окремого модуля системи вектор метричних оцінок (vector of metrics assessment, VMA) має наступний вигляд:

$$VMA = \left\{ \begin{matrix} \text{module\_}name, 35,\ 2,\ 0,\ 16,\ 103,\ 317, 3,\ 16,\ 28,\ 0.813, \\ 865,\ 0.888,\ 0,\ 0.689,\ 0.152,\ 1,\ 10,\ 23.46,\ 3,\ 1.057, 5 \end{matrix} \right\}.$$

Для скорочення обсягу даних аналізу доцільно вибрати з них найбільш інформативні показники. Найбільш інформативними для аналізу дефектності є ті показники, які демонструють тісніший зв'язок із кількістю дефектів (показник bug у VM). Для виміру ступеня зв'язку ми використали коефіцієнт парної кореляції Пірсона (correlation coefficient, CC) між метричними оцінками та виявленими дефектами в модулях систем. Для встановлення закономірностей кореляційних зв'язків ми дослідили двадцять наборів даних різноманітних систем зі сховища [13]. В ході дослідження були встановлені додатні та від'ємні, істотні (CC>0,7) та неістотні (CC<0.1) зв'язки між метричними оцінками та кількістю дефектів. Причому від'ємні CC завжди мали неістотні значення. Дослідження CC показало, що доцільно залишити в наборі даних такі метрики, оцінки яких становили CC≈0.5 або CC>0.5. Оцінки з CC<0.5 потрібно виключити з аналізу. Оцінки за цими метриками мають слабкий кореляційний зв'язок із кількістю дефектів. Ці метрики є недостатньо інформативні для аналізу дефектності коду залежно від його складності. При цьому VMA було скорочено з 20 до 5–7 метрик.

Обрані таким чином метрики відображають різноманітні аспекти складності та істотно (в рази та десятки разів) відрізняються за абсолютними величинами. Наприклад, в одній дослідженій системі метричні оцінки модуля становили: DIT – 8, NOC – 29, NPM – 122, WMC – 130, RFC – 391, LOC – 4275, LCOM – 7399 одиниць. Тому виникає необхідність нормалізації оцінок. Нормалізація дозволить привести всі метричні оцінки до близьких числових значень, що надалі дасть змогу отримати на їх основі *єдину комплексну оцінку складності коду*. Найбільш поширені способи: лінійна та нелінійна нормалізація. Їх порівняльний аналіз виявив таке. Нелінійна нормалізація з використанням гіперболічного тангенса має складніший алгоритм розрахунку, проте не дає будь-яких переваг. Тому була виконана лінійна нормалізація метричних оцінок за формулою:

$$X_{ik}^{n} = \frac{X_{ik} - X_{\min i}}{X_{\max i} - X_{\min i}}, \qquad (1)$$

де X_{ik} – значення *i-ї* метричної оцінки для *k-го* модуля,

X_{ik}^{n} – відповідне нормалізоване значення.

Далі всі відібрані метричні оцінки були нормалізовані за формулою (1) і складені в *єдину комплексну оцінку складності коду* (combined assessment of complexity, CA) за формулою

$$CA_k = \sum_{i=1}^{m} X_{ik}^{n}, \quad (2)$$

де m – кількість відібраних метричних оцінок.

Чим вищі значення CA для модуля, тим складніше його структура, методи, взаємозв'язки.

Далі постало питання про інформативність значень CA для аналізу дефектності коду. Ми дослідили кореляцію між CA та кількістю дефектів у модулях. Було встановлено, що CC між CA та дефектами був дещо більший (на 0,1), ніж найвищий CC для відібраних метрик. Таким чином, відібрані метричні оцінки були зведені до одного показника CA без зменшення ступеня зв'язку з дефектами і без втрати інформативності CA для аналізу дефектності коду. В результаті описаних дій отримано єдину CA замість двадцяти різномасштабних оцінок і скорочено масив вихідних даних у двадцять разів, що дозволить значно знизити апаратне навантаження і період обробки даних. Практичне використання CA значно спрощує оцінювання, візуалізацію та розуміння властивостей модулів системи, а також сприяє глибокому аналізу надійності модулів та системи загалом.

На основі CA ми запропонували ще два показники для оцінювання властивостей системи. Перший показник – це сумарна оцінка складності системи (summary assessment of system complexity, SA) за формулою

$$SA = \sum_{k=1}^{n} CA_k, \quad (3)$$

де n – кількість модулів системи.

Наприклад, для досліджуваних систем значення становили 189, 340, 538, 790, 3459, 3825 одиниць. Мінімальне значення відрізнялось від максимального у 18 разів. Тобто системи відрізнялись своїми властивостями у 18 разів. Другий показник – це середня оцінка складності для модулів системи (average assessment of complexity, AA), розрахована за формулою:

$$AA = SA / n \quad (4)$$

де n – кількість модулів системи.

Практичне значення оцінок за показниками SA й AA полягає в такому. Оцінка SA відображає загальну складність і розмір системи одним числом. Оцінка AA відображає середню складність і розмір модуля системи. Ці оцінки можуть бути використані для порівняння властивостей різних систем та обґрунтування витрат на їх розробку.

Отже, маємо два ключові показники. Це показник складності й показник дефектів у модулях системи. Далі виникають такі запитання. Як чином використати ці дані, щоб отримати показники надійності? Яким чином перетворити нову інформацію на знання? Як використати ці знання для підвищення надійності системи з одночасним зменшенням затрат на її верифікацію? На наш погляд, це можливо за допомогою метрик надійності, запропонованих нами та описаних нижче.

Процедура розробки та аналізу метрик надійності.

Для розробки метрик надійності ми взяли структуровані дані для різних систем зі сховища [13] . Фрагмент даних показано в табл. 1.

Таблиця 1

Фрагмент даних с метричними оцінками та дефектами

	NAME	VERSION	NAME1	WMC	DIT	NOC	CBO	RFC	LCOM	CA	CE	NPM	LOC	BUG
865	xal	2,6	org.apache.xpath.SourceTree	**1**	1	0	1	**2**	0	1	0	1	12	0
866	xal	2,6	org.apache.xalan.xsltc.compile	**11**	5	0	16	**23**	37	3	13	10	141	0
867	xal	2,6	org.apache.xpath.axes.ChildIte	**4**	5	0	5	**9**	6	1	4	3	64	0
868	xal	2,6	org.apache.xml.utils.Trie	**3**	1	0	2	**10**	0	2	1	3	162	1
869	xal	2,6	org.apache.xml.utils.StringBuf	**4**	1	0	7	**9**	0	5	2	3	25	0
870	xal	2,6	org.apache.xalan.xsltc.trax.Tr	**33**	3	0	17	**151**	322	6	16	23	1758	5
871	xal	2,6	org.apache.xalan.xsltc.compile	**4**	3	0	11	**14**	0	0	11	4	44	0
872	xal	2,6	org.apache.xml.utils.Suballoca	**20**	1	0	15	**22**	8	15	0	13	901	1
873	xal	2,6	org.w3c.dom.xpath.XPathExpress	**1**	1	0	0	**1**	0	0	0	1	1	1
874	xal	2,6	org.apache.xml.serializer.Seri	**67**	1	3	12	**111**	1771	3	9	47	958	5
875	xal	2,6	org.apache.xalan.xsltc.cmdline	**1**	4	0	2	**2**	0	1	1	1	5	0
876	xal	2,6	org.apache.xml.serializer.Outp	**6**	1	0	10	**38**	9	6	4	2	388	2
877	xal	2,6	org.apache.xpath.ExpressionNod	**5**	1	0	44	**5**	10	44	0	5	5	0
878	xal	2,6	org.apache.xpath.axes.LocPathI	**52**	4	8	37	**84**	1016	20	20	45	665	1
879	xal	2,6	org.apache.xml.utils.Serializa	**10**	1	0	0	**15**	37	0	0	10	64	0
880	xal	2,6	org.apache.xalan.xsltc.compile	**5**	4	0	14	**10**	4	4	11	4	38	0
881	xal	2,6	org.apache.xalan.xsltc.compile	**2**	4	0	17	**25**	1	1	16	2	137	0
882	xal	2,6	org.apache.xml.serializer.Attr	**6**	2	0	6	**20**	0	6	0	5	124	1
883	xal	2,6	org.apache.xpath.objects.XNode	**7**	5	0	5	**18**	0	1	4	7	115	0
884	xal	2,6	org.apache.xpath.compiler.Psue	**1**	1	0	0	**2**	0	0	0	1	10	0
885	xal	2,6	org.apache.xalan.transformer.T	**36**	1	0	9	**100**	0	1	9	33	914	1

Далі ми нормалізували метричні оцінки модулів за формулою (1) і розрахували CA за формулою (2). Після цього дані були відсортовані за CA та згруповані для кожного інтервалу складності від найменшого до найбільшого значення із кроком 0,2. Запропоновані метрики розраховувались для кожного інтервалу CA та відображались у вигляді графіків або діаграм.

Метрика співвідношення між дефектними та бездефектними модулями.

Перша запропонована метрика обчислюється як співвідношення між дефектними (defect modules, DM) та бездефектними модулями (defect-free modules, DFM), що відображає ступінь дефектності коду системи (Ratio between DM and DFM, **RDM**). Чим вище це співвідношення, тим більше часу потребуватиме верифікація. Для аналізу RDM ми взяли чотири різні системи. Характеристики систем подано в табл. 2. Напівжирним шрифтом позначені максимальні показники.

Таблиця 2

Метрика RDM, показники дефектностіта складності модулів різних систем

Системи	% DM	% DFM	**Метрика RDM**	AA	CA_{max}	SA
Система (a)	22	**78**	0,28	0,56	**6,8**	415
Система (b)	60	40	1,5	0,51	5,1	173
Система (c)	**75**	25	3	**0,67**	5,6	394
Система (d)	99	1	**99**	0,55	4,7	**495**

Графічний вигляд метрики RDM зображено на рис. 1, який відображає залежності DM (область червоного кольору) та DFM (область зеленого кольору) від CA для чотирьох (A, B, C, D) різних систем. На осі абсцис розташовано значення CA, на осі ординат – кількість модулів системи.

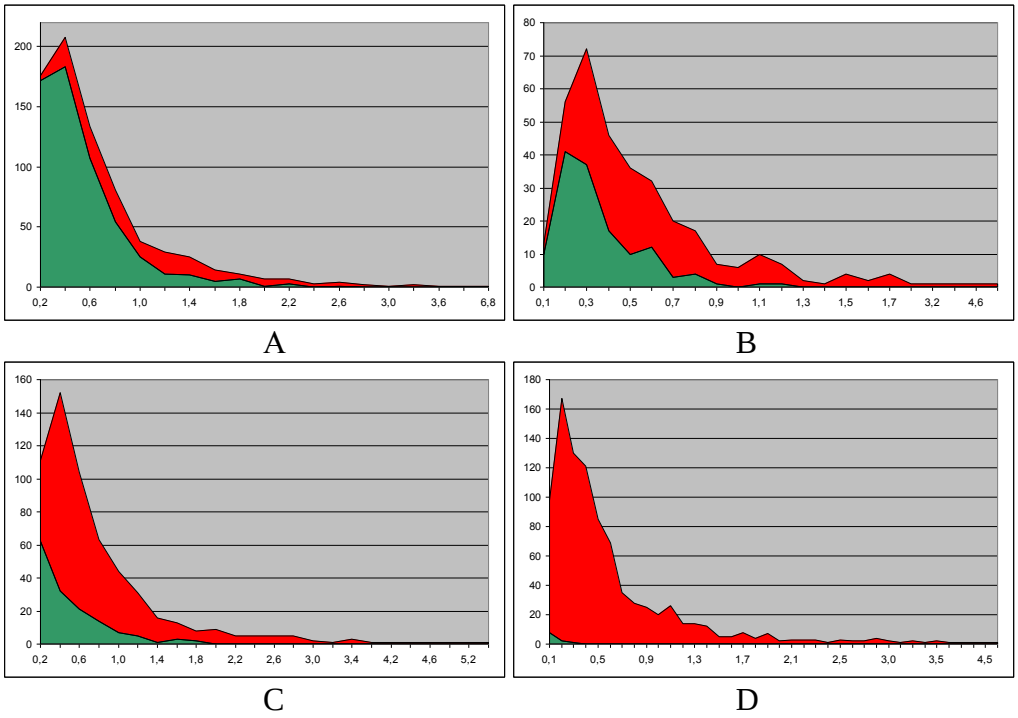


Рис. 1. Графічне зображення метрики RDM для різних систем

На рис. 1 видно, що система A має найнижчий показник дефектності коду. RDM = 0,28. Це показник “чистого коду”. За інших рівних умов верифікація цієї системи забере менше часу і буде дешевшою. SA=415. AA=0,56. Це середні показники. Максимальна CA=6,8. Це найвищий показник серед систем. Окремі модулі цієї системи складніші, ніж модулі інших систем. Щоб уникнути проблем з налагодженням і підтримкою складних модулів, необхідно виконати їх рефакторинг та декомпозицію.

Наступною за рівнем дефектності модулів іде система B. У цієї системи співвідношення між DM та DFM становить відповідно 60% і 40%. Це середні показники. RDM=1,5. SA=173. AA=0,51. Максимальна CA=5,1. Це найнижчі показники серед систем. Ця система складається з найменш складних модулів.

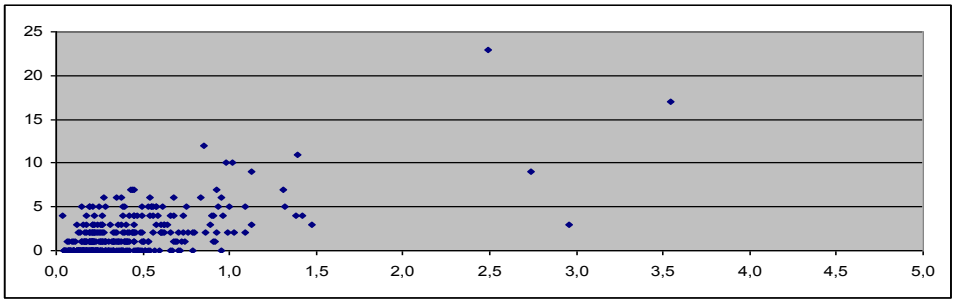
Наступною за рівнем дефектності модулів іде система C. У цієї системи співвідношення між DM та DFM становить відповідно 75 і 25 %. RDM = 3. Це найнижчий показник "сірого коду". SA = 394. Це середній показник. AA = 0,67. Це найвищий показник серед систем. Ця система складається з найбільш складних модулів. Щоб уникнути проблем з їх налагодженням і підтримкою, необхідно виконати рефакторинг і декомпозицію цих модулів.

Система D має найвищий показник дефектних модулів 99%. RDM = 3. Це показник "брудного коду" і низької його надійності. Незалежно від складності та розміру майже всі модулі цієї системи мають дефекти. Менеджерам необхідно виявити причини такого тривожного явища. Верифікація цієї системи буде найбільш тривалою і дорогою серед розглянутих систем. Щоб зменшити витрати, необхідна ретельна інспекція коду до початку його тестування. SA=495. Це найвищий показник серед систем. Ця система сама велика і складна, отже, потребує більше витрат на розробку і верифікацію, ніж системи A, B і C. AA=0,55. Максимальна CA=5,1. Це середні показники серед систем.

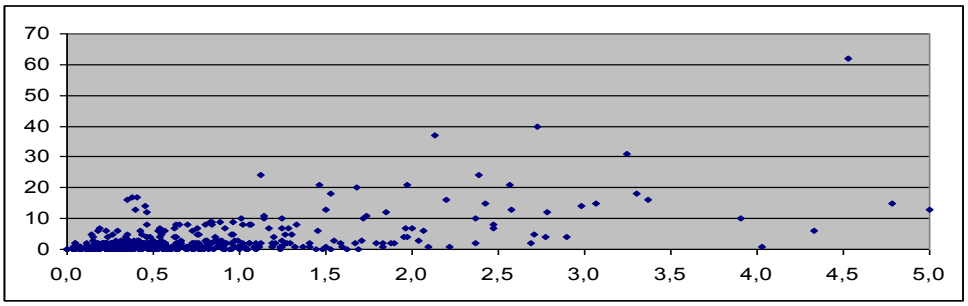
Метрика RDM разом із CA, SA і AA дають фахівцям чітку картину властивостей та надійності розроблюваної системи, дозволяють планувати ресурси і процеси верифікації та рефакторингу.

Для розрахунку CA, SA і AA ми застосовували спеціалізований програмний засіб, розроблений для цілей дослідження. Його простий алгоритм полягає в обчисленні оцінок за формулами (1), (2), (3) і (4). Такий засіб можуть розробити фахівці будь-якої софтверної компанії. У разі паралельної обробки великих обсягів даних програмну реалізацію цього нескладного алгоритму можна розпаралелити на ядра процесора або на робочі вузли апаратного кластера за допомогою системи Spark. Далі ми розглянемо другу запропоновану метрику.

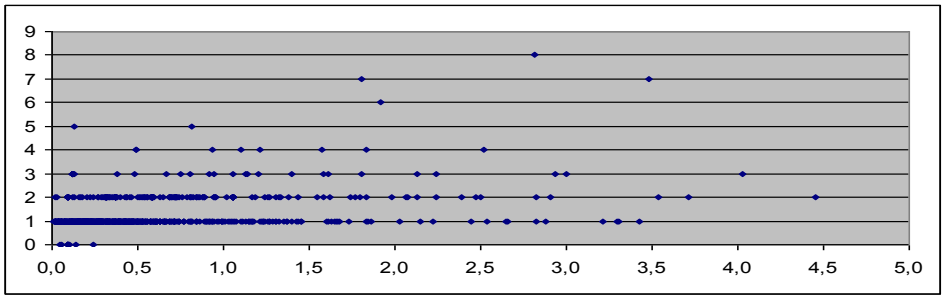
Метрика локалізації дефектів у модулях. Графічна метрика локалізації дефектів у модулях (Defects Localizing in modules, DLM) показує скупчення дефектів у модулях системи для кожного інтервалу складності від найменшого до найбільшого значення CA з кроком 0,2. Діаграми чотирьох різних систем зображено на рис. 2. Системи на рис. 2 не повторюють системи на рис.1. На діаграмах рис. 2 на осі абсцис розташовано значення CA, на осі ординат – кількість дефектів у модулях системи. Крапки на діаграмах відображають дефектні ($y > 0$) та бездефектні ($y = 0$) модулі системи.



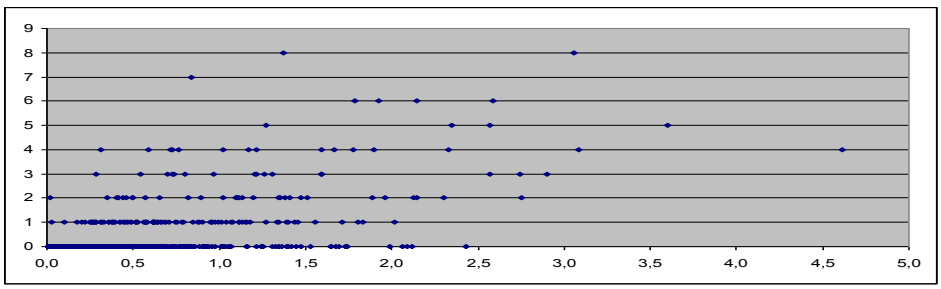
A



B



C



D

Рис. 2. Графічне зображення метрики DLM для різних систем

У системі A основна маса дефектів (найчастіше від 1 до 5) локалізована в модулях із CA<1,5. Це невелика локалізація дефектів, що спрощує і здешевлює верифікацію. Максимальна кількість дефектів в одному модулі понад 20. Система має значну кількість бездефектних модулів.

У системі B дефекти (найчастіше від 1 до 10) більше розсіяні за кодом. У цієї системи дефекти локалізовані в модулях 0<CA<3, і локалізація дефектів більше, ніж у системи A. Верифікація системи B потребує більше часу, зусиль і коштів, ніж верифікація системи A за інших рівних умов. Максимальна кількість дефектів в одному модулі більше 60. Система має значну кількість бездефектних модулів.

Локалізація дефектів у модулях систем C і D схожа, вони більші, ніж у попередніх систем. Верифікація цих систем забере більше часу, ніж попередніх. Максимальна кількість дефектів в одному модулі однакова для цих систем. Відмінність систем C і D полягає в тому, що в системі D багато бездефектних модулів, а в системі C бездефектних модулів тільки 4. Всі інші модулі містять дефекти, найчастіше 1 або 2. Система C має найбільшу локалізацію дефектів.

Якщо ранжувати системи за розміром локалізації дефектів, то найменша локалізація спостерігається у системи A. Далі йде система B, за нею система D. Найбільшу локалізацію дефектів має система C. Якщо ранжувати системи за дефектністю складних модулів, то найменш дефектною буде система A. За 2,5 < CA < 5 система A має всього чотири дефектних модулі, система D має 10 дефектних модулів, системи B і C мають понад 20 дефектних модулів.

Проведений аналіз дозволяє прогнозувати таке. За інших рівних умов найменш тривалою і витратною буде верифікація системи A через найменшу локалізацію дефектів. Унаслідок найбільшої локалізації дефектів і відсутності бездефектних модулів верифікація системи C буде найбільш тривалою і трудомісткою. Найбільшу кількість дефектів буде виявлено в системі B. Цей прогноз, складений на основі аналізу метрики LDM, був підтверджений фактичними даними. Для розглянутих систем загальна кількість дефектів становила: для системи A – 632 дефектів, для системи B – 1596 дефектів, для системи C – 1213 дефектів, для системи D – 338 дефектів.

Практичне значення метрики DLM полягає в такому. Діаграму локалізації дефектів системи, подібної до розроблюваної, можна використовувати

для планування ресурсів верифікації та спрямування зусиль фахівців на модулі з більшою локалізацією дефектів.

Метрика процентного розподілу дефектів у коді. Метрика процентного розподілу дефектів у коді (Defects Percentage Distributing, DPD) обчислювалась як процентне співвідношення кількості дефектних модулів до загальної кількості модулів для кожного інтервалу складності за CA від найменшого до найбільшого значення із кроком 0,2. Графічне зображення метрики для двох систем зображено на рис. 3. На осі абсцис розташовано значення CA, на осі ординат – процент дефектів від їх загальної кількості.

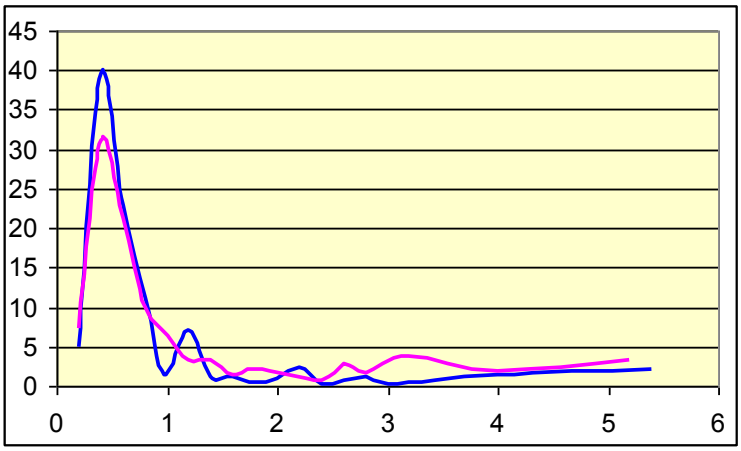


Рис. 3. Графічне зображення метрики DPD для двох систем

Графіки показують, що основна частина дефектів у цих системах перебуває в модулях з оцінкою CA<1. Практичний аспект метрики DPD полягає в можливості використання її для спрямування зусиль фахівців на такі модулі нової системи, які містять найбільшу частину дефектів.

Метрика імовірності виявлення дефектів. Метрика імовірності виявлення дефектів (одного або кількох) у модулі (Probability of Defects Detection, PDD) обчислювалась як імовірність виявлення дефектів у модулях для кожного інтервалу складності за CA від найменшого до найбільшого значення із кроком 0,2. Графічне зображення метрики для двох систем зображено на рис. 4. На осі абсцис розташовано значення CA, на осі ординат – імовірність виявлення дефектів.

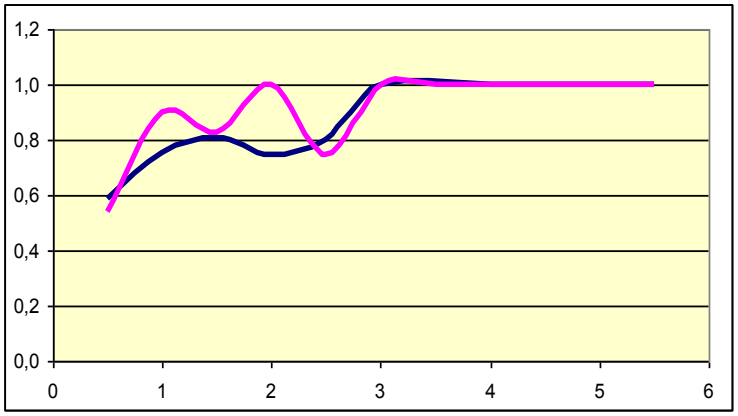


Рис. 4. Графічне зображення метрики PDD для двох систем

Початкова координата залежності на осі Y у цих систем близька і становить приблизно 0,6. Це означає, що з кожних десяти модулів мінімальної складності шість модулів містять дефекти. Обидві криві містять прямий відрізок (y=1) за CA=3. Це та частина коду, в якій всі модулі містять один або кілька дефектів. Практичний аспект метрики полягає в такому. Аналіз DPD подібної системи дозволяє фахівцям виявляти модулі з DPD = 1 в новій системі для обов'язкової їх верифікації.

Метрика модульної щільності дефектів (Modular Defect Density, MDD) обчислювалась як кількість дефектів в одному модулі системи для кожного інтервалу складності за CA від її найменшого до найбільшого значення із кроком 0,2. Після оцінювання MDD ми зобразили залежність значень MDD від CA на рис. 5. На осі абсцис розташовано значення CA, на осі ординат – значення MDD.

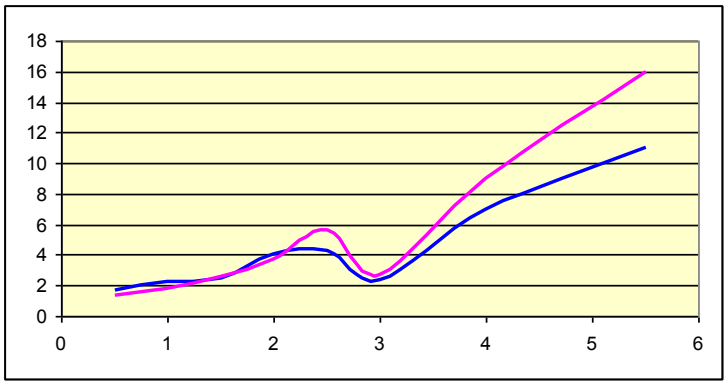


Рис. 5. Графічне зображення метрики MDD для двох систем

На рис. 5 ми бачимо зростання нелінійної залежності, близької до експоненціальної. Практичний аспект метрики полягає в такому. Знання та аналіз MDD дозволяє фахівцям спрямувати зусилля верифікації на модулі з найбільшою кількістю дефектів у них. Наприклад, для цих систем це модулі, для яких 4<CA<5,5. Але слід розуміти, що зазвичай таких модулів небагато, і кількість виявлених у них дефектів становитиме невелику частину від їх загальної кількості.

Висновки з данного дослідження і перспективи подальших розвідок у даному напрямку. В роботі виконано аналіз наявних метрик надійності програмних систем. Виявлені недоліки цих метрик. Установлена необхідність розробки нових метрик надійності на основі залежностей дефектності вихідного програмного коду від його складності. Для оцінювання складності запропоновані показники: комплексна оцінка складності коду модуля, середня оцінка складності модулів системи та сумарна оцінка складності системи.

Описана процедура розробки метрик надійності. На основі комплексних оцінок складності коду модулів і кількості дефектів у модулях запропоновано п'ять метрик надійності коду:

1. Метрика співвідношення між дефектними та бездефектними модулями (Ratio between DM and DFM, RDM);
2. Метрика локалізації дефектів у модулях (Defects Localizing in Modules, DLM);
3. Метрика процентного розподілу дефектів у коді (Defects Percentage distributing, DPD);
4. Метрика імовірності виявлення дефектів у модулях (Probability of Defects Detection, PDD);
5. Метрика модульної щільності дефектів (Modular Defect Density, MDD).

Значення метрик надійності розраховуються для раніше розроблених і верифікованих систем або їхніх частин, для яких відомі метричні оцінки складності та кількість дефектів.

Запропоновані метрики розраховано та візуалізовано для ряда систем. Проведеной аналіз метрик та встановлено напрями їх практичного використання фахівцями софтверних компаній. Метрики надійності можуть бути використані для планування ресурсів та виконання ефективної верифікації новоствореного коду нових ітерацій, частин, версій, функцій або нових систем конкретного розробника. Метрики надійності можуть бути використані для будь-яких систем, подібних до новорозробленої системи за функціональністю, метричними оцінками складності, кваліфікацією розробників, рівнем процесів та методологією розробки.

Надалі необхідно дослідити метрики надійності для подібних систем. На основі метрик складності та надійності доцільно розробити нові моделі та методи підвищення надійності програмних систем.

Список використаних джерел:

1. ISO/IEC 9126-1:2001 Software engineering – Product quality – Part 1: Quality model / ISO: офіційний сайт. URL: https://www.iso.org/standard/22749.html

2. ISO/IEC TR 9126-2:2003 Software engineering – Product quality – Part 2: External metrics / ISO: офіційний сайт. URL: https://www.iso.org/standard/22750.html

3. ISO/IEC TR 9126-3:2003 Software engineering – Product quality – Part 3: Internal metrics / ISO: офіційний сайт. URL: https://www.iso.org/standard/22891.html

4. ISO/IEC 25010:2011 Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models / ISO: офіційний сайт. URL: https://www.iso.org/standard/35733.html

5. IEC 61513:2001 Nuclear power plants – Instrumentation and control systems important for safety – General requirements for systems / IEC Webstore International Electrotechnical Commission : офіційний сайт. URL: https://webstore.iec.ch/publication/19812

6. IEC 60880-2010 Nuclear power plants. Instrumentation and control systems important for safety. Software aspects for computer-based systems performing category A functions / Електронний фонд правової і нормативно-технічної документації: офіційний сайт. URL: http://docs.cntd.ru/document/gost-r-mek-60880-2010

7. IEEE 982.1-2005 – IEEE Standard Dictionary of Measures of the Software Aspects of Dependability / IEEE Xplore Digital Library: офіційний сайт. URL: https://ieeexplore.ieee.org/document/1634994

8. IEEE 610.12-1990 – IEEE Standard Glossary of Software Engineering Terminology / IEEE Xplore Digital Library: офіційний сайт. URL: https://ieeexplore.ieee.org/document/159342

9. IEEE 1061-1998 – IEEE Standard for a Software Quality Metrics Methodology / IEEE Xplore Digital Library: офіційний сайт. URL: https://ieeexplore.ieee.org/ document/749159

10. *Chidamber S., Kemerer C.* A Metrics Suite for Object-Oriented Design. *IEEE Transactions on Software Engineering.* 1994. № 20. P. 476–493.

11. *Табунщик Г. В., Кудерметов Р. К., Брагіна Т. І.* Інженерія якості програмного забезпечення: навчальний посібник. Запоріжжя: ЗНТУ. 2013. 180 с.

12. *Маєвський Д. А.* Проблеми забезпечення надійності при експлуатації динамічних інформаційних систем. *Системи обробки інформації.* 2012. № 7. С. 99–103.

13. Tera-PROMISE Home. The PROMISE Repository of empirical software engineering data / Міжнародна наукова конференція PROMISE: офіційний сайт. URL: http://openscience.us/repo/defect/ck/

References:

1. International Organization for Standardization/International Electrotechnical Commission (2018), ISO/IEC 9126-1:2001 Software engineering – Product quality – Part 1: Quality model, ISO official site, available at: https://www.iso.org/standard/22749.html

2. International Organization for Standardization/International Electrotechnical Commission (2018), ISO/IEC TR 9126-2:2003 Software engineering – Product quality –

Part 2: External metrics, ISO official site, available at: https://www.iso.org/standard/227509.html

3. International Organization for Standardization/International Electrotechnical Commission (2018), ISO/IEC TR 9126-3:2003 Software engineering – Product quality – Part 3: Internal metrics, ISO official site, available at: https://www.iso.org/ standard/22891.html

4. International Organization for Standardization/International Electrotechnical Commission (2018), ISO/IEC 25010:2011 Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models, ISO official site, available at: https://www.iso.org/standard/35733.html

5. International Electrotechnical Commission (2018), IEC 61513:2001 Nuclear power plants – Instrumentation and control systems important for safety – General requirements for systems / IEC Webstore International Electrotechnical Commission, official site, available at: https://webstore.iec.ch/publication/19812

6. International Electrotechnical Commission (2018), IEC 60880-2010 Nuclear power plants. Instrumentation and control systems important for safety. Software aspects for computer-based systems performing category A functions / Electronic Legal and Regulatory Documentation Fund, official site, available at: http://docs.cntd.ru/document/gost-r-mek-60880-2010

7. IEEE Xplore Digital Library (2018), 982.1-2005 – IEEE Standard Dictionary of Measures of the Software Aspects of Dependability / Institute of Electrical and Electronics Engineers, official site, available at: https://ieeexplore.ieee.org/document/1634994

8. IEEE Xplore Digital Library (2018), 610.12-1990 – IEEE Standard Glossary of Software Engineering Terminology / Institute of Electrical and Electronics Engineers, official site, available at: https://ieeexplore.ieee.org/document/159342

9. IEEE Xplore Digital Library (2018), 1061-1998 – IEEE Standard for a Software Quality Metrics Methodology / Institute of Electrical and Electronics Engineers, official site, available at: https://ieeexplore.ieee.org/document/749159

10. Chidamber S. A Metrics Suite for Object-Oriented Design [Text] / S. Chidamber, C. Kemerer // IEEE Transactions on Software Engineering – 1994. – № 20, P. 476-493.

11. Tabunshhy`k G.V., Kudermetov R. K. and Bragina T. I. (2013), Inzheneriya yakosti programnogo zabezpechennya: navchal`ny`j posibny`k [Engineering of the software quality: Manual], Press Zaporizhzhya, ZNTU, 180 p. [Ukraine]

12. Mayevs`ky`j, D. A. (2012), "*Problemy` zabezpechennya nadijnosti pry` ekspluataciyi dy`namichny`x informacijny`x sy`stem*" ["Reliability assurance problems during operation of dynamic information systems"], journal *Sy`stemy` obrobky` informaciyi* [Information processing systems], vol. 7, pp. 99-103 [Ukraine]

13. Tera-PROMISE Home. The PROMISE Repository of empirical software engineering data (2018), International scientific conference PROMISE, official site, available at: http://openscience.us/repo/defect/ck/

DOI: https://doi.org/10.32836/2521-6643-2018.2-56.3
УДК 656:51-74

Н. В. Халіпова, кандидат технічних наук, доцент, доцент кафедри транспортних систем та технологій Університету митної справи та фінансів
І. Ю. Леснікова, кандидат технічних наук, доцент, доцент кафедри транспортних систем та технологій Університету митної справи та фінансів
Н. А. Ісрафілова, студентка Університету митної справи та фінансів

ОПТИМІЗАЦІЯ ТРАНСПОРТНО-ЛОГІСТИЧНИХ ПРОЦЕСІВ ПРОМИСЛОВОГО ПІДПРИЄМСТВА

Аналіз транспортно-логістичних процесів підприємства на сучасному етапі засвідчив нерівномірний стан та певні диспропорції їх розвитку. Виявлено, що проблема являється комплексною і одним з важливих недоліків є неефективний розподіл та спосіб використання наявного автопарку. Встановлено, що для розвитку промислового підприємства важливим аспектом є організація ефективних транспортно-логістичних процесів, при плануванні яких мають застосовуватись загальні принципи, як то повне задоволення транспортних потреб структурних підрозділів підприємства, ефективне використання технічних засобів та різних видів ресурсів, розгляд роботи всіх видів транспорту в комплексі.

Аналіз засвідчує, що при плануванні роботи транспорту найбільш складною ділянкою є оперативне планування, функції якого полягають у встановлені погоджених обсягів роботи транспорту та їх підрозділів на найближчий час, маршрутизації перевезень, організації узгодженої роботи транспортного та структурних підрозділів підприємства. Для безперервного виробництва на підприємстві необхідне постійне оперативне оновлення існуючих рішень щодо транспортно-логістичного забезпечення та складських рішень.

Для вирішення задачі даної виробничої ситуації запропоновано використовувати багатоетапний алгоритм, що включає послідовний розв'язок задач: лінійного програмування з обмеженнями на ресурси підприємства; транспортної задачі і задачі про найкоротшу відстань від постачальників до складів для перевезення заданих обсягів сировини з найменшими витра-

тами; подальшого формування висновків та пропозицій щодо поліпшення розв'язку і прийняття остаточного варіанту. Для розв'язку задач оптимізації використовувалися Надбудови Microsoft Excel "Пошук рішення".

На прикладі ПрАТ "ДКХЗ" холдингу Метінвест проведено аналіз існуючого транспортно-логістичного забезпечення та визначено оптимальні схеми постачання сировини для забезпечення функціонування смолопереробного цеху. Для безперервної роботи смолопереробного цеху необхідно мати відповідні складські ємності для зберігання вихідної сировини. На основі аналізу оптимальних схем постачання сировини для забезпечення виробництва визначено ємності для зберігання та оптимальні схеми доставки смоли кам'яновугільної.

Результати дослідження свідчать про необхідність постійного оперативного оновлення існуючих рішень та можуть бути використані при удосконаленні транспортно-логістичної складової процесів промислових підприємств

Ключові слова: *транспортно-логістичні процеси; промислове підприємство; оптимальні схеми постачання.*

Статья посвящена решению проблемы организации эффективных транспортно-логистических процессов на промышленном предприятии. На примере ЗАО "ДКХЗ" холдинга Метинвест проведен анализ существующего транспортно-логистического обеспечения и определены оптимальные схемы поставки сырья и складские решения. Результаты исследования свидетельствуют о необходимости постоянного оперативного обновления существующих решений и могут быть использованы при совершенствовании транспортно-логистической составляющей процессов промышленных предприятий.

Ключевые слова: *транспортно-логистические процессы; промышленное предприятие; оптимальные схемы поставки.*

Analysis of transport-logistical processes of the enterprise at the present stage showed uneven condition and certain disproportions in their development. Was discovered that the problem is complex and one of the important drawbacks is the inefficient allocation and use of the existing transportation fleet. It is established that for the development of an industrial enterprise an important aspect is the organization of efficient transport and logistics processes, the planning of which should use the general principles, such as full satisfaction of enterprise structural units transport needs, efficient use of technical means and different types of resources, consideration of work of all types of transport in complex.

The analysis shows that when planning the work of transport, the most difficult area is operational planning, whose functions are to establish agreed volumes of transport work and their units in the near future, routing of transportation, organization and coordinated work of transport and structural units of the enterprise. Continuous production at the enterprise requires constant prompt updating of existing solutions for transport and logistics support and warehouse solutions.

To solve the problem of given production situation, it is proposed to use a multi-stage algorithm, which includes a sequential tasks solution: linear programming with limitations on the resources of the enterprise; the transport task and the task of the shortest distance from suppliers to warehouses for transportation of specified volumes of raw materials with the least cost; further formulation of conclusions and recommendations regarding the solution improvement and making the final decision. Microsoft Excel 'Solution Finder' plugin was used to solve our optimization tasks.

On the example of PrJSC Metinvest holding, an analysis of the existing transport and logistics support was carried out and the optimal raw material supply schemes were determined to ensure the operation of the resin-processing manufactory department. For continuous operation of the resin-processing department, it is necessary to have appropriate capacities for raw materials storaging. Based on the analysis of optimal raw material delivery schemes to support manufactoring, storage tanks capacity and the optimal delivery schedules for coal tar have been identified.

The results of the study indicate the need for continuous prompt updating of existing solutions and can be used to improve the transport and logistics component of industrial enterprise processes.

Key words: *transport-logistical processes; industrial enterprise; optimal supply schemes.*

Вступ. Аналіз транспортно-логістичних процесів підприємства на сучасному етапі засвідчив нерівномірність та певні диспропорції їх розвитку. Проблема являється комплексною і одним з важливих недоліків є неефективний розподіл та спосіб використання наявного автопарку. Автомобільний транспорт бере участь у різноманітних виробничих процесах: працює в цехах промислових підприємств, використовується при ремонтах та для перевезення матеріалів і обладнання, при навантажувально-розвантажувальних роботах та ін. Це обумовлює актуальність проблеми удосконалення транспортно-логістичних процесів промислового підприємства.

Постановка задачі. Аналіз сучасного стану досліджень у сфері транспортної логістики свідчить, що ефективна реалізація функції транспорту-

вання неможлива без комплексного планування її разом з іншими логістичними функціями: спільного планування транспортних процесів на різних видах транспорту; забезпечення технологічної єдності транспортно-складського процесу; спільного планування транспортного процесу зі складським та виробничим [1].

На думку спеціалістів важливою перевагою логістичного управління є підвищення рівня саме транспортного обслуговування, що досягається не тільки і не стільки завдяки функціонуванню транспортних підрозділів, скільки в результаті злагодженого виконання комплексу робіт, пов'язаних із постачанням, збутом та перевезенням продукції [2].

Визначенню аспектів спрямованих на ефективну реалізацію функції транспортування на основі застосування транспортних технологій, пов'язаних із логістичними процедурами вибору, обґрунтуванню необхідності їх застосуванні та аналізу організації транспортування в логістичних системах присвячено [3]. Перспективами їх подальших досліджень є пошук нових, максимально ефективних способів оптимізації транспортного процесу, вдосконалення логістичних систем на основі покращення реалізації функції транспортування, виявлення нових напрямів і підходів до розвитку транспортної логістики [3].

На відміну від старих методів ізольованого управління вантажними перевезеннями на підприємствах здійснюється перехід до об'єднаного чи скоординованого управління вантажопотоками. Взаємозв'язок і взаємозалежність усіх логістичних елементів, включно із транспортом, обумовили необхідність застосування комплексного підходу до їх подальшого розвитку [4].

Також необхідна адаптація існуючих положень до специфічних умов діяльності транспортних структурних підрозділів промислових підприємств [5].

Оперативне планування є завершальною ланкою в системі планування діяльності підприємства, виступає як засіб виконання довго-, середньо- та короткострокових планів і є одним із важелів оперативного управління виробництвом. Посилення нестабільності сфери функціонування підприємств у динамічних умовах ринкової економіки підвищує роль оперативного планування. Суть оперативного планування полягає в детальній розробці планів підприємств та їхніх підрозділів (цехів, бригад, ферм, навіть робочих місць) на короткі проміжки часу – окремий виробничий період, місяць, декаду, робочий тиждень, добу, зміну. При цьому опрацювання планів органічно поєднується з розв'язанням питань організації їх виконання та поточного регулювання [6].

Підсумовуючи, можна сказати, що технічна складова організації транспортно-логістичних процесів – важливий аспект розвитку промислового підприємства. Інформаційне забезпечення вражає своїм різноманіттям, про-

те, через швидкий технічний прогрес дуже швидко застаріває, тож існує постійна потреба в дослідженні ефективності нових видів інформаційного забезпечення та їх практичного використання.

Мета статті – це аналіз сучасного стану транспортно-логістичних процесів на промисловому підприємстві та визначення основних напрямків їх удосконалення. На прикладі ПрАТ "ДКХЗ" холдингу Метінвест проаналізувати існуюче транспортно-логістичне забезпечення та визначити оптимальні схеми постачання сировини та складські рішення.

Результати дослідження. Забезпечення раціонального обслуговування транспорту промислових підприємств є складною задачею. Її розв'язання потребує максимального скорочення часу знаходження рухомого складу на підприємстві, їх пробігу по шляхах загального користування та по шляхах промислових підприємств, а також можливу концентрацію переробки вантажів, які відповідають потребам технології виробництва, найкращому використанню транспортних засобів та капіталовкладень. Істотне значення має при цьому чітка взаємодія в роботі зовнішнього транспорту із внутрішнім транспортом підприємств [7].

Приватне акціонерне товариство "Дніпровський коксохімічний завод" (далі – ПрАТ "ДКХЗ") спеціалізується на виробництві коксу, смоли сульфату амонію і продуктів переробки. Продукція споживається металургійними, енергетичними, хімічними та іншими промисловими компаніями. Це обумовлює необхідність забезпечення надійності та якості процесу перевезень, потребує враховувати і задовольняти запити кожного конкретного споживача.

ПрАТ "ДКХЗ" входить до Метінвесту – міжнародної вертикально інтегрованої гірничо-металургійної компанії. У структуру Метінвесту також входять видобувні та металургійні підприємства на Україні, в ЄС і США. Вертикальна інтеграція дозволяє управляти всіма етапами: видобутком сировини, виробництвом, поставками і продажами готової продукції [8].

ПрАТ "ДКХЗ" є одним з небагатьох підприємств в даній галузі в Україні з повним циклом переробки хімічних продуктів коксування. Тут здійснюється підготовка вугільної шихти, виробництво коксу, уловлювання хімічних продуктів коксування, переробка кам'яновугільної смоли.

Підприємство виробляє широкий спектр коксової і хімічної продукції, яка відповідає європейським і міжнародним стандартам. Продукцію підприємства за видами та її структуру зображено у табл. 1 та на рис. 1.

Предметом діяльності ПрАТ "ДКХЗ" є виробництво та реалізація коксової, хімічної продукції та хімічних речовин, виробництво та реалізація іншої продукції виробничо-технічного призначення, зовнішньоекономічна діяльність та ін.

Таблиця 1

Продукція ПрАТ "ДКХЗ" за видами

Продукція ПрАТ "ДКХЗ"	
– кокс доменний – горішок коксовий – дрібняк коксовий – смола кам'яновугільна – амонію сульфат – феноляти	– бензол сирий кам'яновугільний – пек кам'яновугільний – масла кам'яновугільні – полімери бензольних відділень

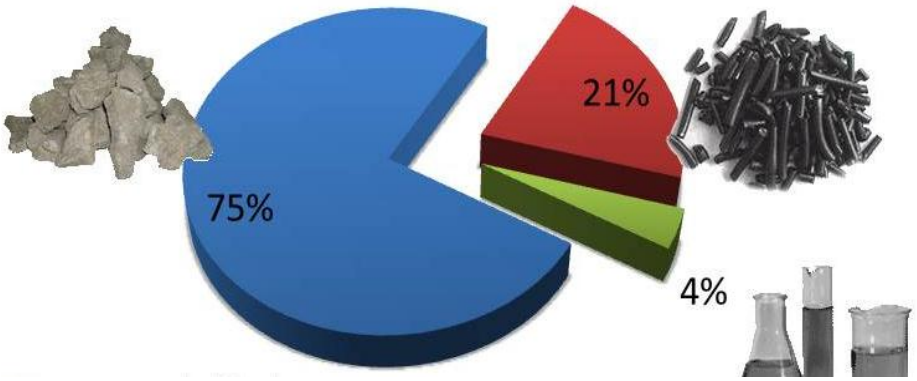


Рис. 1. Структура продукції підприємства: 75 % – кокс валовий, 21 % – продукти переробки смоли, 4 % – інші хімічні продукти

До основних цехів, які зайняті різними стадіями виготовлення виробів основного виробництва, тобто виробів, що йдуть на поставку та реалізацію відносяться: коксовий цех, вуглепідготовчий цех, цех уловлювання хімічних продуктів коксування та смолопереробний цех.

Допоміжні цехи випускають вироби допоміжного призначення, які споживаються усередині заводу та не йдуть на поставку. До них належать: ремонтно-механічній цех, теплосиловий цех, енергоремонтний цех, цех з ремонту коксових печей, автотранспортний цех, цех залізничного транспорту.

Загальнозаводські обслуговуючі господарства організовуються для обслуговування основних і допоміжних цехів. До них відносяться складське та енергетичне господарства, лабораторії.

Для ефективного управління процесом виробництва на підприємстві розроблена оптимальна організаційна структура управління, основною відмінною рисою якої є встановлення підпорядкованості по центрах функціо-

нальної відповідальності. Для централізації ремонтних служб, єдиного планування та організації ремонтів, забезпечення його безаварійної роботи, підвищення якості технічного обслуговування і зниження витрат підприємства на його проведення в 2010 р. був створений Сервісний центр, що інтегрує в своїй структурі механічну і електричну служби [9].

Аналіз системи діяльності автотранспортного цеху вказує на його вагому роль у господарській діяльності. Ним здійснюються перевезення усередині цехів і між ними, забезпечується зв'язок цехів і складів, а також зв'язок з магістральним транспортом при вивозі-завезенні сировини і продукції. Від чіткості і надійності його роботи багато в чому залежить ритм підприємства.

Управління автотранспортним цехом в сучасних умовах потребує добре продуманої організації, що дозволяє приймати оптимальні рішення в умовах нестабільної економічної ситуації, характерної для перехідного періоду на заводі. Одне з головних завдань полягає в тому, щоб домогтися ритмічної роботи всіх ланок управління, високої оперативності й чіткості в аналізі поточної інформації, подальшій підготовці, прийнятті та реалізації управлінських рішень [10].

Основні проблеми виходять зі специфіки функціонування цеху та організації роботи всього заводу. Серед них – застарілі методи контролю та аналізу роботи; недосконале планування та, як наслідок, задоволення заявок не в повному обсязі; необхідність запровадження заходів економії витрат паливно-мастильних матеріалів; утримання специфічних та сезонних видів транспорту. Розв'язання даних проблем повинне бути комплексне.

Логістична система пред'являє до своєї мережі наступні вимоги:

– швидкий і надійний, переважно автоматизований збір інформації і даних про транспортні засоби і виробників товарної продукції;

– структурування внутрішньої інформаційної системи прийняття рішень, що у кожен момент містить актуальну інформацію про хід транспортних процесів.

Також в даний час широко поширюються технології безпаперового обміну інформацією [11].

Загальними принципами планування є повне задоволення транспортних потреб структурних підрозділів підприємства, ефективне використання технічних засобів та різних видів ресурсів, розгляд роботи всіх видів транспорту в комплексі.

При плануванні роботи транспорту найбільш складною ділянкою є оперативне планування. Його функції полягають у встановлені погоджених обсягів роботи транспорту та їх підрозділів на найближчий час, маршрутизації перевезень, організації узгодженої роботи транспортного та структурних підрозділів підприємства.

Оскільки якість планування підвищується разом з ростом повноти інформації і швидкості обробки даних, всі підрозділи підприємства повинні оснащуватися сучасним програмним забезпеченням, що утворить єдину мережу, що безсумнівно значно спростить процес прийому й обробки даних, як вихідних, так і вхідних.

Для безперервного виробництва на підприємстві необхідне постійне оперативне оновлення існуючих рішень щодо транспортно-логістичного забезпечення та складських рішень.

Тож визначимо оптимальні схеми постачання сировини для забезпечення функціонування смолопереробного цеху. Від якості сировини залежать показники готової продукції. Від того, яку сировину та в яких пропорціях додати – залежить виконання плану.

Для безперервної роботи смолопереробного цеху необхідно мати відповідні складські ємності для зберігання вихідної сировини.

В загальному виді постановка задачі наступна. Постачання сировини ведеться від k підприємств використовуючи існуючу транспортну мережу для якої відомі відстані між зв'язними точками (об'єктами мережі) окремих ділянок шляхів можливого постачання.

Загальна схема виробничого процесу наведена на рис. 2.

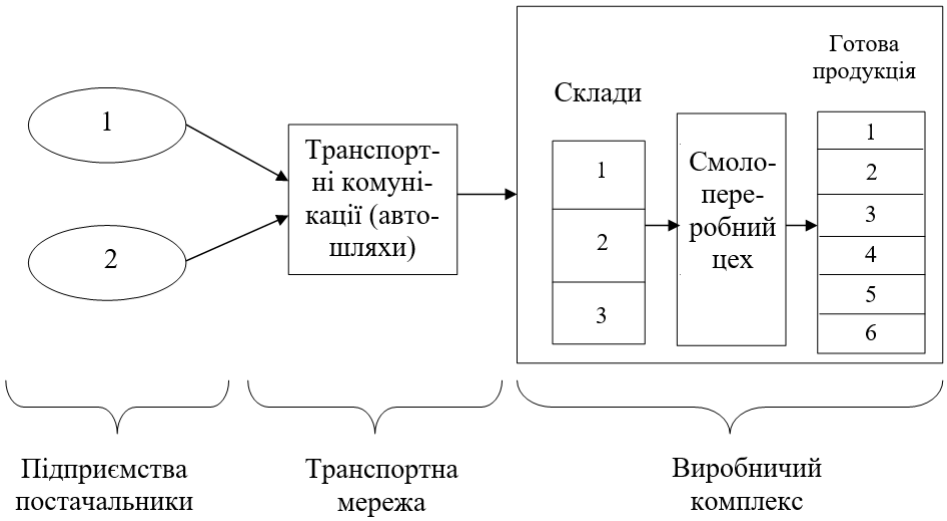


Рис. 2. Загальна схема виробничого процесу

Для забезпечення безперебійного виробництва продукції смолопереробного цеху необхідно розрахувати складські ємності та вибрати схему постачання сировини з інших підприємств.

Необхідно визначити ємність складів сировини згідно з планом виробництва та мінімальною собівартістю виробництва хімічних речовин при обмеженнях на витрати електроенергії A кВт/рік та пару V Гкал.

Питомі норми витрат сировини, електроенергії та пару, а також собівартість переробки 1 т смоли необхідної якості беремо з внутрішніх даних по підприємству.

Введемо наступні умовні позначення:

X_J – кількість кінцевої продукції ($j = 1, n$);

b_i – кількість складів для сировини ($j = 1, m$);

A – задані обсяги електроенергії, кВт/рік;

V – задані обсяги пару, Гкал/рік;

Q – план переробки смоли кам'яновугільної, т/рік;

a_j – питомі норми витрат електроенергії, кВт/т;

V_j – питомі норми витрат пару ГКал/т;

q_{ij} – питомі норми витрат сировини, т/т;

C_j – собівартість смоли кам'яновугільної, грн/т;

C_{ki} – питомі транспортні витрати на один кілометр, грн/км;

x_{ki} – обсяг перевезень з k – го підприємства до i -го складу, т.

Алгоритм вирішення задач для розв'язання даної виробничої ситуації наведено на рис. 3.

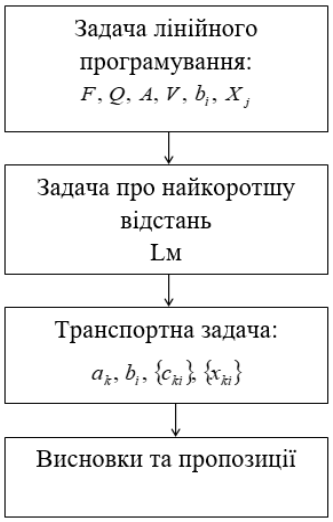


Рис. 3. Алгоритм вирішення задач

У відповідності до рис. 3 необхідно розв'язати наступні задачі:

1. Задача лінійного програмування з урахуванням обмеження

$$F = \sum_{j=1}^{n} e_j \cdot x_j \to \min . \quad (1)$$

2. Визначення кількості планів виробництва за формулою

$$\sum_{j=1}^{n} x_j = Q . \quad (2)$$

3. Оцінка витрат електроенергії за формулою

$$\sum_{j=1}^{n} a_j \cdot x_j \le A . \quad (3)$$

4. Визначення витрати пару за формулою

$$\sum_{j=1}^{n} V_j \cdot x_j \le V . \quad (4)$$

Витрати i-ї сировини визначаємо за формулою

$$\sum_{j=1}^{n} q_y \cdot x_j \le b_i . \quad (5)$$

Транспортна задача.

Цільова функція визначається за формулою

$$F = \sum_{k=1}^{k} \sum_{i=1}^{m} c_{ki} \cdot x_{ki} \to \min . \quad (6)$$

Обсяг перевезення з k – го підприємства до i-го складу визначається через потужності кожного постачальника за формулою

$$\sum_{i=1}^{m} x_{ki} = a_k , (i = \overline{1, m}) . \quad (7)$$

Обсяг перевезення з k – го підприємства до i-го складу визначається через потреби складів у сировині за формулою

$$\sum_{k=1}^{k} x_{ki} = b_k , (k = \overline{1, k}) . \quad (8)$$

Розв'язування задач виробництва реалізується в п'ять етапів, а саме:

1 етап. Розв'язується задача лінійного програмування, але без обмежень на сировину, тобто за формулою

$$\sum_{j=1}^{n} q_y \cdot x_j \le b_i . \quad (9)$$

Згідно з обмеженням на сировину та відомим значенням x_j після рішення задачі лінійного програмування, знаходяться величини b_i (витрати на сировину) за формулою

$$b_i = \sum_{j=1}^{n} q_y \cdot x_i \ . \qquad (10)$$

Ємності складів сировини приймаються b_i. Загальна собівартість дорівнює F.

2 етап. Потужності кожного підприємства-постачальника оцінюються за формулою

$$a_k = \sum_{i=1}^{n} b_i \ . \qquad (11)$$

Розв'язується транспортна задача для $\{a_k\}$, $\{b_i\}$, та $\|C_{ki}\|$, вводячи фіктивний склад. Для одержаного варіанта постачання (прив'язка складів до постачальників $\{x_{ki}\}$, ($(k=\overline{1,k})$ – постачальників, $(i=\overline{1,m})$ – склади) необхідно вибрати найбільш вигідні маршрути постачання сировини.

3 етап. Згідно з транспортною мережею знаходяться найкоротші шляхи від постачальників до складів для перевезення обсягів сировини $\{xk_i\}$.

У результаті рішення цієї задачі знаходяться найкоротші відстані $\{L_{ki}\}$. Потім знаходяться транспортні витрати на 1 км: $C_{ki} = L_{ki} \cdot C_{ki}$.

$$F_{TP} = \sum_{k=1}^{k} \sum_{i=1}^{m} C_{ki} \cdot x_{ki} \ . \qquad (12)$$

4 етап. Знаходиться загальна сума витрат $F_0=F+F_{TP}$ та складається схема виробництва.

5 етап. Пропонуються висновки та пропозиції щодо поліпшення розв'язку. Прийняття остаточного варіанту.

Для вирішення задачі маємо такі вихідні дані: план виробництва Q=10610 т/рік; електроенергія: A=29010 кВт/рік; пар: V=4500 ГКал/рік, ціна ресурсів вказана в табл. 2.

Таблиця 2

Ціна ресурсів

Ресурс	Ціна, грн
Електроенергія (грн/кВт)	1,75
Пар (грн/Гкал)	760
Сировина I (грн/т)	105
Сировина II (грн/т)	110
Сировина III (грн/т)	103

Питомі норми витрат наведено в табл. 3.

Вартісні коефіцієнти перевезення 1 т сировини на 1 км від двох підприємств до трьох складських приміщень (в грн.) представляються у вигляді наступної матриці:

$$C = \begin{Vmatrix} 2 & 2 & 3 \\ 4 & 1 & 2 \end{Vmatrix}$$

Таблиця 3

Питомі норми на тонну переробки смоли кам'яновугільної

Показники, ресурси	Технологія переробки		
	I	II	III
Електроенергія(кВт/т)	3,30	1,80	2,00
Пар (Гкал/т)	0,40	0,46	0,50
Сировина I (т/т)	0,40	0,30	0,17
Сировина II (т/т)	0,45	0,30	0,50
Сировина III (т/т)	0,15	0,40	0,32
Собівартість (грн/т)	416,7	458,5	490,4

Мережа автомобільних шляхів постачання сировини наведена на рис. 4.

Розв'язання задачі виконуємо згідно з алгоритмом:

1. Складаємо математична модель лінійного програмування, яка розв'язується симплекс-методом:

$$F = 416{,}7 \cdot x_1 + 458{,}5 \cdot x_2 + 490{,}4 \cdot x_3 \to \min,$$

$$x_1 + x_2 + x_3 \geq 10610,$$

$$3{,}3 \cdot x_1 + 1{,}8 \cdot x_2 + 2.0 \cdot x_3 \leq 29010,$$

$$0{,}4 \cdot x_1 + 0{,}46 \cdot x_2 + 0{,}5 \cdot x_3 \leq 4500.$$

Розв'язання симплекс-методом знаходимо за допомогою Надбудови Microsoft Excel "Пошук рішення", що зображено на рис. 5.

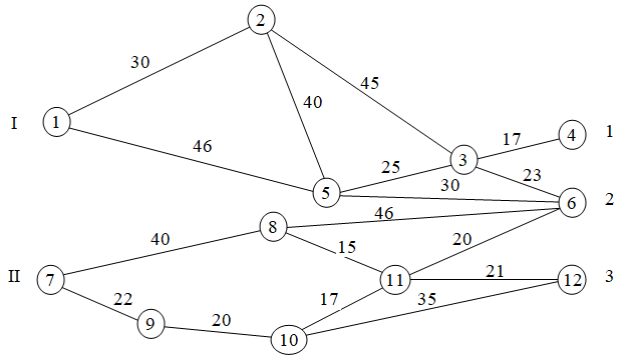


Рис. 4. Мережа автомобільних шляхів постачання сировини

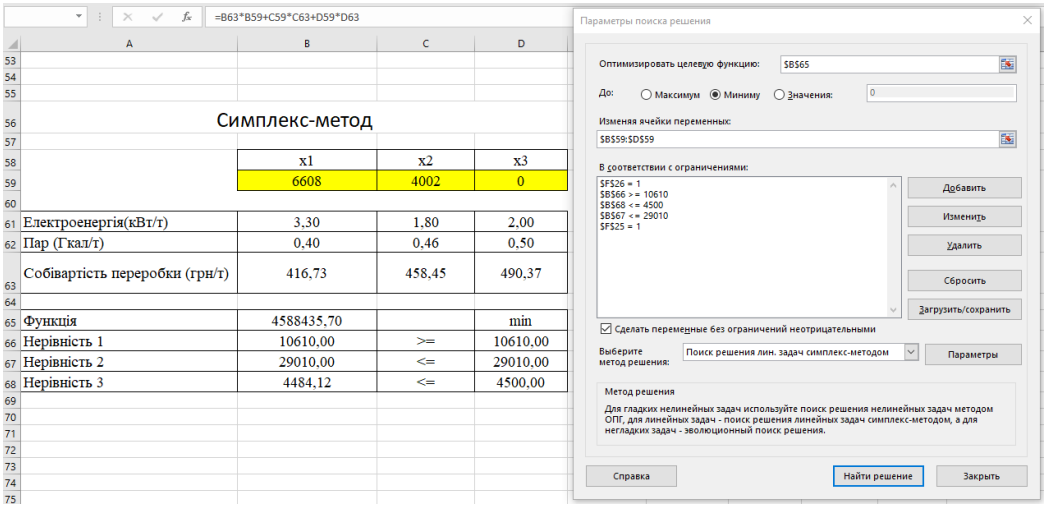


Рис. 5. Знаходження розв’язку задачі лінійного програмування

Розв’язування: $F = 4588435{,}7$ грн, $x_1 = 6608$ т, $x_2 = 4002$ т, $x_3 = 0$ т.

2. Визначаємо обмеженнями на сировину:

$$0{,}40 \cdot x_1 + 0{,}30 \cdot x_2 + 0{,}17 \cdot x_3 \le b_1,$$
$$0{,}45 \cdot x_1 + 0{,}30 \cdot x_2 + 0{,}50 \cdot x_3 \le b_2,$$
$$0{,}15 \cdot x_1 + 0{,}40 \cdot x_2 + 0{,}32 \cdot x_3 \le b_3.$$

Знаходимо потребу у кожному виді сировини:

$$b_1 = 0{,}40 \cdot 6608 + 0{,}30 \cdot 4002 + 0{,}17 \cdot 0 = 3843{,}8\text{т},$$
$$b_2 = 0{,}45 \cdot 6608 + 0{,}30 \cdot 4002 + 0{,}50 \cdot 0 = 4174{,}2\text{т},$$
$$b_3 = 0{,}15 \cdot 6608 + 0{,}40 \cdot 4002 + 0{,}32 \cdot 0 = 2592{,}0\text{т}.$$

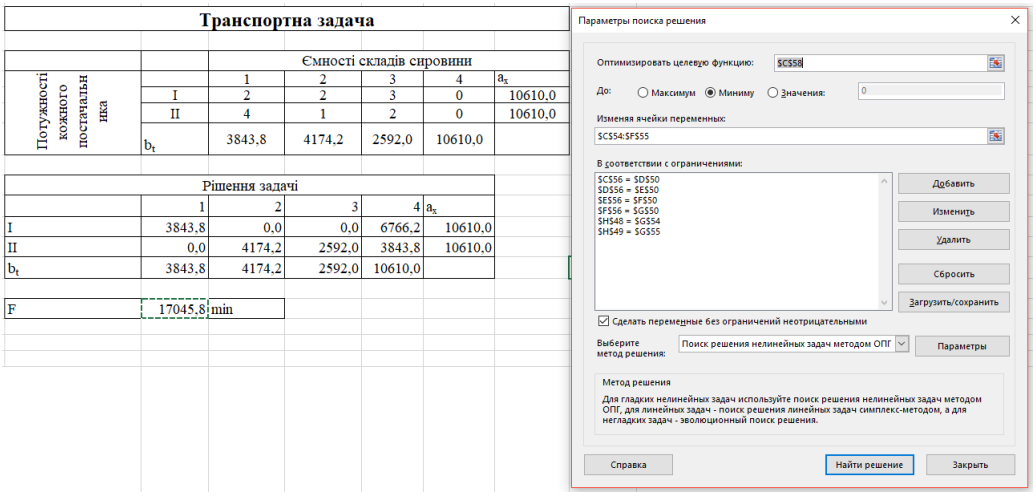
3. Розв’язуємо транспортну задачу, у якій потреба від кожного підприємства-постачальника:

$$a = a_1 = a_2 = b_1 + b_2 + b_3 = 3843{,}8 + 4174{,}2 + 2592{,}0 = 10610\text{ т},$$

Задача розв’язується з фіктивним складом $b_4 = 10610$ т, для якого

$$C_y = 0.$$

Оптимальне розв’язування транспортної задачі знаходимо за допомогою Надбудови Microsoft Excel “Пошук рішення”, що зображено на рис. 6.



Транспортна задача

Потужності кожного постачальника		Ємності складів сировини 1	2	3	4	a_x
	I	2	2	3	0	10610,0
	II	4	1	2	0	10610,0
	b_t	3843,8	4174,2	2592,0	10610,0	

Рішення задачі

	1	2	3	4	a_x
I	3843,8	0,0	0,0	6766,2	10610,0
II	0,0	4174,2	2592,0	3843,8	10610,0
b_t	3843,8	4174,2	2592,0	10610,0	

F	17045,8	min

Рис. 6. Знаходження оптимального розв’язку транспортної задачі

Тож оптимальний розв’язок транспортної задачі наведено в табл. 4.

Таблиця 4

Оптимальне розв’язування транспортної задачі

	Склад 1, т	Склад 2, т	Склад 3, т	Склад 4, т	Всього a_x, т
Постачальник I , т	3843,8	0	0	6766,2	10610,0
Постачальник II, т	0	4174,2	2592,0	3843,8	10610,0
Всього b_t, т	3843,8	4174,2	2592,0	10610,0	

Згідно з оптимальним розв’язком будуємо схему постачання сировини від підприємств до складів, схема зображена на рис. 7.

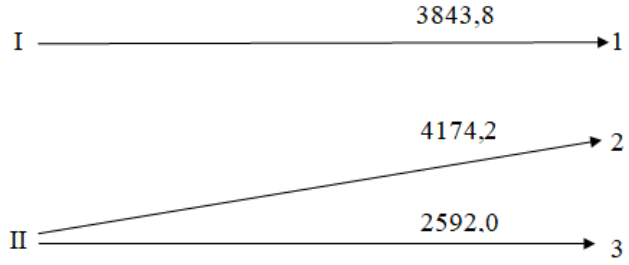


Рис. 7. Схема постачання сировини

4. Для знаходження транспортних витрат за постачання сировини треба знайти найкоротші шляхи транспортування вантажу.

Згідно з оптимальною прив'язкою постачальників до складів знаходимо найкоротші шляхи:

1) Для перевезення з першого підприємства до першого складу необхідно знайти загальну відстань L_{1-4}. Варіанти шляху такі:

$$L_{1-4} = L_{1-2} + L_{2-3} + L_{3-4} = 30 + 45 + 17 = 92, \text{ км};$$
$$L_{1-4} = L_{1-2} + L_{2-5} + L_{5-4} + L_{4-5} = 30 + 40 + 25 + 17 = 112, \text{ км};$$
$$L_{1-4} = L_{1-5} + L_{5-3} + L_{3-4} = 46 + 25 + 17 = 85, \text{ км};$$
$$L_{1-4} = L_{1-5} + L_{5-2} + L_{2-3} + L_{3-4} = 46 + 40 + 45 + 17 = 148, \text{ км}.$$

2) Для перевезення з другого підприємства до другого складу необхідно знайти загальну відстань L_{7-6}. Розглянемо всі варіанти:

$$L_{7-6} = L_{7-8} + L_{8-6} = 40 + 46 = 86, \text{ км};$$
$$L_{7-6} = L_{7-9} + L_{9-10} + L_{10-11} + L_{11-6} = 22 + 20 + 17 + 20 = 79, \text{ км};$$
$$L_{7-6} = L_{7-8} + L_{8-11} + L_{11-6} = 40 + 15 + 20 = 75, \text{ км};$$
$$L_{7-6} = L_{7-9} + L_{9-10} + L_{10-11} + L_{11-8} + L_{8-6} = 22 + 20 + 17 + 15 + 46 = 120 \text{ км}.$$

3) Для перевезення з другого підприємства до третього складу необхідно знайти загальну відстань L_{7-12}. Можливі варіанти:

$$L_{7-12} = L_{7-9} + L_{9-10} + L_{10-11} + L_{11-12} = 22 + 20 + 17 + 21 = 80, \text{ км};$$
$$L_{7-12} = L_{7-9} + L_{9-10} + L_{10-12} = 22 + 20 + 35 = 77, \text{ км};$$
$$L_{7-12} = L_{7-8} + L_{8-11} + L_{11-12} = 40 + 15 + 21 = 76, \text{ км}.$$

Оптимальні маршрути зображено на рис. 8 (виділено жирними лініями).

Тож маємо такі результати:

1-й постачальник→Перший склад: L_{1-4}=85 км,

2-й постачальник→ Другий склад: L_{7-6}=75 км,

2-й постачальний→ Третій склад: L_{7-12}=76 км.

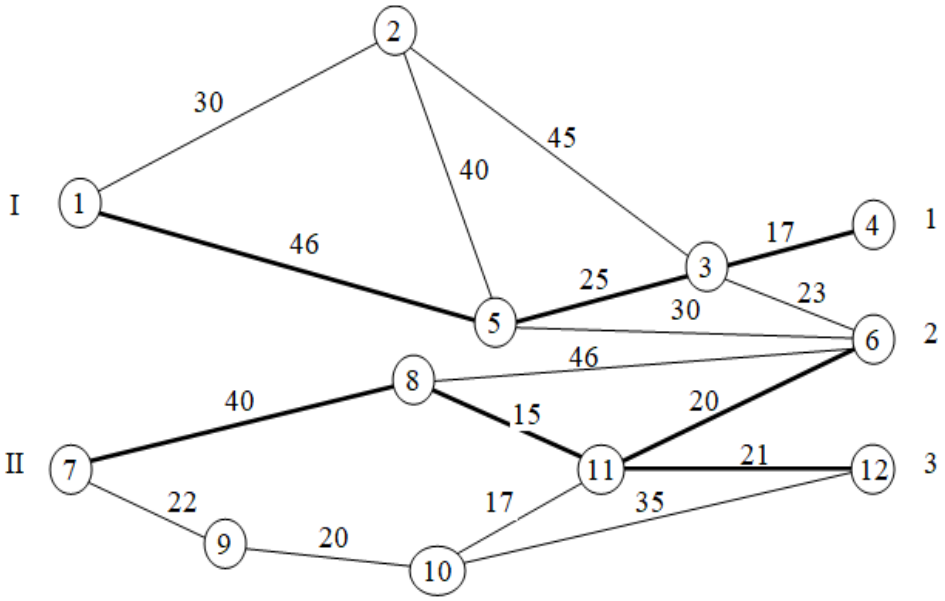


Рис. 8. Найкоротші маршрути доставки сировини

Таким чином, транспортні витрати на перевезення 1 т сировини найкоротшими шляхами дорівнюють:

$C_{11} = 2 \cdot 85 = 170$, грн; $C_{22} = 1 \cdot 75 = 75$, грн; $C_{13} = 2 \cdot 76 = 152$, грн;

Загальні транспортні витрати складають:

$F_{TP} = 170 \cdot 3843{,}8 + 75 \cdot 4174{,}2 + 152 \cdot 2592{,}0 = 1360495{,}0$ грн,

$F_0 = F + F_{TP} = 4588435{,}7 + 1360495{,}0 = 5948930{,}7$ грн.

Висновки та пропозиції:

1. Складські приміщення повинні мати наступну ємність:

– Перший склад – не менше 3843,8 т,

– Другий склад – не менше 4174,2 т ,

– Третій склад – не менше 2592,0 т.

2. Для виконання плану виробництва обсягом 10610 т/рік хімікатів з мінімальною собівартістю треба виробляти тільки перший та другий вид кінцевої продукції обсягами відповідно 6608 т/рік та 4002 т/рік.

3. Перевиконання плану виробництва не передбачається за вибраною цільовою функцією.

4. При виробництві кінцевої продукції є профіцит електроенергії, тому що вона повністю не витрачається при плані 29010 кВт/рік:

$$3{,}3 \cdot 6608 + 1{,}8 \cdot 4002 + 2 \cdot 0 = 13814{,}9 \text{ кВт/рік},$$

а забезпечення паром повністю задовільняє потреби без залишків при плані 4500 ГКал/рік:

$$0{,}4 \cdot 6608 + 0{,}46 \cdot 4002 + 0{,}4 \cdot 0 = 4484{,}1 \text{ ГКал/рік}.$$

5. План виробництва задовільняється повністю, проте зайву електроенергію можливо передавати до інших цехів.

6. Знайдено оптимальні маршрути перевезення, якими рекомендується користуватись надалі.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Важливим аспектом розвитку промислового підприємства є організація ефективних транспортно-логістичних процесів. На прикладі ПрАТ "ДКХЗ" холдингу Метінвест проведено аналіз існуючого транспортно-логістичного забезпечення та визначено оптимальні схеми постачання сировини та складські рішення. Вирішено задачу визначення оптимальних схем постачання сировини для забезпечення виробництва, за якою визначено ємності для зберігання вихідної сировини та оптимальні схеми доставки смоли кам'яновугільної.

Результати дослідження свідчать про необхідність постійного оперативного оновлення існуючих рішень та можуть бути використані при удосконаленні транспортно-логістичної складової процесів промислових підприємств.

Список використаних джерел:

1. *Сергеев В. И.* Корпоративная логистика. 300 ответов на вопросы профессионалов / Под общ. и научн. ред. проф. В. И. Сергеева. – М. : ИНФРА-М, 2004. – 976 с

2. *Кальченко А. Г.* Логістика : навч. посібник / А. Г. Кальченко. – К. : КНЕУ, 2000. – 148 с.

3. *Гринів Н. Т.* Логістичні процедури транспортних технологій / Н. Т. Гринів, С. В. Гагарін, Т.Б. Данилович – Національний університет "Львівська політехніка", 2007. – С. 194–198.

4. *Абрамов А. П.* Маркетинг на транспорте / під загальною ред. д-ра екон. наук, проф. В. Г. Галабурди : підручник для вузів. – М. : Желдориздат. 2001. – 329 с.

5. *Шершньова З. Є.* Стратегічне управління : підручник. – 2-ге вид.,перероб. і доп. / З. Є. Шершньова – К.: КНЕУ – 2014. – 588 с.

6. *Нелеп В. М.* Планування на аграрному підприємстві : підручник / В. М. Нелеп – К.:КНЕУ – 2004. – 495 с.

7. *Яцківський Я. Ю.* Загальний курс транспорту : навчальний посібник / Я. Ю. Яцківський, Д. В. Зеркалов. – [Кн. 1]. – К. : Арістей, – 2007. – 544 с.

8. Офіційний сайт Метінвест [Електронний ресурс]. – Режим доступу : https://metinvestholding.com

9. Офіційний сайт ПрАТ "ДКХЗ" [Електронний ресурс]. – Режим доступу : http://www.dkhz.com.ua/index.php/corpdocs

10. *Мельник О. Г.* Процес оптимізації управлінських рішень / О. Г. Мельник, А. М. Ульянова Національний університет "Львівська політехніка", кафедра менеджменту і міжнародного підприємництва. – 2006. – С. 197–204

11. *Балабан П. Ю.* Торговельна логістика : підручник / П. Ю. Балабан, Н. М. Тягунова, В. І. Місюкевіч. – К. – 2014. – 148 с.

References:

1. Sergeev V. I. Korporativnaya logistika. 300 otvetov na voprosy professionalov / Pod obsh. i nauchn. red. prof. V. I. Sergeeva. – M. : INFRA-M, 2004. – 976 p.

2. Kalchenko A. G. Logistika : Navch. posibnik / A. G. Kalchenko. – K. : KNEU, 2000. – 148 p.

3. Griniv N. T. Logistichni proceduri transportnih tehnologij / N. T. Griniv, S. V. Gagarin, T. B. Danilovich – Nacionalnij universitet "Lvivska politehnika", 2007. – P. 194–198.

4. Abramov A. P. Marketing na transporte / Pod obshej red. d-ra ekon. nauk, prof. V. G. Galaburdy : Uchebnik dlya vuzov. – M. : Zheldorizdat. 2001. – 329 p.

5. Shershnova Z. Ye. Strategichne upravlinnya : Pidruchnik. – 2-ge vid., pererob. i dop. / Z. Ye. Shershnova – K. : KNEU – 2014. – 588 p.

6. Nelep, V. M. Planuvannya na agrarnomu pidpriyemstvi: Pidruchnik / V. M. Nelep – K. : KNEU – 2004. – 495 p.

7. Yackivskij, Ya. Yu. Zagalnij kurs transportu : navchalnij posibnik / Ya. Yu. Yackivskij, D. V. Zerkalov. – [Kn. 1]. – K. : Aristej, – 2007. – 544 p.

8. Oficijnij sajt Metinvest [Elektronnij resurs]. – Rezhim dostupu : https://metinvestholding.com

9. Oficijnij sajt PrAT "DKHZ" [Elektronnij resurs]. – Rezhim dostupu : http://www.dkhz.com.ua/index.php/corpdocs

10. Melnik O. G. Proces optimizaciyi upravlinskih rishen / O. G. Melnik, A. M. Ulyanova Nacionalnij universitet "Lvivska politehnika", kafedra menedzhmentu i mizhnarodnogo pidpriyemnictva. – 2006. – P. 197–204.

11. Balaban P. Yu. Torgovelna logistika: Pidruchnik / P. Yu Balaban, N. M. Tyagunova, V. I. Misyukevich. – K. – 2014. – 148 p.

DOI: https://doi.org/10.32836/2521-6643-2018.2-56.4
УДК 629.78

В. Н. Спиридонов, кандидат технічних наук, доцент кафедри прикладної математики та інформатики Університету митної справи та фінансів
С. А. Разгонов, кандидат технічних наук, доцент кафедри транспортних систем и технологій Університету митної справи та фінансів

ПРО ОДНУ ЗАДАЧУ МОДЕЛЮВАННЯ БОРТОВОЇ УПРАВЛЯЮЧОЇ СИСТЕМИ КОСМІЧНОГО АПАРАТУ

У підсистемі формування командно-програмної інформації космічних апаратів різного призначення реалізовано підхід, що полягає у вирішенні задачі прогнозу стану бортових систем космічних апаратів для сформованої програми управління на моделі бортової апаратури космічного апарата. Результати моделювання призначені для подання повної інформації про стани бортових систем операторам сектора управління під час штатного управління космічних апаратів, при передачі управління черговим змінами, для аналізу нештатних ситуацій. Однак даний підхід можна застосувати до космічних апаратів, які реалізують командно-часовий і програмно-командний методи управління космічних апаратів. Для космічних апаратів, що реалізують більш складний програмно-координатний метод управління, даний підхід не застосовується. Це обумовлено тим, що часова програма управління при цьому методі управління формується на борту космічного апарата бортовою управляючою системою, що має в своєму складі електронно-обчислювальні машини.

У статті розглядається задача моделювання формування часової програми управління бортовою управляючою системою космічного апарата. Запропоновано алгоритм моделювання формування детермінованої складової часової програми управління космічного апарата. Розглянуто дії операторів сектора управління космічного апарата в разі виникнення нештатних ситуацій з управління космічного апарата, коли рішення по управлінню бортовою апаратурою приймаються бортовою управляючою системою.

Ключові слова: *моделювання формування часової програми управління космічного апарата; моделювання бортової керуючої системи космічного апарата.*

В подсистеме формирования командно-программной информации космических аппаратов (КА) различного назначения реализован подход, заключающийся в решении задачи прогноза состояния бортовых систем КА для сформированной программы управления в модели бортовой аппаратуры (БА) КА. Результаты моделирования предназначены для представления полной информации о состояния бортовых систем для операторов сектора управления при штатном управлении КА, при передаче управления очередным дежурным, для анализа нештатных ситуаций. Однако данный подход можно применить к КА, реализующим командно-временной и программно-командный методы управления КА. Для КА, реализующих более сложный программно-координатный метод управления, данный подход не применяется. Это обусловлено тем, что временная программа управления при этом методе управления формируется на борту КА бортовой управляющей системой (БУС), имеющий в своем составе ЭВМ.

В статье рассматривается задача моделирования формирования временной программы управления бортовой управляющей системой КА. Предложен алгоритм моделирования формирования детерминированной составляющей временной программы управления КА. Рассмотрены действия операторов сектора управления КА в случае возникновения нештатных ситуаций по управлению КА, когда решения по управлению бортовой аппаратурой принимаются БУС.

Ключевые слова: *моделирование формирования временной программы управления КА; моделирование бортовой управляющей системы КА*

In the subsystem of forming of command-program information the approach consisting in the task decision of spacecraft onboard systems states prognosis for the formed control program on a model is realized. The modeling results are intended for the presentation of complete information about the spacecraft onboard systems states to the operators of control sector during the normal spacecraft control, to the control transfer by duty groups, analysis of abnormal situations. Summarizing the results it can be argued that the modeling of the deterministic component of control program of various space crafts with program-coordinate control is possible in principle. It is also possible modeling of programs of onboard control system operating in abnormal situations. There is a limitation due to the inability to accurately predict the manner and time of their occurrence. However, when abnormal situations take place and the onboard control system has executed their parrying this information may be obtained in the "OCS report". As a result of analysis of the report, the operator can manually correct the states of the corresponding elements in the model of onboard equipment. In that case the OCS cannot alone perform the parrying of abnormal situation the onboard equipment state information at a given time can be transmitted to ground control center. It is necessary to perform the analyze of abnormal situation and take appropriate measures to parrying it due to the actual and forecasted information about

the functioning of onboard equipment. Therefore, this restriction does not preclude to the using of the proposed methodology for the spacecraft program- coordinate control. The modeling algorithm of forming of the control program determined constituent offers. The actions of control sector operators are considered in that case of abnormal situations appearance when control decisions are made by the spacecraft onboard control system.

The areas development of application of predictive models on-board equipment to solve the problems of analysis, decision-making and parrying of abnormal situations in the spacecraft control circuit is a perspective area of research.

Key words: *modeling of the spacecraft control program forming; modeling of the spacecraft onboard control system.*

Постановка проблеми. Одним з основних напрямків розвитку систем управління космічними апаратами (КА) є підвищення рівня автоматизації процесу управління КА. Одним з варіантів реалізації даного напрямку є застосування програмно-координатного методу управління КА, який передбачає перенесення частини функцій наземного комплексу управління на бортовий комплекс управління КА. Зокрема, мова йде про формування на борту КА часової програми управління (ЧПУ) бортовими системами, яку виконує бортова управляюча система КА. Відсутність інформації в секторі управління КА, як про саму програму управління, так і про зміну стану бортових систем КА і режимах їх роботи під дією команд істотно знижує якість управління КА.

Аналіз останніх досліджень і публікацій. Для управління рядом КА різного призначення запропонований підхід [1], що полягає у вирішенні завдання прогнозу стану бортових систем КА для сформованої програми управління на моделі бортової апаратури КА. Результати моделювання призначені для подання повної інформації про стани бортових систем операторам сектора управління під час штатного управління КА, передачі управління черговим змінами, для аналізу нештатних ситуацій.

В рамках реалізації і розвитку даного підходу запропоновані методики та алгоритми розв'язання деяких задач управління КА [2, 3], що реалізовані у вигляді універсального програмного комплексу формування інформації для управління КА. Комплекс пройшов практичну апробацію і був включений до складу спеціального програмного забезпечення підсистеми формування командно-програмної інформації (КПІ) ряду космічних апаратів різного призначення.

Розглянута методологія управління застосовна для КА командно-часового та програмно-командного управління [4], які передбачають формування часової програми управління в наземному комплексі управління

КА. Однак вона не може бути застосована для управління КА, що реалізують програмно-координатний метод управління [5], при якому часова програма управління бортовими системами КА формується бортовим комплексом управління КА.

Мета статті – постановка і рішення задачі моделювання формування часової програми управління, що виконується бортовою управляючою системою КА, для застосування в контурі управління КА програмно-координатного методу управління.

Виклад основного матеріалу.

В даний час все більшого поширення набуває програмно-координатний метод управління КА. Метод передбачає формування на борту КА часової програми управління з використанням координат цілей і пунктів прийому інформації. Реалізація цього методу управління можлива за допомогою бортової управляючої системи, що має в складі бортову цифрову обчислювальну машину. Програмне забезпечення БУС формує часову програму управління (ЧПУ) за вхідними даними, що періодично закладаються на борт КА, і координатами об'єктів, що зберігаються в ПЗУ БУС [6]. Вхідними даними для розрахунку є плани-завдання на роботу бортових систем КА, що періодично надходять від замовників одержуваної інформації. На їх основі операторами формуються плани-завдання на роботу систем, що забезпечують їх роботу.

Для вирішення поставленого завдання необхідно моделювати роботу БУС в частині формування часової програми управління. Роботи по постановці і вирішенню даної задачі в літературі відсутні.

Як завдання моделювання, розглядається задача імітації роботи бортової управляючої системи в частині формування часової програми управління бортовими системами КА типу “Ресурс-О” за вхідними даними, які передані в КПІ та зберігаються в ПЗУ БУС.

Програми БУС в частині формування режимів роботи бортових систем являють собою жорсткі та гнучкі програми управління. Кожна програма БУС реалізує один з режимів роботи бортової системи. Для гнучких програм часи видачі команд щодо початку циклу управління, наприклад, розрахункового часу перетину екватора або часу початку режиму роботи БС, що задається у вхідних даних, можуть варіюватися в залежності від розв'язуваних цільових завдань. Можуть варіюватися і номера команд управління.

При побудові моделі алгоритму використовувалися наступні проектні рішення:

1. З метою зменшення залежності моделюючих алгоритмів і програм від реальних алгоритмів і програм БУС, коригування яких можливе в процесі розробки математичного забезпечення БУС, моделюючий алгоритм виконаний у вигляді окремих процедур.

2. Кожна процедура моделює роботу однієї бортової системи або групи взаємопов'язаних систем, наприклад, бортового інформаційного комплексу (БІК). При цьому процедури алгоритмів окремих режимів роботи, наприклад, безпосередньої передачі, запису та відтворення БІК, виконані у вигляді окремих блоків алгоритму.

3. Формування більшості режимів роботи бортових систем виконується в залежності від поточних розрахункових координат КА, координат цілей і ППІ, на які скидається отримана інформація. Для реалізації режиму у вхідних даних повинен бути вказаний номер цілі або номер взятий з ППІ.

4. Для режимів роботи БС, формування програм управління якими виконується без урахування координат, наприклад, для проведення операцій фазування коду і підстроювання частоти (ФКПЧ), має бути вказано час початку режиму. У вхідних даних можуть бути задані і деякі характеристики режимів роботи, наприклад, варіанти тривалості та/або інформативності режимів.

5. Для виключення залежності моделюючих алгоритмів і програм від даних, всі дані, що використовуються при вирішенні задачі моделювання, згруповані в два набори даних: "Режими роботи БС" і "Команди БУС".

У наборі даних "Режими роботи БС" все згруповано за наступними змінними або їх комбінаціями (наприклад, якщо задано номер ППІ, то діапазон довгот не встановлено):

РР – режим роботи БС;

ВД – варіант тривалості або інформативності режиму;

ПП – номер взятий з ППІ;

ДН, ДК – початок і кінець діапазону довгот проведення режиму, вибирається з запису набору даних, що містить часові характеристики заданого варіанту режиму роботи:

ДЛ – тривалість проведення режиму;

ТН – відносний час початку режиму;

ТК – відносний час закінчення режиму.

Якщо умова не виконується ні для одного запису набору даних, оператору видається повідомлення про неправильне завданні режиму роботи. Таким чином, завдання моделювання виконує додатково функцію контролю планів-завдань на роботу БС.

Часові характеристики режимів використовуються для розрахунку часу видачі команд включення і виключення режимів.

У наборі даних "Команди БУС" зберігаються номери команд включення (КВ) і виключення (КЗ) для кожного режиму роботи (РР) і варіанту тривалості (або інформативності) режиму (ВД). У наборі даних за заданим значенням вибирається запис, що містить команди включення і виключення режиму роботи БС. При відсутності запису з такими умовами, оператору видається повідомлення про некоректність вихідних даних.

Схема моделюючого алгоритму приведена на рис. 1.

Рис 1. Схема моделюючого алгоритму

Моделюючий алгоритм передбачає виконання таких операцій:

1) послідовне звернення до процедур моделювання режимів роботи БС, при цьому кожною процедурою виконуються наступні операції:

– звернення до відповідного масиву плану-завдання на роботу бортової системи і послідовне зчитування рядків масиву, при цьому для кожного рядка масиву виконується виклик процедури “Вибір даних”;

– процедура “Вибір даних” виконує пошук записів в наборах даних “Режими роботи БС” і “Команди БУС” за параметрами режиму роботи БС, наведеними в рядку плану-завдання;

– отримані дані використовуються процедурою “Формування робочого набору даних” для формування записів робочого набору даних “Програма управління КА”, що містять такі реквізити:

Д – дата видачі команди;

ВР – розрахунковий час видачі команди;

НК – номер виданої команди (КВ або КО);

РР – режим роботи БС;

П – ознака видається команди (БУС або РКНІ);

2) після закінчення циклу обробки всіх рядків плану-завдання, виконується підключення наступної процедури режиму роботи БС;

3) після відпрацювання всіх процедур моделювання режимів роботи БС (частина їх складу приведена на рис. 1) сформований робочий набір даних "Програма управління КА". Записи набору даних сортуються в порядку зростання дати і часу;

4) після формування робочого набору даних "Програма управління КА" процедура "Формування вихідного набору даних" доповнює записи робочого набору даних "Програма управління КА" службовою інформацією "Плану управління КА".

При моделюванні роботи БУС можуть виникнути ситуації, коли частина інформації поточної програми управління може бути сформована при моделюванні попередньої програми управління КА. Це можливо для деяких режимів роботи БС, що перевищують за тривалістю декілька витків, наприклад, при моделюванні роботи корегуючої рухової установки (КДУ). Для врахування таких ситуацій потрібно скорегувати вихідний набір даних попередньої "Програми управління КА" та вибрати записи, які стосуються поточного інтервалу. Ці записи зчитуються в робочий набір даних "Програми управління КА" і впорядковуються в порядку зростання дати і часу видачі команд. Результати моделювання представляються операторам сектора управління у вигляді документа "Програма управління КА".

Розроблена методологія успішно пройшла апробацію при випробуваннях і підготовці до експлуатації спеціального програмного забезпечення КА типу "Ресурс-О" програмно-координатного управління.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

Узагальнюючи отримані результати можна стверджувати, що принципово можливо моделювання детермінованої складової часової програми управління КА програмно-координатного типу управління. Можливо також моделювання роботи програм БУС, що функціонують при виникненні нештатних ситуацій, однак, обмеження виникає в зв'язку з неможливістю точного прогнозування характеру і часу їх виникнення. Проте, при виникненні нештатних ситуацій в тих випадках, коли БУС виконала їх парирування, ця інформація може бути отримана в "звіті БУС". В результаті аналізу звіту оператор може вручну скоригувати стани відповідних елементів в моделі БА. У тому випадку, якщо БУС самостійно не може виконати парирування нештатної ситуації, за сигналом "Виклик НКУ" може бути отримана інформація про стан всіх елементів БА на даний момент часу. На підставі отриманої реальної і прогнозованої інформації про функціонування БА необхідно виконати аналіз нештатної ситуації і вжити відповідних заходів для її парирування. Тому розглянуте обмеження не перешкоджає використанню запропонованої методології при управлінні КА програмно-координатного типу управління.

Розвиток напряму застосування прогнозуючих моделей бортової апаратури для вирішення завдань аналізу, прийняття рішень і парирування нештатних ситуацій в контурі управління КА є перспективним напрямком досліджень.

Список використаних джерел:

1. *Конюхов С. Н.* Об одной задаче моделирования полета космического аппарата / С. Н. Конюхов, А. Г. Меланченко, В. Н. Спиридонов // Ракетно-космическая техника. Сер. 1 – 1989, Вып. 2. – С. 32–37.

2. *Спиридонов В. Н.* Метод моделирования дискретных динамических систем с постоянной структурой / В. Н. Спиридонов // Проблемы управления и информатики. – 2010, № 6. – С. 55–62.

3. *Спиридонов В. Н.* К вопросу применения модели в контуре автоматизированного управления сложным техническим объектом / В. Н. Спиридонов, С. А. Разгонов // Вестник Академии таможенной службы Украины. Сер. Технические науки. - 2013, №1 (49). С. 84-87.

4. *Брега А. Н.* Командно-программное управление полетом Российского сегмента МКС / А. Н Брега, А. А. Коваленко // Космическая техника и технологии. – 2016, № 2 (13). – С. 90–104.

5. *Беляев М. Ю.* Научные эксперименты на космических кораблях и орбитальных станциях. – М. : Машиностроение, 1984. – 264 с.

6. *Микрин Е. А.* Бортовые комплексы управления космическими аппаратами и проектирование их программного обеспечения. – М. : МГТУ им. Н. Э. Баумана, 2003. – 336 с.

References:

1. Konyukhov S. N., Melanchenko A. G., Spiridonov V. N. About one task of modeling of space vehicle flight // Space-rocket technique. Series. 1 – 1989, is. 2. – P. 32–37.

2. Spiridonov V. N. Modeling method of discrete dynamic systems with constant structure // Journal of Automation and Information Sciences, 2010, Issues 6 – P. 55–62.

3. Spiridonov V. N., Razgonov S. A. To question of models in automated control circuit of complex technical object // Announcer of Academy of custom service of Ukraine. – 2013. – № 1 (49). – P. 84–87.

4. Brega A. N. Command and program flight control of the ISS Russian Segment / A. N Brega, A. A. Kovalenko // Space engineering and technology. – 2016, No. 2 (13). P. 90–104.

5. Belyaev M. Yu. Scientific experiments on spaceships and orbital stations. – M. : Mechanical Engineering, 1984.- 264 p.

6. Mikrin E. A. Onboard spacecraft control systems and their software design. – M. : MSTU. N. E. Bauman, 2003. – 336 p.

DOI: https://doi.org/10.32836/2521-6643-2018.2-56.5
УДК 656.086

А. М. Пасічник, доктор фізико-математичних наук, професор кафедри транспортних систем та технологій Університету митної справи та фінансів
А. І. Кузьменко, кандидат технічних наук, доцент кафедри транспортних систем та технологій Університету митної справи та фінансів
О. Д. Фірсов, кандидат фізико-математичних наук, доцент кафедри транспортних систем та технологій Університету митної справи та фінансів

АНАЛІЗ МЕТОДІВ ТА СХЕМ ЕКСПЕРТНОГО ДОСЛІДЖЕННЯ ДОРОЖНЬО-ТРАНСПОРТНИХ ПОДІЙ У ВИПАДКУ НАЇЗДУ АВТОМОБІЛЯ НА ПІШОХОДА

Проведено аналіз та систематизація моделей і схем взаємодії учасників дорожньо-транспортних пригод для визначення їх параметрів і реконструкції з урахуванням дорожньої ситуації, чинників впливу і положення елементів системи "водій – автомобіль – дорога – середовище" на момент виникнення небезпечної ситуації.

Для підвищення достовірності результатів автотехнічної експертизи дорожньо-транспортних пригод запропоновано використовувати комплексний підхід із застосуванням даних теоретичного дослідження і експериментального підтвердження коректності технічних параметрів дорожньо-транспортних подій.

Ключові слова: *транспортний засіб; ДТП; наїзд на пішохода; маневр транспортного засобу; методи дослідження.*

Проведен анализ и систематизация моделей и схем взаимодействия участников дорожно-транспортных происшествий для определения их параметров и реконструкции с учетом дорожной ситуации, факторов влияния и положения элементов системы "водитель – автомобиль – дорога – середа" на момент возникновения опасной ситуации.

Для повышения достоверности результатов автотехнической экспертизы дорожно-транспортных происшествий предложено использовать комплексный подход с применением данных теоретического исследования и экспериментального подтверждения корректности технических параметров дорожно-транспортных происшествий.

Ключевые слова: *транспортное средство; ДТП; наезд на пешехода; маневр транспортного средства; методы исследования.*

The intensity of the use of road transport in various sectors of the economy is growing. This leads to an increase in the accident rate of automobile vehicles and road traffic accidents. Hitting a pedestrian is one of the most common types of traffic accidents. Currently, the total number of deaths on highways in the world is about 1.25 million people. So in 2016 in Ukraine 82.4 thousand traffic accidents with victims were registered. According to the World Bank (2014 estimates), the loss of the Ukrainian economy from road traffic injuries annually amounts to about $ 4.5 billion.

The complexity of the study of traffic accidents involving a car and a pedestrian is in a wide variety of factors that in real conditions determine the sequence of stages of their passage. Therefore, for the reliable qualification of such situations in the investigation of traffic accidents, the development and improvement of models and methods for studying the mechanism for their implementation is important. When conducting an automotive technical examination, it is necessary to establish the circumstances and the mechanism of the accident. The reliability of expert analysis of the mechanism of a traffic accident is based on its phased study and reconstruction.

In the paper was analyzed and systematized the models and patterns of interaction between participants in traffic accidents to determine their parameters and reconstruction taking into account the traffic situation, factors of influence and the position of the elements of the "driver – car – road – environment" system at the time of a dangerous situation.

To increase the reliability of the results of automotive technical expertise of road traffic accidents, it is proposed to use an integrated approach using the data of a theoretical study and experimental confirmation of the correctness of the technical parameters of road traffic accidents. In an expert study of a vehicle's maneuver, it is quite effective to use empirical-statistical models based on experimental tests.

Key words: *vehicles; car accidents; a runover on a pedestrian; car maneuver and research methods*.

Постановка проблеми. В сучасних умовах забезпечення потреб виробництва і населення у перевезеннях призводить до підвищення інтенсивності застосування автомобільного транспорту в різних галузях економіки [1]. При цьому підвищення його ролі у житті людей має не тільки позитивний ефект, але й супроводжується негативними наслідками пов'язаними з високим рівнем аварійності автомобільних транспортних засобів та дорожньо-транспортних подій (ДТП) за їх участю. Одним із найбільш поширених видів ДТП є наїзд автомобіля на пішохода. На даний час загальна кількість загиблих на автомобільних дорогах у світі складає близько 1,25 млн чоловік, на порядок більше людей отримують травми. Так за даними Управління безпеки дорожнього руху МВС з 2014 по 2016 рік в Україні зареєстровано 82,4 тис. ДТП із постраждалими в яких загинуло 13,32 тис. чоловік і 101,5 тис. були травмовані. За оцінкою Всесвітнього банку (розрахунки 2014 р.), втрати української економіки від дорожньо-транспортного травматизму щорічно становлять біля $4,5 млрд [2].

Складність дослідження ДТП за участю автомобіля і пішохода полягає у великому різноманітті факторів, які в реальних умовах визначають послідовність етапів їх проходження. Тому для достовірної кваліфікації таких ситуацій при розслідуванні ДТП особливо важливе значення має розробка та удосконалення моделей та методів дослідження механізму їх здійснення. Механізм дорожньо-транспортної події відображає процес взаємодії елементів системи "водій – автомобіль – дорога – середовище" (ВАДС) у часі та просторі.

Аналіз останніх досліджень і публікацій. Достовірність експертного аналізу механізму дорожньо-транспортної події базується на поетапній її реконструкцію з урахуванням обставин, що характеризуються певним положенням елементів системи ВАДС у певний момент часу. Тому розробці теоретичних і експериментальних методів оцінки безпеки руху, аварійності на автомобільних дорогах та дослідження механізму ДТП з урахуванням впливу різних факторів присвячено цілий ряд наукових праць. Так в роботах [3, 4] наведено особливості проведення аналізу та розслідування обставин здійснення дорожньо-транспортних подій. Підходи та варіанти удосконалення методів автотехнічної експертизи ДТП розглянуті в монографії [5]. Особливості проведення експериментальних досліджень технічних механізмів ДТП у випадку наїзду на пішохода наведені в роботі [6]. Важливість та способи оцінки безпеки руху та аварійності на автомобільних дорогах розглянуті в статті [7].

Аналіз проблемних питань визначення параметрів руху транспортних засобів при дослідженні ДТП проведено в роботі [8]. В статті [9] проведено обгрунтування необхідності комплексного застосування розрахункових і

експериментальних методів дослідження маневру автомобіля. Класичні підходи до проведення автотехнічної експертизи та проведення досліджень за встановлення обставин ДТП викладені в роботі [10]. Системному аналізу різних підходів дослідження технічних механізмів дорожньо-транспортних подій у випадку наїзду автомобіля на пішохода присвячено роботу [11]. При цьому важливе значення приділяється питанням удосконалення експлуатаційних властивостей транспортних засобів [12] та розробці методів і технічних умов їх випробування [13].

Цілями автотехнічної експертизи є встановлення обставин та механізму дорожньо-транспортної події, дорожніх знаків і розміток, технічного стану транспортних засобів та дорожнього покриття. Об'єктами дослідження автотехнічної експертизи є: місце транспортної події, обставини та технічні параметри механізму ДТП, транспортні засоби та їх частини.

Висновок експерта є найважливішим засобом доведення та встановлення відповідальності у справах про дорожньо-транспортні події за участю автотранспортних засобів [10, 14].

Мета статті – аналіз та систематизація моделей і схем взаємодії учасників дорожньо-транспортних подій для визначення параметрів механізмів їх здійснення та проведення реконструкції з урахуванням дорожньої ситуації, факторів впливу та положення елементів системи ВАДС на момент виникнення небезпечної ситуації.

Виклад основного матеріалу. В експертній практиці найбільш часто встановлення причинно-наслідкового зв'язку між невідповідністю виконання правил дорожнього руху і подією здійснюється при:

– перевищенні водієм швидкості руху транспортного засобу;

– несвоєчасному прийнятті ним заходів до запобігання події;

– застосуванні маневру замість гальмування або екстреного гальмування замість повільного зниження швидкості;

– невірно обраній дистанції, невірно обраному інтервалі;

– створенні водієм перешкоди для руху інших транспортних засобів;

– експлуатації технічно несправного транспортного засобу.

В кожному випадку ДТП може бути результатом або зазначених дій водія, що не відповідають вимогам Правил дорожнього руху, або невірних дій інших учасників руху; крім того, подія може статися також у зв'язку з випадковим збігом обставин. Наїздом автомобіля на пішохода вважається ДТП, у процесі якої автомобіль наїхав фронтальною частиною на пішохода або пішохід наткнувся на бічну сторону проїжджаючого автомобіля. При цьому можна виділити ряд характерних особливостей, які впливають на вибір методик розрахунку, а саме:

– умови видимості;

– умови оглядовості;

– режим руху автомобіля: рівномірний без гальмування або уповільнений із гальмуванням;

– напрямок руху пішохода: попутно, назустріч автомобілю, у поперечному напрямку;

– тип удару: фронтальний або боковий.

Більшість випадків дорожньо-транспортних подій наїзду автомобіля на пішохода відбувається в умовах доброї видимості та оглядовості, коли водію ніщо не заважає вірно оцінити ситуацію та своєчасно виконати гальмування. Як свідчить статистика, у більшості випадків ДТП водій не зміг вчасно зреагувати на появу пішохода і продовжував рух, не знижуючи швидкості, а якщо гальмував, то безпосередньо перед наїздом [8, 9].

У разі встановлення обставин ДТП, пов'язаної з наїздом на пішохода, характерними режимами руху автомобіля є рівномірний рух або рух з деяким сповільненням. Це пов'язано з тим, що за час реакції водія (~1,0 сек в нормальних умовах) прискорення автомобіля, якщо воно мало місце, буде несуттєво впливати на зміну швидкості автомобіля.

Напрямок руху пішохода встановлюється слідством у градусах відносно краю проїжджої частини. В автотехнічній експертизі напрямок руху пішохода пов'язується з кутом наїзду. Кут наїзду на пішохода α – це кут між напрямками траєкторії руху автомобіля й пішохода. Для однозначної визначеності розрахунку кут наїзду визначається від напрямку руху автомобіля проти годинникової стрілки. В такому випадку можливі схеми зіткнення автомобіля і пішохода наведені на рис. 1.

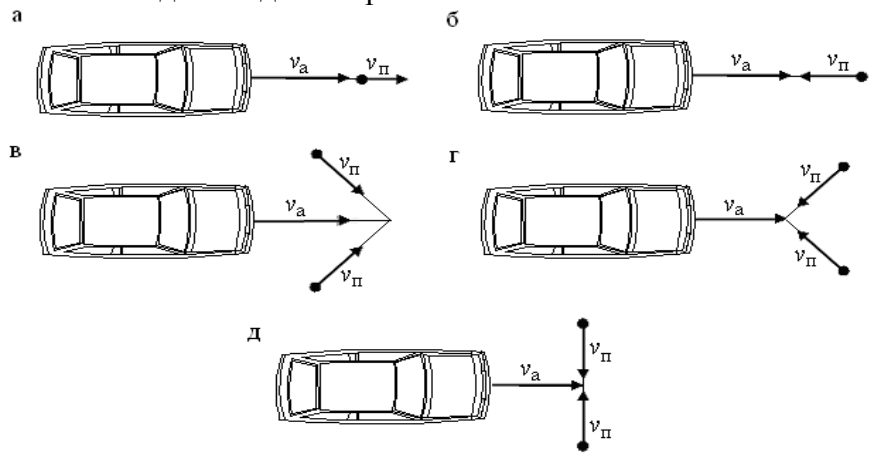


Рис. 1. Можливі схеми ДТП зіткнення автомобіля і пішохода

Залежно від напрямку руху пішохода рис. 1, розрізняють наступні кути наїзду: а – попутний наїзд (α = 0°); б – стрічний наїзд (α = 180°); в – косий попутний наїзд (0< α < 90°, 270 < α < 360°); г – косий стрічний наїзд (90 < α < 180°, 180 < α < 270°); д – прямий відносно руху автомобіля (α = 90°, α = 270°).

За розташуванням місця удару на автомобілі виділяють фронтальний і бічний наїзд. Координата удару вимірюється від переднього кута автомобіля з боку руху пішохода, рис. 2.

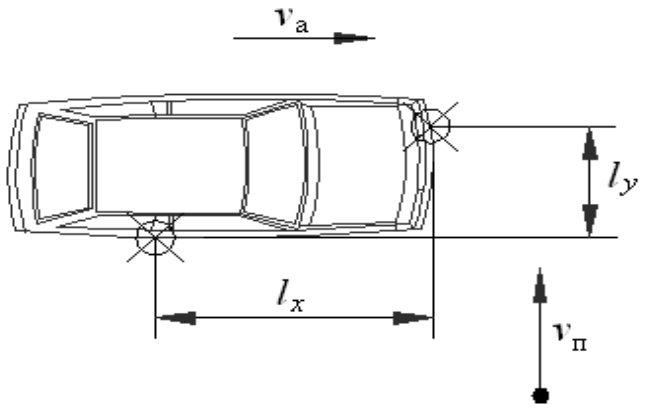


Рис. 2. Координата місця удару на автомобілі
l_y – при фронтальному наїзді; l_x – при бічному наїзді.

Найбільш часто зустрічаються події з фронтальним наїздом на пішохода. Різновидом фронтального наїзду можна вважати удар, нанесений пішоходу задньою частиною автомобіля, при його русі назад.

Для проведення досліджень зі встановлення всіх обставин ДТП, пов'язаних з наїздом автомобіля на пішохода, експерту необхідно знати темп руху пішохода, щоб далі можна було встановити швидкість його руху. Розрізняють такі темпи руху пішохода: повільний крок; спокійний крок; швидкий крок; спокійний біг; швидкий біг.

Швидкість руху пішохода може бути встановлена двома способами – на підставі систематизованих середньостатистичних даних руху пішохода або шляхом проведення слідчого експерименту. У більшості випадків швидкість пішохода встановлюється на основі використання систематизованих середньостатистичних даних. При цьому враховується темп руху пішохода, його стать і вік. Наприклад, середньостатистична швидкість пішохода чоловіка у віці 35 років при повільному темпі руху складає 3,9 км/год, при спокійному темпі – 5,7 км/год, а при швидкому темпі – 6,8 км/год.

Як слідує із практики експертних досліджень наїзду автомобіля на пішохода робиться припущення, що пішохід з моменту виникнення небезпеки рухається прямолінійно й рівномірно. Це допущення ґрунтується на тому, що в разі виникнення небезпечної обстановки водію не слід розраховувати, що пішохід в останню мить змінить характер своїх дій. Відповідно, якщо з моменту виникнення небезпеки для водія пішохід змінював темп або на-

прям свого руху, всі подальші розрахунки можуть проводитись за умов, що пішохід не змінював швидкість і напрям руху [10].

Для більш точного визначення обставин та швидкості руху пішохода використовується експериментальний метод, у якому до слідчого експерименту залучається або сам пішохід учасник ДТП, або схожа з ним особа за фізичними даними, віком і статтю. У ході експерименту на місці події проводиться 3-4 виміри руху пішохода в заданому темпі. Швидкість пішохода розраховується за класичною формулою:

$$v_{\text{п}} = S_n / t_n. \quad (1)$$

де: S_n – шлях пішохода, м; t_n – час руху пішохода, с.

Після цього визначається середня швидкість руху пішохода за всіма вимірами. На точність встановлення швидкості руху пішохода впливають умови проведення експерименту, які мають бути максимально наближені до фактичних обставин ДТП – це пора року, стан покриття проїжджої частини, час доби. Треба також враховувати, що всі подробиці обставин здійснення події добре пам'ятаються протягом перших 10 днів, тому найбільш достовірні результати отримують при проведенні експерименту безпосередньо після ДТП.

Ключовим фактором експертного дослідження всіх обставин наїзду транспортного засобу на пішохода є **встановлення моменту виникнення небезпеки для руху водія**. При дослідженні наїзду на пішохода слідство й експертиза, в першу чергу, повинні з'ясувати питання, коли для водія виникла небезпечна ситуація, тобто небезпека або перешкода для руху. Передбачається, що з цього моменту водій повинен зробити всі дії (гальмування або маневр), що є в його розпорядженні, щоб уникнути або понизити тяжкість наслідків ДТП.

Хоча визначення моменту виникнення небезпечної ситуації відноситься до компетенції слідчого, не виключається право та можливість визначення цього моменту експертом. При цьому, якщо момент, вказаний слідчим суперечитиме дорожній ситуації, що склалася, і виявиться технічно необґрунтованим, то експерт має в своєму висновку навести два варіанти розрахунків і висновків з урахуванням двох моментів виникнення небезпеки.

У загальному випадку, рекомендується за момент виникнення небезпечної ситуації приймати один з наступних моментів:

– перетин пішоходом якої-небудь лінії, що приймається за межу небезпечної зони;

– відстань до пішохода, що дорівнює зупинному шляху ТЗ;

– початок руху або зміна напрямку, темпу руху пішохода, що знаходиться на проїжджій частині;

– пішохід змушений до переміщення в небезпечному напрямі рухом іншого ТЗ;

– пішохід, знаходячись на проїжджій частині, поводиться невпевнено, ймовірні його дії невизначені;

– поява пішохода в полі зору водія в разі обмеженої видимості;

– поява предметів гри дітей на проїжджій частині;

– діти без нагляду дорослих знаходяться на близькій відстані від смуги руху ТЗ, що не виключає можливості попадання їх на проїжджу частину дороги за час наближення до них ТЗ.

У простому випадку, коли пішохід переходить дорогу справа наліво відносно автомобіля, який рухається в крайньому правому або другому ряду, за момент виникнення небезпеки приймається момент перетину пішоходом межі проїжджої частини; аналогічно, якщо пішохід рухається зліва направо та перетинає дорогу з однією смугою в кожному напрямку, рис. 3.

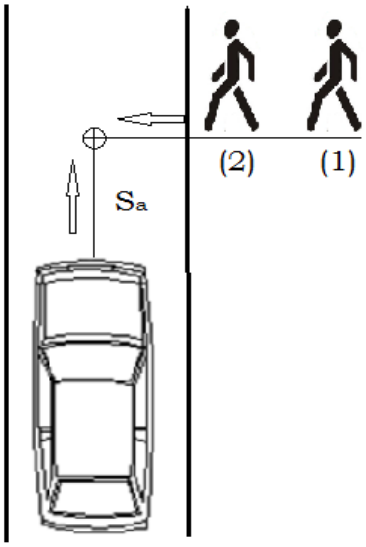


Рис. 3. Виникнення небезпеки для водія при виході пішохода на проїжджу частину

Коли пішохід до виходу на проїжджу частину стоїть біля її краю або рухається до неї кроком, а потім починає перебігати проїжджу частину справа наліво, за момент виникнення небезпеки приймається момент перетину пішоходом межі проїжджої частини, незалежно від її ширини та розташування на ній ТЗ, рис. 4.

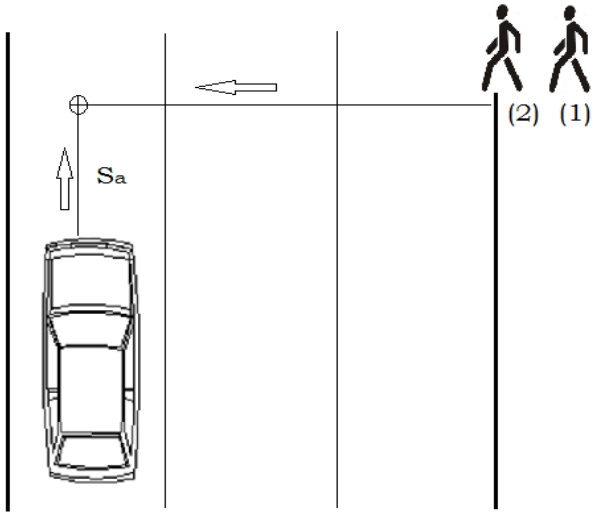
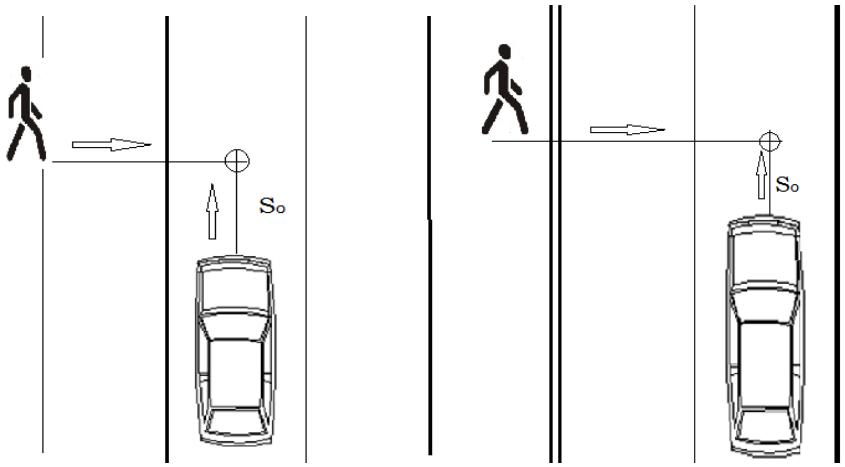


Рис. 4. Виникнення небезпеки для водія з моменту,
коли пішохід починає перебігати проїжджу частину

Якщо дорога має декілька смуг для руху в кожному напрямку й пішохід перетинає дорогу зліва направо в будь-якому темпі, то, незалежно від розташування ТЗ на проїжджій частині, початком небезпеки можна вважати момент, коли ТЗ буде знаходитись на відстані зупинного шляху до лінії руху пішохода (рис. 5).



а) б)

Рис. 5. Виникнення небезпеки на відстані гальмівного шляху

Такий підхід при визначенні моменту небезпеки має сенс, оскільки після перетину пішоходом суцільної лінії ТЗ вже може знаходитися ближче до пішохода ніж довжина зупинного шляху.

Під час руху ТЗ оглядовість дороги може бути обмежена перешкодою у вигляді іншого ТЗ, що рухається попутно чи на зустріч, або нерухомою перешкодою. І якщо пішохід раптово з'являється із-за перешкоди – це є момент появи небезпеки для руху водія, рис. 6.

Небезпечна ситуація, що вимагає від водія вживання негайних заходів, може виникати також, коли водій, хоча й не бачив пішохода, але за різними ознаками може передбачити його появу, наприклад, м'яч, що викотився на проїжджу частину, пішоходи, що вибігають один за одним в умовах обмеженої оглядовості через перешкоду.

Пішоходами можуть бути люди здорові та хворі, вони можуть знаходитися в різному фізичному стані. В силу різних обставин вони можуть не помітити та не врахувати небезпеки від транспортного засобу, що наближається. Знаходячись від пішохода на відстані зупинного шляху, водій повинен негайно застосувати гальмування для запобігання наїзду на пішохода, якщо він продовжує рух в небезпечному напрямі.

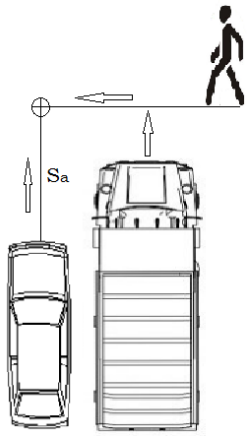


Рис. 6. Виникнення небезпеки для водія, коли пішохід раптово з'являється із-за перешкоди

Діти частіше відволікаються від аналізу та врахування дорожньої обстановки та менше ніж дорослі схильні сприймати небезпеку. Коли діти захоплені рухомими іграми або їх увага відвернута, вони можуть припуститися будь-якої необережності. Малолітні діти взагалі не можуть правильно оцінити виникаючу небезпеку, і подія не виключається, навіть якщо їх увага зосереджена на транспортному засобі, що наближається. При оцінці можли-

вих дій дітей при наближенні до них транспортного засобу ці обставини мають бути враховані. Очевидно, що питання про можливість точного визначення водієм віку дітей не має значення, оскільки у всіх випадках, коли може виникнути сумнів, з погляду безпеки, водій повинен розраховувати на менш сприятливі умови. Тобто небезпечна обстановка виникає у випадку, коли водій бачить дітей шкільного віку, захоплених рухомими іграми, які можуть опинитися в небезпечній зоні, або малолітніх дітей (дошкільного віку) без нагляду дорослих, а також якщо він знаходить інші обставини, наприклад, м'яч на проїжджій частині, що свідчить про можливість раптового виникнення перешкоди на близькій відстані.

Слід вважати, що небезпека для руху транспортного засобу діями пішоходів і дітей не створюється при наступних обставинах:

– пішохід до моменту зближення з ним транспортного засобу при вибраній швидкості не встигає досягти небезпечної зони або встигає вийти за її межі навіть при русі транспортного засобу без гальмування якщо, звичайно, водій не може знайти обставин, які могли б вплинути на характер дій пішохода;

– пішохід, що пропускає транспортний засіб, знаходиться на безпечній відстані від смуги його руху, а водій не може знайти обставин, які могли б змусити пішохода вчинити рухи в небезпечному напрямі;

– діти дошкільного віку знаходяться під наглядом дорослих в безпосередній близькості від смуги руху транспортного засобу та дії дорослих повинні виключати можливість попадання дитини в небезпечну зону (дорослі утримують дітей за руку тощо).

При наближенні до учасників з підвищеною небезпекою для руху, а також у випадках, коли водій, згідно з Правилами дорожнього руху, повинен дотримуватися особливої обережності, йому слід вживати заходів, що зменшують імовірність виникнення небезпечної ситуації – підвищити увагу, понизити швидкість руху транспортного засобу, збільшити інтервал та дистанцію.

На вибір моменту виникнення небезпеки впливають різні чинники такі, як напрям руху пішохода (справа наліво або зліва направо), кількість смуг для руху в кожному напрямку, розташування ТЗ на проїжджій частині, умови видимості та оглядовості, організація переходу проїжджої частини.

Відзначимо, що наведені небезпечні ситуації є типовими і дозволяють експерту дійти правильного висновку про момент виникнення небезпечної обстановки в більшості випадків. Разом з тим, в деяких випадках, залежно від конкретних обставин події, при вирішенні питання про момент виникнення небезпечної ситуації експерт може дійти інших висновків.

Щодо **вдосконалення методів дослідження маневру транспортного засобу**, то правилами дорожнього руху України у разі виникнення перешкоди для руху передбачено два способи запобігання дорожньо-транспортній

події: зниження швидкості руху транспортного засобу аж до повної його зупинки або безпечний об'їзд перешкоди [14]. У зв'язку з цим під час розслідування ДТП суд або органи дізнання часто ставлять експертам запитання: "Чи мав водій транспортного засобу технічну можливість здійснити безпечний об'їзд перешкоди на зазначеній відстані?" [15]. Крім того, в усіх випадках застосування водієм транспортного засобу маневру під час дослідження механізму розвитку дорожньо-транспортної ситуації експерт повинен перевірити вихідні дані на технічну спроможність, тобто перевірити, чи міг транспортний засіб на заданій відстані до перешкоди змінити траєкторію свого руху для уникнення зіткнення із перешкодою. Для цього необхідно провести теоретичні розрахунки траєкторії руху транспортного засобу у процесі маневру.

На сьогодні в експертній практиці досліджуються три види маневру [10]:

– "вхід у поворот" (відвернення від перешкоди), рис. 7, а;

– "вхід-вихід", рис. 7, б;

– "зміна смуги руху", рис. 7, в.

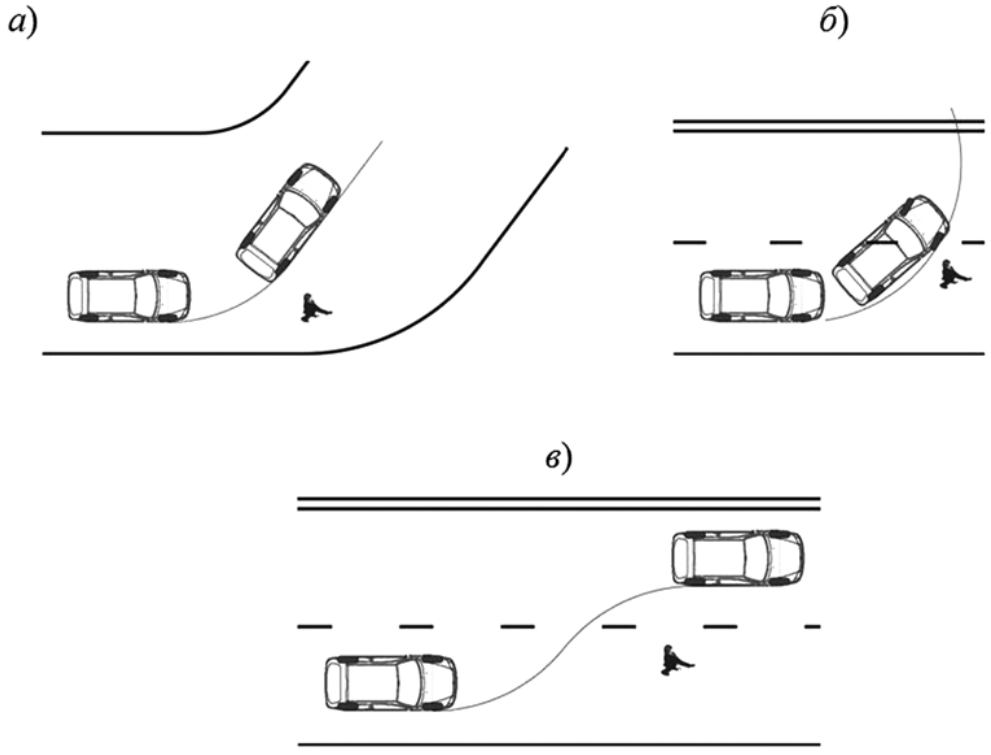


Рис. 7. Види застосування маневру транспортного засобу [15]:
а) "вхід у поворот"; б) "вхід-вихід"; в) "зміна смуги руху"

У випадку маневру “вхід у поворот” водій транспортного засобу повертає рульове колесо з нейтрального положення (відповідно до прямолінійного руху транспортного засобу) на певний кут, після чого фіксує рульове колесо в цьому положенні. Наприкінці маневру транспортний засіб рухається по дузі кола з постійним радіусом. Цей вид маневру застосовується водіями, як правило, у критичних ситуаціях і є найпростішим у виконанні, але й найнебезпечнішим, тому що може призвести до заносу і перекидання транспортного засобу.

У випадку маневру “вхід-вихід” водій транспортного засобу повертає рульове колесо з нейтрального положення, що відповідає прямолінійному руху транспортного засобу, на певний кут, а після бажаної зміни траєкторії руху транспортного засобу – знову у нейтральне положення. Наприкінці маневру транспортний засіб рухається прямолінійно під певним кутом до початкового напрямку його руху. Цей вид маневру також (як і маневр “вхід уповорот”) потребує достатньо великої ширини дороги.

У випадку маневру “зміна смуги руху” водій транспортного засобу повертає рульове колесо з нейтрального положення, що відповідає прямолінійному руху транспортного засобу, на певний кут, після чого через нейтральне положення – у зворотній бік на такий самий кут і знову – у нейтральне положення. Наприкінці маневру транспортний засіб рухається паралельно до початкового напряму його руху. Цей вид маневру водії застосовують не тільки при об’їзді перешкоди, але й при переїзді на сусідню смугу руху та при виконанні обгону транспортного засобу.

Слід зазначити, що розрахунковим шляхом визначити дійсну траєкторію руху транспортного засобу при маневрі досить складно через те, що не можна точно встановити, з якою кутовою швидкістю водій здійснював поворот рульового колеса і як змінювалася ця швидкість у процесі повороту. Тому експерт може визначити лише гранично можливі значення параметрів маневру транспортного засобу.

Під час проведення автотехнічних експертиз дослідження маневру транспортного засобу експерт може обирати той чи інший варіант на основі власного досвіду, що за певних обставин ДТП може призвести до того, що висновки різних автотехнічних експертиз можуть бути навіть протилежними [8]. Крім того, необхідно враховувати, що на даний час автомобілі стали більш безпечними за рахунок застосування нових матеріалів та удосконалення конструкції. Сучасні автомобілі обладнані підсилювачем керма, незалежною багатоважільною підвіскою та ін. Крім того, завдяки впровадженню нових матеріалів і технологій зчеплення сучасних шин з дорожнім покриттям стало значно кращим, ніж кілька десятків років тому.

У зв'язку з цим для достовірних розрахунків маневру сучасного автомобіля достатньо ефективним є застосування емпірично-статистичних моделей побудованих на основі експериментальних випробувань [9, 10]. У відповідності з таким підходом, при проведенні автотехнічної експертизи, розрахунок величини поперечного відхилення смуги руху (модель маневру "вхід у поворот") визначається так:

$$a = R_{\text{пр}} - (R_{\text{пр}}{}^2 - S_{\text{м}}^2)^{1/2}. \quad (2)$$

$$R_{\text{пр}} = \frac{v_a^2}{125 \cdot \theta} + \frac{B_a}{2}. \quad (3)$$

де: $_{\text{пр}}$ – граничне по зчепленню значення радіуса повороту передньої габаритної зовнішньої точки транспортного засобу, м; V_a – експериментально визначена максимальна швидкість руху транспортного засобу при виконанні маневру, км/год; θ – коефіцієнт зчеплення при бічному ковзанні; B_a – габаритна ширина транспортного засобу, м; $S_{\text{м}}$ – відстань, яку подолав транспортний засіб при виконанні маневру, м.

А відповідно величина поперечного зміщення при маневрі "зміна смуги руху" розраховується за формулою:

$$a = 2R_{\text{пр}} - B_{\text{а}} - \left[(2R_{\text{пр}} - B_{\text{а}})^2 - S_{\text{м}}^2\right]^{1/2}. \quad (4)$$

Застосування наведених формул для розрахунку величин зміщення при дослідженні маневру транспортного засобу дозволяє отримати задовільну точність визначення параметрів ДТП.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямку. На основі проведеного аналізу можна зробити висновок, що визначення параметрів та реконструкція ДТП має надзвичайно важливе значення встановлення реальних обставин її виникнення. Тому при проведенні експертизи ДТП необхідно використовувати комплексний підхід із застосуванням даних як теоретичного дослідження так і експериментального підтвердження коректності технічних параметрів ДТП. При експертному дослідженні маневру транспортного засобу достатньо ефективним є застосування емпірично-статистичних моделей побудованих на основі експериментальних випробувань.

В подальших дослідженнях для отримання більш точних та об'єктивних параметрів маневру сучасного автомобіля під час проведення автотехнічної експертизи слід розвивати системний підхід направлений на уточнення розрахункових даних з подальшою їх експериментальною перевіркою.

Список використаних джерел:

1. Автомобільний транспорт України: стан, проблеми перспективи розвитку: [монографія] /Державний автотранспортний науково-дослідний і проектний інститут; за заг. ред. А. М. Редзюка. – К. : ДП "Державтотранс НДІ проект", 2005. – 400 с.

2. Аварійність на дорогах України у 2014 – 2017 рр. [Електронний ресурс]. – Режим доступу: https://ru.slovoidilo.ua/2017/05/04/infografika/obshhestvo/statistika-dtp-ukraine-samaya-vysokaya-smertnost-dorogax-vsex-stran-evropy.

3. Байэтт Р. Расследование дорожно–транспортных происшествий / Р. Байэтт, Р. Уоттс ; пер. с англ. А. Шалатова. – М. : Транспорт, 1983. – 288 с.

4. Коллинз Д. Анализ дорожно-транспортных происшествий / Д. Коллинз, Д. Моррис ; пер. с англ. А. Шалатова. – М. : Транспорт, 1971. – 128 с.

5. Волков В. П. Совершенствование методов автотехнической экспертизы при дорожно-транспортных происшествиях / В. П. Волков, В. Н. Торлин, В. М. Мищенко и др. – Х. : ХНАДУ, 2010. – 476 с.

6. Берус А. Л., К вопросу экспериментального исследования технического механизма дорожно-транспортных происшествий, при наезде на пешеходов / А. Л. Берус // Вісник АМСУ. Техніка. – 2011. – № 1(45). – С. 38–41.

7. Кішка С. П. Способи оцінки безпеки руху та аварійності на автомобільних дорогах / С. П. Кішка // Вісник НТУ. – К.: НТУ, 2012. – Вип. 26. – С. 162–167.

8. Сараєв О. В. Проблемні питання визначення параметрів руху транспортних засобів при дослідженні ДТП / О. В. Сараєв // Вісник ХНАДУ : зб. наук. пр. – 2013. – Вып. 61–62. – С. 174–178.

9. Стариков Е. Л. Синтез расчетного и экспериментального методов исследования маневра автомобиля / Е. Л. Стариков, А. В. Сараев // Криміналістичний вісник : наук.-практ. зб. – 2013. – № 2 (20). – С. 184–192.

10. Туренко А. М. Автотехнічна експертиза. Дослідження обставин ДТП : підруч. для ВНЗ / А. М. Туренко, В. І. Клименко, О. В. Сараєв, С. В. Данець. – Х. : ХНАДУ, 2013. – 320 с.

11. Пасечник А. Н. Экспертиза и системный анализ технических механизмов дорожно-транспортных происшествий в случае наезда на пешехода / А. М. Пасічник, А. Л. Берус // Тези допов. міжн. наук.-практ. конф. Перспект. розвитку інформ. та транспортно-митн. технологій у митній справі. АМСУ, Д., 2011. – С. 374–376.

12. Солтус А. П. Теория эксплуатационных свойств автомобиля / А. П. Солтус. – К.: Аристей, 2005. – 188 с.

13. Засоби транспортні дорожні. Стійкість. Методи визначення основних параметрів випробування: ДСТУ 3310-96. – [Чинний від 1997-01-01]. – К. : Держстандарт України, 1996. – 10 с.

14. Правила дорожнього руху. Офіційне видання / [кол.авт. наук-досл. центру безп. дор. руху та ГУДАІ МВС України]. – К. : Арій, 2009. – 64 с.

15. Старіков Є. Л. Вдосконалення методів дослідження маневру транспортного засобу / Є. Л. Стариков // Криміналістичний вісник : наук.-практ. зб. – 2013. – № 2 (20). – С. 201–209.

References:

1. Avtomobil′nyy transport Ukrayiny: stan, problemy perspektyvy rozvytku: [monohrafiya] /Derzhavnyy avtotransportnyy naukovo-doslidnyy i proektnyy instytut; za zah. red. A. M. Redzyuka. – K. : DP "Derzhavtotrans NDI proekt", 2005. 400 s.

2. Avariynist′ na dorohakh Ukrayiny u 2014 – 2017 rr. [Elektronnyy resurs]: Rezhym dostupu: https://ru.slovoidilo.ua/2017/05/04/infografika/obshhestvo/ statistika-dtp-ukraine-samaya-vysokaya-smertnost-dorogax-vsex-stran-evropy.

3. Bayétt R. Rassledovanye dorozhno–transportnykh proysshestvyy / R. Bayétt, R. Uott·s ; per. s anhl. A. Shalatova. – M. : Transport, 1983. – 288 s.

4. Kollynz D. Analyz dorozhno-transportnykh proysshestvyy / D. Kollynz, D. Morrys ; per. s anhl. A. Shalatova. – M. : Transport, 1971. – 128 s.

5. Volkov V. P. Sovershenstvovanye metodov avtotekhnycheskoy ékspertyzy pry dorozhno-transportnykh proysshestvyyakh / V. P. Volkov, V. N. Torlyn, V. M. Myshchenko y dr. – KH. : KHNADU, 2010. – 476 s.

6. Berus A. L., K voprosu éksperymental′noho yssledovanyya tekhnycheskoho mekhanyzma dorozhno-transportnykh proysshestvyy, pry naezde na peshekhodov / A. L. Berus // Visnyk AMSU. Tekhnika. – 2011. – № 1(45). – S. 38–41.

7. Kishka S. P. Sposoby otsinky bezpeky rukhu ta avariynosti na avtomobil′nykh dorohakh / S. P. Kishka // Visnyk NTU. – K.: NTU, 2012. – Vyp. 26. – S. 162–167.

8. Sarayev O. V. Problemni pytannya vyznachennya parametriv rukhu transportnykh zasobiv pry doslidzhenni DTP / O. V. Sarayev // Visnyk KHNADU : zb. nuk. pr. – 2013. – Vyp. 61–62. – S. 174–178.

9. Starykov E. L. Syntez raschetnoho y éksperymental′noho metodov yssledovanyya manevra avtomobylya / E. L. Starykov, A. V. Saraev // Kryminalistychnyy visnyk : nauk.-prakt. zb. – 2013. – № 2 (20). – S. 184–192.

10. Turenko A. M. Avtotekhnichna ekspertyza. Doslidzhennya obstavyn DTP : pidruch. dlya VNZ / A. M. Turenko, V. I. Klymenko, O. V. Sarayev, S. V. Danets'. – KH. : KHNADU, 2013. – 320 s.

11. Pasechnyk A. N. Ékspertyza y systemnyy analyz tekhnycheskykh mekhanyzmov dorozhno-transportnykh proysshestvyy v sluchae naezda na peshekhoda / A. M. Pasichnyk, A. L. Berus //Tezy dopov. mizhn. nauk.-prakt. konf. Perspekt. rozvytku inform. ta transportno-mytn. tekhnolohiy u mytniy spravi. AMSU, D., 2011. – S. 374–376.

12. Soltus A.P. Teoryya éxpluatatsyonnykh svoystv avtomobylya / A.P. Soltus. – K.: Arystey, 2005. – 188 s.

13. Zasoby transportni dorozhni. Stiykist′. Metody vyznachennya osnovnykh parametriv vyprobuvannya: DSTU 3310-96. – [Chynnyy vid 1997-01-01]. – K.: Derzhstandart Ukrayiny, 1996. – 10 s.

14. Pravyla dorozhn′oho rukhu. Ofitsiyne vydannya / [kol.avt. Nauk-dosl. tsentru bezp. dor. rukhu ta HUDAI MVS Ukrayiny]. – K.: Ariy, 2009. – 64 s.

15. Starykov E. L. Vdoskonalennia metodiv doslidzhennia manevru transportnoho zasobu / E. L. Starykov // Kryminalistychnyy visnyk : nauk.-prakt. zb. – 2013. – № 2 (20). – S. 201–209.

DOI: https://doi.org/10.32836/2521-6643-2018.2-56.6
УДК 004.056.2

В. Я. Пєвнєв, кандидат технічних наук, доцент кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. Н. Є. Жуковського "Харківський авіаційний інститут"

МОДЕЛІ ЗАГРОЗ І ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ІНФОРМАЦІЇ

Проведено аналіз визначення поняття цілісності інформації в різних галузях науки і прикладних дисциплінах. Запропоновано визначення цілісності інформації для інфокомунікаційних систем. Розглянуто можливі загрози цілісності інформації протягом її життєвого циклу. Проведено аналіз загроз цілісності інформації щодо об'єктів інфокомунікаційних систем та методів забезпечення цілісності. Розглянуто методи забезпечення та контролю цілісності з подальшим відновленням в інфокомунікаційних системах.

Ключові слова: *цілініcть інформації; модель цілісності; загрози; об'єкти загроз; методи забезпечення; контроль цілісності*.

Проведен анализ определения понятия целостности информации в различных областях науки и прикладных дисциплинах. Предложено определение целостности информации для инфокоммуникационных систем. Рассмотрены возможные угрозы целостности информации в течение её жизненного цикла. Проведен анализ угроз целостности информации по объектам инфокоммуникационных систем и методов обеспечения целостности. Рассмотрены методы обеспечения и контроля целостности с последующим восстановлением в инфокоммуникационных системах.

Ключевые слова: *целостность информации; модель целостности; угрозы; объекты угроз, методы обеспечения; контроль целостности*.

The analysis presented in the paper shows that there is no unambiguous interpretation of many terms in the modern community of scientists and practitioners. On this basis, one can conclude that there is a need for uniform interpretation of terms. This will allow representatives of different fields to communicate more closely. The integrity model and threats in the infocommunication systems makes it possible to understand the place of information integrity in modern systems. Currently,

violation of information integrity is the most dangerous impact on all systems, including critical ones. The impact on information, from the point of view of integrity, can be its distortion and imposition. For the purpose of protection, both organizational and technical methods. From the economic point of view, the construction of technical means of protection systems is unprofitable. However, the cost of these systems of defense in oftentimes can be less than, than possible damage that can be inflicted as a result of attacks. The threat model proposed in the article reflects both the objects targeted by the threats and the threats themselves. Based on the results of the analysis, we can conclude that the most vulnerable elements are software. The number of attacks on software is more than 53 percent. The paper describes the possible methods and means of providing and monitoring the information integrity. Among them it is possible to allocate both well known methods (for example, noise proof coding), and methods which are rather seldom used for maintenance of information integrity (steganography). The methods of providing of integrity of information can be divided into two large groups. To the first group will be belongs methods that directly provide to integrity of information. Methods that allow you to control the integrity of information and, if necessary, restore the message belong to the second group. Some methods are used both in the first and in second groups. For example, facilities of anti-virus defense allow both to protect a computer from a virus (first group) and recover the damaged file (second group). The analysis which has been spent, shows variety of forms and methods of construction of systems of maintenance of information integrity.

Key words: *model of information integrity; threat; objects of threats; methods of providing; control of integrity*.

Постановка проблеми. Забезпечення інформаційної безпеки під час використання інфокомунікаційних систем (ІКС) передбачає розв'язання проблем забезпечення цілісності, доступності та конфіденційності, хоча в останніх публікаціях і європейських стандартах до цих трьох китів додаються автентичність, підзвітність, безвідмовність і надійність [1]. У більшості систем, включаючи системи, в яких циркулює інформація з обмеженим доступом, найбільш гострою проблемою є забезпечення цілісності інформації (ЦІ).

Аналіз останніх досліджень і публікацій. Що таке цілісність інформації? На жаль, нинішнього часу в різних галузях науки і прикладних дисциплінах немає єдиного поняття цілісності. Необхідність єдиного визначення обумовлюється тим, що в системі потрібно мати один термін для позначення одного явища, дії або предмета дослідження. У якості цього терміна можна було використанне поняття достовірності, але цей термін більш підходить, коли йдеться про відповідність даних явищу, яке вони описують.

Цілісність повинна відноситьсь і прив'язуватись до системи, в якій проводиться обробка інформації, і забезпечується її незмінність. У табл. 1 подано визначення поняття цілісності в різних галузях [1–4].

Таблиця 1

Порівняння поняття цілісності

Найменування галузі	Поняття цілісності	Синоніми
Теорія інформації	Відсутня	Достовірність і повнота
Теорія зв'язку	Відсутня	Достовірність
Теорія інформаційної безпеки	Властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення	
Теорія функціональної безпеки	Властивість виключати непередбачені зміни системи і послуг, що надаються	
Теорія баз даних	Коректність даних та їх несуперечність, а також повнота і правильність інформації, яка вміщується в БД	
Представлена робота	Здатність системи за допомогою вбудованих засобів протягом заданого часу протидіяти несанкціонованій зміні інформації та (або) відновлювати викривлену інформацію	

Виходячи з вищенаведеного, можна зробити висновок про актуальність розгляду методів досягнення ЦІ в ІКС.

Під цілісністю розуміється здатність системи за допомогою вбудованих засобів протягом заданого часу протидіяти несанкціонованій зміні інформації та/або відновлювати викривлену інформацію

Слід зазначити, що ні доступності, а тим більше конфіденційності, без забезпечення ЦІ досягти неможливо. Наприклад, за сучасними вимогами до криптосистем, незначна зміна вихідного тексту повинна приводити до значної зміни шифрованої послідовності. Якщо в процесі передачі спотвориться один біт переданої шифрограми, то після розшифровки отриманий текст дуже відрізнятиметься від початкового. Отже, можна говорити про проблему забезпечення ЦІ, яка нині не розв'язана повною мірою.

Мета статті – розробка моделі цілісності інформації в ІКС та аналіз сучасних методів і засобів забезпечення цілісності інформації.

Виклад основного матеріалу. Виходячи з визначення ЦІ, можна виділити такі впливи на інформацію [5]:

– модифікацію інформації;

– підміну інформації;

– знищення інформації.

Модифікація передбачає зміни будь-якої частини інформації. Ці зміни можуть бути як випадковим, так і навмисними. В даному випадку вони можуть бути санкціонованими або несанкціонованими.

Підміна передбачає нав'язування неправдивої інформації шляхом заміни істинної (первісної) інформації. Знищення найчастіше пов'язується зі знищенням фізичного носія інформації та/або розмагнічуванням (форматуванням) електронних носіїв.

Розглянемо можливі загрози ЦІ протягом її життєвого циклу. При використанні неповних та/або помилкових даних під час створення (появи) інформації можна отримати інформацію, що не відповідає дійсності, про ті чи інші події. Адекватність прийнятого рішення, заснованого на такій інформації, викликає сумніви.

Під час обробки інформації порушення ЦІ може виникнути внаслідок технічних несправностей, алгоритмічних і програмних помилок, помилок і деструктивних дій обслуговуючого персоналу, зовнішнього втручання, шкідливих і програм, що руйнують (вірусів, троянів, черв'яків, логічних бомб).

У ході передачі на інформацію можуть впливати різні завади як природного, так і штучного походження. При цьому можливо її спотворення або стирання (знищення). Крім цього, можливе перехоплення інформації з метою її модифікації і подальшого нав'язування.

У ході зберігання основними загрозами є несанкціонований доступ з метою модифікації (аж до знищення) інформації, шкідливі програми (віруси, трояни, черв'яки, логічні бомби) і технічні несправності.

В процесі старіння основними загрозами інформації, поряд з погрозами під час зберігання, можна вважати втрату технологій, здатних відтворити ту чи іншу інформацію, і фізичне старіння носіїв інформації.

Слід зазначити, що на всіх етапах життєвого циклу існує загроза ЦІ через технічні системи, що використовуються. Це банальні несправності, збої електроживлення, електромагнітні імпульси тощо.

Під час утилізації про забезпечення ЦІ не йдеться.

Тому можна зробити висновок про те, що загрози ЦІ виникають протягом усього життєвого циклу інформації з моменту її появи до початку утилізації.

Якщо класифікувати загрози ЦІ за ознакою частоти загроз, то можна зробити такий висновок. У ході розгляду 128 загроз цілісності [6–9] 21 загрозу представляли несанкціоновані дії щодо всіх складових ІКС. Наприклад, існують загрози:

– несанкціонованого доступу до системи зберігання даних з віртуальної та (або) фізичної мережі;

– несанкціонованого редагування реєстру;

– несанкціонованого доступу до локального комп'ютера через клієнта грід-системи;

– перехоплення управління середовищем віртуалізації.

За кількістю ці загрози були на першому місці. Другу групу загроз становили шкідливі програми. До них нлежать і так звані віруси. Загальна кількість цих загроз дорівнює 20. Серед них:

– загроза спотворення інформації, що вводиться і виводиться на периферійні пристрої;

– загроза впровадження шкідливого коду в BIOS;

– загроза несанкціонованого вимкнення або обходу механізму захисту від запису в BIOS;

– загроза зараження комп'ютера під час відвідування неблагонадійних сайтів;

– загроза поширення "поштових черв'яків".

На третьому місці – загрози, які виникають у мережі. Кількість цих загроз дорівнює 15. У діапазоні 8–6 загроз містяться загрози виходу процесу за межі віртуальних машин, порушення в хмарних технологіях, зміни конфігурації програмного забезпечення та апаратних засобів, незаконне використання привілеїв, зміни формату даних і використання слабих криптографічних даних. У кінці списку загроз ще 6 загроз, які трапляються 1–3 рази.

Під час аналізу загроз ЦІ були розглянуті елементи ІКС. Серед них виділено програмну складову, що являла собою сукупність прикладного програмного забезпечення, системного програмного забезпечення, в якому був окремо виділений BIOS, і мережного програмного забезпечення. Окремо розглядалися апаратне забезпечення і апаратні пристрої, грід-системи й робочі станції. Також було виділено об'єкти мережної структури, до яких належать: мережний вузол, мережний трафік і вся сукупність інформаційної системи. Окремо було розглянуто сховище великих даних і хмарна система, а також окремі об'єкти (об'єкти файлової системи, віртуальні машини, облікові дані користувачів, носії обміну інформацією та ін.), на які було спрямовано різноманітні загрози. Перелік цих об'єктів і кількість загроз, спрямованих на ці об'єкти, подано в табл. 2.

В цілому виділено 18 об'єктів, на які було спрямовано 128 загроз ЦІ. Велика частина загроз була спрямована на програмне забезпечення діяльності ІКС. Слід зазначити, що невисокий відсоток загроз, спрямований на мережну складову, не повинен викликати подив. Тут не враховувалося використання мережних механізмів для проникнення в комп'ютери, програмну складову або в хмарні системи.

Таблиця 2

Об’єкти загроз

Об’єкти загроз	Кількість загроз			
	Спрямовані	Багатовекторні	Разом	Разом у відсотках
Апаратне забезпечення, апаратний пристрій	4	16	20	7,4
Грід-системи	2	1	3	1,1
Робоча станція		2	2	0,7
Прикладне програмне забезпечення	3	35	38	14,0
Системне програмне забезпечення	9	43	52	19,1
BIOS	12	3	15	5,5
Мережне програмне забезпечення	4	36	40	14,7
Програмне забезпечення (взагалі)	28	117	145	53,3
Об’єкти файлової системи	1	13	14	5,1
Віртуальна машина	4	7	11	4,0
Мережний вузол		11	11	4,0
Інформаційна система	1	10	11	4,0
Мережний трафік	1	6	7	2,6
Мережна система (взагалі)	2	27	29	10,7
Хмарна система	5	8	13	4,8
Сховище великих даних, метадані, база даних		11	11	4,0
Облікові дані користувача		5	5	1,8
Носій обміну інформацією	1	7	8	2,9
Реєстр		8	8	2,9
Засоби захисту інформації		3	3	1,1
Взагалі	47	225	272	100,0

У табл. 2 виділено загрози, спрямовані на конкретні об’єкти, серед яких виділяється за кількістю цих загроз BIOS, і загрози, спрямовані одночасно на кілька об’єктів.

Проаналізуємо сучасні методи й засоби забезпечення цілісності інформації. Методи забезпечення ЦІ можна розбити на дві великі групи. До першої групи зараховуємо методи, які безпосередньо забезпечують ЦІ. До другої групи – методи, які дозволяють контролювати ЦІ і, в разі необхідності, відновлювати повідомлення (рис. 1).

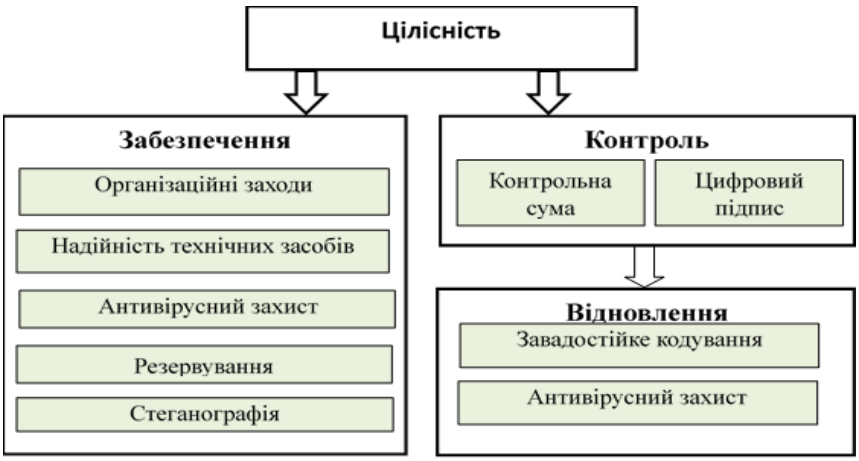


Рис. 1. Методи забезпечення ЦІ

Поширеним і досить ефективним методом забезпечення ЦІ є організація доступу до інформації та обладнання, що використовується. Даний метод належить до організаційних і передбачає досить великий перелік заходів, починаючи від добору співробітників і закінчуючи роботою з технікою і документами [10].

Серед них можна виділити технології захисту, обробки та зберігання документів, атестацію приміщень і робочих зон, порядок ЦІ від випадкових та/або несанкціонованих дій персоналу тощо. Для забезпечення ЦІ в ІКС особливу увагу слід приділити захисту операційних систем (ОС), що забезпечують функціонування практично всіх складових системи. Найбільш дієвим механізмом розмежування доступу для ОС є ізольоване програмне середовище (ІПС) [11]. ІПС підвищує стійкість ІКС до різних шкідливих програм і програм, що руйнують, дозволяючи забезпечити ЦІ.

Надійність технічних засобів. Необхідною умовою забезпечення ЦІ є наявність високонадійних технічних засобів (ТЗ), які включають в себе як апаратну, так та/або програмну складові [12]. Таке обладнання повинно забезпечувати як високу відмовостійкість, так і ЗІ від можливих загроз.

Одним із найбільш поширених засобів підвищення надійності ТЗ є резервування. Якщо розглядати ТЗ з точки зору інформаційної складової, то підвищення надійності досягається за рахунок послідовного з'єднання елементів системи, що відповідають за дану складову. Якщо послідовно з'єднати два комп'ютери, поставивши на кожен із них свій антивірус, то ймовірність проникнення шкідливої програми зменшується. Однак при цьому зменшується ймовірність безвідмовної роботи ТЗ, що складається з двох комп'ютерів, які послідовно з'єднані.

Для забезпечення заданої надійності (гарантоздатності) такого інформаційно-технічного комплексу необхідно застосовувати послідовно-паралельну архітектуру побудови систем ТЗ.

ТЗ припускають і можливість використання виділених та/або фізично захищених лінії зв'язку, наприклад броньовані кабелі з контролем цілісності оболонки.

До ТС забезпечення ЦІ належать також і засоби захисту від електромагнітного імпульсу (ЕМІ). Вражаючими факторами ЕМІ є високоінтенсивні електромагнітні поля, які або безпосередньо впливають на радіоелектронні засоби (РЕЗ), або трансформуються в небезпечних трактах цих засобів у наведені струми й напруги [13]. Найбільш ефективним методом зменшення інтенсивності ЕМІ є екранування – розміщення обладнання в електропровідному корпусі, який перешкоджає проникненню електромагнітного поля від джерела до обладнання, що захищається. Однак в більшості випадків обладнання, яке захищають, має зовнішні комунікації, що призводить до проникнення в екранований простір наведених завадових струмів і напруги, що викликають пошкодження елементної бази РЕЗ. Рішенням є методи обмеження наведених напруг і струмів за амплітудою і спектром у зовнішніх трактах РЕЗ і електромагнітна розв'язка зовнішніх ланцюгів РЕЗ від екранованих пристроїв. Для обмеження наведень за амплітудою і спектром використовуються іскрові і газорозрядні розрядники, напівпровідникові обмежувальні пристрої, варистори і спеціальні нелінійні опори. До обмежувача спектра належать прохідні конденсатори, дроселі та фільтри [13].

Електромагнітна розв'язка досягається за допомогою ізолювальних трансформаторів, дроселів, оптронів, елементів оптоелектроніки. Застосування оптоелектронних схем дозволяє зменшити число замкнутих контурів і забезпечити електричну розв'язку кола. Крім цього, системи на базі оптоелектроніки некритичні до впливу перешкоджаючих електромагнітних полів унаслідок того, що носіями інформації в цих системах є електрично нейтральні фотони. Ще однією перевагою оптоелектронних систем стало обмеження смуги пропускання, особливо на високих частотах, й що тим самим є бездротовими обмежувачами високочастотних завадових наведень на вхідні кола РЕЗ, які властиві ЕМІ [13].

Стиснення даних. Як відомо [14], стиснення це заміна послідовності символів іншою послідовністю меншої довжини або оптимальне кодування. Забезпечення ЦІ досягається за рахунок зменшення обсягу інформації, що передається. Це зменшення можна досягти за рахунок оптимального кодування джерела. Однак такий метод у даний час практично не використовується з огляду на те, що під час цифрової обробки сигналу вигідніше, з точки зору організації обчислювального процесу, під кожен символ виділяти однакову кількість біт.

Найчастіше використовується метод динамічного стиснення. За такого підходу структура стисненого повідомлення включає в себе словник і стислу інформацію. Зменшення обсягу переданої інформації досягає 20 разів (залежно від типу інформації, що передається). Однак, якщо під час передачі або зберігання виявляється помилка, особливо в словнику, то виникає ефект розмноження помилок, що призводить до значного спотворення або знищення інформації.

У працях [15–16] подано спосіб стиснення інформації, що дозволяє зменшити розмір файлів невеликої довжини (менше 1000 біт) до 75 відсотків. Основна ідея даного способу – використання шести біт для кодування переданого символу й декількох кодових таблиць, попередньо розміщених у користувачів ІКС.

Стеганографія. З цим терміном знайомі всі, хто займається питаннями ЗІ. Нині можна виділити три тісно пов'язаних між собою напрямки стеганографії: приховування даних, цифрові водяні знаки і заголовки. За прихованої передачі інформації одночасно із забезпеченням конфіденційності [17] вирішується й питання забезпечення ЦІ. Не можна змінити того, чого не бачиш – головний аргумент використання стеганографії для забезпечення ЦІ.

Одним із найпростіших способів прихованої передачі є відправлення повідомлення всередині іншого повідомлення. Це може бути якийсь контейнер, наприклад, у згрупованому об'єкті що на другому плані міститься текстове повідомлення, написане білим по білому. До цього методу можна зарахувати і використання спеціальних сигналів, наприклад широкосмугових шумоподібних або ортогональних.

Головним недоліком використання стеганографії для забезпечення ЦІ є значно більшим обсягом контейнера в порівнянні з обсягом повідомлення. Але цей недолік можна нівелювати, передаючи в якості контейнера корисну інформацію, не критичну до ЦІ.

Про використання методів стеганографії з метою забезпечення ЦІ не прийнято говорити, хоча вони є найбільш ефективними для досягнення поставленої мети.

Антивірусний захист. Однією із загроз ІБ є шкідливі програми, в яких окремим класом виділяються віруси. Їх безліч видів і типів, вони відрізняються між собою способами впливу на різні файли, розміщенням у пам'яті ЕОМ або програмах, об'єктами впливу. Але головна властивість вірусів – здатність до розмноження. Це властивість виділяє їх серед безлічі шкідливих програм і робить найбільш небезпечними.

Одним із найбільш дієвих способів забезпечення ЦІ є добре продуманий і надійний захист від вірусів. Найбільш поширеним способом захисту від вірусів є використання антивірусних програм, яких у даний час достатня кількість. Однак необхідно пам'ятати, що жодна програма не гарантує виявлення невідомого вірусу.

Евристичні сканери, що застосовуються, теоретично можуть виявити невідомі віруси за непрямими ознаками, не завжди дають правильний діагноз. Прикладом подібних помилок можуть служити дві антивірусні програми, які запущені на одному комп'ютері. Практично будь-який користувач стикався з ситуацією, коли файли одного антивірусу приймалися за шкідливу програму іншим антивірусом.

Найкращим засобом захисту від вірусів є використання локальних мереж, які не мають зв'язку з інтернетом. При цьому необхідно жорстко контролювати різні носії інформації з прикладними програмами, за допомогою яких можна занести вірус.

Резервування. Під резервуванням розуміється в даному контексті можливість програмних засобів створювати свої копії в процесі виконання програм. Створюються так звані точки відкоту, до яких програма працювала правильно. Якщо в результаті збоїв або інших причин сталося порушення ходу виконання програми, то вона відкочується до заздалегідь визначеної точки і продовжує своє виконання. Найчастіше точки відкоту створюються користувачем шляхом вибору часу створення такої точки.

Аналіз сучасних методів і засобів контролю цілісності інформації. Перевірку цілісності повідомлення можна проводити двома методами. До першого методу належать контрольна сума, в якій виділяються безпосередньо контрольна сума і хеш сума. До другого методу – цифровий підпис.

Контрольна сума. Під терміном "контрольна сума" розуміється метод перевірки цілісності прийнятої інформації на приймальній стороні. Суть контрольної суми полягає в діленні повідомлення на деяку, заздалегідь визначену константу, де сумою виступає залишок від ділення. Найбільш проста контрольна сума – перевірка на парність, що відповідає діленню на два. Зазвичай в якості дільника використовують поліноми 8, 16 або 32 ступенів.

Контрольною сумою може бути перевірка на парність різних комбінацій переданих біт. У цьому випадку можна говорити не тільки про виявлення помилок, а й про їх виправлення. Цей принцип лежить в основі систем завадостійкого кодування, що дозволяє відновлювати як поодинокі, так і кратні помилки в прийнятих повідомленнях. В цьому випадку можна говорити не тільки про контроль цілісності, а й про забезпечення цілісності.

Подальшим розвитком контрольних сум стало використання хеш функцій, які мають деякі відмінності від перевірки на парність. Найголовніша відмінність – це наявність лавинного ефекту, коли результат застосування хеш функції залежить від кожного біта повідомлення. Окрім цього, ці функції мають постійний розмір, незалежно від довжини повідомлення, обчислювальне неможливо згенерувати два різних повідомлення з однаковими хешами, обчислюванням неможливо відновити повідомлення зі значення хешу.

У деяких випадках як хеш функції використовуються алгоритми блокового шифрування, при цьому значення хешу залежатиме не лише від самого повідомлення, але й від секретного ключа, використовуваного в алгоритмі шифрування.

Електронний підпис. Електронний підпис – це механізм перевірки ЦІ, котра приймається. Електронний підпис – електронні дані, які додаються підписувачем до других електронних даних або логічно з ними пов'язуються і використовуються ним як підпис [18]. Документ, який підписується, представляється у відкритому вигляді, тобто незашифрованим. На стороні відправника обчислюється хеш документа, який необхідно передати. Отриманий хеш шифрується за допомогою особистого ключа відправника і відсилається разом із документом, що передається. На приймальній стороні обчислюється хеш документа, розшифровується отриманий разом з документом хеш за допомогою відкритого ключа і порівнюються два отриманих хеша. Якщо вони збігаються, то документ у процесі передачі не був спотворений, в іншому випадку він відкидається.

Головною проблемою отримання пари ключів є знаходження простих чисел великої розмірності, на яких ґрунтується побудова асиметричної системи шифрування. Нині розміри ключів сягають чотирьох кілобіт, що відповідає десятковим числам розміром приблизно в 1300D. Це означає, що прості числа, які використовуються які основа системи, повинні мати розмір не менше 650D. Побудова простих чисел таких розмірів складна обчислювальна задача. У працях [19–21] пропонується підхід до побудови простих чисел великої розмірності.

Аналіз сучасних методів і засобів відновлення цілісності інформації. Завадостійке кодування. Найуразливішою інформація буває в процесі її передачі. Це можна пояснити тим, що така міра забезпечення ЦІ, як розмежування доступу знімає багато загроз, але вона неможлива у використанні в каналі зв'язку бездротових ліній. Інформація найбільш вразлива саме на таких ділянках ІКС. Очевидно, що при навмисному впливі на сигнал, котрий передається, забезпечити ЦІ неможливо. Для виправлення помилок, що виникли в результаті природних явищ, технічних збоїв, використовується завадостійке кодування інформації (ЗКІ).

Вивчення ЗКІ почалося практично відразу після виходу в світ праці [22]. Найбільш відомими в нашій країні є дослідження [23–25], де представлені й проаналізовані різні методи ЗКІ. Головною ідеєю виправлення помилок, що виникають у процесі передачі, є введення надмірності в повідомлення, що передається. Чим більше необхідно виправити помилок, тим більшою має бути надмірність.

Нині все більшу популярність завойовує "м'яке" декодування, яке ґрунтується на спільному конструюванні коду й багатьох сигнальних точок.

Така сигнально кодова конструкція забезпечує вищу ефективність і більший енергетичний виграш від кодування, ніж послідовне застосування ЗКІ і модуляції [26].

У працях [27–28] запропоновано та обґрунтовано метод забезпечення ЦІ в системах передачі інформації, що базується на контролі парності в мініблоках та контрольній сумі. Даний метод найбільш ефективний під час роботи з кратними помилками, має високу швидкість відновлення інформації.

Резервування. Даний метод забезпечення ЦІ використовується в основному при передачі і зберіганні інформації. Під час передачі можливий багатократний повтор повідомлення в один напрям або розсилка повідомлень в усі можливі напрями. Даний підхід можна розглядати як один із методів ЗКІ.

При зберіганні ідея резервування досить проста – створення копій отриманих файлів та їх зберігання окремо від первинних документів. Найчастіше такі сховища створюються в географічно рознесених місцях. Як приклад можна розглянути сучасні хмарні технології.

Одним із головних недоліків резервування інформації є підвищення можливості її несанкціонованого зняття, тому що інформація, яка розміщується на зовнішніх пристроях зберігання, є незахищеною.

Антивірусний захист. На відміну від застосування антивірусного захисту при забезпеченні ЦІ за якого антивірусна програма виявляє вірус до моменту зараження, в даному випадку ці засоби виступають як засоби відновлення інформації. Якщо в результаті сканування виявляється файл, пошкоджений вірусом, то в багатьох випадках такі файли відновлюються. Відновлення відбувається шляхом знищення коду віруса, який був поміщений у тіло файлу і на його місце переписується оригінальний код. У деяких випадках файл відновленню не підлягає, і він поміщається в карантин. Відновлення таких файлів можливо тільки за рахунок резервування.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Аналіз, який був представлений в роботі, показує, що в сучасній спільності вчених і практиків немає однозначного тлумачення багатьох термінів. Виходячи з цього, можна зробити висновок про необхідність уніфікованого тлумачення термінів. Це дозволить тісніше спілкуватися представникам різних напрямків.

Модель цілісності і загроз в ІКС дозволяє усвідомити місце ЦІ в сучасних системах. В даний час порушення ЦІ є найбільш небезпечним впливом на всі системи, включаючи і критичні. Для забезпечення ЦІ використовуються як організаційні, так і технічні методи і засоби. Побудова систем ТЗІ, з економічної точки зору, є збитковою. Проте вартість цих систем захисту в багато разів може бути менше, ніж можливі збитки, що можуть бути завдані в результаті атак.

В роботі наведені можливі методи і засоби забезпечення та контролю ЦІ. Серед них можна виділити як добре відомі методи (наприклад, завадостійкого кодування), так і методи, які порівняно рідко використовуються для забезпечення ЦІ (стеганографія). Аналіз, який було проведено, показує різноманітність форм і методів побудови систем забезпечення ЦІ.

Список використаних джерел:

1. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги [Чинний від 2015.12.18]. – Київ: Держспоживстандарт України, 2016. – 22 с.
2. Шеннон К. Работы по теории информации и кибернетике. / К. Шеннон – М. : Изд-во иностранной литературы, 1963. 830 с.
3. Kharchenko V. S. Multiversion Systems: Models, Reliability, Design Technologies // Proceeding of 10th European Conference on Safety and Reliability, Munich, Germany, 13-17 September, 1999, vol. 1. – P. 73–77.
4. ISO/IEC 2382:2015. Information technology. Vocabulary [Електронний ресурс] – Режим доступа: https://www.iso.org/standard/63598.html – 3.01.2018 р.
5. Певнев В. Я. Методы обеспечения целостности информации в инфокоммуникационных системах / В. Я. Певнев // Вісник Національного технічного університету "ХПІ". Серія: Техніка та електрофізика високих напруг. - 2015. - № 51. - С. 74-77.
6. Karlsson J. Routing Security in Ad-hoc Networks / J. Karlsson, L. S. Dooley, G. Pulkkis // Issues in Informing Science and Information Technology. Vol. 9. – 2012. P. 369–383.
7. Luna, J. Leveraging the Potential of Cloud Security Service-Level Agreements through Standards [Text] / J. Luna, N. Suri, M. Iorga and A. Karmel // IEEE Cloud Computing. – 2015. – Vol. 2, Issue 3. – P. 32–40. doi: 10.1109/mcc.2015.52
8. Juliadotter, N. Cloud Attack and Risk Assessment Taxonomy [Text] / N. Juliadotter, K. Choo // IEEE Cloud Computing. – 2015. – Vol. 1, Issue 2. – P. 14–20. doi: 10.1109/mcc.2015.2
9. Комаров М. Ю. Аналіз і дослідження загроз для захищеного вузла інтернет доступу / М. Ю. Комаров, С. Ф. Гончар // Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія : Технічні науки. – 2018. – Т. 29 (68), № 4 (1). – С. 165–168.
10. Цуранов М. В., Струков В. М., Пєвнєв В. Я. Методи та засоби боротьби з правопорушеннями в інформаційної сфері : навч посібник. / Цуранов М. В., Струков В. М., Пєвнєв В. Я. – Харків : ХНУВС, 2015. – 256 с.
11. Проскурин В. Г., Крутов С. В., Мацкевич И. В. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных система : учеб.пособие для вузов / Проскурин В. Г., Крутов С. В., Мацкевич И. В. – М. : Радио и связь. 2000. – 168 с

12. Захист інформації. Технічний захист інформації. Терміни і визначення: ДСТУ 3396.2-97. – [Чинний від 1998.01.01]. – К. : Держстандарт України, 1998. – 20 с.

13. Кравченко В. И. Оружие на нетрадиционных принципах: Электромагнитное оружие / В. И. Кравченко – Харків : НТУ "ХПИ", 2009. – 266 с.

14. Смирнов М., Ватолин Д., Ратушняк А., Юкин В. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео./ М. Смирнов, Д. Ватолин, А. Ратушняк, В. Юкин. – М.: Диалог-МИФИ. 2002. – 384 с.

15. Певнев В. Я. Построение оптимальных кодовых таблиц / В. Я. Певнев, М. В. Цуранов // Системи обробки інформації. – 2012. – № 4(102). – С. 56–59.

16. Tsuranov M. The Method of Data Integrity Assurance for Increasing IoT Infrastructure Security / V. Pevnev, Y. Novakov, M. Tsuranov, V. Kharchenko// InfoTech-2017: proc. of the 31 th IC on Information Technologies (September 20-21, 2017, Sofia). Sofia: 2017. – P. 27–36

17. Oleshchenko V. Development of digital steganography techniques for copyright protection, based on the watermark / V. Oleshchenko, V. Pevnev // Сучасні інформаційні системи. – 2017. – Т. 1, № 1. – С. 57–60.

18. Про електронні довірчі послуги: Закон України від 05.10.2017 №2155-VIII. [Електронний ресурс]. – Режим доступа : https://zakon.rada.gov.ua/laws/show/2155-19/ed20171005 – 3.01.2018 р.

19. Певнев В. Я. Методика построения псевдопростых чисел / В. Я. Певнев // Системи обробки інформації. – 2016. – № 3(140). – С. 30–34.

20. Генератор простых чисел. Кафедра систем інформації: Зб. наукових праць / Певнев В. Я. – Харків : ТОВ "Щедра садиба плюс", 2014. – С. 140–146.

21. Pevnev V. Pseudoprime Numbers: Basic Concepts and the Problem of Security / V. Pevnev // ICTERI Applications: Integration, Harmonization and Knowledge Transfer: proc. 13th Int. Conf. ICTERI 2017 (May 15-18, 2017, Kyiv). CEUR-WS.org, online-c.583-593

23. Шеннон К. Е. Математическая теория связи. Работы по теории информации и кибернетики / К. Е. Шеннон //– М.: ИЛ. 1963. – 476 с.

24. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки / У. Питерсон, Э. Уэлдон // – М. : Мир, 1976. – 594с.

25. Галлагер Р. Теория информации и надежная связь / Р. Галлагер // – М. : Сов. радио, 1974. – 568 с.

26. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / Р. Морелос-Сарагоса // – М. : Техносфера. 2005. – 320 с.

27. Пєвнєв В. Я. та ін. Спосіб відновлення інформації при обміні даними у телекомунікаційних системах. – Патент на корисну модель № 26778, МПК HO4L 12/00, заяв. 23.04.07, опубл. 10.10.2007, Бюл. No 16.

28. Пєвнєв В. Я. Теоретичне обґрунтування методу відновлення повідомлення, прийнятого з помилками / В. Я. Пєвнєв, М. В. Цуранов // Системи обробки інформації. – 2013. – № 2 (109). – С. 194–196.

References:

1. DSTU ISO/IEC 27001:2015 Metody zakhystu systemy upravlinnya informatsiynoyu bezpekoyu. [Chynnyy vid 2015-12-18]. Vyd. ofits. Kyyiv, DP "UkrNDNTS" 2016. 22 p.

2. Shennon K. Raboty po teorii informatsii i kibernetike. M.: Izd-vo inostrannoy literatury, 1963. 830 p.

3. . Kharchenko V. S. Multiversion systems: Models, Reliability, Design Technologies: Proc. 10th European Conference of Safety and Reliability. Munich, 1999. P. 73–77.

4. ISO/IEC 2382:2015, Information technology – Vocabulary https://www.iso.org/standard/63598.html

5. Pevnev V. Ya. Metody obespechenyya tselostnosty ynformatsyy v ynfokommunykatsyonnykh systemakh. Visnyk NTU "KHPI". Seriya: Tekhnika ta elektrofizika vysokykh napruh. Kharkiv, 2015. № 51. P. 74–77

6. Karlsson J., Dooley L. S., Pulkkis G. Routing Security in Ad-hoc Networks. IISIT in Informing Science and Information Technology. 2012. Vol. 9. P. 369–383

7. Luna J., Suri N., Iorga M., Karmel A. Leveraging the Potential of Cloud Security Service-Level Agreements through Standards IEEE Cloud Computing. 2015. Vol. 2. Issue 3. P. 32–40.

8. Juliadotter N., Choo K. Cloud Attack and Risk Assessment Taxonomy.IEEE Cloud Computing. 2015. Vol. 1, Issue 2. P. 14–20.

9. Komarov M. Yu., Honchar S. F Analiz i doslidzhennya zahroz dlya zakhyshchenoho vuzla Internet dostupa. Informatyka, obchyslyuval′na tekhnika ta avtomatyzatsiya. Tom 29 (68). CH. 1 № 4. 2018. P. 165–168.

10. Tsuranov M. V., Strukov V. M., Pevnev V. Ya.. Metody ta zasoby borot′by z pravoporushennyamy v informatsiynoyi sferi: navch posibnyk. Kharkiv: KHNUVS, 2015. – 256 p.

11. Proskurin V. G., Krutov S. V., Matskevich I. V. Programmno-apparatnyye sredstva obespecheniya informatsionnoy bezopasnosti. Zashchita v operatsionnykh sistemakh: Ucheb.posobiye dlya vuzov M.:Radio i svyaz'. 2000. 168 p.

12. DSTU 3396.2-97. Zakhist ínformatsíĭ. Tekhníchniy zakhist ínformatsíĭ. Termíni ta viznachennya. [Chynnyy vid 1998.01.01]. Vyd. ofits. Kyyiv, DERZHSTANDART UKRAYINY 1997. 22 p.

13. Kravchenko V. I. Oruzhiye na netraditsionnykh printsipakh: Elektromagnitnoye oruzhiye. Kharkív: NTU "KHPI", 2009. 266 p.

14. Smirnov M., Vatolin D., Ratushnyak A., Yukin V. Metody szhatiya dannykh. Ustroystvo arkhivatorov, szhatiye izobrazheniy i video. M. : Dialog-MIFI. 2002. P. 384.

15. Pevnev V., Tsuranov M. The construction of the optimal code tables. Systemy obrobky informatsiyi. 2012. № 3 (108), p. 27–30.

16. Pevnev V., Novakov Y., Tsuranov M, Kharchenko V. The Method of Data Integrity Assurance for Increasing IoT Infrastructure Security. InfoTech-2017: proceedings of the 31 th IC on Information Technologies. Sofia, 2017. P. 27–36.

17. Oleshchenko V, Pevnev V. Development of digital steganography techniques for copyright protection, based on the watermark. Advanced information systems. 2017. № 1. P. 57–60.

18. Pro elektronni dovirchi posluhy: Zakon Ukrayiny vid 05.10.2017 №2155-VIII. Vidomosti Verkhovnoyi Rady Ukrayiny. 2017 r., № 45. P. 400

19. Pevnev V. Ya. Metodyka postroenyya psevdoprostykh chysel Systemy obrobky informatsiyi. 2016. № 140 (3). P. 30–34.

20. Pevnev V. Ya. Henerator prostykh chysel. Kafedra system ynformatsyy: sb. nauch. tr. Khar′kov, 2014. P. 140–146.

21. Pevnev V. Pseudoprime Numbers: Basic Concepts and the Problem of Security. ICTERI Applications: Integration, Harmonization and Knowledge Transfer: proc. 13th Int. Conf. ICTERI 2017 (Kyiv, May 15–18, 2017), CEUR-WS.org, online – C. 583–593

22. Matskevich I. V. M. :Radio i svyaz'. 2000. P.168

23. Shennon K. Ye. Matematicheskaya teoriya svyazi. Raboty po teorii informatsii i kibernetiki. M.: IL. 1963. P.476

24. Piterson U., Ueldon E. Kody, ispravlyayushchiye oshibki. M. : Mir, 1976. P.594

25. Gallager, R. Teoriya informatsii i nadezhnaya svyaz’. M. : Sov. radio, 1974. P. 568

26. Morelos-Saragosa R. Iskusstvo pomekhoustoychivogo kodirovaniya. Metody,algoritmy, primeneniyeM.: Tekhnosfera. 2005. P.320.

27. Pevnev V.YA. Sposíb vídnovlennya ínformatsíЇ pri obmíní danimi u telekomunікatsíynikh sistemakh / Pêvnêv V. YA. i dr. // D.p. № 26778. Byul., 2007. – № 16.

28. Pevnev V. Ya., Tsuranov M. V. Teoretichne obg̀runtuvannya metodu vídnovlennya povídomlennya, priynyatogo z pomilkami. Sistemi obrobki ínformatsíЇ . 2013. № 2 (109). P. 194–196.

DOI: https://doi.org/10.32836/2521-6643-2018.2-56.7
UDC: 621.311 : 621.317.613 : 621.316.935.5

V. A. Pobihailo, Associate Professor, PhD. tehn. Sciences, Associate Professor of Power Supply National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"

SHORT CIRCUIT CURRENT LIMIT CONTROL

The scientific and practical relevance of improving the functioning of credit limit short – circuit (short circuit), formulated the goal and objectives of research. As a solution proposed research and the way to manage complex limitation of short circuit currents in electricity supply production systems under the reactor – controlled shunt. The algorithm of the system reactor – controlled shunt. For the first time the schemes cause – effect relationships occurrence of short – circuit currents – Figure Ysikavy according to ISO 9004.

Key words: *short-circuit current; reactor; Ishikawa; IS0 9004 performance; limitations; fuse; controlled shunt; reduced losses.*

У зв'язку зі зростанням рівнів та кількості струмів короткого замикання, існують проблеми, пов'язані з підвищенням ефективності методів та засобів обмеження струмів короткого замикання, які є актуальними у контексті розвитку енергетичного сектору України. Проблеми ускладнюються тим, що в системах електропостачання виробничих систем є значна кількість устаткування, яку необхідно замінити за умовами короткого замикання і устаткування з відпрацьованим терміном служби або значною зношеністю, а промисловість не забезпечує потреби виробничих систем в електроустаткуванні. Тому питання про спосіб вирішення цих проблем, повинне вирішуватися на основі техніко-економічного аналізу. Ключовим аспектом тут є інтенсифікація темпів зменшення витрат електроенергії у виробничих системах електропостачання, що може бути досягнуто шляхом впровадження нових або з підвищеною ефективністю існуючих методів та

засобів обмеження струмів короткого замикання. Присутня наукова та практична актуальність вдосконалення функціонування засобів обмеження струмів короткого замикання, сформульована мета та завдання наукового дослідження. В якості рішення уперше запропоновано та досліджено спосіб управління обмеження струмів короткого замикання у виробничих системах електропостачання з використанням струмообмежуючого реактора з керованим шунтом. Розроблено алгоритм дії системи "реактор - керований шунт". Вперше побудовано схему причинно-наслідкових зв'язків виникнення струмів КЗ у виробничих системах електропостачання - використовуючи діаграму "аналізу кореневих причин" Ісікава, відповідно до ISO 9004. Запропонований спосіб обмеження струмів КЗ в виробничих системах електропостачання і обладнання для його реалізації за схемою "реактор – керований шунт", яка повністю компенсує всі недоліки, що виникають при обмеженні струмів КЗ в виробничих системах електропостачання за схемою обмеження "реактор - нерегульований шунт". Слід також зазначити, що обмеження струмів КЗ в виробничих системах електропостачання за схемою "реактор - керований шунт" має певні суттєві переваги перед іншими існуючими на сьогоднішній день засобами обмеження струмів КЗ, а отримані нові науково-обгрунтовані теоретичні і практичні результати, що дають підстави для подальшого розвитку нових методів і засобів обмеження струмів КЗ в системах електропостачання виробничих систем з урахуванням усіх особливостей, а результати проведення повномасштабного експерименту з незначною похибкою підтвердили математичну модель системи "реактор - не керований шунт".

Ключові слова: *струм короткого замикання; реактор; Ісікава; IS0 9004; ефективність; обмеження; запобіжник; керований шунт; зниження втрат.*

1. Introduction

Amid growing levels of short-circuit currents, issues related to increasing the efficiency of methods and means of limiting short-circuit currents are central in the context of development of Ukraine's energy sector. A key factor here is intensifying pace of decreasing electricity losses in power supply production systems (PSPS), which could be achieved through implementation of new and improved efficiency of existing methods and means of limiting short circuit currents.

Studies indicate that addressing the issue of reducing electricity losses in the absence of short circuit currents in the PSPS calls for new approaches. This is due to an ongoing increase in the efficiency of the means and methods of limiting short circuit currents used today, as well as broad application of fundamentally new means and methods of limiting short circuit currents – devices controlling the

means of limiting short circuit currents, built on decision theory [1].

The analysis of existing means and methods of limiting short circuit currents shows that, by increasing the efficiency of short circuit currents limiting devices based on decision theory, it is possible to reduce the costs of maintenance of short circuit current limiting equipment through reduced losses in the absence of short circuit currents, i.e. deliver actual energy saving while limiting short circuit currents in the PSPS [2].

To reduce the impact of short circuit (s/c) currents on the power supply system, various means and methods are developed and applied, allowing limiting magnitude, as well as their duration.

2. Aim and objectives of the study

The study aims to increase the efficiency of the means of short circuit current limiting devices in the production systems by optimizing their operation modes.

To achieve this goal, the following objectives are addressed:

- analysis of methods and means of limiting SC currents in the PSPS;
- developing a controlled shunt reactor suite based on decision theory;
- building the algorithm of controlled shunt reactor suite operation based on the decision theory.

3. Solution to the task at hand

During operation of the PSPS of industrial facilities, short circuits occur frequently, leading to disturbances in the normal operation of electrical installations and possible disruption of electricity supply to consumers. Based on the main cause and effect relationships of the occurrence of short circuit currents, we are able to build a scheme of cause and effect relationships of the occurrence of short circuit currents (Ishikawa iteration scheme), according to ISO 9004 presented in Fig. 1.

Short circuits in electrical installations have the following consequences: damage to electrical equipment, wear and tear on circuit breakers, lowered voltage in the grid, fires and other damages. In its physical nature, the SC current is a continuous random process. The totality of characteristics describing the probable nature of the various parameters and conditions of short circuits are the probable characteristics of short circuits in an electrical installation.

In order to reduce the impact of short circuit currents on electrical equipment, various methods and means of limiting short circuit currents have been proposed and used [2, 3]. Taking into account the specific character of PSPS development, as well as technical and economic characteristics, fundamentally new means of limiting the short circuit current are being developed and investigated, allowing to limit the magnitude of the short circuit current as well as its duration.

The benefits and disadvantages of the existing methods and means of limiting the short circuit current are also being analysed.

As we know, the most common means of limiting short circuit currents in 6-10 kV grids in Ukraine are unregulated single and dual linear concrete reactors. They differ in their structural design, as well as technical and economic characteristics and parameters. GOST 18624-73 offers a general classification of reactors for different purposes.

Along with the existing methods and means of limiting the short circuit currents decision theory also has its application. Let us consider a decision-making method that can be based on pattern recognition theory, whose application allows us to recognize the normal, pre-emergency and emergency operation modes of power supply of production systems.

To resolve the problem of increasing the efficiency of the short circuit current limiting devices, we suggest a suite and a method of controlling the limitation of the short circuit currents in the PSPS according to the controlled shunt reactor scheme, whereby the inductive resistance is switched on and off automatically in the event of short circuit current [4].

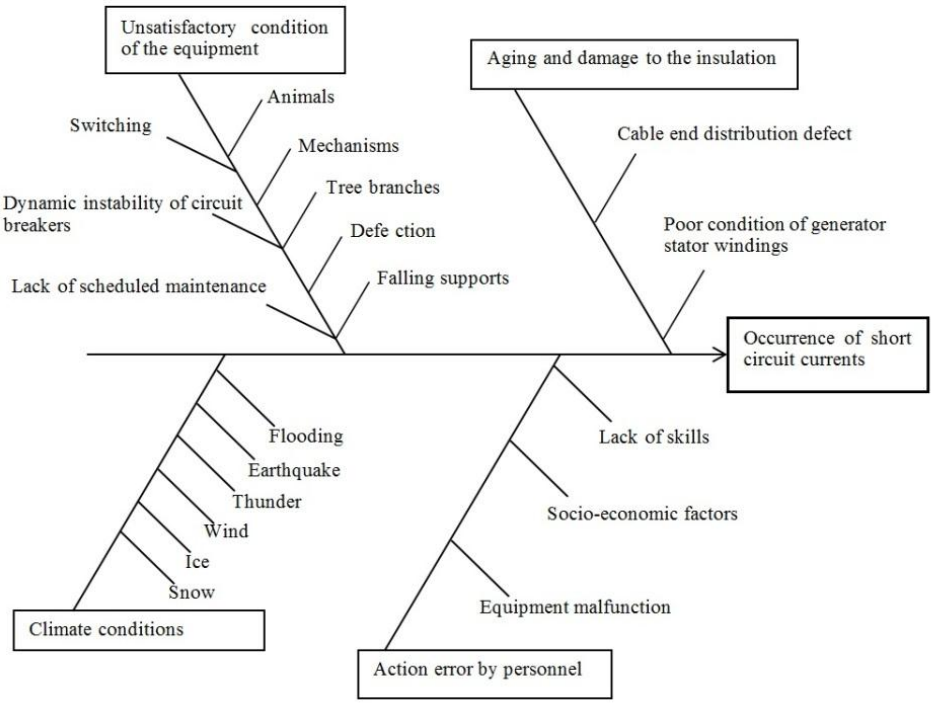


Fig. 1. Scheme of cause and effect relationships of short circuit currents.

The device's operation principle is to compare the measured current with the reference value and to form a control signal that affects the inductive resistance.

Fig. 2 shows a structural diagram of a short – circuit current limiting device. A current-limiting resistance (current – limiting reactor) 2, shunted with a high – speed switching element *3*, is included in the section of the electric system *1*. A current measuring unit *4* connected to the analyzer *5* is connected to the electric system, whose control output of which through the device *6 is* connected to the control input of the high – speed switching element *3*.

Under normal conditions, device *3* (shunt inductance) passes current and have a parallel connection of the inductance and the switching element with resistance lower than the inductance resistance.

In emergency mode, information from the current measuring unit *4 is* fed to the analyzer *5*. In case of the current change $\Delta I_p \geq \delta I$, the control point mode is emergency mode, and the device *6* generates a control signal that turns off the switching unit *3*, while the inductive resistance *2* limits the short – circuit current accordingly.

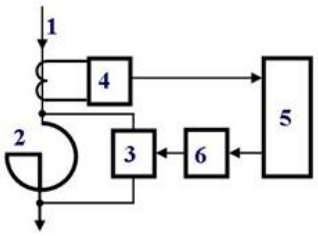


Fig. 2. Shows a structural diagram of a short – circuit current limiting device.

Periodically in time segments $\Delta t=T/N$, where N is the number of control points (Fig. 3), the value of the actual current of the electric network I_{ca} is measured at control points over the monitoring time interval T. Further the discrepancy ΔI_t between the actual I_F and the set (reference) current I_{cr} for a controlled time interval T is determined, i.e.

$$\Delta I_{т} = \sqrt{\sum_{t=1}^{n} (I_F - I_{cr})^2},$$

where I_{cr} is a value that accounts for the conditions for starting the electromotive load.

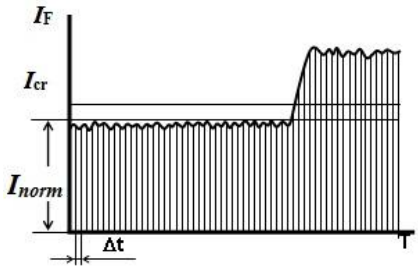


Fig. 3. Schedule current of the electric network.

If $\Delta I_t \geq \delta I$ (where the value δI, is the setting determined by the operating mode), a control action is formed that disconnects the switching unit. The algorithm limiting the s/c current is shown in Fig. 4.

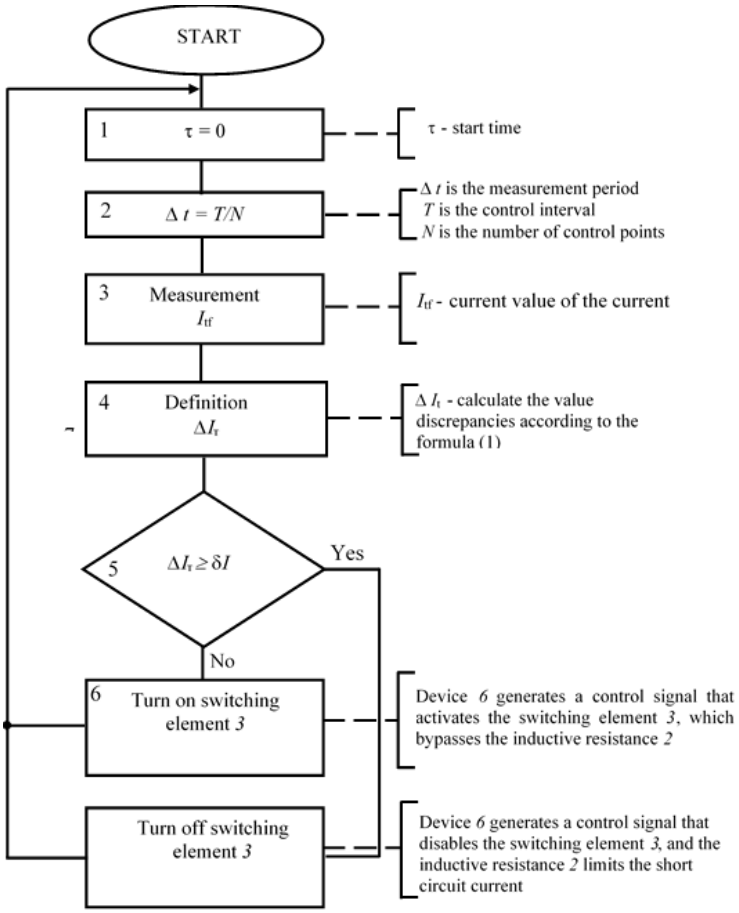


Fig. 4. Algorithm of the analyzer operation.

The proposed method of limiting short circuit currents in the PSPS and the suite for its implementation under the controlled shunt reactor scheme fully compensates for all the disadvantages that occur when limiting short circuit currents in the PSPS under the unregulated shunt reactor scheme [3].

It should also be noted that the limitation of short circuit currents in the PSPS under the controlled shunt reactor scheme has certain advantages over other means of limiting short circuit currents, in particular:

- room for further development and improvement of this system of limitation of short circuit currents;
- performance and reliability;
- compliance with energy-saving requirements;
- ability of collecting and proper use of currents statistics in the PSPS.

Economic rationale for the proposed solution

The economic effect of introducing the proposed automatic s/c current control device is determined in accordance with the following methodology.

After installing the device on a 6 – 35 kV network, the total active power losses in three – phase groups of reactors should decrease as follows [2]:

$$\Delta P_{Э\Sigma} = (1-1/K_2)\sum_{i=1}^{n} 3\Delta P_{Hi}(I_{Mi}^2 / I_{Hi}^2),\ \text{kW},$$

where $K_2 = R_p(1+K_1)^2/(X_p K_1)$; $K_1 = R_{\text{device}} / X_p$; $I_м = I_{\text{device}} + I_p$; $I_м$ is over current; P_H is nominal losses in the reactor; X_{p} is reactance of the reactor; R_{p} is the resistance of the reactor; R_{device} is the resistance of the s/c current control device; I_{p} is the current going through the reactor; I_{device} is current going through the s/c current control device.

Reactive losses at $R_{\text{device}} \le X_{\text{p}}$ are almost completely eliminated and the total technical effect will be

$$\Delta Q_{E\Sigma} = \sum_{i=1}^{n} 3I_{мi}^2 X_{\text{p}i} \cdot 10^{-3}, \text{kVAr}.$$

Annual energy savings are mostly determined based on the “losses time”:

$$\tau_a = (0.124\ T_{\text{ma}}/10^4)^2\ 8760, \text{ h/year};$$
$$\tau_{\text{p}} = (0.124 \cdot T_{\text{mr}}/10^4)^2\ 8760, \text{ h/year};$$

where T_{ma}, T_{mr} are the maximum number of using active and reactive loads, respectively.

In this case, annual energy savings from installing a short – circuit current control device will be (in kW·h and kVAr·h, respectively):

$$\Delta W_{S\Sigma} = \Delta P_{S\Sigma}\tau_a$$
$$\Delta V_{S\Sigma} = \Delta Q_{S\Sigma}\tau_p.$$

In accordance with the single – rate tariffs currently used in Ukraine, only the actual energy consumption is billed at the rates established for classes 1 and 2 of industrial consumers with connected capacity of $S_c \geq 750$kV·A. Based on the tariff structure, direct savings in cost terms for a short – circuit current limiting control device installed in reacted lines can be presented as

$$S = (\alpha \Delta W_{S\Sigma} + \gamma \Delta V_{S\Sigma}) 10^{-2} = (\alpha \Delta P_{S\Sigma} \tau_a + \gamma \Delta Q_{S\Sigma} \tau_p) 10^{-2},$$

where α_{min}, α_{max} are active energy coefficients; γ_{min}, γ_{max} are reactive energy coefficients.

4. Conclusions

Existing devices and methods for limiting the short – circuit currents have a number of significant drawbacks:

– single use of work, requiring fuse replacement after burnout;

– electric arc at the time of burnout, which is a conductor of short – circuit currents;

– insufficient operational reliability;

– unstable current – time characteristics;

– limited application in terms of rated currents and rated voltages;

– no option of external control, such as by automatic reclosers of the protected circuit.

The device for short – circuit current limitation control designed by the authors, where the inductance is switched on and off automatically when a short – circuit current occurs, has none of the above drawbacks.

References:

1. Pobigaylo, V.A. Tool strumoobmezhennya as one of the effective ways of energy use / / Pobigaylo V.A., Rosen V.P. Proceedings of the National University "Lviv Polytechnic". Electricity and electromechanical systems. – 2001. – № 421. – S. 181–188.

2. Pobigaylo V. A. Analysis approaches k Decision Problems restrictions currents in short zamikanyya proyzvodstvennih and энerhetycheskyh systems / Rosen V. P., Taradai V. I., Nesen L. I., Pobigaylo V. A. IEE "KPI". – Kiev : 1999. – 18 p. – Eng. – Dep. HNTB of Ukraine on 26.07.99, № 225 Uk99 / / anoth. in the same. VINITI RAS № 10 (333), 1999.

3. Pobigaylo V. A. A mathematical model of the limiting current devices under the "reactor – fuse" / Rosen V. P., Solovey O. I., Momot D. E., Pobigaylo V. A. Proceedings of the National Technical University of Ukraine "KPI". A series of mining. – 2000 – № 4. – S. 82–90.

4. Pobigaylo V. A. The way to limit short-circuit currents and device for its implementation // Rosen V. P., Kalynchyk V. P., Momot D. E., Pobigaylo V. A. Patent of Ukraine № 2002021620 from 15.11.2002.

Шановні автори!

Просимо враховувати такі вимоги до рукописів статей і порядку їх подання до друку:

1. Приймаються роботи, **написані українською, російською, англійською мовами,** обсягом 0,5–1 авт. арк.

2. Рукопис статті повинен мати такі елементи:

– на початку статті **англійською мовою:** прізвище ініціали автора, назва статті, адресні дані авторів (назва установи, закладу, відомча належність, адреса організації, місто, країна), розширена англомовна анотація (від 1800 знаків), ключові слова, пристатейні списки використаних джерел у романському алфавіті (латиницею);

– **прізвище та ініціали автора, науковий ступінь, посада (укр. мовою);**

– **назва статті (українською мовою);**

– **УДК;**

– **анотація українською мовою** (3–5рядків);

– **основний текст статті;**

– **список використаних джерел.**

3. Основний **текст статті** складається з таких структурних елементів:

Ключові слова (4–5 слів).

Постановка проблеми.

Аналіз останніх досліджень і публікацій. Мета статті.

Виклад основного матеріалу.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі.

Список використаних джерел оформлюється відповідно до ДСТУ 8302:2015. Зазначені елементи виділяються в рукописі **напівжирним шрифтом.**

4. Текст статті має бути набраний в текстовому редакторі Microsoft Word. Поля з усіх сторін – 20 мм. Шрифт – Times New Roman 14 з інтервалом 1,5.

Посилання на літературу здійснюються безпосередньо в тексті. У квадратних дужках зазначається порядковий номер використаного джерела в порядку згадування, а через кому – конкретна сторінка.

5. До редакції подаються:

– **паперовий варіант статті за підписом автора;**

– **електронний варіант статті;**

– **завірена рецензія доктора або кандидата наук відповідного профілю (крім випадків, коли автор сам має науковий ступінь доктора наук);**

– **довідка** про автора українською мовою (прізвище, ім'я, по батькові повністю, організація, посада, адреса, науковий ступінь, вчене звання, контактні телефони, електронна адреса).