ISSN 2521-6643

Системи та технології

№ 1 (57) 2019

Системи та технології

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

№ 1 (57)

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
2019

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 № 11 від 25.03.2019 р.)

DOI: https://doi.org/10.32836/2521-6643-2019-1-57
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 № 61.

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 18.06.19. 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/10.32836/2521-6643-2019-1-57-1
УДК 621.039:623.746

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

МІНІМІЗАЦІЯ ЧАСУ ПОЧАТКУ ВИКОНАННЯ ФЛОТОМ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ЗАВДАННЯ З РАДІАЦІЙНОГО МОНІТОРИНГУ В НОВІЙ ЗОНІ ВІДПОВІДАЛЬНОСТІ

З*апропоновано підхід щодо мінімізації часу очікування початку виконання флотом безпілотних літальних апаратів (далі – БПЛА) завдання з радіаційного моніторингу в новій зоні відповідальності. Наведено приклад реалізації підходу для флоту, що складається з п'яти БПЛА "Фурія" з електричним двигуном і виконує завдання збирання та передачі інформації до кризового центру в п'яти зонах відповідальності (один БПЛА виконує завдання у своїй власній зоні) в межах тридцятикілометрової зони Запорізької АЕС. Розглянуто шість можливих нових зон відповідальності та визначено мінімальний час очікування початку виконання БПЛА флоту завдання у кожній із цих зон.*

Ключові слова: *безпілотний літальний апарат; атомна електростанція; зона відповідальності; радіаційний моніторинг; стартова позиція; проміжна посадка; модель оптимізації.*

Предложен подход к минимизации времени ожидания начала выполнения флотом беспилотных летательных аппаратов (далее – БПЛА) задачи по радиационному мониторингу в новой зоне ответственности. Приведен пример реализации подхода для флота, состоящего из пяти БПЛА "Фурия" с электрическим двигателем и выполняет задание по сбору и передаче информации в кризисный центр в пяти зонах ответственности (один БПЛА выполняет задачи в своей собственной зоне) в пределах тридцатикилометровой зоны Запорожской АЭС. Рассмотрены шесть возможных новых зон ответственности и определено минимальное время ожидания начала выполнения задачи БПЛА флота в каждой из этих зон.

Ключевые слова: *беспилотный летательный аппарат; атомная электростанция; зона ответственности; радиационный мониторинг; стартовая позиция; промежуточная посадка; модель оптимизации.*

The analysis of possible applications of unmanned aerial vehicles for performing radiation monitoring missions was carried out. This paper proposes an approach to minimization of the waiting time to start performing a radiation monitoring mission via a fleet of unmanned aerial vehicles (hereafter UAVs) in the new zone of responsibility. The approach includes the following steps: distribution of UAVs in the zones of responsibility and setting the time for performing a mission for each UAV; determination of the starting position location where UAVs battery can be replaced; defining the new zone of responsibility and time for performing a mission in the zone; construction of an algorithm for calculating parameters necessary for solving the optimization problem; formulation of the optimization problem and constraints. Parameters to be calculated: the UAV flight time from the current mission zone to: a) starting position; b) a new zone (with making the intermediate landing and without making one); a flight time from the new zone to the starting position; the UAV battery life required for performing the mission in the new zone; the waiting time to start performing the mission in the new zone and the current battery life for the UAV at the start of its mission in the new zone for the following cases: a) the UAV reaches the new zone with making the intermediate landing, b) the UAV reaches the new zone without making one. An example of the proposed approach implementation for a fleet, consisting of five Ukrainian electric UAVs "Furiia" and performing missions in five zones of responsibility (one UAV performs a mission in one zone) within the Zaporizhzhia NPP thirty-kilometre radius zone is given. Six possible new zones are considered and the waiting time to start performing a mission in each of these zones is given. It has been get that UAV 5, UAV 4 and UAV 2 can be assigned to three zones, two zones and one zone, respectively. UAV 1 and UAV 2 can not be used in any new zone. Note that the UAV 5 can be used once without making the intermediate landing at the starting position for its battery replacement and twice with making the intermediate landing. Further studies should take into account the following cases: the fleet consists of various UAVs, two or more UAVs should be assigned to the new zone.

Key words: *unmanned aerial vehicle; nuclear power plant; zone of responsibility; radiation monitoring; starting position; intermediate landing; optimization model.*

Постановка проблеми. Після застосування під час аварії на японській атомній електростанції (далі – АЕС) "Фукусіма-1" в Японії безпілотного літального апарату літакового типу Global Hawk для отримання у режимі реального часу зображення руйнувань інфраструктури станції БПЛА стали все частіше використовувати для підвищення ефективності застосування системи радіаційного моніторингу [1; 2] (наприклад, автоматизованої системи

контролю радіаційної обстановки (АСКРО) [3]). Залежно від типу бортового обладнання БПЛА можуть залучатися для виконання таких завдань:

– дослідження районів радіаційних аварій, виявлення джерел радіоактивного забруднення та встановлення особливостей руху радіоактивних хмар;

– забезпечення складання карт радіоактивного забруднення;

– відбір проб ґрунту для встановлення ступеня його радіоактивного забруднення;

– пошук постраждалих унаслідок аварії на АЕС та забезпечення їх медикаментами, засобами захисту і продовольством;

– створення бездротового каналу передачі даних від датчиків стаціонарних постів контролю АСКРО до кризового центру;

– дублювання стаціонарних постів контролю АСКРО в частині вимірювання потужності дози гамма-випромінювання;

– дослідження об'єктів ядерної енергетики на предмет відповідності стандартам з ядерної безпеки;

– періодичний контроль радіаційної обстановки у 30-кілометровій зоні.

Переваги використання БПЛА під час радіаційного моніторингу порівнянно з пілотованими літаками такі: низька вартість, більша маневреність, можливість керування з незабрудненої місцевості, зліт і посадка в обраних для користувача місцях та у визначені користувачем проміжки часу.

Аналіз останніх досліджень і публікацій. Останні дослідження показують, що найбільш ефективно використовувати флот БПЛА під час радіаційного моніторингу не автономно, а як рухому складову інтегрованої системи моніторингу аварій на АЕС [4–11].

Так, наприклад, тематична група з радіологічних і ядерних загроз критичній інфраструктурі розробила різні сценарії одночасного застосування флотів БПЛА і груп наземних роботів під час роботи у складі системи радіаційного моніторингу [4].

Детальний аналіз різних концепцій побудови бортового обладнання БПЛА, що відповідає за виконання завдань радіаційного моніторингу, а також перелік різних сценаріїв вимірювання потужності дози гамма-випромінювання залежно від специфіки місцевості та розміщеної на ній інфраструктури містяться у [5].

Мобільна система моніторингу навколишнього середовища АЕС з використанням систем відеоспостереження та вимірювання потужності експозиційної дози з прив'язкою до просторової системи координат на базі безпілотного авіаційного комплексу представлена у [6; 7].

Концепція побудови системи післяаварійного моніторингу аварій на АЕС на основі БПЛА, яка передбачає підвищення надійності та стійкості наявної системи моніторингу за рахунок розміщення її мережі зв'язку на базі флоту БПЛА різного типу (БПЛА-датчики, БПЛА-ретранслятори, БПЛА-спостерігачі (оснащені відеокамерою), наведена у [8–10]. У подальшому ця система була вдосконалена за рахунок реалізації у ній технології Інтернету – дронів [11].

Однак, розглядаючи різні концепції побудови систем моніторингу на основі БПЛА, автори часто залишають за рамками досліджень питання особливостей застосування БПЛА під час зміни сценаріїв розвитку радіаційної аварії. Такі зміни можуть потребувати перерозподілу БПЛА флоту після появи нових зон відповідальності. У таких випадках важливо визначити БПЛА, що якнайшвидше зможе почати виконання завдання в новій зоні відповідальності після завершення поточного завдання [12; 13].

Мета статті – розробка підходу до мінімізації часу очікування початку виконання флотом БПЛА завдання в новій зоні відповідальності під час радіаційного моніторингу.

Виклад основного матеріалу. Розглянемо флот БПЛА, в якому кожний БПЛА i ($i=\overline{1,n}$) виконує завдання з радіаційного моніторингу у своїй зоні відповідальності Z_i. В певний момент часу флот БПЛА може отримати заявку на виконання завдання у новій зоні відповідальності Z_{n+1}.

Оскільки флот не має вільних БПЛА, відправлення будь-якого БПЛА i у нову зону відповідальності Z_{n+1} можливе тільки після завершення виконання ним свого поточного завдання у зоні Z_i.

Задача: мінімізувати час очікування початку виконання флотом завдання у новій зоні відповідальності τ_{n+1}^{w}.

Оберемо такі обмеження та допущення:

– БПЛА флоту є ідентичними;

– виконання завдання у зоні Z_{n+1} потребує залучення одного БПЛА;

– БПЛА може бути залучений для виконання завдання у зоні Z_{n+1} тільки після завершення виконання ним завдання у поточній зоні відповідальності;

– БПЛА після виконання завдання у зоні Z_{n+1} повинен повернутися на стартову позицію;

– БПЛА може дістатися зони Z_{n+1} або з проміжною посадкою на стартовій позиції для заміни батареї (ресурсу батареї недостатньо для виконання

завдання у зоні Z_{n+1} та повернення на стартову позицію), або без такої посадки (ресурсу батареї достатньо для виконання завдання у зоні Z_{n+1} та повернення на стартову позицію).

Уведемо такі параметри:

X_i (м), Y_i (м) – географічні координати Гауса–Крюгера центра зони Z_i;

X_{n+1} (м), Y_{n+1} (м) – географічні координати Гауса–Крюгера центра зони Z_{n+1};

X_{SP} (м), Y_{SP} (м) – географічні координати Гауса–Крюгера центра стартової позиції;

v_{cr} – крейсерська швидкість БПЛА (км/год);

τ_i – час, який потребує БПЛА *i* для завершення виконання свого завдання в зоні Z_i (хв);

τ_{n+1} – час, необхідний для виконання завдання у зоні Z_{n+1}(хв);

τ_i^{cbl} – часовий ресурс батареї БПЛА *i* в момент отримання заявки на виконання завдання в зоні Z_i (хв);

τ_{rl} – час, необхідний для заміни батареї на стартовій позиції (хв);

τ_{bl} – часовий ресурс нової батареї (хв).

Алгоритм розрахунку показників, необхідних для формулювання оптимізаційної задачі (мінімізація часу очікування початку виконання флотом завдань у новій зоні відповідальності), включає такі кроки.

1. Розрахунок часу польоту БПЛА із зони Z_i до зони Z_{n+1} без проміжної посадки на стартовій позиції для заміни батареї:

$$T_{i,n+1} = \frac{6\sqrt{(X_i - X_{n+1})^2 + (Y_i - Y_{n+1})^2}}{100 v_{cr}} \text{ (хв).} \quad (1)$$

2. Розрахунок часу польоту БПЛА із зони Z_{n+1} до стартової позиції:

$$T_{n+1,SP} = \frac{6\sqrt{(X_{n+1} - X_{SP})^2 + (Y_{n+1} - Y_{SP})^2}}{100 v_{cr}} \text{ (хв).} \quad (2)$$

3. Розрахунок часу польоту БПЛА із зони Z_i до стартової позиції:

$$T_{i,SP} = \frac{6\sqrt{(X_i - X_{SP})^2 + (Y_i - Y_{SP})^2}}{100 v_{cr}} \text{(хв)}. \quad (3)$$

4. Розрахунок часу польоту БПЛА із зони Z_i до зони Z_{n+1} з проміжною посадкою на стартовій позиції для заміни батареї:

$$T_{ri,n+1} = T_{i,SP} + \tau_{rl} + T_{n+1,SP} \text{ (хв)}. \quad (4)$$

5. Розрахунок часу очікування початку виконання завдань БПЛА *i* у зоні Z_{n+1} без проміжної посадки на стартовій позиції для заміни батареї:

$$\tau_i^w = \tau_i + T_{i,n+1} \text{(хв)}. \quad (5)$$

6. Розрахунок часу очікування початку виконання завдань у зоні Z_{n+1} з використанням БПЛА *i*, який дістається цієї зони, роблячи проміжну посадку на стартовій позиції для заміни батареї:

$$\tau_{ri}^w = \tau_i + T_{ri,n+1} \text{(хв)}. \quad (6)$$

7. Розрахунок часового ресурсу батареї БПЛА *i*, який дістається зони Z_{n+1}, не роблячи проміжної посадки на стартовій позиції для заміни батареї, на початку виконання завдання у цій зоні:

$$\tau_{i,n+1}^{cbl} = \tau_i^{cbl} - \tau_i^w \text{ (хв)}. \quad (7)$$

8. Розрахунок часового ресурсу батареї БПЛА *i*, який дістається зони Z_{n+1}, роблячи проміжну посадку на стартовій позиції для заміни батареї, на початку виконання завдання у цій зоні:

$$\tau_{ri,n+1}^{cbl} = \tau_{bl} - T_{n+1,SP} \text{ (хв)}. \quad (8)$$

9. Розрахунок часового ресурсу батареї БПЛА, який необхідний для виконання завдання у зоні Z_{n+1}:

$$\tau_{n+1}^{cbl} = \tau_{n+1} + T_{n+1,SP} \text{ (хв).} \quad (9)$$

Постановка задачі мінімізації часу очікування початку виконання флотом завдання у новій зоні відповідальності Z_{n+1} з урахуванням показників, розрахованих за формулами (1)–(9), передбачає такі етапи.

1. Ідентифікація змінних:

a_i – варіант використання БПЛА *i* для виконання завдання у зоні Z_{n+1} без проміжної посадки на стартовій позиції для заміни батареї (a_i=1, якщо цей варіант використовується, a_i = 0 – у протилежному випадку);

a_{ri} – варіант використання БПЛА *i* для виконання завдання у зоні Z_{n+1} з проміжною посадкою на стартовій позиції для заміни батареї (a_{ri}=1, якщо цей варіант використовується, a_{ri} = 0 – у протилежному випадку).

2. Запис цільової функції:

$$\tau_{n+1}^{w} = \sum_{i=1}^{n} \tau_i^w a_i + \sum_{i=1}^{n} \tau_{ri}^w a_{ri} \to \min. \quad (10)$$

3. Уведення необхідних обмежень:

$$\sum_{i=1}^{n} \tau_{i,n+1}^{cbl} a_i + \sum_{i=1}^{n} \tau_{ri,n+1}^{cbl} a_{ri} \geq \tau_{n+1}^{cbl}, \quad (11)$$

$$a_i \in \{0,1\}, a_{ri} \in \{0,1\}, i = \overline{1,n}, \quad (12)$$

$$\sum_{i=1}^{n} a_i + \sum_{i=1}^{n} a_{ri} = 1. \quad (13)$$

Наведемо приклад реалізації запропонованого підходу.

Припустимо, що флот, який складається з п’яти БПЛА українського виробництва “Фурія” з електричним двигуном, застосовується для виконання завдань з радіаційного моніторингу в межах 30-кілометрової зони Запорізької АЕС (рис. 1). Кожен БПЛА виконує завдання у своїй зоні відповідальності.

У певний момент флот БПЛА отримує заявку на проведення моніторингу в новій зоні відповідальності Z_6. Розглянемо випадки, коли почергово, як ця зона, виступають зони 6(1), 6(2), 6(3), 6(4), 6(5) та 6(6) (рис. 1). Необхідно мінімізувати час очікування початку виконання флотом завдання у кожній із цих зон, тобто визначити параметри $\tau^w_{6(1)}, \tau^w_{6(2)}, \tau^w_{6(3)}\ \tau^w_{6(4)}, \tau^w_{6(5)},\ \tau^w_{6(5)}$.

Параметри, необхідні для проведення розрахунків за формулами (1)–(9), подано в табл. 1.

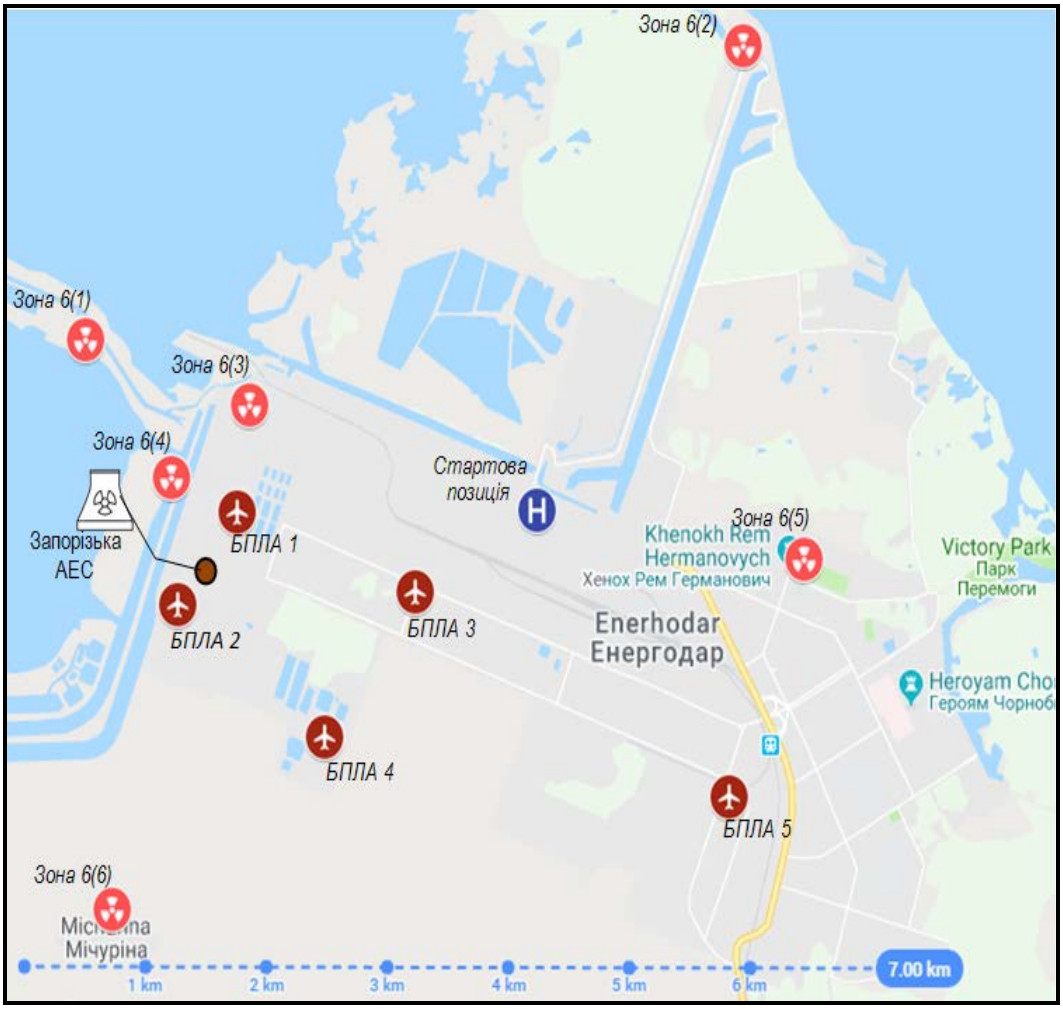


Рис. 1. Флот БПЛА, який здійснює радіаційний моніторинг у межах 30-кілометрової зони Запорізької АЕС, поточні та нові зони його відповідальності

Таблиця 1

Параметри, необхідні для проведення розрахунків за формулами (1)–(9)

Назва параметра, його позначення і розмірність	Значення параметра
крейсерська швидкість БПЛА v_{cr} (км/год)	40
час, необхідний для заміни батареї на стартовій позиції τ_{rl} (хв)	7
часовий ресурс нової батареї τ_{bl} (хв)	150
час, який потребує БПЛА 1 для завершення виконання свого завдання у зоні 1 τ_1 (хв)	14
часовий ресурс батареї БПЛА 1 на момент отримання заявки на виконання завдання у новій зоні τ_1^{cbl} (хв)	36
час, який потребує БПЛА 2 для завершення виконання свого завдання у зоні 2 τ_2 (хв)	11
часовий ресурс батареї БПЛА 2 на момент отримання заявки на виконання завдання у новій зоні τ_2^{cbl} (хв)	32
час, який потребує БПЛА 3 для завершення виконання свого завдання у зоні 3 τ_3 (хв)	13
часовий ресурс батареї БПЛА 3 на момент отримання заявки на виконання завдання у новій зоні τ_3^{cbl} (хв)	35
час, який потребує БПЛА 4 для завершення виконання свого завдання у зоні 4 τ_4 (хв)	11
часовий ресурс батареї БПЛА 4 на момент отримання заявки на виконання завдання у новій зоні 4 τ_4^{cbl} (хв)	36
час, який потребує БПЛА 5 для завершення виконання свого завдання у зоні 5 τ_5 (хв)	10
часовий ресурс батареї БПЛА 5 на момент отримання заявки на виконання завдання у новій зоні 5 τ_5^{cbl} (хв)	41

Використовуючи формули (1)–(9) та параметри, задані табл. 1, визначимо необхідні показники й отримаємо відповідно до формули (10) цільову функцію, а відповідно до формули (11) – обмеження і подамо їх у вигляді табл. 2.

Обмеження, отримані з використанням виразів (12) і (13), загальні для всіх випадків, що розглядаються, і можуть бути записані так:

$$a_i \in \{0,1\},\ a_{ri} \in \{0,1\},\ i = \overline{1,5}; \qquad \sum_{i=1}^{5} a_i + \sum_{i=1}^{5} a_{ri} = 1.$$

Таблиця 2

Цільова функція та обмеження для визначення мінімального часу очікування початку виконання флотом БПЛА завдання у відповідній новій зоні відповідальності

№ нової зони	Цільова функція та обмеження для визначення часу очікування початку виконання флотом БПЛА завдання у відповідній зоні відповідальності
6(1)	$\tau^{w}_{6(1)} = 19a_1 + 14a_2 + 20a_3 + 24a_4 + 28a_5 + 38a_{r1} + 49a_{r2} + 39a_{r3} + + 34a_{r4} + 44a_{r5} \to \min.$ $19a_1 + 18a_2 + 17a_3 + 20a_4 + 22a_5 + 144(a_{r1} + a_{r2} + a_{r3} + a_{r4} + a_{r5}) \geq 21.$
6(2)	$\tau^{w}_{6(2)} = 22a_1 + 20a_2 + 20a_3 + 20a_4 + 18a_5 + 30a_{r1} + 28a_{r2} + 27a_{r3} + + 27a_{r4} + 26a_{r5} \to \min.$ $14a_1 + 10a_2 + 15a_3 + 26a_4 + 23a_5 + 145(a_{r1} + a_{r2} + a_{r3} + a_{r4} + a_{r5}) \geq 24.$
6(3)	$\tau^{w}_{6(2)} = 15a_1 + 13a_2 + 16a_3 + 15a_4 + 17a_5 + 9a_{r1} + 27a_{r2} + 26a_{r3} + + 26a_{r4} + 25a_{r5} \to \min.$ $21a_1 + 17a_2 + 19a_3 + 21a_4 + 24a_5 + 146(a_{r1} + a_{r2} + a_{r3} + a_{r4} + a_{r5}) \geq 16.$
6(4)	$\tau^{w}_{6(2)} = 15a_1 + 12a_2 + 16a_3 + 14a_4 + 18a_5 + 0a_{r1} + 28a_{r2} + 27a_{r3} + + 27a_{r4} + 26a_{r5} \to \min.$ $21a_1 + 18a_2 + 19a_3 + 22a_4 + 23a_5 + 145(a_{r1} + a_{r2} + a_{r3} + a_{r4} + a_{r5}) \geq 21.$
6(5)	$\tau^{w}_{6(2)} = 21a_1 + 19a_2 + 18a_3 + 17a_4 + 13a_5 + 28a_{r1} + 26a_{r2} + 25a_{r3} + + 25a_{r4} + 24a_{r5} \to \min.$ $15a_1 + 11a_2 + 17a_3 + 19a_4 + 28a_5 + 147(a_{r1} + a_{r2} + a_{r3} + a_{r4} + a_{r5}) \geq 29.$
6(6)	$\tau^{w}_{6(2)} = 19a_1 + 14a_2 + 18a_3 + 14a_4 + 18a_5 + 32a_{r1} + 30a_{r2} + 29a_{r3} + + 29a_{r4} + 28a_{r5} \to \min.$ $17a_1 + 16a_2 + 17a_3 + 22a_4 + 23a_5 + 143(a_{r1} + a_{r2} + a_{r3} + a_{r4} + a_{r5}) \geq 20.$

Результати розв’язку оптимізаційних задач, поданих у табл. 2, наведено в табл. 3 та проілюстровано за допомогою рис. 2.

№ нової зони	Час, необхідний для виконання завдання у новій зоні, хв	БПЛА, що виконуватиме завдання	Час очікування початку виконання БПЛА завдань у новій зоні, хв	Проміжна посадка для заміни батареї
6(1)	15	БПЛА 5	19	–
6(2)	19	БПЛА 5	26	+
6(3)	12	БПЛА 2	13	–
6(4)	16	БПЛА 4	14	–
6(5)	26	БПЛА 5	24	+
6(6)	13	БПЛА 4	14	–

Рис. 2. Маршрути руху БПЛА до нових зон відповідальності

Аналіз отриманих результатів дає змогу зробити такі висновки.

Найбільш затребуваним є БПЛА 5, який швидше за інших БПЛА може розпочати виконання завдання у нових зонах 6(1), 6(2) та 6(5). При цьому переліт до зон 6(2) і 6(5) можливий лише з проміжною посадкою на стартовій позиції для заміни батареї.

Незатребуваними є БПЛА 1 та БПЛА 3.

Розрахунки показали, що не завжди географічна близькість БПЛА до нової зони відповідальності робить його найоптимальнішим для спрямування

в цю зону. Це пояснюється тим, що, крім часу польоту з поточної зони відповідальності до нової зони, враховуються ще такі часові показники, як час, що потребує БПЛА для завершення виконання свого завдання у поточній зоні, а також часовий ресурс батареї БПЛА на момент отримання заявки на виконання завдання в новій зоні. Велике значення першого часового показника та мале значення другого можуть не дозволити географічно ближче розташованому до нової зони відповідальності БПЛА мати перевагу над іншими. Так, наприклад, до зони 6(1) за наявних вихідних даних мав спрямовуватись найдальше розташований від неї БПЛА 5. Однак за умови завершення виконання всіма БПЛА своїх поточних завдань на момент отримання заявки та з достатнім часовим ресурсом батареї у кожного з них для її обслуговування для виконання завдання у зоні 6(1) було б обрано БПЛА 1.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Проведено аналіз можливих застосувань БПЛА під час радіаційного моніторингу. Запропоновано підхід до мінімізації часу очікування початку виконання флотом БПЛА завдання з радіаційного моніторингу в новій зоні відповідальності. Цей підхід передбачає розгляд таких питань: розподіл БПЛА за зонами відповідальності та встановлення часу на виконання завдання кожним із них; визначення місця розташування стартової позиції зі створенням на ній умов для заміни батареї; отримання флотом заявки на виконання завдання у новій зоні відповідальності та визначення часу на виконання цього завдання; побудова алгоритму розрахунку параметрів, необхідних для розв’язання оптимізаційної задачі; формулювання оптимізаційної задачі (мінімізація часу очікування початку виконання флотом БПЛА завдання з радіаційного моніторингу в новій зоні відповідальності) та обмежень. Параметри, що розраховуються: час польоту БПЛА із зони виконання завдання до: а) стартової позиції; б) нової зони (з проміжною посадкою та без проміжної посадки); час польоту з нової зони до стартової позиції; часовий ресурс батареї БПЛА, необхідний для виконання завдання у новій зоні; час очікування початку виконання завдання в новій зоні та часовий ресурс батареї БПЛА на початку виконання завдань у новій зоні для випадків: 1) БПЛА дістається цієї зони, роблячи проміжну посадку; 2) БПЛА не робить проміжної посадки.

Наведено приклад реалізації запропонованого підходу для флоту, що складається з п’яти БПЛА українського виробництва “Фурія” з електричним двигуном і застосовується для виконання завдань з радіаційного моніторингу в межах 30-кілометрової зони Запорізької АЕС (один БПЛА виконує завдання у своїй власній зоні). Розглянуто шість можливих нових зон відповідальності та визначено час очікування початку виконання БПЛА флоту завдання у кожній із цих зон. Установлено, що БПЛА 5, БПЛА 4 та БПЛА 2 можуть бути залучені до виконання завдання у трьох, двох та одній зоні відповідно. БПЛА 1 та БПЛА 2 не залучаються для виконання завдання

у жодній із розглянутих нових зон. Зазначимо, що БПЛА 5 один раз дістається своєї нової зони відповідальності без проміжної посадки на стартовій позиції для заміни батареї та двічі зі здійсненням такої посадки.

Запропонований підхід і розроблене для його реалізації програмне забезпечення можуть використовуватися операторами наземного пункту управління та персоналом кризового центру для відпрацювання оптимальних управлінських рішень щодо використання флоту БПЛА як складової частини системи моніторингу під час реагування на радіаційні аварії.

Подальші дослідження мають бути спрямовані на створення підходів щодо застосування під час радіаційного моніторингу флоту різнотипних БПЛА з можливістю спрямування до нової зони відповідальності двох та більше БПЛА.

Список використаних джерел:

1. *Al Rashdan A. Y., St Germain S. W.* Automation of data collection methods for online monitoring of nuclear power plants. Idaho Falls, Idaho: Idaho National Laboratory, 2018. 19 p.

2. Application of a territorial remote radiation monitoring system at the Chornobyl nuclear accident site / *Volodymyr Burtniak, Yurii Zabulonov, Maksym Stokolos, Leonid Bulavin and oth //* Journal of Applied Remote Sensing. 2018. № 12. P. 046007. DOI: 10.1117/1.JRS.12.046007.

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

4. *Schneider F., Gaspers B., Peräjärvi K., Gårdestig M.* Current state of the art of unmanned systems with potential to be used for radiation measurements and sampling. Report EUR 27224 EN. Luxembourg: Publications Office of the European Union, 2015. 63 p.

5. *Connor D. T., Martin P. G., Scott T. B.* Airborne radiation mapping: overview and application of current and future aerial systems // International journal of remote sensing. 2016. Vol. 37. P. 5953–5987. DOI: 10.1080/01431161.2016.12524.

6. *Babak S.* Radiation monitoring of environment using unmanned aerial complex // The Avdanced Science Journal. 2014. Vol. 12. P. 41–44.

7. *Бабак С. В.* Мониторинг окружающей среды АЭС с использованием систем видеонаблюдения и измерения мощности экспозиционной дозы на базе беспилотного авиационного комплекса // Системи обробки інформації. 2015. Вип. 7 (132). С. 190-194.

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

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

10. Система послеаварийного мониторинга АЭС с использованием беспилотных летательных аппаратов: модели надежности / *В. С. Харченко, М. А. Ястребенецкий, Г. В. Фесенко, А. А. Саченко и др.* // Ядерна та радіаційна безпека. 2017. №4 (76). С. 50–55.

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

12. *Моисеев В. С., Гущина Д. С., Моисеев Г. В.* Основы теории создания и применения информационных беспилотных авиационных комплексов: монография. Казань. 2010. 196 с.

13. *Fesenko H.* Optimal redistribution of UAVs in case of changing monitoring zones after a NPP accident // Dependable systems, services and technologies: proceedings of 2018 IEEE 9th international conference. Kyiv, 2018. P. 49–53. DOI: 10.1109/DESSERT.2018.8409097.

References

1. Al Rashdan A. Y. and St Germain S. W. (2018), Automation of data collection methods for online monitoring of nuclear power plants, Press Idaho National Laboratory, Idaho Falls, Idaho, 19 p. [USA].

2. Burtniak V., Zabulonov Yu., Stokolos M., Bulavin L. Krasnoholovets V. (2018), “Application of a territorial remote radiation monitoring system at the Chornobyl nuclear accident site”, Journal of Applied Remote Sensing, 2018, vol. 12. P. 046007. DOI: 10.1117/1.JRS.12.046007.

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

4. Schneider F., Gaspers B., Peräjärvi K. and Gårdestig M. (2015), Current state of the art of unmanned systems with potential to be used for radiation measurements and sampling. Report EUR 27224 EN. Publications Office of the European Union, Luxembourg, 63 p.

5. Connor D. T., Martin P. G. and Scott T. B. (2016), “Airborne radiation mapping: overview and application of current and future aerial systems”. International journal of remote sensing, vol. 37, pp. 5953-5987. DOI: 10.1080/01431161.2016.12524.

6. Babak S. (2014), “Radiation monitoring of environment using unmanned aerial complex”, The Avdanced Science Journal, vol. 12, pp. 41–44.

7. Babak S. V. (2015), *“Monitoring okruzhayuschey sredyi AES s ispolzovaniem sistem videonablyudeniya i izmereniya moschnosti ekspozitsionnoy dozyi na baze bespilotnogo aviatsionnogo kompleksa”* [“Monitoring of NPP environment using video surveillance and exposure dose measurement systems on the basis of unmanned aerial complex”], Journal *Systemy obrobky informatsii* [Information Processing Systems], vol. 7 (132), pp. 190–194 [Ukraine].

8. 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].

9. Sachenko A. A., Kochan V. V., Kharchenko V. S., Jastrebeneckij M. A., Fesenko H. V. and Janovskij M. Je. (2017), *“Sistema posleavarijnogo monitoringa AJeS s ispol'zovaniem bespilotnyh letatel'nyh apparatov: koncepcija, principy postroenija”* [“NPP post-accident monitoring system based on unmanned aircraft vehicle: Reliability models], Journal *Yaderna ta radiatsiina bezpeka* [Nuclear and Radiation Safety], vol. 1 (73), pp. 24–29 [Ukraine].

10. 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]].

11. 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.

12. Moiseev V. S., Gushina D. S. and Moiseev G. V. (2010), *Osnovy teorii sozdaniya i primeneniya informacionnyh bespilotnyh aviacionnyh kompleksov* [Fundamentals of the theory of creation and use of information unmanned aircraft complexes], Monograph, Kazan', 196 p. [Russia].

13. Fesenko H. (2018), “Optimal redistribution of UAVs in case of changing monitoring zones after a NPP accident”, Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, Kyiv, pp. 49–53. DOI: 10.1109/DESSERT.2018.8409097 [Ukraine].

DOI: https://doi.org/10.32836/2521-6643-2019-1-57-2
УДК 622:658.012.011.56

О. В. Бориченко, кандидат технічних наук,
доцент кафедри електропостачання
Національного технічного університету
України “Київський політехнічний інститут
імені Ігоря Сікорського”

ВИЗНАЧЕННЯ ОБ’ЄКТІВ ДЛЯ ОПЕРАТИВНОГО КОНТРОЛЮ ЕНЕРГОЕФЕКТИВНОСТІ В СИСТЕМІ ЕНЕРГЕТИЧНОГО МЕНЕДЖМЕНТУ

Розглянуто актуальне питання визначення об’єктів, для яких можливо та доцільно впроваджувати системи оперативного контролю енергоефективності. При визначенні об’єктів слід ураховувати основні вимоги, яким мають відповідати такі об’єкти. Серед таких вимог – розташування об’єктів в одному або суміжному приміщеннях, єдиний технологічний процес і керування цими об’єктами невеликою кількістю операторів. Відповідно до зазначених вимог у статті запропоновано алгоритм вибору об’єктів для створення систем оперативного контролю.

Ключові слова: *впровадження систем оперативного контролю енергоефективності; рівень енергоефективності підприємства; використання енергоресурсів.*

В работе рассмотрен актуальный вопрос определения объектов, для которых возможно и целесообразно внедрять системы оперативного контроля энергоэффективности. При определении объектов следует учитывать основные требования, которым должны соответствовать такие объекты, а именно: расположение объектов в одном или смежном помещениях, единый технологический процесс и управление этими объектами небольшим количеством операторов. В соответствии с указанными требованиями в работе предложен алгоритм выбора объектов для создания систем оперативного контроля.

Ключевые слова: *внедрение систем оперативного контроля энергоэффективности; уровень энергоэффективности предприятия; использование энергоресурсов.*

To achieve a high level of energy efficiency in any enterprise, it is necessary to periodically evaluate the level of effectiveness of energy saving activities, that is, to carry out operational control of energy efficiency. One of the most problematic places in creating energy control systems is the facilities for which it is possible and appropriate to control. When determining the objects for which it is expedient to create an operational control system, it is necessary to take into account the basic requirements that such facilities should meet. Among such requirements: the location of objects in one or adjacent premises, a single technological process and the management of these objects of a small number of operators. In accordance with these requirements, an algorithm for selecting objects for creating an operational control system is proposed. At the first stage all equipment of the enterprise should be divided into a small number of groups on a technological basis. The next step is building energy consumption balances separately for each of the technological processes of production of all types of enterprise products. To compile energy consumption balances, a methodology for constructing optimal energy balance models can be applied. Based on the calculated values of energy consumption for the production of each type of product, equipment can be distributed into smaller groups based on two criteria. These criteria include the location of equipment and their power supply from the same power points. The resulting equipment groups are the previous objects, but this does not mean that an operational control system is appropriate for such facilities. In this paper, solution of additional problems is proposed, in particular:

– *determination of the composition of factors that affect the amount of energy consumption;*

– *expediency of installing additional meters for energy consumption, production and other parameters;*

– *estimation of monetary expenses for creation of systems;*

– *estimation of energy saving potential;*

– *financial analysis of the feasibility of creating systems.*

Thanks to this, it is possible to reasonably determine the objects for which it is technically possible and financially feasible to create an operational control system.

Key words: *implementation of operational control systems of energy efficiency, energy efficiency level of the enterprise, use of energy resources.*

Постановка проблеми. Підвищення рівня енергоефективності підприємства – це одне з головних завдань сучасного виробництва. Значну частку собівартості виробленої продукції становить складова за використані енергоресурси. Зважаючи на постійне підвищення тарифів на паливно-енергетичні ресурси, доцільно зробити аналіз і контроль енергоспоживання й максимальне його скорочення для підвищення конкурентоспроможності товарів на вітчизняному й міжнародному ринках.

Розв’язання цих проблем має розпочинатися з удосконалення систем управління підприємством, особливо з оптимізації систем управління енергоспоживанням шляхом упровадження систем енергетичного менеджменту (СЕнМ) на підприємствах як на основі міжнародних, так і національних стандартів з енергетичного менеджменту [1; 2].

Для зменшення рівня енергоспоживання не достатньо лише впроваджувати відповідні заходи з енергоефективності. Одним із головних завдань є оперативний контроль енерговикористання. Для досягнення цієї мети необхідно будувати й упроваджувати системи оперативного контролю і планування на об’єкті.

Системи оперативного контролю використовуються для невеликих локальних виробничих об’єктів. Це можуть бути окремі установки, агрегати, технологічні процеси.

Згідно з рекомендаціями міжнародного стандарту ISO 50001:2011 [1], визначення об’єктів оперативного контролю встановлюється виходячи з енергоємності (визначається найбільш енергоємний об’єкт, у ньому – найбільш енергоємна ділянка, в якій розміщена сама енергоємна установка). Однак належність установки до енергоємної далеко не завжди достатня умова того, щоб даний об’єкт був предметом контролю, в першу чергу, (раніше за інші об’єкти, менш енергоємні). Це пов’язано як із фінансовими обмеженнями та економічною доцільністю реалізації такої системи оперативного контролю, так і з технічними можливостями її реалізації для конкретного об’єкта.

Тому актуально розроблення алгоритму визначення об’єктів, для яких технічно можливо та економічно доцільно створювати і впроваджувати системи оперативного контролю енергоефективності.

Аналіз останніх досліджень і публікацій. Методику побудови та функціонування систем оперативного контролю ефективності енерговикористання упродовж тривалого часу застосовують у зарубіжних країнах [3–7]. Такі системи зарекомендували себе в зарубіжній практиці як дієвий інструмент оперативного контролю ефективності використання електричної енергії на локальних технологічних об’єктах. Однак у цих працях не визначено підхід щодо вибору об’єктів, для яких доцільно створювати такі системи.

Праці [8, 9] присвячено питанням побудови систем моніторингу результатів енергозбереження в системах енергетичного менеджменту, проте ще не вирішено питання обґрунтування вибору об’єктів для створення таких систем.

Методику побудови систем оперативного контролю ефективності енергоспоживання досліджено в [10]. Однак у цьому дослідженні не до кінця роз-

крито питання вибору об’єктів, але описано встановлення центрів обліку енергії для більш енергоємних споживачів.

Питання вибору обладнання, для якого передусім, необхідно впроваджувати заходи з енергозбереження в системі енергетичного менеджменту, розглядалося в [11], але цей підхід підкреслює неточність та необґрунтованість припущень щодо вибору об’єктів для створення систем оперативного контролю енергоефективності.

Розглянуті вище публікації щодо питань побудови систем оперативного контролю або взагалі не стосуються вирішення питань визначення об’єктів оперативного контролю, або це питання досліджено досить фрагментарно.

Мета статті – створення методичних основ вибору об’єктів для побудови та функціонування систем оперативного контролю енергоефективності на підприємстві.

Виклад основного матеріалу. Однією з функцій систем оперативного контролю енергоспоживання є планування та здійснення заходів, необхідних для підтримання запланованого рівня ефективності використання палива чи енергії або для підвищення цього рівня. При побудові таких систем залишається не вирішеним питання, які саме обирати об’єкти для впровадження систем оперативного контролю енергоспоживання.

Традиційно системи оперативного контролю ефективності енерговикористання створюють і застосовують для окремих установок, агрегатів, невеликих їх груп або для простих технологічних процесів.

На будь-якому виробничому об’єкті кількість технологічних установок вимірюється сотнями або навіть тисячами. Для здійснення оперативного контролю енергоефективності потенційно існує потреба у побудові сотень відповідних систем, що пов’язано зі значними витратами часу й коштів. Причому доцільність цих витрат далеко не завжди очевидна.

Вибір окремих технологічних установок, їхніх груп або технологічних процесів, для яких можливо й доцільно створення локальних систем контролю ефективності енерговикористання, є досить складним завданням. Виконання цього завдання має здійснюватись “індивідуально” для кожного виробничого об’єкта.

Визначаючи локальні технологічні об’єкти, для яких можливо й доцільно створення систем оперативного контролю ефективності енерговикористання, насамперед слід брати до уваги основні вимоги, яким мають відповідати такі об’єкти. Зокрема [12]:

− обладнання, для якого планується побудувати окрему систему оперативного контролю енергоефективності, має бути розташовано в одному або у суміжних виробничих приміщеннях, щоб існувала можливість організації єдиного обліку його спільного енергоспоживання;

− таке обладнання має бути об’єднано єдиним технологічним процесом, тобто спільно використовуватись для виробництва одного й того ж різновиду продукції або кількох її видів;

− обладнанням, яке планується включити до однієї локальної системи оперативного контролю енергоефективності, має керувати невелика кількість операторів, щоб вплив людського фактора на процес споживання енергії був якомога меншим.

Беручи до уваги зазначені вище основні вимоги, загальний алгоритм розв’язання задачі вибору технологічних об’єктів для побудови локальних систем оперативного контролю ефективності енерговикористання на будь-якому підприємстві може бути таким.

На першому етапі все основне й допоміжне обладнання підприємства попередньо має бути розділено на певну порівняно невелику кількість груп. Найбільш доцільно здійснювати такий розподіл за технологічним принципом. Тобто наявне технологічне обладнання потрібно розподілити між технологічними процесами виробництва всіх видів продукції підприємства.

З цією метою, перш за все, необхідно скласти схеми відповідних технологічних процесів, які мають відображати послідовність виконання окремих операцій та взаємозв’язок між ними, а також відомості про обладнання, на якому виконуються ці операції, із зазначенням видів енергоресурсів, що при цьому споживаються.

Наступним кроком розв’язання задачі має бути побудова балансів споживання енергії окремо для кожного технологічного процесу виробництва всіх видів продукції підприємства. Зокрема, для складання балансів споживання електричної енергії у процесах виробництва кожного виду продукції може бути застосовано методику побудови оптимальних розрахункових моделей електробалансів [13].

На підставі побудованих за цією методикою балансів енергоспоживання і складених технологічних схем фактичні обсяги споживання енергії за попередні періоди на підприємстві можуть бути обґрунтовано розподілені між усіма видами продукції. Тим самим можна отримати псевдостатистичні дані про споживання електричної енергії на виробництво кожного різновиду продукції, необхідні на подальших етапах визначення технологічних об’єктів для створення локальних систем оперативного контролю енергоефективності на підприємстві.

Зокрема, наступним кроком розв’язання цієї задачі має бути розподіл основного та допоміжного обладнання, що належить до технологічного процесу виробництва кожного виду продукції, на дрібніші групи. Таке подальше групування обладнання має здійснюватись за двома критеріями.

Перший із цих критеріїв – місце розташування відповідного обладнання у тих чи інших будівлях, спорудах чи виробничих приміщеннях. Очевидно, що до однієї групи має бути зараховано обладнання, розташоване в одній і тій самій будівлі чи споруді, або в одному чи у суміжних приміщеннях.

Другим критерієм подальшого групування технологічного обладнання підприємства мають бути схеми внутрішнього електропостачання відповідних будівель, споруд і виробничих приміщень. Отже, обладнання, розташоване в одному й тому ж або в суміжних приміщеннях, може (й повинно) бути додатково розподілене на ще дрібніші групи, живлення яких електроенергією здійснюється від одних і тих же силових пунктів.

Одержані в результаті зазначеного додаткового розподілу групи технологічного обладнання – попередні об’єкти, для яких на підприємстві фізично можуть бути побудовані локальні системи оперативного контролю ефективності енерговикористання. Однак це ще не означає, що побудова систем оперативного контролю енергоефективності для цих об’єктів доцільна.

Таким чином, для остаточного розв’язання задачі, що розглядається, необхідно додатково проаналізувати попередньо встановлені групи обладнання з погляду доцільності створення для них систем оперативного контролю ефективності енерговикористання.

Цей аналіз так само потребує розв’язання низки додаткових задач. Основні з них такі:

− визначення складу чинників (параметрів технологічного процесу, зовнішніх умов тощо), які впливають на обсяги споживання енергії кожною з попередньо визначених груп обладнання;

− визначення додаткових приладів обліку споживання енергії, виробництва продукції, а також параметрів, що характеризують виробничі умови, необхідних для побудови систем оперативного контролю енергоефективності для кожної з груп обладнання;

− оцінка грошових витрат на побудову і функціонування таких систем контролю;

− оцінка потенціалу енергозбереження, що матиме місце завдяки створенню систем оперативного контролю ефективності енерговикористання для кожної з груп обладнання, що розглядаються;

− фінансовий аналіз доцільності створення локальних систем контролю енергоефективності для попередньо визначених груп обладнання.

Структурну схему алгоритму визначення об’єктів для побудови та функціонування систем оперативного контролю енергоефективності на підприємстві зображено на рис. 1.

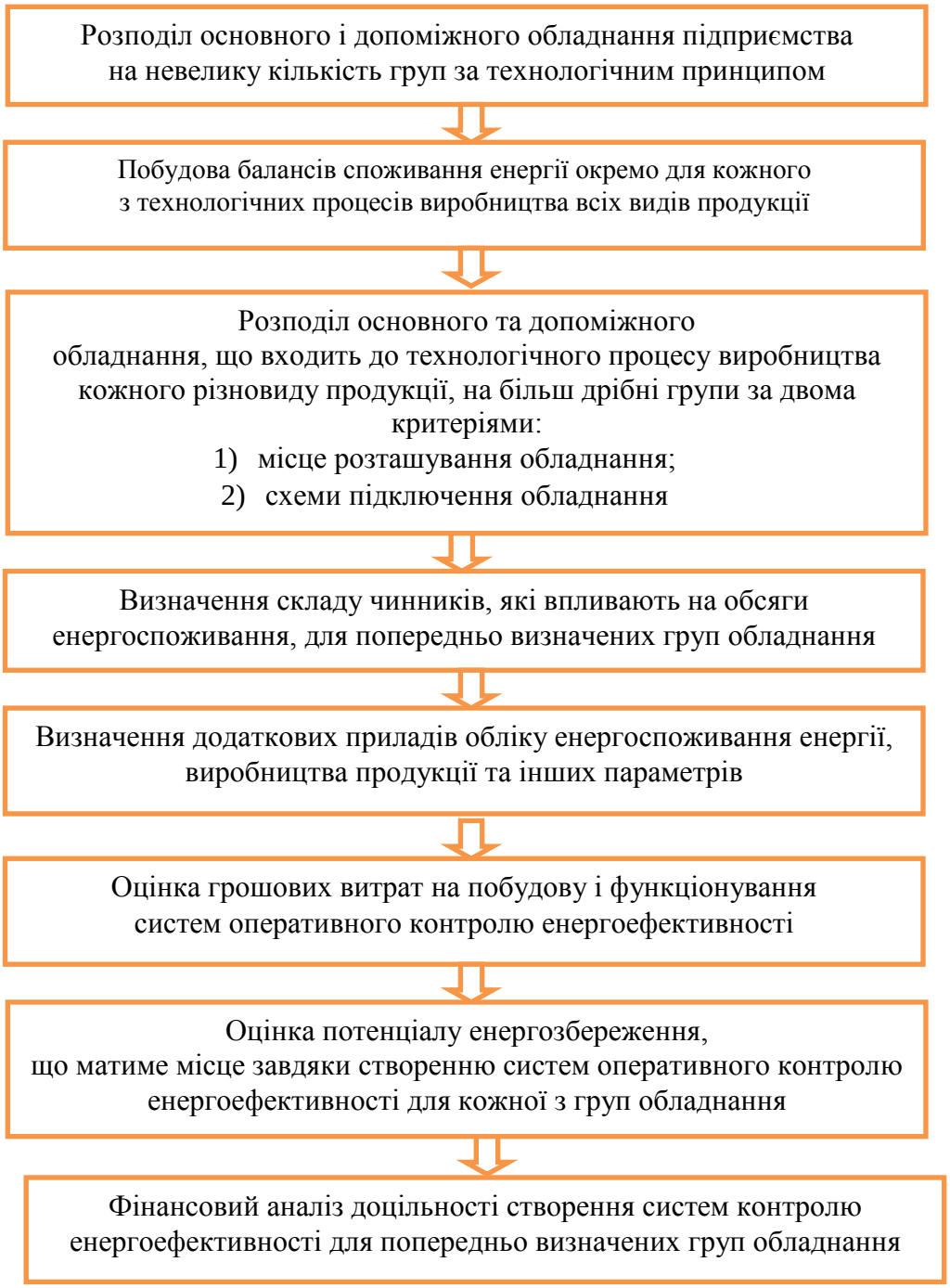


Рис. 1. Структурна схема алгоритму визначення об’єктів для побудови систем оперативного контролю енергоефективності

Приклад практичного застосовування. Алгоритм вибору об'єктів, для яких необхідно будувати системи оперативного контролю енерговикористання, проілюстровано на прикладі плавильної дільниці одного з підприємств кольорової металургії. Для зазначеної дільниці з застосуванням різних методів було розраховано кілька варіантів вибору об'єктів з метою побудови систем оперативного контролю енерговикористання, зокрема використано АВС-аналіз [14], що ґрунтується на групуванні об'єктів залежно від значущості й за конкретною ознакою. Спочатку необхідно обрати вибірку об'єктів, що були б об'єднані спільною ознакою, наприклад, це може бути величина енергоспоживання кожного виду обладнання окремого виробничого підрозділу. В подальшому розраховується сумарна величина споживання енергії для виробничого підрозділу в цілому:

$$W_{\text{сум}} = W_1 + W_2 + ... + W_n, \tag{1}$$

де $W_1, W_2, ..., W_n$ – річне енергоспоживання окремого n-го об'єкта вибірки;

n – відповідний номер об'єкта вибірки.

Підставляючи відповідні значення у формулу (1), отримаємо:

$$W_{\text{сум}} = 1166760 + 207424 + ... + 1248 = 1978922,93 \text{ кВт·год.}$$

Потім для кожного об'єкта вибірки визначається його частка енергоспоживання в загальній величині споживання енергії виробничого підрозділу, а також частка за зростаючим підсумком для кожного об'єкта відповідно за формулами:

$$K_n = \frac{W_n}{W_{\text{сум}}} \cdot 100; \tag{2}$$

$$K_{\text{зр.}} = K_n + K_{n+1}. \tag{3}$$

Підставляємо значення у формули (2), (3) й відповідно отримаємо:

$$K_n = \frac{1166760}{1978922,93} \cdot 100 = 58,96, \; K_{\text{зр.}} = 58,96 + 10,48 = 69,44.$$

Визначивши для кожного об'єкта виробничого підрозділу значення його частки за зростаючим підсумком, аналізуємо отримані значення розрахованих $K_{\text{зр.}}$ і проводимо групування цих об'єктів таким чином:

− об'єкти вибірки, для яких частка за зростаючим підсумком наближується до 80 %, це нижня межа групи А. Верхня межа групи А – це перша позиція у переліку об'єктів вибірки відповідного підрозділу;

− об'єкт вибірки, для якого частка за зростаючим підсумком наближається до 95 %, – це нижня межа групи В;

− усі інші об'єкти вибірки, для яких частка за зростаючим підсумком більша 95 %, належать до групи С.

Результати розрахунків за допомогою АВС-аналізу для визначення об’єктів з метою побудови систем оперативного контролю енерговикористання подано в табл. 1.

Таблиця 1

Результати розрахунків з використанням АВС-аналізу

№ з/п	Найменування енергоспоживального обладнання	Річне електроспоживання, кВт·год	Частка електроспоживання, %	Зростаючий підсумок	Група АВС-аналізу
1	Піч індукційна тигельна	1 166 760,00	58,96	58,96	**A**
2	Стерилізатор паровий № 1, 2, 3, 4	207 424,00	10,48	69,44	**A**
3	Камера сушильна № 1, 2	105 737,63	5,34	74,78	**A**
4	Освітлення:	101 860,74	5,15	79,93	**A**
5	Електротепловентилятор	66 672,00	3,37	83,30	**B**
6	Пристрій каталітичного допалювання	56 000,00	2,83	86,13	**B**
7	Насос обігового водопостачання № 1	51 393,00	2,60	88,73	**B**
8	Насос вакуумний водокільцевий	33 408,00	1,69	90,42	**B**
9	Підспінювач	25 928,00	1,31	91,73	**B**
10	Витяжна вентиляція В-20, В-21	17 779,20	0,90	92,62	**B**
11	Машина дробоструменевого очищення	17 472,00	0,88	93,51	**B**
12	Охолоджувач	16 704,00	0,84	94,35	**B**
13	Витяжна вентиляція вібросита	16 704,00	0,84	95,20	**C**
14	Припливна вентиляція ПУ-1	16 668,00	0,84	96,04	**C**
15	Верстак збирання модельних блоків	15 001,20	0,76	96,80	**C**
16	Рольганг	14 699,52	0,74	97,54	**C**
17	Вентилятор	11 136,00	0,56	98,10	**C**
18	Припливна вентиляція ПУ-2	10 000,80	0,51	98,61	**C**

Як видно з табл. 1, за результатами розрахунку до складу групи А входять чотири об'єкти, які мають найбільшу частку в загальному електроспоживанні всієї дільниці, отже, саме для таких об'єктів, у першу чергу, необхідно будувати системи оперативного контролю енерговикористання.

Для прикладу подальших розрахунків обираємо тигельну піч (перша позиція у групі А).

Наступним кроком є визначення складу чинників, що впливають на зміну обсягів енергоспоживання тигельної печі. З цією метою використано методи експертних оцінок, які детально описано в [15]. Група експертів сформована з обслуговуючого та виробничого персоналу підприємства. Щоб визначити, які саме чинники найбільше впливають на зміну обсягів енергоспоживання тигельної печі, експерти запропонували оцінити вплив відповідного чинника за лінгвістичною шкалою. Після оброблення результатів опитування експертів з використанням апарату нечіткої логіки [15] було визначено, що найсуттєвішими чинниками, які впливають на зміну обсягів електроспоживання тигельної печі, є:

- кількість переплавленого металу, т;
- температура плавлення металу, ºС.

У подальшому з метою побудови систем оперативного контролю енергоефективності для кожної з груп обладнання слід визначити додаткові прилади обліку споживання енергії, виробництва продукції, а також параметрів, що характеризують виробничі умови, та оцінити грошові витрати на побудову і функціонування таких систем контролю.

До витрат на побудову систем оперативного контролю енергоефективності входять витрати на придбання та встановлення приладів обліку споживання електричної енергії, а також необхідних додаткових вимірювальних приладів відповідних технологічних параметрів. Вартість приладів для вимірювання дорівнює $B_{\text{прил}} = 7500$ у. о., крім того, вартість навчання та підготовка персоналу – $B_{\text{навч}} = 2000$ у. о. Сумарні витрати на побудову таких систем становлять 9500 у. о.

Витрати на функціонування систем оперативного контролю енергоефективності включають витрати на збирання та оброблення даних, витрати на вимірювання та ануїтет.

Витрати на вимірювання даних визначаються за формулою:

$$B_{\text{вим}} = T_{\text{вим}} \cdot n_{\text{чол}} \cdot \overline{ЗП} \cdot k_{\text{вим}}, \qquad (4)$$

де $T_{\text{вим}}$ – час, потрібний на одне вимірювання, год;

$\overline{ЗП}$ – середня заробітна плата працівника, у. о./год;

$n_{\text{чол}}$ – кількість працівників, які здійснюють вимірювання;

$k_{\text{вим}}$ – кількість вимірювань за місяць.

Приймаємо: $T_{\text{вим}} = 0{,}5$ год; $n_{\text{чол}} = 1$, $\overline{ЗП} = 25$ у. о./год; $k_{вим} = 22$ рази (одне вимірювання кожного робочого дня). Підставляємо відповідні значення у формулу (4) і розраховуємо витрати на вимірювання показників, необхідних для функціонування систем оперативного контролю енергоефективності:

$$B_{\text{вим}} = 0{,}5 \cdot 1 \cdot 25 \cdot 22 = 275 \text{ у. о.}$$

Витрати на збирання даних можуть бути розраховані за формулою:

$$B_{\text{зб}} = T_{\text{зб}} \cdot n_{\text{чол}} \cdot \overline{ЗП} \cdot k_{\text{зб}}, \quad (5)$$

де $T_{\text{зб}}$ – час, необхідний для збирання інформації за відповідний період.

Приймаємо: $T_{\text{зб}} = 1$ год, $n_{\text{чол}} = 1$, $\overline{ЗП} = 25$ у. о./год., $k_{\text{зб}} = 22$ рази. Підставляємо відповідні значення у формулу (5) і визначаємо витрати на збирання даних:

$$B_{\text{зб}} = 1 \cdot 1 \cdot 25 \cdot 22 = 550 \text{ у. о.}$$

Витрати на оброблення даних визначаються за формулою:

$$B_{\text{об.д}} = T_{\text{об.д}} \cdot n_{\text{чол}} \cdot \overline{ЗП} \cdot k_{\text{об.д}}, \quad (6)$$

де $T_{\text{об.д.}}$ – час, необхідний для оброблення даних за відповідний період.

Приймаємо: що $T_{\text{об.д}} = 1$ год, $n_{\text{чол}} = 1$, $\overline{ЗП} = 25$ у. о./год, $k_{\text{об.д}} = 22$ рази (періодичність оброблення даних за місяць). Підставляємо відповідні значення у формулу (6) і розраховуємо витрати на оброблення даних, необхідних для функціонування систем оперативного контролю енергоефективності:

$$B_{об.д} = 1 \cdot 1 \cdot 25 \cdot 22 = 550 \text{ у. о.}$$

Сумарні витрати на функціонування систем оперативного контролю енергоефективності становлять 1375 у. о.

Необхідно також урахувати амортизаційні витрати. Для цього слід розрахувати ануїтет:

$$A = k \cdot B_{\text{прил}}, \quad (7)$$

де k – коефіцієнт ануїтету, який розраховується за формулою:

$$k = \frac{i \cdot (1+i)^n}{(1+i)^n - 1}, \tag{8}$$

де i – ставка дисконта; n – кількість періодів, протягом якого діє ануїтет.

Приймаємо ставку дисконту за 22 %, кількість періодів установлюємо 10 років (приймаємо за термін експлуатації приладів обліку).

Підставляємо відповідні значення у формулу (8) і розраховуємо коефіцієнт ануїтету:

$$K = \frac{0,22/10 \cdot (1+0,22/10)^{10}}{(1+0,22/10)^{10} - 1} = 0,11.$$

Таким чином, щорічні амортизаційні відрахування визначаються за формулою (7).

$$A = 0,11 \cdot 9500 = 1045 \text{ у. о.}$$

Надалі необхідно оцінити потенціал енергозбереження, що матиме місце завдяки створенню систем оперативного контролю ефективності енерговикористання для обраного об’єкта. Економія електричної енергії в результаті побудови таких систем за міжнародним досвідом становить 5–10 % вартості електричної енергії за рік [10]. Для тигельної печі грошова економія електричної енергії – 12737 у. о.

Ураховуючи обчислені витрати на побудову та функціонування систем оперативного контролю енергоефективності, а також визначений потенціал енергозбереження, необхідно проаналізувати з фінансового боку доцільність створення таких локальних систем для попередньо визначених груп обладнання. Прийняття рішень про фінансову доцільність створення систем оперативного контролю для відповідної групи обладнання має базуватися на визначенні економічних критеріїв, а саме [16]:

- простий і динамічний терміни окупності;
- чиста приведена вартість;
- внутрішня норма рентабельності.

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

1. Під час проведення дослідження проаналізовано методи й підходи до визначення технологічних об’єктів, для яких доцільно створювати системи оперативного контролю енергоефективності. Однак у більшості праць розв’язання цієї задачі не розглядалось або було запропоновано здійснювати такий вибір лише за енергоємністю обладнання.

2. У визначенні об’єктів, для яких доцільн й технічно можливо створення систем оперативного контролю енергоефективності, слід ураховувати основні вимоги, яким мають відповідати такі об’єкти. Серед зазначених вимог є розташування об’єктів в одному або суміжних виробничих приміщеннях, єдиний технологічний процес та керування цими об’єктами невеликою кількістю операторів.

3. У статті запропоновано алгоритм вибору об’єктів для створення систем оперативного контролю. По-перше, все обладнання підприємства має бути розділено на невелику кількість груп за технологічним принципом. По-друге, слід побудувати баланси споживання енергії окремо для кожного з технологічних процесів виробництва всіх видів продукції підприємства. Виходячи з двох критеріїв, на основі отриманих розрахункових значень споживання енергії на виробництво кожного різновиду продукції може бути здійснений розподіл обладнання на дрібніші групи. До таких критеріїв належать місце розташування обладнання та їх живлення енергією від одних і тих же силових пунктів. Отримані групи обладнання являють собою попередні об’єкти, однак це не означає, що для таких об’єктів доцільно створення систем оперативного контролю енергоефективності.

4. З межою забезпечення можливості обґрунтовано визначати об’єкти, для яких технічно можливо і фінансово доцільно створення систем оперативного контролю енергоефективності, запропоновано розв’язання додаткових задач. Основними з яких є: визначення складу чинників, які впливають на обсяги енергоспоживання кожною з визначених груп обладнання; обґрунтування доцільності встановлення додаткових приладів обліку енергоспоживання, виробництва продукції та інших параметрів; оцінка грошових витрат на створення систем контролю; оцінка потенціалу енергозбереження та фінансовий аналіз доцільності створення систем.

Список використаних джерел:

1. ISO 50001:2011 Energymanagement systems. Requirements with guidanceforuse.

2. *Иншеков Е., Сафьянц А., Сафьянц С., Чернявский А.* Внедрение системы энергетического менеджмента на базе стандарта ISO 50001:2011: Путеводитель для специалистов компаний и предприятий. Киев: Проект “Энергоэффективная и направленная на уменьшение изменения климата модернизация промышленности в Донецкой области”. 2014. 36 с.

3. *Pooley John* Quick Start Guide to Energy Monitoring &Targeting (M&T) // Effective Energy Management Guide. 2005. URL: http://www.oursouthwest.com/SusBus/susbus9/ m&tguide.pdf

4. Computer Based Monitoring And Targeting On A Hot Rolling Mill // Energy Effiiciency Enquiries Bureau, ETSU, Harwell, Oxfordshire, 0X11. Best Practice Programme. 1992. 26 p.

5. Waste avoidance methods / Energy Effiiciency Office. Best Practice Programme. Fuel Efficiency Booklet 13. Crown copyright. 1995. 18 p.

6. Monitoring and Targeting in large companies // Energy Effiiciency Enquiries Bureau, ETSU, Harwell, Oxfordshire, 0X11. Good Practice Guide 112. 1998. 45 p.

7. *Jones Phil.* Getting started with Monitoring & Targeting (M&T) // Fundamental Series. 2004. № 7. P. 29–32.

8. *Хайд Д., Лоскутов А. В.* Целевой энергетический мониторинг в системе энергетического менеджмента // Промышленная энергетика. 1998. № 4. С. 2–4.

9. *Loskutov A.* Monitoring and Targeting in Russian Industry // Seminar "Energy management: Low cost energy saving Techniques": Sofia, Bulgaria. 1997. April.

10. *Праховник А. В., Трапп Г. Р.* Контроль і нормалізація енергоспоживання // Управління енерговикористанням : зб. доп. Київ: Альянс за збереження енергії. 2001. С. 387–398.

11. Системи енергетичного менеджменту. Вимірювання рівня досягнутої енергоефективності з використанням базових рівнів енергоспоживання та показників енергоефективності. Загальні положення і настанова : ДСТУ ISO 50006:2014, IDT ДСТУ ISO 50006:2016 [Чинний від 2016-04-29]. Київ: Держспоживстандарт України, 2016. 56 с. (Національні стандарти України).

12. *Находов В. Ф., Бориченко О. В.* Концепція побудови інтегрованих систем контролю ефективності використання електричної енергії на виробничо-господарських об'єктах // Енергетика: економіка, технології, екологія. 2013. № 1. С. 72–79.

13. *Находов, В.Ф., Бориченко О. В.* Побудова оптимальних розрахункових моделей електробалансів виробничо-господарських об'єктів // Промислова електроенергетика та електротехніка. Промелектро : інформ. зб. 2010. № 6. С. 47–51.

14. A Complete Guide to ABC Analysis in Customer Segmentation and Inventory. URL: https://www.cleverism.com/complete-guide-abc-analysis-customer-segmentation-inventory/

15. *Находов В. Ф., Бориченко О. В., Іванько Д. О., Єгорова І. О.* Комплексний підхід до визначення складу чинників, що впливають на величину енергоспоживання при впровадженні систем оперативного контролю енергоефективності // Енергетика: економіка, технології, екологія. 2014. № 2. С. 68–79.

16. *Тарасюк Г. М.* Управління проектами: [навч. посіб. для студ. вищ. навч. закл.] [2-е вид.]. Київ: Каравела, 2006. 320 с.

References:

1. ISO 50001:2011 (2011), Energymanagement systems. Requirements with guidanceforuse. ISO.

2. Inshekov E., Safyants A., Safyants S. and Chernyavsky A. (2014), *Vnedreniye sistemy energeticheskogo menedzhmenta na baze standarta ISO 50001:2011: Putevoditel' dlya spetsialistov kompaniy i predpriyatiy* [Introduction of the energy management system based on the ISO 50001: 2011 standard: A guide for specialists of companies and enterprises], The project "Energy Efficient and Climate Change Mitigation Modernization of Industry in the Donetsk Region", Kyiv, 36 p. [Ukraine].

3. Pooley J. (2005), Quick Start Guide to Energy Monitoring & Targeting (M&T) // Effective Energy Management Guide, available at: http://www.oursouthwest.com/eemg/notices/ effective-energy-mgt-mandtguide.pdf

4. Computer Based Monitoring And Targeting On A Hot Rolling Mill // Energy Effiiciency Enquiries Bureau, ETSU, Harwell, Oxfordshire, 0X11. Best Practice Programme, 1992. 26 p.

5. Waste avoidance methods // Energy Effiiciency Office. Best Practice Programme. Fuel Efficiency Booklet 13. Crown copyright, 1995. 18 p.

6. Monitoring and Targeting in large companies // Energy Effiiciency Enquiries Bureau, ETSU, Harwell, Oxfordshire, 0X11. Good Practice Guide 112, 1998. 45 p.

7. Jones Phil (2004), Getting started with Monitoring & Targeting (M&T), Journal Fundamental Series, vol. 7, pp. 29–32.

8. Khayd D. and Loskutov A. V. *"Tselevoy energeticheskiy monitoring v sisteme energeticheskogo menedzhmenta"* ["Target energy monitoring in the energy management system"], Journal *Promyshlennaya energetika* [Industrial energy], vol. 4, pp. 2–4 [Russia].

9. Loskutov A. (1997), Monitoring and Targeting in Russian Industry // Seminar "Energymanagement: LowcostenergysavingTechniques". Sofia, April [Bulgarie].

10. Prakhovnyk A. V. and Trapp H. R. (2001), *Kontrol' i normalizatsiia enerhospozhyvannia* [Control and normalization of energy] : a collection of reports / Upravlinnia enerhovykorystanniam; Alians za zberezhennia enerhii, Kyiv, pp. 387–398 [Ukraine].

11. DSTU ISO 50006:2014. *Systemy enerhetychnoho menedzhmentu. Vymiriuvannia rivnia dosiahnutoi enerhoefektyvnosti z vykorystanniam bazovykh rivniv enerhospozhyvannia ta pokaznyki v enerhoefektyvnosti. Zahalni polozhennia i nastanova* [Energy management systems. Measurement of the level of achieved

energy efficiency using baseline energy consumption and energy efficiency indicators. General provisions and guidelines], Derzhspozhyvstandart Ukrainy, Kyiv, 2016, 56 p. [Ukraine].

12. Nakhodov V. F. and Borychenko O. V. (2013), *"Kontseptsiia pobudovy intehrovanykh system kontroliu efektyvnosti vykorystannia elektrychnoi enerhii na vyrobnycho-hospodarskykh obiektakh"* ["Concept of construction of integrated systems for monitoring the efficiency of electric energy use at industrial and economic objects"], Journal *Enerhetyka: ekonomika, tekhnolohiyi, ekolohiya* [Energy: economics, technology, ecology], vol. 1, pp. 72–79 [Ukraine].

13. Nakhodov V. F. and Borychenko O. V. (2010), *"Pobudova optymalnykh rozrakhunkovykh modelei elektrobalansiv vyrobnycho-hospodarskykh obiektiv"* ["Construction of the optimal calculation models for electrobalances of production and economic objects"], Journal *Promyslova elektroenerhetyka ta elektrotekhnika* [Industrial Electroenergetics and Electrical Engineering], information collection, vol. 6, pp. 47–51 [Ukraine].

14. A Complete Guide to ABC Analysis in Customer Segmentation and Inventory, available at: https://www.cleverism.com/complete-guide-abc-analysis-customer-segmentation-inventory/

15. Nakhodov V. F., Borychenko O. V., Ivan'ko D. O. and Yehorova I. O. (2014), *"Kompleksnyy pidkhid do vyznachennya skladu chynnykiv, shcho vplyvayut' na velychynu enerhospozhyvannya pry vprovadzhenni system operatyvnoho kontrolyu enerhoefektyvnosti"* ["A comprehensive approach to determining the composition of factors affecting the amount of energy consumption when implementing systems of operational control of energy efficiency"], Journal *Enerhetyka: ekonomika, tekhnolohiyi, ekolohiya* [Power engineering: economics, technologies, ecology], vol. 2, pp. 68–79 [Ukraine].

16. Tarasyuk G. M. (2006), *Upravlinnya proektamy* [Project Management], tutorial, press Karavela, Kyiv, 320 p. [Ukraine].

DOI: https://doi.org/10.32836/2521-6643-2019-1-57-3
UDC 658.338

S. I. Dotsenko, Associate Professor,
Doctor of Technical Sciences,
Professor of the Department of Specialized
Computer Systems, Ukrainian State University
of Railway Transport
S. S. Kamenskyi, Postgraduate Student
of the Department of Specialized Computer
Systems, Ukrainian State University
of Railway Transport

ARCHITECTURE DEVELOPMENT OF INFORMATION SYSTEM OF AN ENTERPRISE

In the paper the analysis of methods of modeling of activity of the enterprise is carried out. It is shown that at present there is no single commonly accepted method for modeling the activity of an enterprise. And this, in turn, prevents the development of a single tool for its simulation. This circumstance follows from the initial position of the theory and practice of enterprise modeling and business processes, namely, the process approach to the presentation of the activity. The method of establishing unambiguous correspondence (likeness) of architectures of the functional, organizational and infor-mation representations of the enterprise is proposed.

Key words: *system; representation; similarity; information representation; functional representation.*

Проаналізовано методи моделювання діяльності підприємства. Показано, що нині немає єдиного загальновизнаного методу моделювання діяльності підприємства. А це, зі свого боку, перешкоджає розробці єдиного інструментарію для його моделювання. Ця обставина випливає з вихідної позиції теорії та практики моделювання підприємства й бізнес-процесів, зокрема процесного підходу до подання діяльності. Запропоновано метод установлення однозначної відповідності (подібності) архітектур функціонального, організаційного та інформаційного подань підприємства.

Ключові слова: *система; подання; подібності; подання інформації; функціональне подання.*

Проанализированы методы моделирования деятельности предприятия. Показано, что в настоящее время нет единого общепризнанного метода моде-

лирования деятельности предприятия. А это, в свою очередь, препятствует разработке единого инструментария для его моделирования. Это обстоятельство следует из исходной позиции теории и практики моделирования предприятия и бизнес-процессов, а именно процессного подхода к представлению деятельности. Предложен метод установления однозначного соответствия (подобия) архитектур функционального, организационного и информационного представлений предприятия.

Ключевые слова: *система; представление; сходства; представление информации; функциональное представление.*

Problem formulation. Any modern enterprise is considered to be a complex system, the studying of which has to be done using the appropriate business models. So occurs the task of forming an integrated representation of the enterprise on the basis of relevant models.

According to the international standard ISO 19439 [1] next terms for the following models of representation of enterprises were defined:

- 3.32 *function view*: enterprise model view that enables the representation and modification of the processes of the enterprise, their functionalities, behaviors, inputs and outputs;
- 3.40 *information view*: enterprise model view that enables the representation and modification of the enterprise information as identified in the function view;
- 3.52 *organization view*: enterprise model view that enables the representation and modification of the organizational and decisional structure of the enterprise and the responsibilities and authorities of the individuals and organizational units within the enterprise;
- 3.61 *resource view*: enterprise model view that enables the representation and modification of enterprise resources.

But this standard doesn't cover requirements for formulating models according to defined views. Also the task of integrating these representations of enterprise models is not covered. In this case, under integration you can understand the formation of an integrated modeling environment. Therefore, there is the task of studying the methodologies for the formation of these models of enterprise representation. An important issue is finding answer to the question: is there an internal link between the models or not?

For example, the definition of information representation tells us that this representation "allows you to represent and change the information about an enterprise identified in a functional representation". It means that the information is identified in a functional representation and then presented in an information representation. It follows that these two representations must be connected. So next question appears: in what form this link is realized?

Analysis of recent researches and publication. In article [2] was presented an analysis of existing tools for modeling business processes with the use of information technology, and their comparative characteristics. A. M. Vendrov mentioned [2]:

"The main area of application of business models is the reengineering of business processes. It provides the construction of models of current and future activities, as well as the plan and program of transition from the one state to another. Any modern enterprise is a complex system, its activities include performing tens of thousands of functions that mutually influence each other and operations. Man is not able to understand how such a system functions in detail – it goes beyond capabilities. Therefore, the main idea of creating so-called "AS-IS" models (as it is) and "AS-TO-BE" (as it should be) is to understand what the enterprise is doing (and will be doing) and how it is operating (and will be operating) to achieve its goals".

The most known are next models of business processes:

– function analysis method **SADT** (Structured Analysis and Design Technique), that was formalized and published as IDEF0 in 1981 [3];

– method for process modelling **IDEF3**. The IDEF3 method is a scenario-driven process flow description capture method intended to capture the knowledge about how a particular system works [4];

– data flow model also known as **DFD** (Data Flow Diagram) [5];

– method **ARIS** (ARchitecture of integrated Information Systems) [6];

– Ericsson Penker extension of UML (Unified Modelling Language);

– modelling method used in **RUP** (Rational Unified Process) [7].

For business processes modelling next perspective research is being carried out:

Project UEML (Unified Enterprise Modelling Language) [8]. The basis for the project are the models of GERAM (Generalized Enterprise Reference Architecture and Methodology) and Zakhman.

The OMG project is a consortium of software developers and users representing various commercial, government and academic organizations with a total of 800 participants [9]. The work of OMG in the field of business process modeling relates mainly to the concept of Model Driven Architecture (MDA) [10]. According to [11]:

"MDA also known as Model Driven Architecture. This is an architecture that describes a new way of software development. As it is flows from the model name within the framework of this architecture the creation of applications is based on the development of a program model. The obvious advantages of this approach are:

– independence of the model from the development tools provides the possibility of implementation on any software platform;

– an application implemented in the MDA architecture can be easily migrated from one operating system to another;

– significant savings in resources while implementing the program on several software platforms simultaneously;

– the architecture allows some kind of automation for the programming process".

In [12] mentioned:

"In fact, the development of enterprise architecture can solve one of the significant problems of interaction between business and IT, which has the name "alignment" that means synchronizing the capabilities and needs of business and IT... Thus, the use of information technology to solve business problems occurs through the following processes, which, as usual, go parallel way:

– modeling of information (development of the information architecture), which ensures the execution of business processes of organization (meeting existing information requirements);

– formation of a portfolio of application systems (definition of the architecture of applications), which process this information in accordance with some functional requirements;

– construction of infrastructure (technological architecture forming), which provides the work of application systems at the level described in the operational requirements (reliability, scalability, etc.)".

From the above review of the latest research and publications, the task of integrating the enterprise with the means of information technology is relevant and at present time number of projects are being implemented it.

However, it should be noted that the determining factor in the formation of the investigated methodologies is the approach in the form of representations of the enterprise "AS-IS".

At the same time, various forms of representation for an existing enterprise are formed on the basis of consideration of its activities from different points of view.

On the other hand, the question arises whether there is at least one of the views defined in ISO 19439, which can be recognized as an ideal, independent of the forms of activity of any enterprise? That is realization of the concept "AS-TO-BE".

After all, if such a representation exists, then there is a problem of matching between this representation and other representations, as it is supposed, for example, in the ARIS method.

In work [13] was performed a comparison of the functional representations of human activity architectures on the basis of the functional system architecture, in accordance with the theory of functional systems of academician P. K. Anokhin and the architecture of the functional representation of the control system for a certain stratum of control parameters according to M. Yu. Melzer's theory of dialogue management [14]. Their similarity has been proved, which ensured the establishment of an ideal architecture for the functional representation of the enterprise.

On the basis of this model, in work [15] was performed a comparison of the functional representation architecture of the enterprise and the architecture of its organizational representation. On the basis of the fact that the functions defined in the functional representation of the enterprise are realized by specialists who are part of the respective functional units of the enterprise, similarity is established between these representations. In this case, the architecture of a functional representation is recognized as the primary in relation to the architecture of the organizational representation.

So, the problem of determination the level of relations between the functional representation of the enterprise and information representations on the one hand, and organizational representation and information on the other arises. At the same time, two approaches to solving the problem should be considered: on the basis of the principles of physiological cybernetics and on the basis of the principles of technical cybernetics.

Purpose of the article is to determine the level of relations between the functional representation of the enterprise and information representations on the one hand, and organizational representation and information on the other.

Main material. From the above it follows that the solution of the set of tasks is possible by analyzing the functional view and identifying on its basis the information view on the basis of the principles of technical cybernetics, or by analyzing an organizational view that is similar to the functional in accordance with the principles of physiological cybernetics and the identification on its basis the information view.

Unfortunately, the theory of functional systems, like physiological cybernetics, develops independently from the theory of information systems, which is part of technical cybernetics.

In order to establish correspondence between functional and informational views in terms of technical cybernetics, one must first consider the method of SADT functional simulation, as well as the method of modeling DFD data flows.

A. M. Vendrov characterizes the method of functional modeling in the following way [*2*, 9]:

“The SADT method is most suitable for describing the top level management processes. Its main advantages are as follows: ...the completeness of the description of the business process (management, information and material flows, feedback)”.

In this methodology, information flows link the corresponding functions (functional blocks) among themselves. In this case, the functional model in the form of the IDEF0 diagram only displays the information links between the functional blocks. In this presentation there are no important elements of the company’s information view: sources of data and sources of knowledge, which are the basis for the formation of relevant databases and knowledge bases of information

management systems of the enterprise. Also the task of forming an ideal architecture of a functional representation of activity, that is, in the form of "AS-TO-BE", is not covered.

According to [*2*, 13] method of data flow modeling DFD:

"...is defined as a hierarchy of diagrams of data streams describing the asynchronous process of transforming information from its introduction to the system to the consumer. Sources of information (external entities) generate information flows (data streams) that transfer information to subsystems or processes. Those, in turn, transform information and generate new streams that transfer information to other processes or subsystems, data stores or external entities-consumers of information".

According to this methodology, "sources of information generate information flows that transfer information to subsystems or processes". That is, the specified flows in this approach are recognized as dependent on the functional representation of the activity and are determined by the architecture of the system of processes and subsystems, as well as the presence in this architecture of processes and subsystems of data drives. This methodology corresponds to the SADT methodology of functional modeling, since it is based on a process approach to enterprise performance representation.

This methodology does not imply the establishment of an ideal information representation architecture in the form of "AS-TO-BE". Instead, the principle of forming an information representation architecture in the form of "AS-IS" is implemented. Consequently, the functional view of the enterprise and its corresponding presentation in the form of data flow diagrams will always be unique for each enterprise.

A similar situation arises when applying the ARIS modeling method [*2*, 19]:

"The ARIS modeling method is based on Professor August-Wilhelm Scheer's theory of integrated IC construction, which defines the principles of visual representation of all aspects of the operation of the analyzed companies. ARIS supports four types of models that reflect different aspects of the researched system: organizational models...; functional models...; information models...; management models... The ARIS method allows you to describe the organization's activities from different points of view and establish relationships between different models. However, such an approach is difficult to implement in practice, as it entails a high cost of resources (human and financial) for a long time. In addition, the ARIS tool environment is expensive and difficult to use".

In this method of enterprise integration it is possible to "establish connections bet-ween different models"; however, the task of forming at least one representation in the form of "AS-TO-BE" – the ideal representation – is not covered.

It follows that in the theory of information systems (technical cybernetics) at this time there are different approaches for modeling the enterprise in the form of different views. The task is to integrate these views in two ways:

– establishing links between different model representations (ARIS method);

– formation of an integrated modeling environment for specific forms of business representation (ISO 19439).

On the other hand, in the theory of physiological cybernetic systems on the basis of the theory of functional systems, the architectonics of a functional system, that does not depend on the level of organization of the organism, is proposed. In [13] it is proved that the specified architecture is similar to the architecture of the control system for human machine (automated) systems. At the same time, the architecture of the control system for the strategy of control parameters is similar for all five control parameters that are formed in the hierarchical production management system.

Proving the similarity of the architecture of functional and organizational views [15] allows us to proceed to the solution of the similarity problem between the functional and informational views, as well as organizational and informational views.

The functions defined in the functional view carry out the transformation of the information coming into the functional blocks, that is, it is possible to establish the form and content of the input and output information for each functional block. However, the functions implementation involves the transformation of information. This aspect in the functional representation is not disclosed. It can only identify data sources. Therefore, it is possible to develop a method for modeling DFD data flows. In the functional representation in the explicit form there are no sources of information and knowledge. So it is not possible to establish a correspondence between the functional and informational representation.

While considering the architecture of an organizational view, which is similar to the functional representation architecture, there is another situation. Fig. 1 shows the proposed organizational structure of the enterprise [15]. The structure of the organizational representation architecture includes the units responsible for implementing the corresponding functions according to the architecture of the functional view. It is clear that these divisions are generally sources of data, information and knowledge. Depending on this, in the architecture of the information view of the enterprise activity, it is necessary to provide appropriate data storage, information and knowledge in the form of the appropriate databases.

In the proposed architecture of the information view of the enterprise activities, sources of data, information and knowledge have been identified. They are specialists of the relevant units. On the basis of their knowledge, conceptual models of the corresponding subject areas are formed. At the same time, the data are formed into relevant databases using known database management systems. Knowledge, as a rule, is presented in the form of expert systems. Fig. 2 proposes the creation of a knowledge base in the form of an automated workstations.

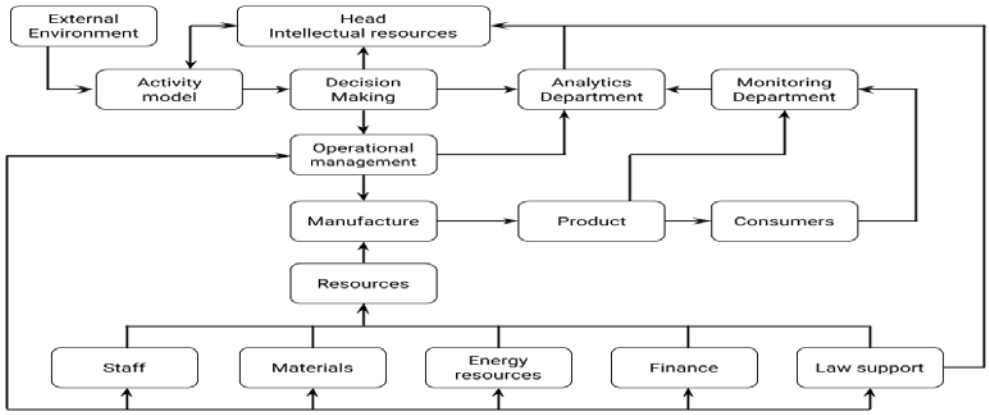


Fig. 1. Organizational structure of the enterprise

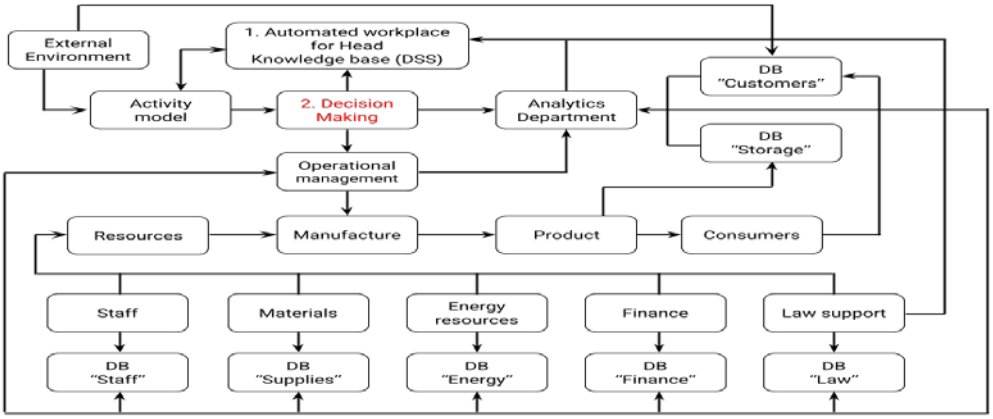


Fig. 2. Architecture of information ensuring of the enterprise

According to the proposed architecture of the information view, the main consumer of data is “Analytics Department”. In accordance with the architecture of functional representation, based on the theory of functional systems, this department implements the function of ensuring the correspondence of the obtained result and the established goals. In this department operative decisions are made to adjust the activity in case of obstacles on the way to achieving the goal of activity.

Fig. 2 shows the architecture of the information view, which corresponds to the architecture of the organizational structure of the enterprise.

From the foregoing we can make a conclusion that there is a similarity between the functional and informational views at the data source level.

In an explicit form, the sources of information and knowledge in the functional view are not identified. Their identification is possible only in organizational view.

It should be noted that the task of unambiguous definition of the content of the concepts of “data” and “information” needs separate consideration.

Thus, the problem of establishing unambiguous correspondence (similarity) of the architectures of the functional, organizational and information views of the enterprise is solved. This allows you to offer a model architecture for the specified views for any enterprise.

Conclusions and further researches directions. From the analysis of the modeling techniques of the enterprise, it follows that at this time there is no single universal method of modeling the enterprise. And this, in turn, prevents the development of a single toolkit for its simulation. This circumstance stems from the original position of the theory and practice of enterprise modeling and business processes, in particular form the process approach to the presentation of activities. Since the result of the process always depends on the management and used resources, it is always unique. Therefore, the model of any process will always be unique.

Unambiguousness can only be realized if the result of the process will always be the same, that is, independent of the resources used, external conditions and control actions.

From the made review of the methods of forming the architectures of views of the activities of enterprises follows:

1. The architecture of the functional view of the enterprise activity is isomorphic for all levels of organization of the enterprise.

2. The architecture of the functional view of the enterprise activity is primary in relation to the organizational view architecture.

3. The architecture of the functional view of the enterprise is the basis for the development of a similar organizational architecture to it.

4. The architecture of the organizational view of the enterprise’s activity is isomorphic for any enterprise, since the architecture of the functional view of that activity is also isomorphic.

5. The architecture of the organizational view of the enterprise is the basis for the development of an information view’s architecture similar to it.

6. The architecture of the information view in general should include three levels of representation: the data level; the level of information; the level of knowledge.

List of sources used:

1. ISO 19439:2006 Enterprise integration – Framework for enterprise modeling (IDT). URL: https://www.iso.org/standard/33833.html

2. *Ведров А. М.* Методы и средства регулирования бизнес-процессов (обзор) // Jet Info: информационный бюллетень. 2004. № 10(137). 32 с.

3. *Черемных С. В., Семенов И. О., Ручкин В. С.* Структурный анализ систем. IDEF-технологии. Москва: Финансы и статистика, 2003. 157 р.

4. *Бистерфельд О. А.* Моделирование бизнес-процессов с использованием методологии IDEF3: учебно-методическое пособие/ РГУ им. С. А. Есенина. Рязань: РГУ, 2008. 44 с.

5. *Калашян А. Н., Калянов Г. Н.* Структурные модели бизнеса/ под ред. А. Н. Калашян. Москва: Финансы и статистика, 2003. 256 с.

6. *Шматалюк А., Ферапонтов М., Громов А., Каменнова М.* Моделирование бизнеса. Методология ARIS. Москва: Весть-Метатехнология, 2001. 333 с.

7. *Крачтен Ф.* Введение в Rational Unified Process. Москва: Вильямс, 2002, 297 с.

8. Report on the State of the Art in Enterprise Modeling. Project UEML: Unified Enterprise Modeling Language. September 27th 2002. URL: http://www.ueml.org

9. Business Process Definition Metamodel. Request For Proposal. OMG Document: bei/200301. URL: http://www.omg.org

10. *Кузнецов М.* MDA – новая концепция интеграции приложений место в ИТ // Открытые системы. СУБД. 2003. № 9. URL: http://www.osp.ru/os/2003/09/183391

11. *Марков Е.* Архитектура, управляемая моделью. URL: http://rudocs.exdat.
com/docs/index-215822.html?page=12

12. *Данилин А. В., Слюсаренко А. И.* Лекция 3: Архитектура предприятия: основные определения. Москва: Национальный Открытый Университет ИНТУИТ, 2016. URL: http://rudocs.exdat.com/docs/index-215822.html?page=6

13. *Доценко С. І.* Архітектоніка функціональної системи як елемент організації діяльності в загальній теорії підприємства // Вісник Національного технічного університету "ХПІ": збірник наукових праць. Серія: Технічний прогрес та ефективність виробництва. Харків: НТУ "ХПІ". 2013. № 44(1017). С. 41–48.

14. *Мельцер М. И.* Диалоговое управление производством (модели и алгоритмы). Москва: Финансы и статистика. 1983. 240 с.

15. *Доценко С. І., Савенко В. І.* Теоретичне обґрунтування ізоморфізму організаційної структури підприємства // Енергетика та комп'ютерно-інтегровані технології в АПК. Харків: ХНТУСГ. 2017. № 1 (6). С. 43–47.

References:

1. ISO 19439:2006 Enterprise integration – Framework for enterprise modeling (IDT).

2. Vendrov A. M. (2004), *Metody i sredstva modelirovaniya biznes-protsessov (obzor)* [Methods and tools for modeling business processes (overview)] // *Jet Info Informatsionnyi bolleten'* [Jet Info Information talk], vol 10 (137), 32 p. [Russia].

3. Cheremnykh S. V., Semenov I. O. and Ruchkin V. S. (2003), *Strukturnyi analiz sistem: IDEFtekhnologii* [Structural Systems Analysis: IDEF Technology], press *Finansy i statistika* [Finance and Statistics], Moscow, 208 p. [Russia].

4.Bisterfel'd O. A. (2008), *Modelirovanie biznes-protsessov s ispol'zovaniem metodologii IDEF3 : uchebno-metodicheskoe posobie* [Modeling

business processes using the IDEF3 methodology: a training manual], press Ryaz. gos. un-t im. S. A. Esenina, Ryazan', 44 p. [Russia].

5. Kalashyan A. N. (2003), *Strukturnye modeli biznesa: DFD tekhnologi* [Structural business models: DFD technology], press *Finansy i statistika* [Finance and Statistics], Moscow, 256 p. [Russia].

6. Kamennova M., Gromov A., Ferapontov M. and Shmatalyuk A. (2001), *Modelirovanie biznesa. Metodologiya ARIS* [Business modeling. ARIS Methodology], press Vest' Metatekhnologiya, Moscow, 327 p. [Russia].

7. Krachten F. (2002), *Vvedenie v Rational Unified Process* [Introduction to the Rational Unified Process], press Vil'yams, Moscow, 240 p. [Russia].

8. UEML (2002), Report on the State of the Art in Enterprise Modeling. Project UEML: Unified Enterprise Modeling Language, September 27th, available at: http://www.ueml.org (accessed 01.01.2019).

9. Business Process Definition Metamodel. Request For Proposal. OMG Document: bei/200301, available at: http://www.omg.org (accessed 01.01.2019).

10. Kuznetsov M. (2003), *"MDA – novaya kontseptsiya integratsii prilozhenii"* ["MDA is a new application integration concept"], *Otkrytye sistemy* [Open systems], vol. 9 [Russia].

11. Markov E. (2011), *Arkhitektura, upravlyaemaya model'yu* [Model Driven Architecture], available at: http://rudocs.exdat.com/docs/index-215822.html?page=12 (accessed 01.01.2019) [Russia].

12. Danilin A. V. and Slyusarenko A. I., *Lektsiya 3: Arkhitektura predpriyatiya: osnovnye opredeleniya* [Lecture 3: Enterprise Architecture: Basic Definitions], available at: http://rudocs.exdat.com/docs/index-215822.html?page=6 (accessed 01.01.2019) [Russia]

13. Dotsenko S. I. (2013), *"Arkhitektonika funktsional'noyi systemy yak element orhanizatsiyi diyal'nosti v zahal'niy teoriyi pidpryyemstva"* ["Architectonics of the functional system as an element of organization of activity in the general theory of the enterprise"]. *Visnyk Natsional'noho tekhnichnoho universytetu "KhPI". Zbirnyk naukovykh prats'. Seriya: Tekhnichnyy prohres ta efektyvnist' vyrobnytstva* [Bulletin of the National Technical University "KhPI". Collection of scientific works. Series: Technical progress and production efficiency], press NTU "KhPI", Kharkiv, vol. 44 (1017), 166 p., – pp. 41–48 [Ukraine].

14. Mel'tser M. Y. (1983), *Dyalohovoe upravlenye proyzvodstvom (modely i alhoritmy)* [Interactive production management (models and algorithms)], press Finansy i statistika, Moscow, 240 p. [Russia].

15. Dotsenko S. I. and Savenko V. I. (2017), *"Teoretychne obgruntuvannya izomorfizmu orhanizatsiynoyi struktury pidpryyemstva"* ["Theoretical substantiation of the isomorphism of the organizational structure of the enterprise"] *Enerhetyka ta komp'yuterno-intehrovani tekhnolohiyi v APK* [Power engineering and computer-integrated technologies in the agroindustrial complex], press KhNTUSH, Kharkiv, vol. 1 (6), pp. 43–47 [Ukraine].

DOI: https://doi.org/10.32836/2521-6643-2019-1-57-4
УДК 004.942 + 621.398

Б. Ю. Волочій, доктор технічних наук, професор кафедри теоретичної радіотехніки та радіовимірювань Національного університету "Львівська політехніка"
М. М. Змисний, кандидат технічних наук, старший викладач кафедри теоретичної радіотехніки та радіовимірювань Національного університету "Львівська політехніка"
В. А. Онищенко, кандидат технічних наук, провідний науковий співробітник Наукового центру Академії сухопутних військ імені Петра Сагайдачного
Ю. П. Сальник, кандидат технічних наук, заступник начальника наукового центру Академії сухопутних військ імені Петра Сагайдачного
О. П. Шкілюк, кандидат технічних наук, асистент кафедри теоретичної радіотехніки та радіовимірювань Національного університету "Львівська політехніка"

ОЦІНКА МОЖЛИВОСТЕЙ КОМПЛЕКСУ ОХОРОННОЇ СИГНАЛІЗАЦІЇ З РІЗНОЮ КІЛЬКІСТЮ СЕЙСМІЧНИХ ДАТЧИКІВ БІЛЯ ЗОНИ КОНТРОЛЮ

Ефективність комплексів охоронної сигналізації, якщо важлива достовірність класифікації рухомих об'єктів, оцінюється такими показниками: ймовірність виконання завдання; ймовірність часткового виконання завдання; ймовірність "обману" оператора; ймовірність невиконання завдання. Відповідно, показники ефективності комплексів охоронної сигналізації, залежать від показників функціональності його складових: ймовірнос-

ті фіксації рухомого об'єкта сейсмічним датчиком, ймовірності правильної класифікації типу рухомого об'єкта та ймовірності приймання радіосигналу системою приймання та відображення інформації. В статті описується дискретно-неперервна стохастична модель реакції комплек-су охоронної сигналізації на перетин рухомим об'єктом зони контролю, біля якої встановлено три сейсмічні датчики. На приймальній стороні комплексу використано мажоритарний принцип прийняття рішення про тип рухомого об'єкта. Здійснено порівняльний аналіз ефективності комплексів охоронної сигналізації з установленням одного, двох або трьох сейсмічних датчиків біля зони контролю.

Ключові слова: *сейсмічний датчик; комплекс охоронної сигналізації.*

Эффективность комплексов охранной сигнализации, когда важна достоверность классификации подвижных объектов, оценивается следующими показателями: вероятность выполнения задания; вероятность частичного выполнения задания; вероятность "обмана" оператора; вероятность невыполнения задачи. Соответственно, показатели эффективности комплексов охранной сигнализации зависят от показателей функциональности его составляющих: вероятности фиксации движущегося объекта сейсмическим датчиком, вероятности правильной классификации типа подвижного объекта и вероятности принятия радиосигнала системой приема и отображения информации. В статье описывается дискретно-непрерывная стохастическая модель реакции комплекса охранной сигнализации на пересечение движущимся объектом зоны контроля, возле которой установлены три сейсмических датчика. На приемной стороне комплекса использовано мажоритарный принцип принятия решения о типе подвижного объекта. Осуществлен сравнительный анализ эффективности комплексов охранной сигнализации с установлением одного, двух или трех сейсмических датчиков у зоны контроля.

Ключевые слова: *сейсмический датчик; комплекс охранной сигнализации.*

The efficiency of guard signaling complexes (GSC), when a validity of classification of moving objects (MO) is very important, is evaluated by the following indexes: probability of GSC task execution; probability of partial execution of the task; probability of user's "deception". Accordingly, the performance indicators of the GSC, in turn, depend on the indexes of the functionality of its constituents: probability of fixation of moving object by seismic sensor, probability of correct classification of MO type and probability of receiving radio signal by the system of receiving and displaying information (RDI).

The discrete-continuous stochastic model of GSC reaction to moving object which crosses control zone, where three seismic sensors are installed, was developed. Majority principle of identifying the type of moving object was used in the receiver of GSC. A comparative analysis of the efficiency of guard signaling complexes using one, two and three sensors in control zone are carried out.

The GSC reaction is described by these procedures:

Procedure 1 – detecting of moving object by seismic sensor. A moving object may be detected or not detected, however, the autonomous system of detection, object classification and transmitting radio signals with seismic sensors in control zone, is workable. A moving object may not be detected in the following cases: it passed a seismic sensor at a safe distance; a moving object used special equipment that cannot be detected or was wearing special uniform; unsuitable place of seismic sensor location.

Procedure 2 – classification of moving object. Alternative events are inherent in classification procedure, so can be performed correctly or incorrectly. The error in classification may be caused by corrupted method of processing seismic signal in autonomous system of detection, object classification and transmitting radio signals. Message with the result of MO classification is transmitted.

Procedure 3 – delivering message with information about MO to system of RDI. The process of delivering radio signal about MO may be successful or not. Failure of message delivery to RDI may be caused by conditions of radio-wave transmission, presence of radio interference of natural and enemy-caused character.

Procedure 4 – taking decision about type of moving object in RDI using majority principle 2 out of 3.

In the model of GSC reaction to MO control zone crossing it is taken into account the that a message about MO from different seismic sensors comes to SRDI not at the same time. That is why the process of forming states of majority element, where a corresponding decision is formed, has certain duration.

A comparative analysis of the effectiveness of guard signaling complexes using one, two and three sensors in control zone are carried out.

Key words: *seismic sensor; guard signaling complex.*

Постановка проблеми. На етапі системотехнічного проектування комплексу охоронної сигналізації (КОС) необхідно провести дослідження ефективності його застосування з різними варіантами його реалізації. Відповідно до результатів дослідження треба сформувати вимоги до складових КОС. Проектований КОС повинен: виконувати фіксацію рухомих об’єктів (РО) сейсмічним датчиком, за сейсмічними сигналами здійснювати класифікацію типів РО та передавати повідомлення через радіоканал від автоном-

них систем виявлення, класифікацію об’єктів і передавання радіосигналів (ВКОПР) до системи приймання і відображення інформації (СПВІ).

У практиці проектування КОС широко застосовується використання сейсмічних датчиків (СД) [1; 2]. Основні переваги використання СД: експлуатаційні умови передбачають приховане розміщення СД у ґрунті; принцип фіксації рухомих об’єктів СД пасивний, бо не передбачає випромінення енергії в навколишнє середовище тощо [3; 4].

Ефективність КОС (рис. 1) оцінюється такими показниками ефективності: ймовірність виконання завдання системою; ймовірність часткового виконання завдання системою; ймовірність “обману” оператора; ймовірність невиконання завдання КОС. Вищезгадані показники ефективності КОС так само залежать від значень показників функціональності його складових: імовірності фіксації рухомого об’єкта СД, імовірності правильної класифікації типу РО та ймовірності приймання радіосигналу системою приймання та відображення інформації. Під “виконанням завдання” розуміємо подію, коли РО перебуває в зоні контролю і оператор КОС отримує повідомлення про РО. Часткове виконання завдання властиве КОС зі встановленням двох або трьох СД. Під частковим виконанням завдання розуміємо подію, коли РО перебуває в зоні контролю, а схема збігу або мажоритарний елемент не видають (оператор не отримує) будь-яке повідомлення (правильне чи неправильне). Скажімо, у СПВІ надійшло одне повідомлення з правильним або неправильним визначенням типу РО. Під “обманом” користувача розуміємо подію, коли РО перебуває в зоні контролю, а схема збігу або мажоритарний елемент формують (оператор КОС отримує) повідомлення з неправильно визначеним типом РО. Під “невиконанням завдання” розуміємо подію, коли РО перебуває в зоні контролю, а до СПВІ не надійшли повідомлення від жодного СД. У всіх випадках повідомлення про РО доставляється оператору з певною ймовірністю. Ефективність комплексу охоронної сигналізації зі встановленням одного і двох СД біля зони контролю досліджена в попередніх працях [5–7].

Для проведення порівняльних досліджень необхідно розробити модель реакції КОС на перетин РО зони контролю з розміщеннями в ній трьох сейсмічних датчиків. Для підвищення достовірності класифікації РО запропоновано використати на приймальній стороні КОС мажоритарний принцип “2 із 3” прийняття рішення про тип РО [8, 9]. Таким чином, актуальним є завдання розроблення моделі реакції КОС на перетин рухомим об’єктом зони контролю з розміщеннями біля неї трьох сейсмічних датчиків. Розроблена модель дасть можливість провести дослідження ефективності КОС від чутливості сейсмічного датчика (ймовірність фіксації РО), від ефективності методу класифікації (ймовірність правильної класифікації) та від ефектив-

ності системи передавання радіосигналів (ймовірність отримання радіосигналу). Крім цього, розроблена модель дасть можливість підтвердити очікувану перевагу КОС із використанням мажоритарного принципу прийняття рішення про тип РО. Отже, об'єктом дослідження є реакція КОС на перетин РО зони контролю, біля якої встановлено три СД.

Рис. 1. Показники ефективності комплексу охоронної сигналізації та показники функціональності його складових

Складне завдання розроблення методу класифікації РО з використанням сигналів від сейсмічних датчиків. Тому необхідно шукати такі принципи побудови КОС (технічні рішення), щоб знизити вимоги до методу класифікації (до значення показника функціональності методу класифікації).

У зв'язку із цим порушуються два питання. Наскільки можна знизити значення показника функціональності методу класифікації, якщо:

1) замість одного СД установлювати біля зони контролю два СД і на приймальній стороні використати схему збігу для прийняття рішення про тип РО;

2) замість двох СД установлювати біля зони контролю три СД й на приймальній стороні використати мажоритарний принцип прийняття рішення про тип РО за правилом голосування "2 із 3"?

Експериментальні дослідження проведено методом комп'ютерного моделювання з використанням програмного засобу ASNA [10, 109–121] і

формалізованого представлення об’єкта дослідження у вигляді структурно-автоматної моделі [11]. Програмний засіб ASNA виконує такі функції:

1) на основі структурно-автоматної моделі здійснює побудову моделі об’єкта дослідження у вигляді графа станів і переходів;

2) на основі графа станів здійснює формування системи диференціальних рівнянь Колмогорова – Чепмена; результатом розв’язання системи диференціальних рівнянь є розподіл імовірностей перебування в станах;

3) з урахуванням необхідних станів визначає показники надійності, функціональності та ефективності об’єкта дослідження.

Мета статті – здійснити порівняльний аналіз ефективності КОС з використанням одного, двох або трьох СД. Для цього необхідно здійснити розроблення структурно-автоматної моделі реакції КОС на перетин РО зони контролю з використанням трьох СД та мажоритарного принципу прийняття рішення про тип РО за правилом голосування “2 із 3” на приймальній стороні. Структурно-автоматні моделі реакції КОС із встановленням у зоні контролю одного і двох СД розроблені авторами подані в [5; 6; 12].

Виклад основного матеріалу. *1. Реакція комплексу охоронної сигналізації на перетин рухомим об’єктом зони контролю, коли біля неї встановлено три сейсмічні датчики*

До складу КОС входять: система приймання і відображення інформації та три СД з автономними системами ВКОПР. Структурну схему КОС подано на рис. 2. До системи приймання й відображення інформації для прийняття рішення про правильність класифікації типу РО включено (введено) й використано програмно-апаратний модуль, у якому реалізовано мажоритарний принцип прийняття рішення з правилом голосування “2 із 3”. Реакцію КОС на перетин РО зони контролю подано таким чином. Рухомий об’єкт пересувається через зону контролю. Навколо зони контролю розташовані три СД (СД1, СД2, СД3), які мають фіксувати появу РО в зоні контролю. Зокрема, кожен із СД з певною ймовірністю може зафіксувати або не зафіксувати РО. Тобто на РО можуть зреагувати всі три СД, або тільки два СД, або тільки один СД. Не виключається ситуація, коли пересування РО може бути не зафіксовано жодним СД. Це обумовлюється кількома чинниками, такими як різна відстань проходження РО від СД, станом ґрунту, способом пересування РО. Після того, як СД відреагував на РО, його автономна система ВКОПР виконує завдання класифікації РО. Класифікація може бути правильною або неправильною. Після здійснення класифікації передавач автономної системи відправляє повідомлення про РО до СПВІ. Проте повідомлення може бути доставлено або не доставлено. Слід зазначити, що мажоритарний елемент зможе видати правильне повідомлення про тип РО тільки тоді, коли надійдуть сигнали з правильною класифікацією або від

трьох, або від двох автономних систем ВКОПР. Якщо сигнал від одного СД не надходить, а два інших сигнали надходять з правильною і неправильною класифікацією РО, то в СПВІ формується повідомлення “тип РО не визначено”.

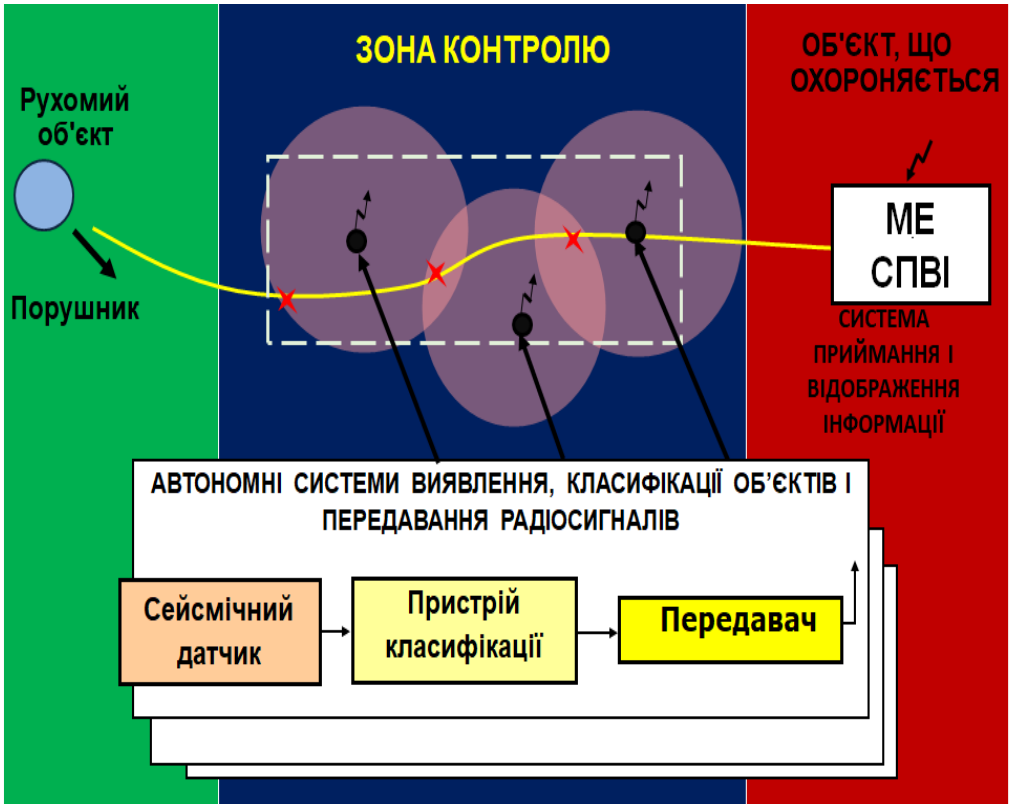


Рис. 2. Розміщення трьох сейсмодатчиків у зоні контролю біля маршруту пересування РО і структура автономної системи ВКОПР для кожного з них

У розробленій моделі враховано такі процедури, які формують поведінку КОС у процесі перетину РО зони контролю.

Процедура 1. Фіксація сейсмічним датчиком рухомого об’єкта.

Рухомий об’єкт може бути зафіксований або не зафіксований СД, при цьому автономна система ВКОПР із СД, установлена в зоні контролю, технічно справна і готова до роботи.

Рухомий об’єкт може бути не зафіксованим СД у таких випадках: РО пройшов на безпечній відстані від СД, РО використовував спеціальне обладнання проти виявлення або був одягнений у спеціальну форму, специфічне (невдале) місце розташування СД.

Процедура 2. Класифікація рухомого об’єкта.

Процедурі класифікації властиві альтернативні події, тобто вона може бути виконана правильно або неправильно. Помилка в класифікації РО може бути через недосконаліть методу оброблення сейсмічного сигналу в автономній системі ВКОПР. Повідомлення з результатом класифікації РО передається до системи передавання радіосигналів.

Процедура 3. Доставлення радіосигналів з інформацією про рухомий об’єкт до системи приймання та відображення повідомлення.

Процедура доставлення радіосигналу про РО може бути або успішною або ні. Недоставлення повідомлення про РО в СПВІ може бути спричинено умовами поширення радіохвиль, наявністю радіозавад природного й техногенного характеру.

Процедура 4. Прийняття в системі приймання та відображення інформації рішення про тип рухомого об’єкта з використанням мажоритарного принципу.

Правильне рішення у СПВІ приймається в таких ситуаціях:

1. Коли на мажоритарний елемент (МЕ) надійшли сигнали від усіх трьох СД, при цьому РО був правильно класифікований.

2. На МЕ надійшли сигнали з правильною класифікацією з першого та другого СД. Третій СД або не зафіксував РО, або від нього не доставлено повідомлення з правильною класифікацією, або доставлено повідомлення з неправильною класифікацією.

3. На МЕ надійшли сигнали з правильною класифікацією від першого та третього СД. Із сигналом від другого СД трапилися ситуації, описані у пункті 2.

4. На МЕ надійшли сигнали з правильною класифікацією від другого та третього СД. Із сигналом від першого СД трапилися ситуації, описані у пункті 2.

2. Розроблення структурно-автоматної моделі реакції комплексу охоронної сигналізації на перетин рухомим об’єктом зони контролю

Для розроблення структурно-автоматної моделі [13] реакції КОС на перетин РО зони контролю необхідно здійснити розроблення опорного графа станів та переходів [14]. Для розроблення опорного графа необхідно насамперед обрати актуальні показники функціональності складових КОС та визначити базові події, які представляють усі процеси й процедури, закладені в алгоритм її поведінки, а також показати зовнішні і внутрішні процеси, з якими взаємодіє кожен канал КОС протягом часу виконання завдання. Необхідно також обґрунтувати компоненти вектора стану, який представлятиме зміну станів у реакції КОС.

Таблиця 1

Пари подій, які фіксують початок і закінчення процедур, що формують реакцію КОС на перетин РО зони контролю

№ з/п	Подія-початок	Подія-закінчення	Середні значення тривалостей процедур
1	Початок перебування РО в зоні контролю	Подія 1: фіксація РО першим СД	T_{f1}
2	Початок процедури класифікації РО, зафіксованого першим СД	Подія 2: закінчення процедури класифікації РО, зафіксованого першим СД	$t_c << T_{f1}$
3	Початок процедури доставлення повідомлення про РО, зафіксованого першим СД	Подія 3: закінчення процедури доставлення повідомлення про РО, зафіксованого першим СД	$t_d << T_{f1}$
4	Момент фіксації РО першим СД	Подія 4: фіксація РО другим СД	T_{f2}
5	Початок процедури класифікації РО, зафіксованого другим СД	Подія 5: закінчення процедури класифікації РО, зафіксованого другим СД	$t_c << T_{f2}$
6	Початок процедури доставлення повідомлення про РО, зафіксованого другим СД	Подія 6: закінчення процедури доставлення повідомлення про РО, зафіксованого другим СД	$t_d << T_{f2}$
7	Момент фіксації РО другим СД	Подія 7: фіксація РО третім СД	T_{f3}
6	Початок процедури класифікації РО, зафіксованого третім СД	Подія 8: закінчення процедури класифікації РО, зафіксованого третім СД	$t_c << T_{f3}$
7	Початок процедури доставлення повідомлення про РО, зафіксованого третім СД	Подія 9: закінчення процедури доставлення повідомлення про РО, зафіксованого третім СД	$t_d << T_{f3}$
8	Початок процедури прийняття рішення мажоритарним елементом	Подія 10: Закінчення процедури прийняття рішення мажоритарним елементом	$t_{me} << T_{f1}+T_{f2}+T_{f3}$

2.1. Визначення базових подій

Згідно з процедурами, які виконуються в КОС, складаємо перелік подій. Події потрібно відображати попарно, фіксуючи початок і закінчення відповідної процедури (табл. 1). Події, що відповідають закінченню процедур, є базовими подіями для розроблення моделі.

Оскільки тривалості процедур: класифікації РО t_c та доставлення повідомлення про РО t_d є значно меншими від тривалості перебування РО в зоні контролю T_{f1}, T_{f2}, T_{f3}, то в моделі їх значення прийнято рівними нулю. Тому далі події 1, 4, 7 вважатимуться базовими, а події 2, 3, 5, 6, 8, 9, 10 зведеними до них відповідно. Виходячи із цього, під час розроблення САМ використано такі базові події:

- Базова подія 1 "Фіксація РО першим СД" та зведені з нею: подія 2 "Закінчення процедури класифікації рухомого об'єкта сейсмічним датчиком 1"; подія 3 "Закінчення процедури доставлення повідомлення про рухомий об'єкт сейсмічним датчиком 1".
- Базова подія 4 "Фіксація РО другим СД" та зведені з нею: подія 5 "Закінчення процедури класифікації рухомого об'єкта сейсмічним датчиком 2"; подія 6 "Закінчення процедури доставлення повідомлення про рухомий об'єкт сейсмічним датчиком 2".
- Базова подія 7 "Фіксація РО третім СД" та зведені з нею: подія 8 "Закінчення процедури класифікації рухомого об'єкта сейсмічним датчиком 3"; подія 9 "Закінчення процедури доставлення повідомлення про рухомий об'єкт сейсмічним датчиком 3".
- Базова подія 10 "Видача рішення мажоритарним елементом". Беручи до уваги, що тривалість процедури "прийняття рішення мажоритарним елементом" набагато менша від інтервалів часу між моментами фіксації рухомого об'єкта сейсмодатчиком, у моделі БП10 вона зведена з базовою подією БП7.

2.2. Показники функціональності складових КОС, представлені в розробленій моделі

У моделі реакції КОС на перетин РО зони контролю з мажоритарним принципом прийняття рішення про правильність класифікації типу РО представлено такі показники функціональності:

- P_{uf} – ймовірність фіксації сейсмічним датчиком рухомого об'єкта.
- P_{uk} – ймовірність правильної класифікації рухомого об'єкта.
- P_{ud} – ймовірність доставлення повідомлення про рухомий об'єкт.

- T_{f1} – середнє значення інтервалу часу від моменту появи РО в зоні контролю до моменту, коли РО має бути зафіксованим СД1.
- T_{f2} – середнє значення інтервалу часу від моменту фіксації РО сейсмодатчиком СД1 до моменту, коли РО має бути зафіксованим СД2.
- T_{f3} – середнє значення інтервалу часу від моменту фіксації РО сейсмодатчиком СД1 до моменту, коли РО має бути зафіксованим СД3.

2.3. Призначення компонент вектора стану

Під час побудови графа станів кожен стан КОС описуватимемо вектором, який складається з таких компонентів:

V1 – ця компонента вектора стану показує можливу реакцію КОС після БП1, ЗБП2 та ЗБП3: V1 = 1 – рухомий об'єкт зафіксовано СД1, правильно класифіковано, успішно доставлено повідомлення про РО в СПВІ; V1 = 2 – рухомий об'єкт зафіксовано СД1, неправильно класифіковано, успішно доставлено повідомлення про РО в СПВІ; V1 = 3 – рухомий об'єкт не зафіксовано СД1.

V2 – Ця компонента вектора стану показує можливу реакцію КОС після БП4, ЗБП5 та ЗБП6: V2 = 1 – рухомий об'єкт зафіксовано СД1, правильно класифіковано, успішно доставлено повідомлення про РО в СПВІ; V2 = 2 – рухомий об'єкт зафіксовано СД1, неправильно класифіковано, успішно доставлено повідомлення про РО в СПВІ; V2 = 3 – рухомий об'єкт не зафіксовано СД1. У початковому стані V2 = 0.

V3 – Ця компонента вектора стану показує можливу реакцію КОС після БП7, ЗБП8 та ЗБП9: V3 = 1 – рухомий об'єкт зафіксовано СД1, правильно класифіковано, успішно доставлено повідомлення про РО в СПВІ; V3 = 2 – рухомий об'єкт зафіксовано СД1, не правильно класифіковано, успішно доставлено повідомлення про РО в СПВІ; V3 = 3 – рухомий об'єкт не зафіксовано СД1. У початковому стані V3 = 0.

V4 – Ця компонента вектора стану показує можливі стани КОС про виконання завдання: (V4 = 1) – оператор отримав повідомлення з правильно визначеним типом РО; (V4 = 2) – обман оператора (оператор отримав повідомлення з неправильно визначеним типом РО); (V4 = 3) – оператор отримав повідомлення про наявність (присутність) РО в зоні контролю без визначення його типу; (V4 = 4) – оператор не отримав жодного повідомлення, хоча РО перетнув зону контролю. В початковому стані V4 = 0.

Формалізоване подання об'єкта дослідження у вигляді структурно-автоматної моделі в діалогових вікнах програмного засобу ASNA зображено на рис. 3, 4, 5.

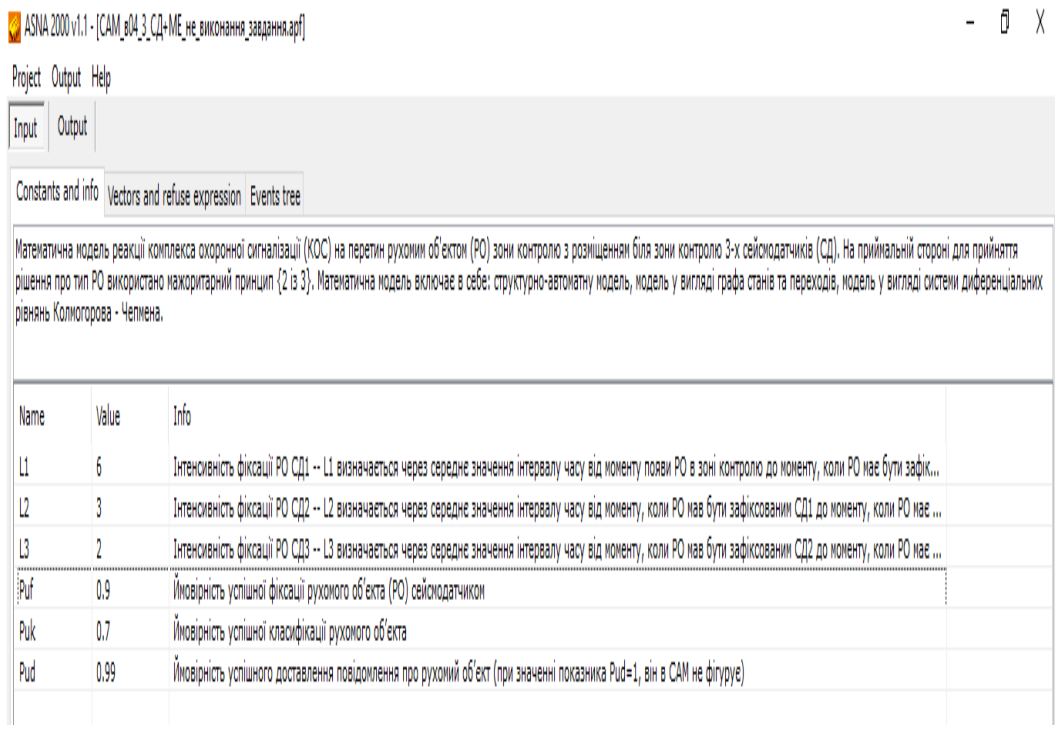


Рис. 3. Введені показники функціональності складових комплексу охоронної сигналізації, їх значення та коментар

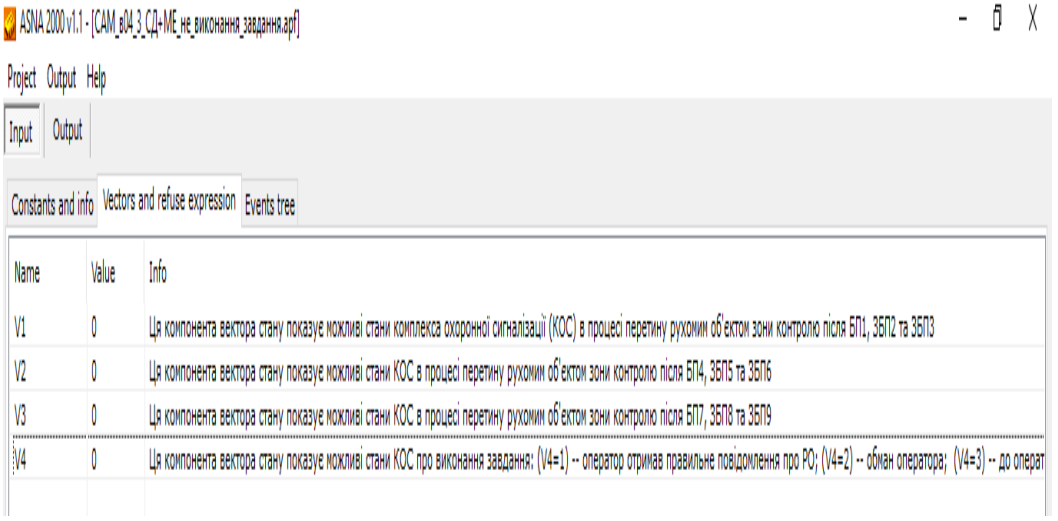
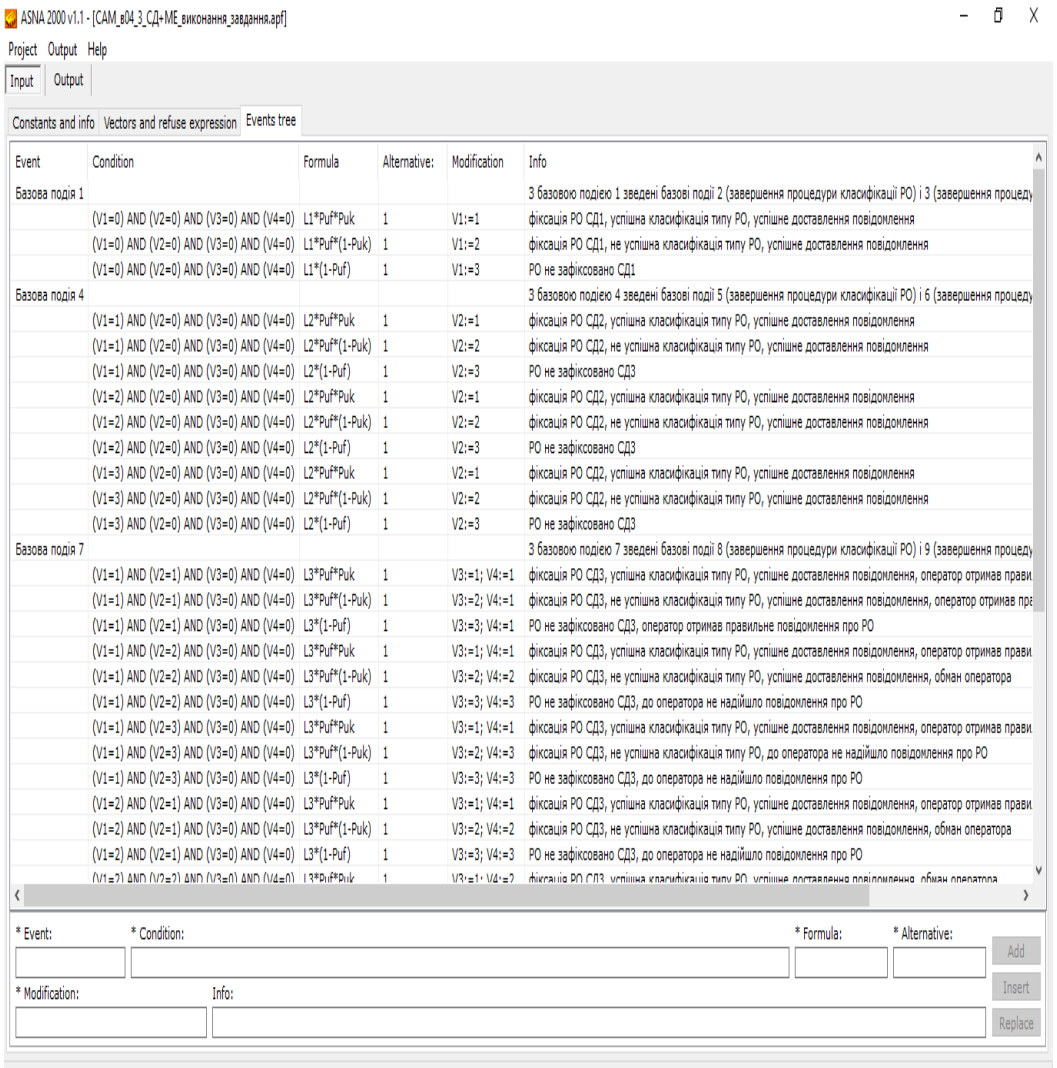


Рис. 4. Введені компоненти вектора стану, їх значення в початковому стані та коментар

2.4. Визначення компонент структурно-автоматної моделі

Для побудови моделі базовими є визначені 3 події. Наслідки, до яких приводить та чи інша подія, залежать від умов і обставин, за яких ця подія реалізується. Умова – це складова опису ситуації, обов'язкова для даної події. Обставина – це складова опису ситуації, яка може супроводжувати, а може й не супроводжувати дану подію. Тому кожній базовій події ставлять у відповідність логічні вирази, що представляють усі актуальні для неї ситуації.



Event	Condition	Formula	Alternative:	Modification	Info
Базова подія 1					З базовою подією 1 зведені базові події 2 (завершення процедури класифікації РО) і 3 (завершення процеду
	(V1=0) AND (V2=0) AND (V3=0) AND (V4=0)	L1*Puf*Puk	1	V1:=1	фіксація РО СД1, успішна класифікація типу РО, успішне доставлення повідомлення
	(V1=0) AND (V2=0) AND (V3=0) AND (V4=0)	L1*Puf*(1-Puk)	1	V1:=2	фіксація РО СД1, не успішна класифікація типу РО, успішне доставлення повідомлення
	(V1=0) AND (V2=0) AND (V3=0) AND (V4=0)	L1*(1-Puf)	1	V1:=3	РО не зафіксовано СД1
Базова подія 4					З базовою подією 4 зведені базові події 5 (завершення процедури класифікації РО) і 6 (завершення процеду
	(V1=1) AND (V2=0) AND (V3=0) AND (V4=0)	L2*Puf*Puk	1	V2:=1	фіксація РО СД2, успішна класифікація типу РО, успішне доставлення повідомлення
	(V1=1) AND (V2=0) AND (V3=0) AND (V4=0)	L2*Puf*(1-Puk)	1	V2:=2	фіксація РО СД2, не успішна класифікація типу РО, успішне доставлення повідомлення
	(V1=1) AND (V2=0) AND (V3=0) AND (V4=0)	L2*(1-Puf)	1	V2:=3	РО не зафіксовано СД3
	(V1=2) AND (V2=0) AND (V3=0) AND (V4=0)	L2*Puf*Puk	1	V2:=1	фіксація РО СД2, успішна класифікація типу РО, успішне доставлення повідомлення
	(V1=2) AND (V2=0) AND (V3=0) AND (V4=0)	L2*Puf*(1-Puk)	1	V2:=2	фіксація РО СД2, не успішна класифікація типу РО, успішне доставлення повідомлення
	(V1=2) AND (V2=0) AND (V3=0) AND (V4=0)	L2*(1-Puf)	1	V2:=3	РО не зафіксовано СД3
	(V1=3) AND (V2=0) AND (V3=0) AND (V4=0)	L2*Puf*Puk	1	V2:=1	фіксація РО СД2, успішна класифікація типу РО, успішне доставлення повідомлення
	(V1=3) AND (V2=0) AND (V3=0) AND (V4=0)	L2*Puf*(1-Puk)	1	V2:=2	фіксація РО СД2, не успішна класифікація типу РО, успішне доставлення повідомлення
	(V1=3) AND (V2=0) AND (V3=0) AND (V4=0)	L2*(1-Puf)	1	V2:=3	РО не зафіксовано СД3
Базова подія 7					З базовою подією 7 зведені базові події 8 (завершення процедури класифікації РО) і 9 (завершення процеду
	(V1=1) AND (V2=1) AND (V3=0) AND (V4=0)	L3*Puf*Puk	1	V3:=1; V4:=1	фіксація РО СД3, успішна класифікація типу РО, успішне доставлення повідомлення, оператор отримав прави
	(V1=1) AND (V2=1) AND (V3=0) AND (V4=0)	L3*Puf*(1-Puk)	1	V3:=2; V4:=1	фіксація РО СД3, не успішна класифікація типу РО, успішне доставлення повідомлення, оператор отримав пра
	(V1=1) AND (V2=1) AND (V3=0) AND (V4=0)	L3*(1-Puf)	1	V3:=3; V4:=1	РО не зафіксовано СД3, оператор отримав правильне повідомлення про РО
	(V1=1) AND (V2=2) AND (V3=0) AND (V4=0)	L3*Puf*Puk	1	V3:=1; V4:=1	фіксація РО СД3, успішна класифікація типу РО, успішне доставлення повідомлення, оператор отримав прави
	(V1=1) AND (V2=2) AND (V3=0) AND (V4=0)	L3*Puf*(1-Puk)	1	V3:=2; V4:=2	фіксація РО СД3, не успішна класифікація типу РО, успішне доставлення повідомлення, обман оператора
	(V1=1) AND (V2=2) AND (V3=0) AND (V4=0)	L3*(1-Puf)	1	V3:=3; V4:=3	РО не зафіксовано СД3, до оператора не надійшло повідомлення про РО
	(V1=1) AND (V2=3) AND (V3=0) AND (V4=0)	L3*Puf*Puk	1	V3:=1; V4:=1	фіксація РО СД3, успішна класифікація типу РО, успішне доставлення повідомлення, оператор отримав прави
	(V1=1) AND (V2=3) AND (V3=0) AND (V4=0)	L3*Puf*(1-Puk)	1	V3:=2; V4:=3	фіксація РО СД3, не успішна класифікація типу РО, до оператора не надійшло повідомлення про РО
	(V1=1) AND (V2=3) AND (V3=0) AND (V4=0)	L3*(1-Puf)	1	V3:=3; V4:=3	РО не зафіксовано СД3, до оператора не надійшло повідомлення про РО
	(V1=2) AND (V2=1) AND (V3=0) AND (V4=0)	L3*Puf*Puk	1	V3:=1; V4:=1	фіксація РО СД3, успішна класифікація типу РО, успішне доставлення повідомлення, оператор отримав прави
	(V1=2) AND (V2=1) AND (V3=0) AND (V4=0)	L3*Puf*(1-Puk)	1	V3:=2; V4:=2	фіксація РО СД3, не успішна класифікація типу РО, успішне доставлення повідомлення, обман оператора
	(V1=2) AND (V2=1) AND (V3=0) AND (V4=0)	L3*(1-Puf)	1	V3:=3; V4:=3	РО не зафіксовано СД3, до оператора не надійшло повідомлення про РО

Рис. 5. Фрагмент уведеної структурно-автоматної моделі реакції КОС на перетин РО зони контролю, біля якої встановлено 3 СД

2.5. Формування моделі у вигляді системи диференціальних рівнянь Колмогорова – Чепмена

Математична модель КОС із 3 СД та мажоритарним принципом прийняття рішення про тип РО зображена у вигляді системи лінійних однорідних диференціальних рівнянь першого порядку (1). Математична модель формується згідно з графом станів і переходів, який має 34 стани та 37 переходів.

2.6. Валідація дискретно-неперервної стохастичної моделі реакції КОС на перетин зони контролю з трьома СД і з мажоритарним принципом прийняття рішення про тип рухомого об'єкта

Значення показників функціональності складових КОС, що використані в проведених дослідженнях 1–3:

- Ймовірність фіксації РО сейсмічним датчиком – $P_{uf} = 0.9$.
-

$$\begin{cases} \frac{dP_1(t)}{dt} = -(\lambda_1 \cdot P_{uf} \cdot P_{uk} + \lambda_1 \cdot P_{uf} \cdot (1-P_{uk}) + \lambda_1 \cdot (1-P_{uf})) \cdot P_1(t); \\ \frac{dP_2(t)}{dt} = -(\lambda_2 \cdot P_{uf} \cdot P_{uk} + \lambda_2 \cdot P_{uf} \cdot (1-P_{uk}) + \lambda_2 \cdot (1-P_{uf})) \cdot P_2(t); \\ \frac{dP_3(t)}{dt} = -(\lambda_2 \cdot P_{uf} \cdot P_{uk} + \lambda_2 \cdot P_{uf} \cdot (1-P_{uk}) + \lambda_2 \cdot (1-P_{uf})) \cdot P_3(t); \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \frac{dP_{12}(t)}{dt} = -(\lambda_3 \cdot P_{uf} \cdot P_{uk} + \lambda_3 \cdot P_{uf} \cdot (1-P_{uk}) + \lambda_3 \cdot (1-P_{uf})) \cdot P_{12}(t); \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \frac{dP_{34}(t)}{dt} = \lambda_3 \cdot P_{uf} \cdot P_{uk} \cdot P_5(t) + \lambda_3 \cdot P_{uf} \cdot (1-P_{uk}) \cdot P_6(t) + \lambda_3 \cdot P_{uf} \cdot P_{uk} \cdot P_7(t) \cdot \\ + \lambda_3 \cdot P_{uf} \cdot P_{uk} \cdot P_8(t) + \lambda_3 \cdot P_{uf} \cdot P_{uk} \cdot P_{11}(t) + \lambda_3 \cdot P_{uf} \cdot P_{uk} \cdot P_8(t) \end{cases} \quad (1)$$

- Ймовірність правильної класифікації типу РО – (P_{uk} = var)
- Ймовірність приймання радіосигналу системою приймання та відображення інформації – $P_{ud} = 1$.
- Середнє значення інтервалу часу від моменту появи РО в зоні контролю до моменту, коли РО має бути зафіксованим СД1 – $T_{f1} = 10$ хв.
- Середнє значення інтервалу часу від моменту фіксації РО сейсмічним датчиком СД1 до моменту, коли РО має бути зафіксованим СД2 – $T_{f2} = 20$ хв.
- Середнє значення інтервалу часу від моменту фіксації РО сейсмічним датчиком СД2 до моменту, коли РО має бути зафіксованим СД3 – $T_{f3} = 30$ хв.

*Дослідження 1. Визначення залежності зміни показника ефективності КОС (**імовірність виконання завдання КОС**) за різних значень імовірності успішної класифікації рухомого об'єкта.*

Результат проведеного дослідження (рис. 6) показав, що для забезпечення високого значення ймовірності виконання КОС, значення ймовірності успішної класифікації має бути не нижче 0,99. Підвищення вимог до пристрою класифікації не дає значного покращання показника ефективності КОС.

*Дослідження 2. Визначення залежності зміни показника ефективності КОС (**імовірність часткового виконання завдання КОС**) за різних значень імовірності успішної класифікації рухомого об'єкта.*

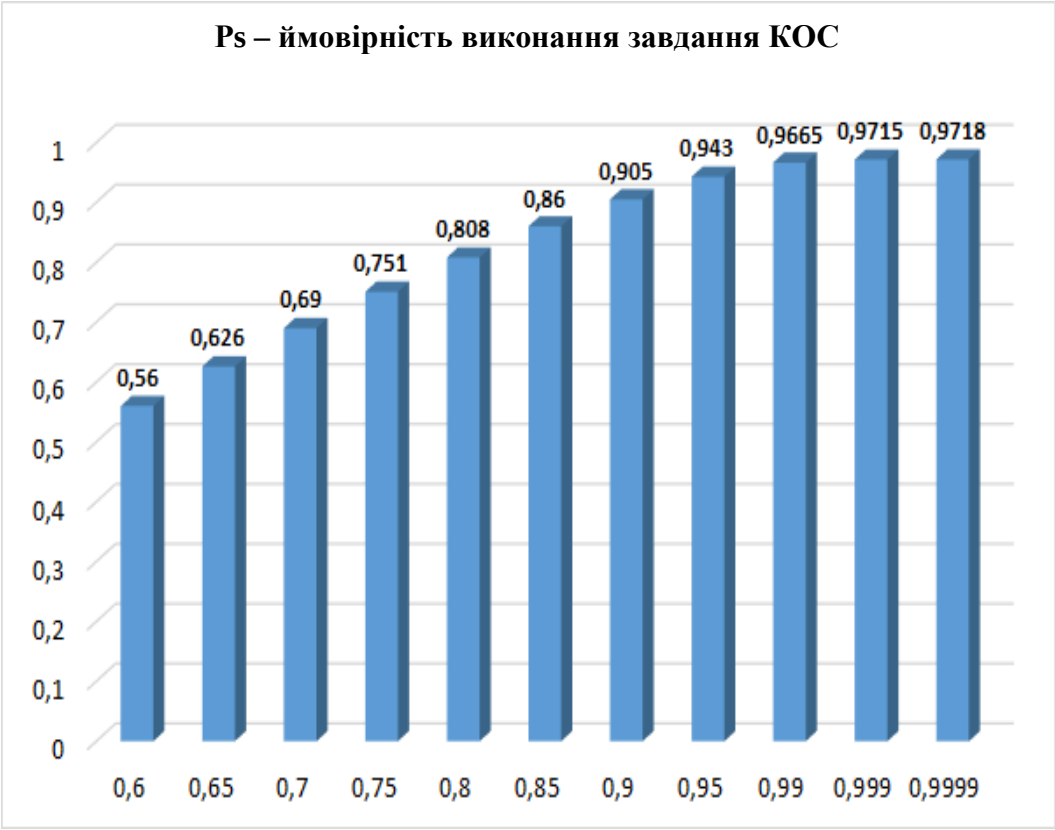


Рис. 6. Залежність імовірності виконання завдання КОС
від зміни значення ймовірності успішної класифікації рухомого об'єкта

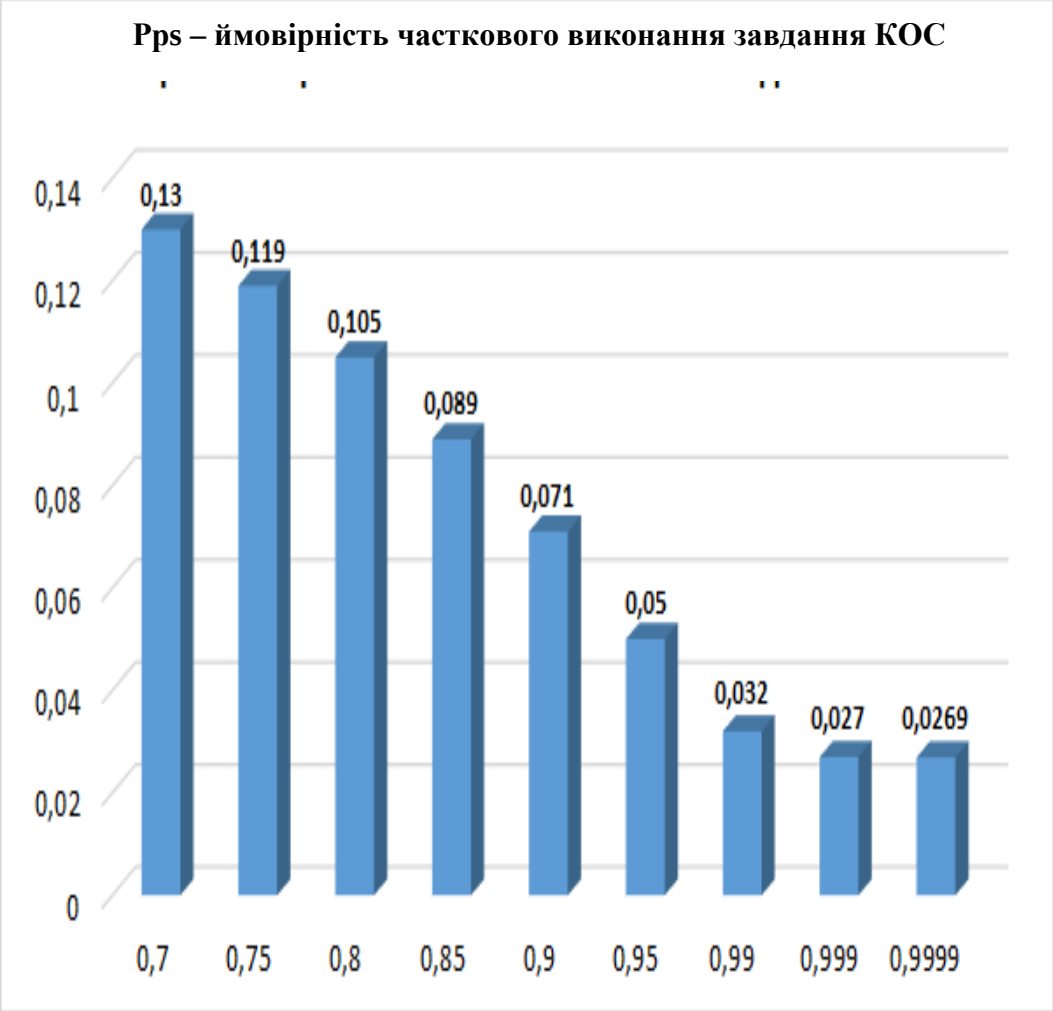


Рис. 7. Залежність імовірності часткового виконання завдання КОС від зміни ймовірності успішної класифікації рухомого об’єкта

Результат проведеного дослідження (рис. 7) свідчить, що для забезпечення низького значення ймовірності часткового виконання КОС значення ймовірності успішної класифікації має бути не нижче 0,99. Подальше підвищення вимог до пристрою класифікації не дає значного зниження ймовірності часткового виконання завдання.

*Дослідження 3. Визначення залежності зміни показника ефективності КОС (**імовірність “обману” оператора**) за різних значень ймовірності успішної класифікації рухомого об’єкта.*

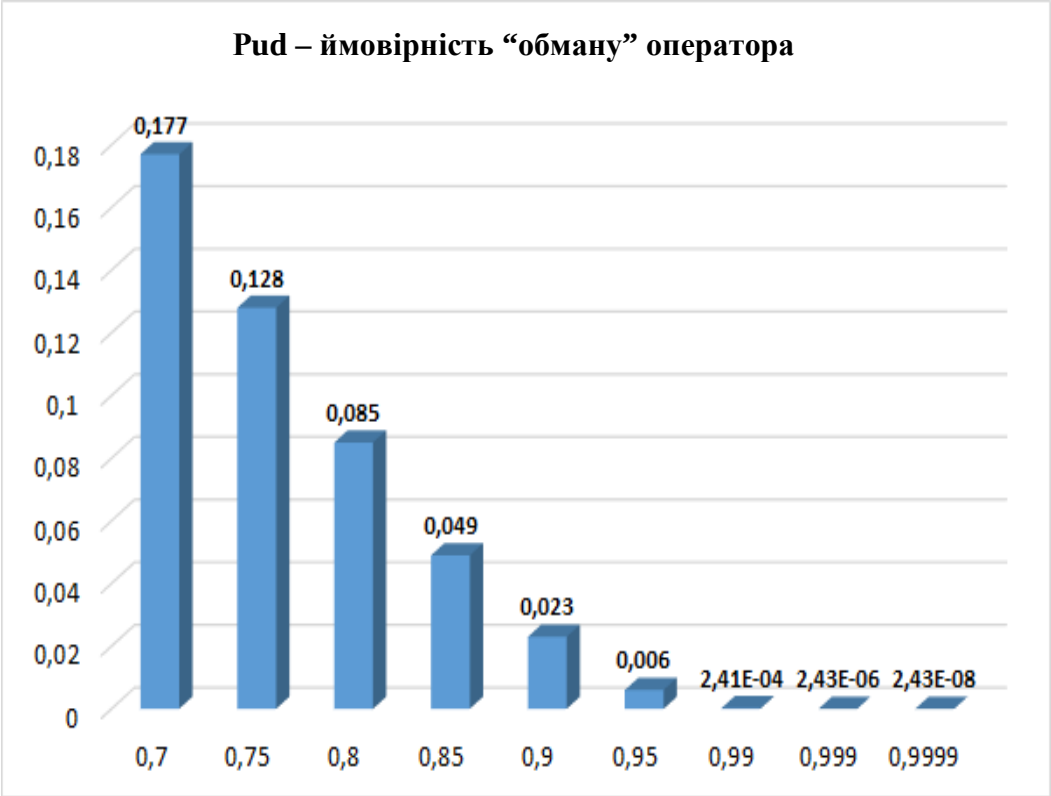


Рис. 8. Залежність імовірності “обману” оператора
від зміни ймовірності успішної класифікації рухомого об’єкта

Результат проведеного дослідження (рис. 8) свідчить, що для забезпечення низького значення ймовірності “обману” користувача КОС значення ймовірності успішної класифікації має бути не нижче 0,95. Підвищення вимог до пристрою класифікації не дають значного покращання показника ефективності КОС.

Дослідження 4. Порівняльне дослідження ефективності КОС із трьома варіантами кількості сейсмічних датчиків біля зони контролю

Дослідження проводилося за таких значень показників функціональності складових КОС:

- імовірність фіксації РО сейсмічним датчиком у зоні контролю – $P_{uf} = 0{,}9$;
- імовірність правильної класифікації РО – $P_{uk} = 0{,}9$;
- імовірність приймання радіосигналу СПВІ – $P_{ud} = 1$.

Результати дослідження подано на рис. 9.

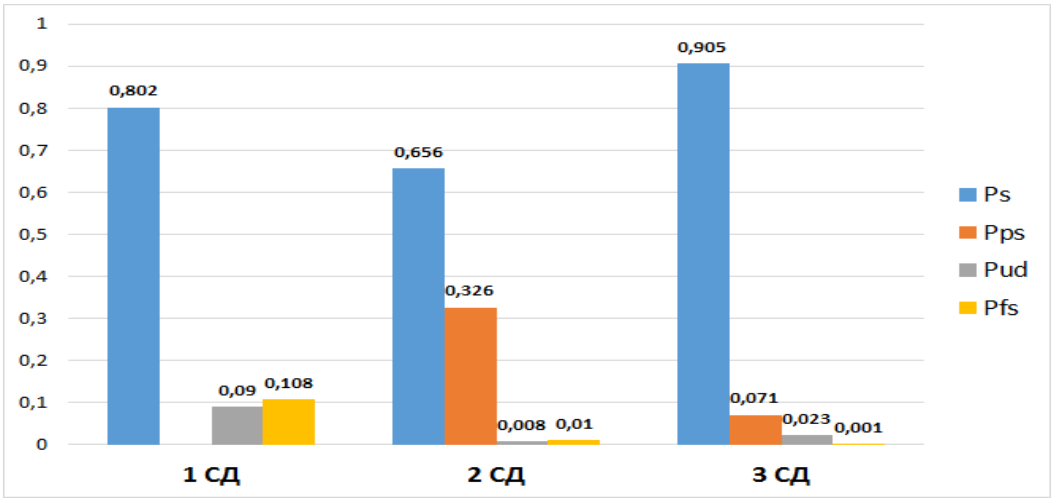


Рис. 9. Порівняння ефективності КОС із встановленням 1, 2 або 3 сейсмічних датчиків біля зони контролю

Отримані результати дослідження підтвердили ефективність використання КОС із розміщенням у зоні контролю трьох СД з мажоритарним принципом прийняття рішення про тип РО. Застосування КОС із трьома СД у зоні контролю і мажоритарним принципом прийняття рішення про тип РО в порівнянні КОС із одним та двома СД забезпечує: найбільше значення ймовірності виконання завдання КОС; зниження значення ймовірності невиконання завдання КОС у порівнянні КОС із одним СД на два порядки, а в порівнянні КОС із двома СД – на один порядок; зниження значення ймовірності "обману" оператора (P_{ud}) майже в 4 рази. Крім того, використання КОС із розміщенням у зоні контролю трьох СД з мажоритарним принципом прийняття рішення в порівнянні КОС із двома СД і прийняттям рішення про тип РО за збігом сигналів знижує ймовірність часткового виконання завдання більше ніж у 3 рази.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Проведені дослідження показали, що комплекс охоронної сигналізації з використанням у зоні контролю одного сейсмічного датчика має високе значення ймовірності "обману" оператора, ймовірності невиконання завдання КОС та водночас відносно низьке значення ймовірності виконання завдання КОС. Використання в зоні контролю двох СД дає можливість приймати рішення про тип РО через збіг повідомлень. Такий спосіб забезпечує найменше значення ймовірності "обману" оператора в порівнянні з двома іншими варіантами реалізації КОС, проте суттєво знижує ймовірність виконання завдання КОС, а також має досить велике значення ймовірності часткового виконання КОС.

Запропоновано встановлювати в зоні контролю три СД, що дає можливість використовувати мажоритарний принцип для прийняття рішення про тип РО. Отримані результати дослідження підтвердили ефективність і надійність використання такого КОС.

Продовження досліджень будуть проведені з метою врахування впливу ненадійності сейсмічних датчиків та автономних систем виявлення, класифікації об'єктів і передавання радіосигналів на значення показників ефективності комплексу охоронної сигналізації. Це питання важливе для довготривалої експлуатації комплексу охоронної сигналізації.

Список використаних джерел:

1. *Zvezhynskii S. S.* Perimeter concealed seismic detection means // Special equipment. 2004. № 2. P. 20–28; № 3. P. 26–37.

2. *Zvezhynskii S. S.* Problem of choosing perimeter detection means // BDI. 2002. № 4 (44). P. 36–41.

3. Pricon. Technical Information. URL: http://www.signalsecurity.gr/html/pdf/brochures/psicon_brochure.pdf

4. Quantum multichannel seismic-acoustic system. URL: http://qtsi.com/wpcontent

5. *Volochiy B. Yu., Onishchenko V. A.* Research of the dependence of the guard signaling complex on the location of seismic sensors // Східноєвропейський журнал передових технологій. Інформаційно-керуючі системи. 2014. Том 2. № 9 (68). С. 54–60.

6. *Волочій Б. Ю., Онищенко В. А.* Моделювання реакції комплексу охоронної сигналізації на появу рухомого об'єкту при розміщенні сейсмодатчиків в дальній та ближній зонах контролю // Воєнно-технічний збірник. 2014. № 1 (10). С. 7–13.

7. *Volochiy B. Yu., Onishchenko V. A.* Modelling the reaction of guard signaling complex on appearance of moving object when seismosensors are deployed in far and close control zones // Modern problems of radio engineering, telecommunications and computer science: proceedings of the International Conference TCSET'2014 Dedicated to the 170th anniversare of Lviv Polytechnic National University, Lviv-Slavske, Ukraine: Publishing House of National University "Lviv Polytechnic", 2014. P. 252–254.

8. *Koren Israel, Krishna C. Mani.* Fault tolerant systems // Morgan Kaufmann Publishers is an imprint of Elsevier. 2007. 378 p.

9. *Shooman Martin L.* Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design. John Wiley & Sons, Inc. New York, 2002. 528 p.

10. *Волочій Б. Ю., Озірковський Л. Д.* Системотехнічне проектування телекомунікаційних мереж: Практикум. Львів: Видавництво Львівської політехніки, 2012. 128 с.

11. *Федасюк Д. В., Волочій С. Б.* Методика розроблення структурно-автоматних моделей відмовостійких систем з альтернативними продовженнями випадкових процесів після процедур контролю, перемикання і відновлення // Вісник Національного університету “Львівська політехніка” : “Комп’ютерні науки та інформаційні технології”. 2017. № 864. С. 49 –62.

12. *Волочій Б. Ю., Онищенко В. А., Сальник Ю. П.* Методика синтезу комплексу охоронної сигналізації при розміщенні сейсмодатчиків в дальній та ближній зонах контролю // Радіоелектроніка та телекомунікації. Вісник Національного університету “Львівська політехніка”. 2015. № 818. С. 32–40.

13. *Fedasiuk D. V., Volochiy S. B.* Method of development of structural automaton models of discrete continuous stochastic systems // Scientific journal “Radioelectronic and computer systems”. 2016. № 6 (80). P. 24–34.

14. *Волочій Б. Ю.* Технологія моделювання алгоритмів поведінки інформаційних систем. Львів: “Львівська політехніка”, 2004. 220 с.

15. *Volochiy B., Onishchenko V., Zmysnyi M., Kulyk I.* Assessment of potential capabilities of guard signaling complex using seismic sensors // IEEE 9th International Conference on Dependable Systems, Services and Technologies, DESSERT’2018. P. 460–467.

REFERENCES

1. Zvezhynskii S. S. (2004), “Perimeter concealed seismic detection means”, Journal Special equipment. vol. 2, pp. 20–28; vol. 3, pp, 26–37.

2. Zvezhynskii S. S. (2002), Problem of choosing perimeter detection means, Journal BDI, vol. 4 (44), pp. 36–41.

3. Pricon. Technical Information, available at: http://www.signalsecurity.gr/html/pdf/brochures/psicon_brochure.pdf

4. Quantum multichannel seismic-acoustic system, available at: http://qtsi.com/wpcontent/

5. Volochiy B. Yu. and Onyshchenko V. A. (2014), “Research of the dependence of the guard signaling complex on the location of seismic sensors”, *Skhidnoyevropeys’kyy zhurnal peredovykh tekhnolohiy. Informatsiyno-keruyuchi systemy* [Eastern-European Journal of Enterprise Technologies], vol 2, No. 9 (68), pp. 54–60 [Ukraine].

6. Volochiy B. Yu. and Onyshchenko V. A. (2014), *“Modeliuvannia reaktsii kompleksu okhoronnoi syhnalizatsii na poiavu rukhomoho obiektu pry rozmishchenni seismodatchykiv v dalnii ta blyzhnii zonakh kontroliu”* [“Simulation of the reaction of the alarm system complex to the appearance of a moving object during the deployment of seismic sensors in the distant and near-control areas”], *Voienno-tekhnichnyi zbirnyk* [Military-technical collection], vol 1 (10), ASV, Lviv, pp. 7–13 [Ukraine].

7. Volochiy B. Yu. and Onyshchenko V. A. (2014), Modelling the reaction of guard signaling complex on appearance of moving object when seismosensors are deployed in far and close control zones, Modern problems of radio engineering, telecommunications and computer science: proceedings of the International Conference TCSET'2014 Dedicated to the 170th anniversare of Lviv Polytechnic National University, Lviv-Slavske, Publishing House of National University "Lviv Polytechnic", pp. 252–254 [Ukraine].

8. Koren Israel and Krishna C. Mani (2007), Fault tolerant systems, Morgan Kaufmann Publishers is an imprint of Elsevier, 378 p.

9. Shooman Martin L. (2002), Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design, John Wiley & Sons, Inc., New York, 528 p.

10. Volochiy B. Yu. and Ozirkovskyi L. D. (2012), *Systemotekhnichne proektuvannia telekomunikatsiinykh merezh* [System engineering design of telecommunication networks], Workshop, Press NU «L'vivs'ka politekhnika», Lviv, 128 p. [Ukraine].

11. Fedasiuk D. V. and Volochiy S. B. (2017), *"Metodyka rozroblennia strukturno-avtomatnykh modelei vidmovostiikykh system z al'ternatyvnymy prodovzhenniamy vypadkovykh protsesiv pislia protsedur kontroliu, peremykannia i vidnovlennia"* ["Methods of developing structural automaton models of fault-tolerant systems with alternative continuation of random processes after control, switching and restoration procedures"], *Visnyk Natsionalnoho universytetu "Lvivska politekhnika"*, series *"Komp'yuterni nauky ta informatsiini tekhnolohii"* [Bulletin of the National University "L'viv Polytechnic", series "Computer Science and Information Technologies", vol. 864, pp. 49–62 [Ukraine].

12. Volochiy B. Yu., Onyshchenko V. A. and Salnyk Yu. P. (2015), *"Metodyka syntezu kompleksu okhoronnoyi syhnalizatsiyi pry rozmishchenni seysmodatchykiv v dal'niy ta blyzhniy zonakh kontrolyu"* ["The method of synthesis of the alarm system complex for the deployment of seismic sensors in the far and near areas of control"], Bulletin of L'viv Polytechnic National University "*Radioelektronika ta telekomunikatsiyi"* [Electronics and Telecommunications], vol. 818, pp. 32–40 [Ukraine].

13. Fedasiuk D. V. and Volochiy S. B. (2016), "Method of development of structural automaton models of discrete continuous stochastic systems", Scientific journal "Radioelectronic and computer systems", vol. 6 (80), pp. 24–34.

14. Volochiy B. Yu. (2004), *Tekhnolohiya modelyuvannya alhorytmiv povedinky informatsiynykh system* [Technology of modeling of algorithms of behavior of information systems], Press NU "L'vivs'ka politekhnika", L'viv, 220 p. [Ukraine].

15. Volochiy B., Onyshchenko V., Zmysnyi M. and Kulyk I. (2018), Assessment of potential capabilities of guard signaling complex using seismic sensors, IEEE 9th International Conference on Dependable Systems, Services and Technologies, DESSERT'2018, pp. 460–467.

DOI: https://doi.org/10.32836/2521-6643-2019-1-57-5
УДК 004.056

Ю. Л. Поночовний, кандидат технічних наук, старший науковий співробітник, доцент кафедри інформаційних систем та технологій Полтавської державної аграрної академії
С. Ю. Рогочий, магістр Полтавського національного технічного університету імені Юрія Кондратюка
О. І. Шарай, магістр Полтавського національного технічного університету імені Юрія Кондратюка
В. О. Кнуренко, магістр Полтавського національного технічного університету імені Юрія Кондратюка
В. С. Воронянський, викладач Полтавського коледжу нафти і газу Полтавського національного технічного університету імені Юрія Кондратюка

ДОСЛІДЖЕННЯ БАЗ ВРАЗЛИВОСТЕЙ ДЛЯ ПАРАМЕТРИЗАЦІЇ МАРКОВСЬКИХ МОДЕЛЕЙ ОЦІНЮВАННЯ ДОСТУПНОСТІ ВЕБ-РЕСУРСІВ

Досліджено актуальне питання оцінювання параметрів вразливостей веб-ресурсів для використання як вхідних даних у марковських моделях доступності. Наведено розрахунки інтенсивності прояву вразливостей доступності веб-серверів сімейства Apache на основі вибірок за 2015 та 2016 рр. У статті розглянуто зв'язки між базами вразливостей, зокрема між базою CVE та іншими відкритими та платними репозитаріями. Основна увага приділяється питанням актуалізації наведеної у відкритих базах інформації, уточненню часу фіксації вразливості в базі та формуванню вибірок на основі множини критеріїв відбору.

Ключові слова: *вразливості веб-ресурсів; оцінювання параметрів; інтенсивність прояву; критичність вразливості.*

Рассмотрены актуальные вопросы оценки параметров уязвимостей веб-ресурсов для использования в качестве входных данных в марковских моделях доступности. Приведены расчеты интенсивности проявления уяз вимостей доступности веб-серверов семейства Apache на основе выборок за 2015 и 2016 гг. В статье рассматриваются связи между базами уязви-мостей, в частности, между базой CVE и другими открытыми и платны-ми репозитариями. Основное внимание уделяется вопросам актуализации приведенной в открытых базах информации, уточнению времени фиксации уязвимости в базе и формированию выборок на основе множества крите-риев отбора.

Ключевые слова: *уязвимости веб-ресурсов; оценивание параметров; ин-тенсивность проявления; критичность уязвимости.*

In this paper we consider issues of obtaining information from open data-bases of vulnerabilities and the creation of excerpt according to several criteria. The relevance of the topic is due to the need to ensure the parameterization of samples. Simulation helps increase the likelihood of detecting a vulnerability be-fore it is used by attackers. The issues of assessing the parameters of vulnerabili-ties of web resources are considered. These parameters are used as input in Mar-kov availability models. Availability is included in the set components of infor-mation security (confidentiality, integrity, availability).

The article discusses the relationship between databases of vulnerabilities. The relationships between the CVE database and other open and paid reposito-ries are analyzed. Analyzed the current state of relations (uplink or downlink). The focus is on issues of updating the information given in open databases. The activity of the database, their openness, paid access or the possibility of trial / limited use are determined.

For processing, information from the NVD vulnerability database in the form of archived XML files was obtained and refined. The following parameters were used as input parameters for Markov models: the intensity of the manifesta-tion of vulnerabilities and the criticality of the attack. The calculations of the in-tensity of the availability of vulnerabilities of Apache family of web servers based on samples for 2015 and 2016 are given. Attention is paid to the specification of the time of fixation of vulnerabilities in the database and the formation of samples based on a set of selection criteria from the open bases of vulnerabilities of NVD and CVE.

The results of the study showed that in 2016, new vulnerabilities from the sample were recorded 3.23 times faster, but at the same time, their criticality de-creased by 3 % on average. The tendency of gradual growth of interest to net-work software products, in particular Apache web servers, is confirmed.

To speed up and more convenient excerpt creation, it is advisable to develop software that automatically creates the necessary excerpte after selecting the formation criteria. Also, to improve the results of the study, it is necessary to refine the vulnerability information in several open bases.

Key words: *vulnerability of web resources; parameter estimation; intensity of manifestation, critical score.*

Постановка проблеми. За останні десятиліття залежність сучасного суспільства від комп'ютерних систем істотно зросла. Банківські операції, управління торгівлею ринків, автоматизовані військові й державні системи все більше залежать від комп'ютерних систем. У результаті ризик реалізації різних класів атак, які базуються на експлуатації наявних вразливостей у програмно-апаратному забезпеченні, для критично важливих об'єктів дуже великий [1].

Як наслідок, в наші дні проводяться великомасштабні дослідження проблем безпеки та кібербезпеки, викликаних уразливостями програмно-апаратного забезпечення [2]. Незважаючи на наявні загрози, суспільство вже ніколи не відмовиться від використання мережі Інтернет і комп'ютерних мереж в цілому, адже вони дають величезні можливості у фінансовій, політичній, військовій та інших галузях. Постійне вдосконалення технологій безпеки в інформаційному світі не може гарантувати абсолютну захищеність комп'ютерних систем.

Вразливості виявлялись у всіх основних операційних системах і додатках. Так як постійно знаходять нові вразливості, єдиний шлях зменшити ймовірність їх використання зловмисниками полягає у виконанні безперервного моніторингу захищеності, що передбачає постійне відстеження появи вразливостей, оперативне встановлення оновлень та використання інструментів протидії можливим атакам.

Наприклад, вразливість операційної системи може призвести до витоку комерційної інформації, що спричинить значні фінансові втрати. У таких умовах корисно було б мати змогу оцінювати, прогнозувати безпеку комп'ютерної системи, її компонентів, локальних і веб-ресурсів. Одним зі способів прогнозування безпеки є моделювання процесів виявлення й усунення вразливостей на основі статистичних даних, зібраних за певний період життєвого циклу (далі – ЖЦ) програмних засобів.

Аналіз останніх досліджень і публікацій. Із кожним роком спостерігається підвищення зацікавленості науковців і незалежних дослідників-ентузіастів як до питання виявлення та занесення нових вразливостей до відомих БД, так і до використання доступної в БД інформації для оцінювання захищеності інформаційних систем і веб-ресурсів.

Нині існує цілий ряд інформаційних ресурсів Інтернет, які надають інформацію про вразливості на сторінках своїх сайтів. Одна з найвідоміших баз вразливостей – "Загальні вразливості та ризики" (Common Vulnerabilities and Exposures – CVE) компанії MITRE [3]. Базу CVE більшість дослідників вважає єдиним і первинним постачальником ідентифікаторів вразливостей. Ці ідентифікатори використовуються для однозначного позначення однієї й тієї ж уразливості іншими відомими базами даних (Secunia [4], Security Focus [4] та ін.), базами експлойтів (Exploit Database [6] тощо) і бюлетенями безпеки (Microsoft Security Bulletin [7], US-CERT [8], Android Security Bulletin [9] тощо). Недолік БД CVE – це відсутність в описі вразливостей специфікації програмно-апаратного забезпечення. Для визначення цієї специфікації потрібно використовувати першоджерела, які надали інформацію. Наприклад, база даних вразливостей NVD [10] дозволяє точно ідентифікувати вразливий програмний продукт та його версію, отримати інформацію про спосіб атаки, за якої дана вразливість виявляє себе, різновид загрози та іншу корисну інформацію.

У працях науковців досліджувались питання формування альтернативних (більш зручних) БД [11], використання інформації з БД вразливостей для побудови моделей захищеності [2; 12; 13]. На особливу увагу заслуговують дослідження ризиків, пов'язаних із віднаходженням та експлуатацією вразливостей веб-ресурсів. Такі дослідження можна умовно поділити на аналіз ризиків на основі статичних імовірнісних моделей [14] та дослідження зміни у часі показників захищеності систем, зокрема доступності, на основі динамічних марковських моделей [13; 15]. Питання параметризації динамічних моделей частково були розглянуті в [16; 17].

Мета статті – параметризація вразливостей на основі вибірок із відкритих баз даних. Для розв'язання задачі необхідно послідовно побудувати вибірку з бази, уточнити отримані дані та отримати кількісні оцінки.

Виклад основного матеріалу. Стан досліджень у питаннях інформаційної та кібербезпеки потребує адекватного уявлення ситуації сьогодення. Із часом виявляються нові вразливості у розробленому програмному забезпеченні, виходять нові версії програм, розробляють як експлойти (скрипти та програми для використання вразливостей), так і патчі, що усувають виявлені вразливості. Через певні причини (досить часто через фінансування) припиняють функціонування великі й малі проекти, що розробляють і супроводжують бази вразливостей. Нині щодо фінансування, наповнення та супроводу, а також підтримки взаємозв'язків опорною БД вразливостей є база CVE. Ця база підтримує взаємозв'язки з іншими репозитаріями, що відображено на відповідній сторінці ресурсу [18]. На момент написання статті нараховується 83 посилання на інші репозитарії, але, що важливо, деякі з них уже припинили підтримку проектів.

Під час дослідження джерел взаємозв'язків бази CVE було розглянуто бази даних із різними моделями доступу (рис. 1). Основними видами доступу є відкритий і закритий. Відкрита БД забезпечує доступ до даних про вразливості для користувачів без будь-яких обмежень. Доступ до даних у закритій базі неможливий без виконання певних умов, заданих власником БД (як правило, платний доступ).

Також існують закриті БД, що дають користувачеві обмежений, або навіть повний доступ на пробний період. Навпаки, деякі відкриті БД частково обмежують інформацію про вразливість. Такі способи доступу до БД не можна зараховувати до основних через тимчасовість/обмеженість такого доступу (на рис. 1 позначено БД із пробним періодом/обмеженим функціоналом).

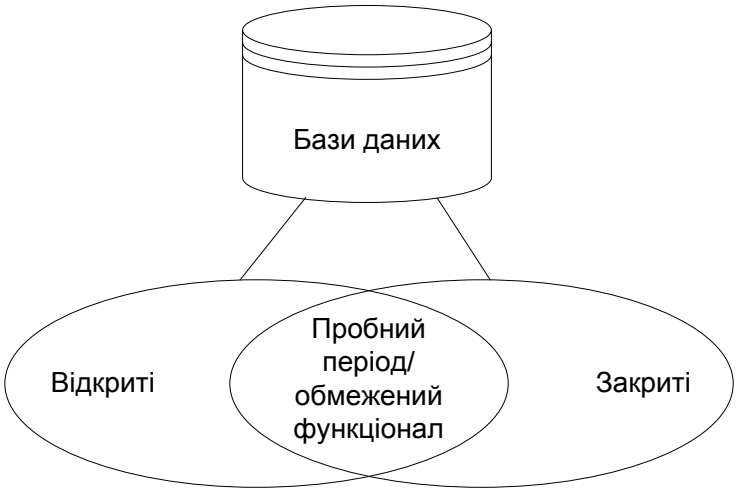


Рис. 1. Класифікація вразливостей БД за способом доступу

Репозитарії, відмічені у БД CVE, також можна розділити на групи (рис. 2) за характером контенту та його відношенням до певного об'єднувального фактора (найчастіше таким фактором є компанія–розробник програмного забезпечення). Універсальні БД не мають основного критерію для відбору вразливостей у свої бази; спеціалізовані БД мають єдину тему, що об'єднує інформацію про вразливості. Зі свого боку спеціалізовані поділяються на БД, в яких зібрані вразливості продуктів якогось одного виробника (загальні за виробником) та БД, які накопичують інформацію про вразливості одного типу продуктів різних виробників (спеціалізовані за продуктом).

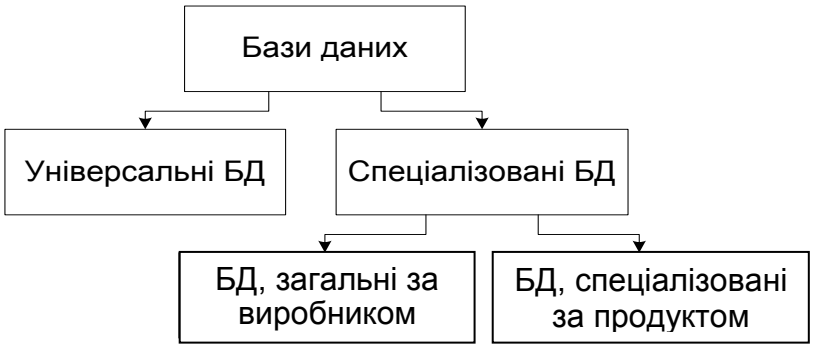


Рис. 2. Типізація вразливостей БД

Проект CVE розробила і підтримує компанія MITRE з 1999 р. На січень 2019 р. БД нараховує 143 934 записи (111 623, за даними веб-сайту). В табл. 1 відібрані БД, що були представлені у списку перехресних посилань бази CVE, та активні станом на кінець 2018 р. Головними причинами припинення роботи решти репозитаріїв стали банкрутство та реструктуризація компаній, що створили ці БД.

Таблиця 1

БД перехресних посилань бази CVE
(активні станом на кінець 2018 р.)

Назва	URL адреса	Тип
1	2	3
AIXAPAR	http://www-01.ibm.com/support/search.wss?rs=0&apar=only	закрита (безкоштовна 30-денна версія)
APPLE	http://lists.apple.com/archives/security-announce	відкрита
CERT	http://www.cert.org/advisories	відкрита
CERT-VN	http://www.kb.cert.org/vuls	відкрита
CHECKPOINT	http://www.checkpoint.com/defense/advisories/public/summary.html	відкрита
CISCO	http://www.cisco.com/en/US/products/products_security_advisories_listing.html	відкрита
CONECTIVA	http://lwn.net/Alerts/Conectiva/	відкрита
DEBIAN	http://www.debian.org/security/	відкрита
EXPLOIT-DB	http://www.exploit-db.com	відкрита
FEDORA	https://lists.fedoraproject.org/archives/list/announce@lists.fedoraproject.org/	відкрита

Закінчення табл. 1

1	2	3
FREEBSD	http://www.freebsd.org/security/	відкрита
GENTOO	http://www.gentoo.org/security/en/glsa/	відкрита
JVN	http://jvn.jp/en/report/index.html	відкрита
JVNDB	http://jvndb.jvn.jp/	відкрита
MANDRAKE	http://lwn.net/Alerts/Mandrake/	відкрита
MS	http://www.microsoft.com/technet/security/current.aspx	відкрита
NETBSD	http://www.netbsd.org/Security/advisory.html	відкрита
OPENBSD	http://www.openbsd.org/security.html	відкрита
REDHAT	http://www.redhat.com/support/errata/index.html	відкрита
SECTRACK	http://www.securitytracker.com	закрита (час пробної версії не зазначений)
SECUNIA	http://secunia.com/advisories/	відкрита
SLACKWARE	http://www.slackware.com/security/	відкрита
SREASON	http://securityreason.com/security_alert	відкрита
SUSE	https://www.suse.com/support/update/	відкрита
TURBO	http://www.turbolinux.com/security/	відкрита
UBUNTU	http://www.ubuntu.com/usn/	відкрита
VIM	http://www.attrition.org/pipermail/vim/	відкрита
XF	https://exchange.xforce.ibmcloud.com/	закрита (безкоштовна 30-денна версія)

Формування вибірки для оцінювання вхідних параметрів марковських моделей доступності

Як вхідні параметри марковських моделей оцінювання доступності може бути використано інтенсивність вияву вразливостей та критичність атаки [17]. Для оцінювання середнього значення інтенсивності вияву вразливостей при допущеннях, зазначених у [16], можливо використання часових міток – часу фіксації вразливості в БД (якщо вразливість зафіксовано в різних репозитаріях, необхідно визначити найраніший час внесення вразливості в БД).

Дослідження дат, що містяться в файлах форматів CVE, CVRF і NVD, показують, що публікація однієї й тієї ж вразливості в NVD відбувається значно пізніше (як правило, через кілька тижнів, а іноді й місяців), ніж у CVE або CVRF. Даний факт може свідчити про те, що фахівцям, які супроводжують базу NVD, потрібно більше часу перед публікацією інформації

про вразливість, щоб зібрати більше інформації про неї (метрики критичності вразливості, список вразливих продуктів, тип загрози, що подається вразливістю, та іншу корисну інформацію). Порівняння дат публікації інформації про вразливість у базі даних NVD з інформаційними бюлетенями розробників вразливих програмних продуктів, у яких анонсується випуск виправлень для усунення вразливостей, показує, що ці дати переважно збігаються. Отже, було висунуто припущення про те, що дату публікації інформації про вразливість у базі NVD можна вважати датою випуску оновлення, що усуває вразливість. Водночас дату публікації інформації про вразливість у базі даних CVE (у форматі CVRF) можна вважати датою офіційного виявлення (розкриття) вразливості.

За основу під час об'єднання інформації про вразливість із різних джерел (CVE, CVRF і NVD), були прийняті такі допущення [12]: 1) датою розкриття вразливості вважати мінімальну з дат у розглянутих джерелах даних; 2) датою усунення вразливості вважати максимальну з дат урозглянутих джерелах даних. При цьому слід зазначити, що дати модифікації запису про вразливість не беруть участі в пошуку дат розкриття й усунення, оскільки вони не відображають стадію вразливості, а лише той факт, що цей запис було змінено.

Отримання дат виявлення і усунення вразливостей дає змогу застосувати апарат марковського моделювання та систем масового обслуговування для оцінювання рівня вразливості усієї комп'ютерної системи. У цілому алгоритм отримання цих параметрів на основі статистичного аналізу узагальненої бази даних про вразливості складається з таких етапів:

1) фільтрація вразливостей із досліджуваного програмного продукту й для необхідного інтервалу часу;

2) групування вразливостей за однією з дат, залежно від типу, від параметра, який потрібно отримати в результаті;

3) перерахунок абсолютної дати виявлення вразливості в інтервальну, відносно початку досліджуваного інтервалу, в годинах;

4) дослідження закону розподілу з оцінюванням значень його параметрів.

Для формування підмножин-вибірок вразливостей (на прикладі сімейства веб-серверів Apache) було застосовано такі критерії відбору:

– атрибут "cvss:access-vector" – значення мережне, (Network, N);

– атрибут "cvss:availability-impact" – значення часткове, (Partial, P) та повне, (Complete, C);

– атрибут "vuln:product" – значення "*Apache*";

– атрибут "vuln:published-datetime" – значення, що містить досліджуваний часовий проміжок (конкретний рік).

Для аналізу невеликої кількості вразливостей можна скористатися сторінкою розширеного пошуку в базі NVD [19]. У розширеному пошуку в базі дані видачі розділень на сторінки по 20 записів на кожній (рис. 3).

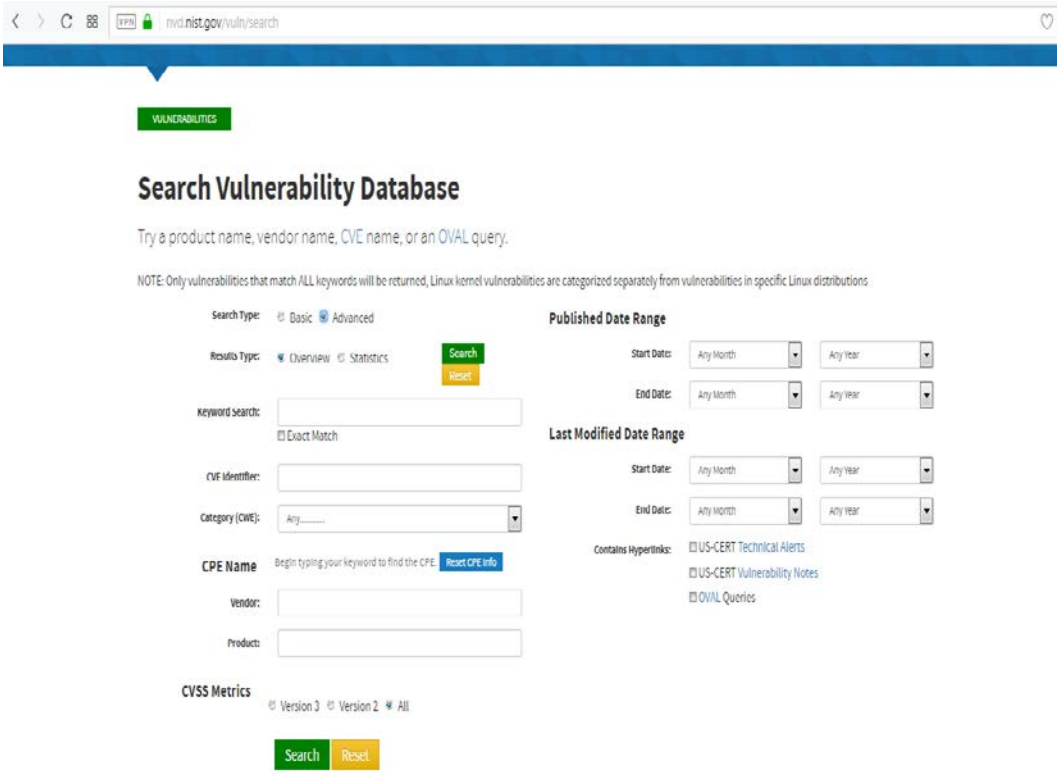


Рис. 3. Веб-інтерфейс розширеного пошуку NVD
для формування підмножин вразливостей доступності

Це суттєво ускладнює отримання й обробку вибірки великого обсягу та робить недоцільним ручну обробку даних для виконання поставлених завдань. Тому обрано більш прийнятний варіант обробки бази вразливостей у вигляді XML-документів. Для цього необхідно завантажити з сайту NVD архівний файл за відповідний рік. В отриманих у результаті фільтрації множинах вразливостей необхідно зафіксувати параметри “published” та “base_score”.

Було розглянуто дві вибірки з БД для вразливостей доступності сімейства веб-серверів Apache у 2015, 2016 рр. Результати оцінювання параметрів експоненціального розподілу отримано за допомогою інструментарію “Distribution fitting tool” пакета Matlab.

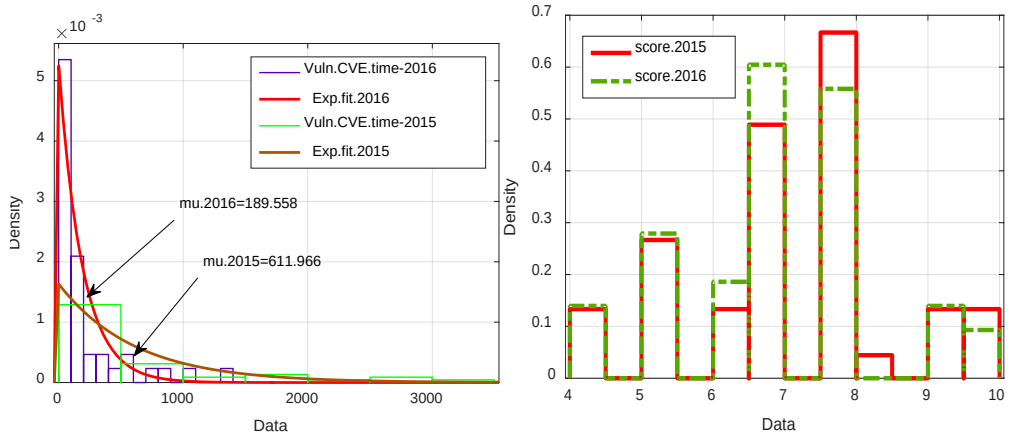


Рис. 4. Результати оцінювання параметрів вияву вразливостей доступності серверів Apachey 2015, 2016 рр.

Оскільки інформація про вразливості може надійти в базу як від спеціалістів з безпеки, так і після їх експлуатації зловмисниками, то час реєстрації вразливості відображає ступінь зацікавленості дослідниками конкретним елементом веб-сервера. Очевидна тенденція поступового зростання зацікавленості до мережених програмних продуктів, зокрема веб-серверів Apache [15]. Так, середній час реєстрації нових вразливостей доступності серверів Apachey 2016 р. скоротився у 3,23 раза порівняно з 2015 р. Також слід зазначити, що середня критичність вразливостей у 2015 р. (6,96) була більшою за цей же показник 2016 р. (6,78).

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Розглянуто питання параметризації вразливостей на основі вибірок із відкритих баз для використання у якості вхідних даних марковських моделей оцінювання доступності веб-ресурсів.

Проаналізовано актуальний стан зв'язків відкритої бази вразливостей CVE з іншими базами вразливостей. Визначено активність БД, їх відкритість, платний доступ чи можливість пробного/обмеженого використання. Розглянуто отримання та уточнення інформації з бази даних вразливостей NVD.

Виконано параметризацію вразливостей веб-серверів сімейства Apache на річних інтервалах 2015, 2016 рр. на основі вибірок із відкритих баз вразливостей. Результати дослідження показали, що у 2016 р. нові вразливості з вибірки фіксувалися у 3,23 раза швидше, але при цьому в середньому їхня критичність зменшилась на 3 %.

Для прискорення й зручнішою створення вибірок доцільно розробити програмне забезпечення, яке автоматично створюватиме необхідну вибірку після вибору критеріїв формування. Також для покращання результатів дослідження слід уточнювати інформацію про вразливість у декількох відкритих базах.

Список використаних джерел

1. *Присяжний Д. П.* Удосконалення захисту веб-ресурсів від атак на основі комбінованого евристично-статистичного підходу // Реєстрація, зберігання і обробка даних. 2016. Т. 18. № 1. С. 63–69.

2. *Федорченко А. В., Чечулин А. А., Котенко И. В.* Исследование открытых баз уязвимостей и оценка возможности их применения в системах анализазащищенности компьютерных сетей // Информационно-управляющие системы. 2014. № 5. С. 72–79.

3. Common Vulnerabilities and Exposures / The MITRE Corporation. URL: http://cve.mitre.org

4. Secunia Research Community / Flexera Software LLC. URL: https://secuniaresearch.flexerasoftware.com. 15.01.2019 p.

5. Security Focus database of computer security / SecurityFocus Symantec Corporate Offices. URL: http://www.securityfocus.com

6. Exploit Database by Offensive Security / Exploit Database by Offensive Security. URL: https://www.exploit-db.com

7. Microsoft Security Bulletins / Microsoft Corporation. URL: https://docs.microsoft.com/en-us/ security-updates/securitybulletins/securitybulletins

8. CERT Vulnerability Notes Database / Carnegie Mellon University Software Engineering Institute. URL: https://www.kb.cert.org/vuls

9. Android Security Bulletins / Android by Google LLC and the Open Handset Alliance. URL: https://source.android.com/security/bulletin

10. National vulnerability database / NIST Computer Security Division, Information Technology Laboratory. URL: https://nvd.nist.gov

11. *Федорченко А. В., Чечулин А. А., Котенко И. В.* Построение интегрированной базы уязвимостей // Известия вузов. Приборостроение. 2014. Т. 57. № 11. С. 62–67.

12. *Белобородов А. Ю., Горбенко А. В.* Применение баз данных уязвимостей в задачах исследования безопасности программных средств // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка. 2015. Вип. 165. С. 83–85.

13. *Алаа Мохаммед Абдул-Хади, Поночовный Ю. Л., Харченко В. С.* Разработка базовых марковских моделей для исследования готовности коммерческих веб-сервисов // Радіоелектронні і комп'ютерні системи. 2013. Вип. 5 (64). С. 186–191.

14. *Царегородцев А. В., Макаренко Е. В.* Методика количественной оценки риска в информационной безопасности облачной инфраструктуры организации // Дайджест-финансы. 2015. № 1 (233). С. 56–67.

15. *Kharchenko V., Ponochovnyi Y., Mustafa Qahtan Abdulmunem A.-S., Andrashov A.* Availability models and maintenance strategies for smart building automation systems considering attacks on component vulnerabilities // Advances in Intelligent Systems and Computing. 2018. Vol. 582. P. 186–195.

16. *Алаа Мохаммед Абдул-Хади.* Оценка интенсивности атаки на уязвимости доступности коммерческих веб-сервисов // Системи обробки інформації. 2013. Вип. 6 (113). С. 204–208.

17. *Харченко В. С., Алаа Мохаммед Абдул-Хади, Поночовный Ю. Л.* Формирование подмножеств уязвимостей доступности коммерческих веб-сервисов // Системи обробки інформації. 2013. Вип. 8 (115). С. 240–243.

18. CVE Reference Key/Maps / The MITRE Corporation. URL: https://cve.mitre.org/data/refs/index.html

19. NVD – Search and Statistics / NIST Computer Security Division, Information Technology Laboratory. URL: https://nvd.nist.gov/ vuln/search

References:

1. Prisyashniy D. P. (2016), *"Udoskonalennya zakhystu veb-resursiv vid atak na osnovi kombinovanoho evrystychno-statystychnoho pidkhodu"* ["Improving the protection of web resources from attacks on the basis of a combined heuristic-statistical approach"], Collection of scientific works *Reyestratsiya, zberihannya i obrobka danykh* [Registration, storage and processing of data], tom 18, vol. 1, pp. 63–69 [Ukraine].

2. Fedorchenko A. V., Chechulin A. A. and Kotenko I. V. (2014.), *"Issledovaniye otkrytykh baz uyazvimostey i otsenka vozmozhnosti ikh primeneniya v sistemakh analizazashchishchennosti komp'yuternykh setey"* ["Study of open databases of vulnerabilities and assessment of their applicability in computer security analysis systems"], Journal *Informatsionno-upravlyayushchiye sistemy* [Information Control Systems], vol. 5, pp. 72–79 [Russia].

3. Common Vulnerabilities and Exposures / The MITRE Corporation, available at: http://cve.mitre.org – 15.01.2019.

4. Secunia Research Community / Flexera Software LLC, available at: https://secuniaresearch.flexerasoftware.com – 15.01.2019.

5. SecurityFocus database of computer security / SecurityFocus Symantec Corporate Offices, available at: http://www.securityfocus.com – 15.01.2019.

6. Exploit Database by Offensive Security / Exploit Database by Offensive Security, available at: https://www.exploit-db.com - 15.01.2019.

7. Microsoft Security Bulletins / Microsoft, available at: https://docs.microsoft.com/en-us/security-updates/securitybulletins – 15.01.2019.

8. CERT Vulnerability Notes Database / Carnegie Mellon University Software Engineering Institute, available at: Access mode: https://www.kb.cert.org/ vuls – 15.01.2019.

9. Android Security Bulletins / Android by Google LLC and the Open Handset Alliance, available at: https://source.android.com/security/bulletin – 15.01.2019.

10. National vulnerability database / NIST Computer Security Division, Information Technology Laboratory, available at: https://nvd.nist.gov – 15.01.2019.

11. Fedorchenko A. V., Chechulin A. A. and Kotenko I. V. (2014), *"Postroyeniye integrirovannoy bazy uyazvimostey"* ["Building Integrated Vulnerability Base"] Collection of scientific works *Izvestiya vuzov. Priborostroyeniye* [Izvestiya Vuzov. Instrument making], vol. 57, No. 11, pp. 62-67 [Russia].

12. Beloborodov A. Yu. and Gorbenko A. V. (2015), *"Prymenenye baz dannykh uyazvymostey v zadachakh yssledovanyya bezopasnosty prohrammnykh sredstv"* ["Using vulnerability databases in software security research tasks"], *Visnyk Kharkivs'koho natsional'noho tekhnichnoho universytetu sil's'koho hospodarstva imeni Petra Vasylenka* [Bulletin of Kharkiv National Technical University of Peter Vasilenko], vol. 165, pp. 83–85 [Ukraine].

13. Alaa Mohammed Abdul-Hadi, Ponochovny Yu. L. and Kharchenko V. S. (2013), *"Razrabotka bazovykh markovskikh modeley dlya issledovaniya gotovnosti kommercheskikh veb-servisov"* ["Development of basic Markov models for the study of the availability of commercial web services"], Journal *Radíoyelektronní í komp'yuterní sistemi* [Radio and Computer and Computer Systems, vol. 5 (64), pp. 186–191 [Ukraine].

14. Tsaregorodtsev A. V. and Makarenko E. V. (2015), *"Metodika kolichestvennoy otsenki riska v informatsionnoy bezopasnosti oblachnoy infrastruktury organizatsii"* ["Method of quantitative risk assessment in the information security of the organization's cloud infrastructure"], Journal *Daydzhest-finansy* [Digest Finance], vol. 1 (233), pp. 56–67 [Russia].

15. Kharchenko V., Ponochovnyi Yu., Mustafa Qahtan Abdulmunem A.-S. and Andrashov A. (2018), "Availability models and maintenance strategies for smart building automation systems considering attacks on component vulnerabilities", Advances in Intelligent Systems and Computing, vol. 582, pp. 186–195.

16. Alaa Mohammed Abdul-Hadi (2013), *"Otsenka intensivnosti ataka na uyazvimosti dostupnosti kommercheskikh veb-servisov"* ["Assessment of the intensity of the attack on the vulnerability of the availability of commercial web services"], Journal *Systemy obrobky ínformatsíi* [Processing Systems Information], vol. 6 (113), pp.204–208 [Ukraine].

17. Kharchenko V. S. Alaa Mohammed Abdul-Hadi and Ponochovny Yu. L. (2013), *Formirovaniye podmnozhestv uyazvimostey dostupnosti kommercheskikh veb-servisov* ["Formation of subsets of accessibility vulnerabilities in commercial web services"], Journal *Sistemi obrobki ínformatsíí*

DOI: https://doi.org/10.32836/2521-6643-2019-1-57-6
УДК 62-526

О. В. Іванченко, кандидат технічних наук,
доцент кафедри інформаційних систем
та технологій Університету митної справи
та фінансів

АНАЛІТИКО-СТОХАСТИЧНИЙ МЕТОД ПОБУДОВИ СТРУКТУРНИХ СХЕМ БЕЗПЕКИ КІБЕРНЕТИЧНИХ АКТИВІВ СИСТЕМИ SCADA КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Забезпечення інформаційної безпеки систем диспетчеризації та збирання даних типу SCADA, які застосовуються у відповідному контурі управління критичної інфраструктури (КІ) – одне з найважливіших завдань, які виконуються за напрямом критичний комп'ютинг та інженерія безпеки. Наочним прикладом цього є атаки на компоненти критичної енергетичної інфраструктури (КЕІ), коли фактично зловмисні впливи на кібернетичні активи системи SCADA призводили до відключення обласних енергетичних кластерів КЕІ. Тому актуальність статті, яка присвячена розробці методу побудови структурних схем безпеки SCADA КІ на основі оцінювання рівня надійності, готовності компонентів та можливості протидії зловмисним впливам на загальні кібернетичні активи, не викликає сумніву.

Ключові слова: *система SCADA; критична інфраструктура; кібернетичні активи; структурна схема безпеки; аналітико-стохастичне оцінювання.*

Обеспечение информационной безопасности систем диспетчеризации сбора данных типа SCADA, используемых в соответствующем контуре управления критической инфраструктуры (КИ), является одной из важнейших задач, которые решаются в рамках исследований, проводимых в сфере критического компьютинга и инженерии безопасности. Атаки на компоненты критической энергетической инфраструктуры (КЭИ), когда фактически злонамеренные воздействия на кибернетические активы системы SCADA приводили к отключению областных энергетических кластеров, – яркое тому свидетельство. Поэтому актуальность статьи, которая посвящена разработке метода построения структурных схем безо-

пасности SCADA КИ на основе оценивания уровня надёжности, готовности компонентов и возможности противодействия злонамеренным воздействиям на общие кибернетические активы, не вызывает сомнения.

Ключевые слова: *критическая инфраструктура; кибернетические активы; структурная схема безопасности; аналитико-стохастическое оценивание.*

Safety and security of supervisory control and data acquisition systems (SCADA), which utilize in corresponding management circuit of a critical infrastructure (CI) is one of the most important task that to be explored. This task is also serious issue for critical computing and security engineering realm. Familiar examples of the negative events for critical energy infrastructure's (CEI) components, when malicious deliberate impacts on cyber assets of SCADA system led to outages of the regional energy clusters are bright evidences of this issue. Therefore, the presented paper is devoted to a technique development of security block diagrams for CI SCADA systems based on assess of dependability and availability of their components considering malicious deliberate impacts on overall cyber assets. In fact, it is also undoubtedly distinct significant issue into critical computing realm. Proposed technique is developed based on taxonomy for risk assess considering some negative factors. These negative factors can influence on overall availability and cybersecurity of the CI. Therefore, how to get safety and security assessments and further how to ensure effective functioning of SCADA CI is a distinct significantissue, which to be explored. The technique involves concrete steps in order to build fault tree for cyber assets of the SCADA CI. Next step allows to write overall equation for system failure based on the use of received fault tree. In addition, the researcher continues to build a reliability block of diagram (RBD) in order to estimate overall availability level for cyber assets of the SCADA CI. Using RBD and information about deliberate malicious impacts (DMIs), researcher can be built a DMI block diagram in order to estimate probability assessment for different DMIs. As general results, the researcher can determine probability of compromize operation, when intruders want to implement the DMI. Thus, if you wanted to perform a deep analysis of safety and security of the SCADA system of the CI considering different negative events, such as sudden and hidden failures, accidents and disaster of the CI, including DMIs, you would be able to use the proposed technique.

Key words: *critical infrastructure; cyber assets; security block diagrams; analytical and stochastic assessments.*

Постановка проблеми. У сучасному суспільстві критична інфраструктура (КІ) є важливою складовою, яка безпосередньо впливає на якість життя людей та визначає певний рівень національної безпеки будь-якої країни. Тому інтенсифікація розвитку КІ супроводжується сталим зростанням ресурсів, сервісів та відповідної продукції, які постачаються саме нею, чому значною мірою сприяє широкомасштабне впровадження інформаційних технологій та розширення відповідних кібернетичних активів інфраструктури. Безумовно, це призводить до підвищення ефективності управління КІ на основі застосування програмно-апаратних засобів, які об'єднуються в системи диспетчеризації та збирання даних типу SCADA. Водночас замкнений контур управління КІ створюється за рахунок повсюдного використання технологій цифрової трансформації, звичайного та промислового Інтернету речей (IoT, IIoT) тощо.

Однак процес упровадження цих новітніх технологій супроводжується зниженням рівня функціональної та інформаційної безпеки КІ, що особливо чітко спостерігається на прикладі критичної енергетичної інфраструктури (КЕІ). Зокрема, відбуваються аварії, інциденти і катастрофи КЕІ, наприклад аварії на Саяно-Шушенській ГЕС (Росія, 2009 р.), на АЕС Фукусіма (Японія, 2011 р.), відомі випадки каскадних відключень енергопостачання в США та Європі, включаючи відключення вітчизняних обленерго за останні чотири роки. Відомо [1], що під час відключень українських обласних енергетичних кластерів здійснювалися зловмисні впливи на контур управління КЕІ з реалізацією хакерських атак на систему SCADA. Ці та інші фактори негативного впливу створили відповідні передумови для виникнення науково-прикладної проблеми, яка полягає в необхідності розробки методу оцінювання і контролю рівня функціональної, інформаційної безпеки системи SCADA КІ з урахуванням її мережних кібернетичних активів.

Аналіз останніх досліджень і публікацій. Розгляд публікацій за напрямом досліджень розпочнемо з праць [2; 3], присвячених цифровим пристроям функціонального контролю інформаційно-управляючих систем (ІУС) на основі застосування FPGA-логіки, тобто логіки, яка побудована на програмованих логічних інтегральних схемах. Нині застосування FPGA-логіки дає можливість покращити функціональність і відмовостійкість компонентних складових ІУС. Тому цілком виправдане прагнення як виробників, так і персоналу КІ використовувати FPGA-логіку для створення пристроїв оцінки та контролю функціональної безпеки систем SCADA інфраструктурного рівня.

У дослідженні [4] розглянуто моделі готовності, які застосовуються для оцінки рівня відмовостійкості систем SCADA з урахуванням можливості управління з використанням віддалених терміналів (ВТ). Значна ча-

стина роботи висвітлює особливості застосування методу розбудови діаграм відмовостійкості саме для ВТ. Слід також зазначити, що для досягнення необхідного рівня кібербезпеки систем SCADA деякі автори пропонують застосовувати випробувальний стенд, до складу якого входять різноманітні компоненти, включаючи ВТ, інфокомунікаційні системи, фізичну інфраструктуру, сенсори та виконавчі механізми. Архітектурна реалізація стенда подана в праці [5].

Водночас у праці [6] відображено процес ітераційного моделювання для забезпечення надійного функціонування інфокомунікаційних мереж системи SCADA, яка входить до складу ІУС критичної енергетичної інфраструктури. Фактично автори реалізували процес моделювання відповідно до конкретних сценаріїв розвитку подій на основі застосування програмного інструментарію Möbius [7].

З погляду викладення фундаментальних основ застосування відомих аналітико-стохастичних методів та моделей, цікава праця [8], присвячена аналізу можливостей застосування відомих методів структурних схем надійності (ССН) [9], дерева відмов (ДВ) [10; 11], марковських моделей і стохастичних мереж Петрі [12–14] для оцінювання готовності різноманітних комп'ютерних систем критичного призначення. Моделювання процесів зміни рівня готовності, надійності та живучості комп'ютерних віртуальних систем, хмарної приватної та мобільної інфраструктур на основі застосування відомих методів ССН, ДВ [9–11] і неперервних марковських ланцюгів відображено в [15–18]. Марковський процес моделювання лежить також в основі аналітико-стохастичного підходу, який застосовується для аналізу та оцінки ефективності заходів щодо забезпечення необхідного рівня кібербезпеки системи домашнього Інтернету з урахуванням вразливостей компонентних складових [19].

В окремих випадках дослідження та аналіз заходів безпеки систем SCADA може здійснюватись із застосуванням немарковського апарата моделювання. Це стосується ситуацій, коли не спостерігається марковська властивість, скажімо, перевищено період виконання сезонного технічного обслуговування та діагностики технологічного комп'ютерного обладнання SCADA; коли протягом декількох років не проводиться оновлення програмного забезпечення системи SCADA; внаслідок помилок обслуговуючого персоналу виникають непередбачені тривалі простої обладнання SCADA тощо. Серед немарковських моделей, як правило, перевагу віддають напівмарковським моделям. Це пов'язано з тим, що цей тип моделей дозволяє враховувати як різні режими застосування за призначенням, так і різноманітну природу виникнення негативних явищ для ІУС КІ. Отже, на відміну

від марковського, напівмарковський процес моделювання (НПММ) може бути реалізовано для багатофункціональних компонентів КІ, які застосовуються за призначенням протягом випадкового і детермінованого інтервалів часу з урахуванням усієї попередньої історії розвитку та для різноманітних стохастичних залежностей параметрів об'єкта дослідження [20]. Тому на основі НПММ було виконано аналіз ефективності системи контролю та моніторингу технічного стану критичної інфраструктури [20; 21], обґрунтовано перехід до управління КІ за технічним мегастаном з урахуванням надійності її компонентних складових [22; 23]. У праці [24] розглянуто, яким чином НПММ може бути застосовано для аналізу аварій та інцидентів критичної енергетичної інфраструктури. Порівняльний аналіз кількісних результатів марковського та НПММ моделювання підтверджує [20], що напівмарковський процес моделювання краще відображає реальну ситуацію щодо інформаційно-технічного стану КІ і повною мірою відповідає вимогам критичного комп'ютингу [25].

Не зважаючи на відповідність певним нормативним вимогам, нині відомі факти та наслідки хакерських атак на кіберактиви національної КІ [1], що підтверджують її вразливість. Цей негативний фактор впливу, який створено ненавмисно штучно, відображає кіберфізичну природу КІ [26] та відкриває різноманітні можливості щодо втручання в контур управління інфраструктури завдяки використанню активів системи SCADA. Відповідно до [27], серйозною загрозою для систем SCADA можуть бути вразливості їхнього програмного забезпечення, які створюють передумови для успішної реалізації кібератак різноманітного походження. Ці обставини викликають серйозну стурбованість як у виробників, так і в користувачів систем SCADA, які закликають створювати законодавчу базу для розробки різних механізмів забезпечення кібербезпеки [28].

Справжнім відкриттям щодо реалізації зловмисних впливів (ЗЛВ) на кібернетичні ресурси SCADA стали віруси Stuxnet і Flame, які у 2010 та 2012 рр. були реалізовані у вигляді розподіленої бот-мережі, завдяки чому в усьому світі було інфіковано від 50 до 100 тисяч комп'ютерних систем одночасно [29; 30]. Отже, в минулі роки й досі актуальне завдання – створення ефективного кіберзахисту всіх видів активів КІ, включаючи системи SCADA.

Заходи кіберзахисту SCADA системи КІ можуть бути реалізовані на рівні архітектурних рішень. Так, у [31–34] розглянуто й виконано аналіз архітектурних рішень щодо забезпечення кіберзахисту типової системи SCADA як на рівні додатків, каналів передачі даних, так і на мережному рівні.

Подальші перспективи розвитку систем SCADA значною мірою залежать від можливостей застосовувати додаткові хмарні ресурси та сервіси, що дуже посилює інформаційно-обчислювальний потенціал і розширює динамічний діапазон управління КІ. Виходячи з цього, виправданим є застосування мобільної хмарної інфраструктури (МХІ) в системі управління КІ. Для оптимізації енергоспоживання та частотного діапазону кінцевих пристроїв МХІ в [35] автори використали напівмарковські моделі прийняття рішень. Останні дослідження у сфері кібербезпеки ІУС КІ [36] підтверджують високу ефективність застосування адаптивних багатофункціональних хмарних систем як брандмауерів, які використовуються для двосторонньої фільтрації інформаційного трафіку. В працях [37; 38] викладено результати досліджень щодо застосування додаткового хмарного ресурсу з метою створення системи управління інтелектуальною розподіленою енергетичною інфраструктурою майбутнього.

Мета статті. За результатами виконаного аналізу можна зробити висновок, що для посилення наявної системи функціональної та інформаційної безпеки КІ необхідно вдосконалювати відомі аналітико-стохастичні методи оцінювання рівня готовності та кібербезпеки SCADA. Виходячи із цього, мета статті – розробка аналітико-стохастичного методу побудови структурних схем безпеки (ССБ) системи SCADA критичної інфраструктури з урахуванням аспектів, пов’язаних із забезпеченням доступності та захисту її кібернетичних активів від зловмисних впливів і проникнень.

Виклад основного матеріалу. Особливо гостро проблема забезпечення доступності та захисту кібернетичних активів стоїть перед національною КЕІ. Про це свідчить зростання кількості кібератак та суттєве зниження готовності фізичних активів національної КЕІ за останні п’ять років. Значною мірою цьому сприяє той факт, що рівень зношеності енергетичного обладнання національної мережі КЕІ перевищує 70 %.Саме ці два потужних негативних фактори впливу враховуватимемо в розбудові структурних схем безпеки SCADA КІ.

Як базову розглянемо спрощену архітектурну реалізацію кібернетичних активів SCADA КІ (рис. 1). Основною функцією системи на мережному рівні є обробка даних, які надходять безпосередньо від КІ, а також контроль та моніторинг інформаційно-технічних станів, параметрів інфраструктури. Згідно з рис. 1 перший рівень створено мережею кінцевих пристроїв, до складу яких входять програмні логічні контролери (ПЛК) та пристрої зв’язку з об’єктом (ПЗО). Фактично ПЛК та ПЗО забезпечують обробку інформації від сенсорних систем і модулів КІ.

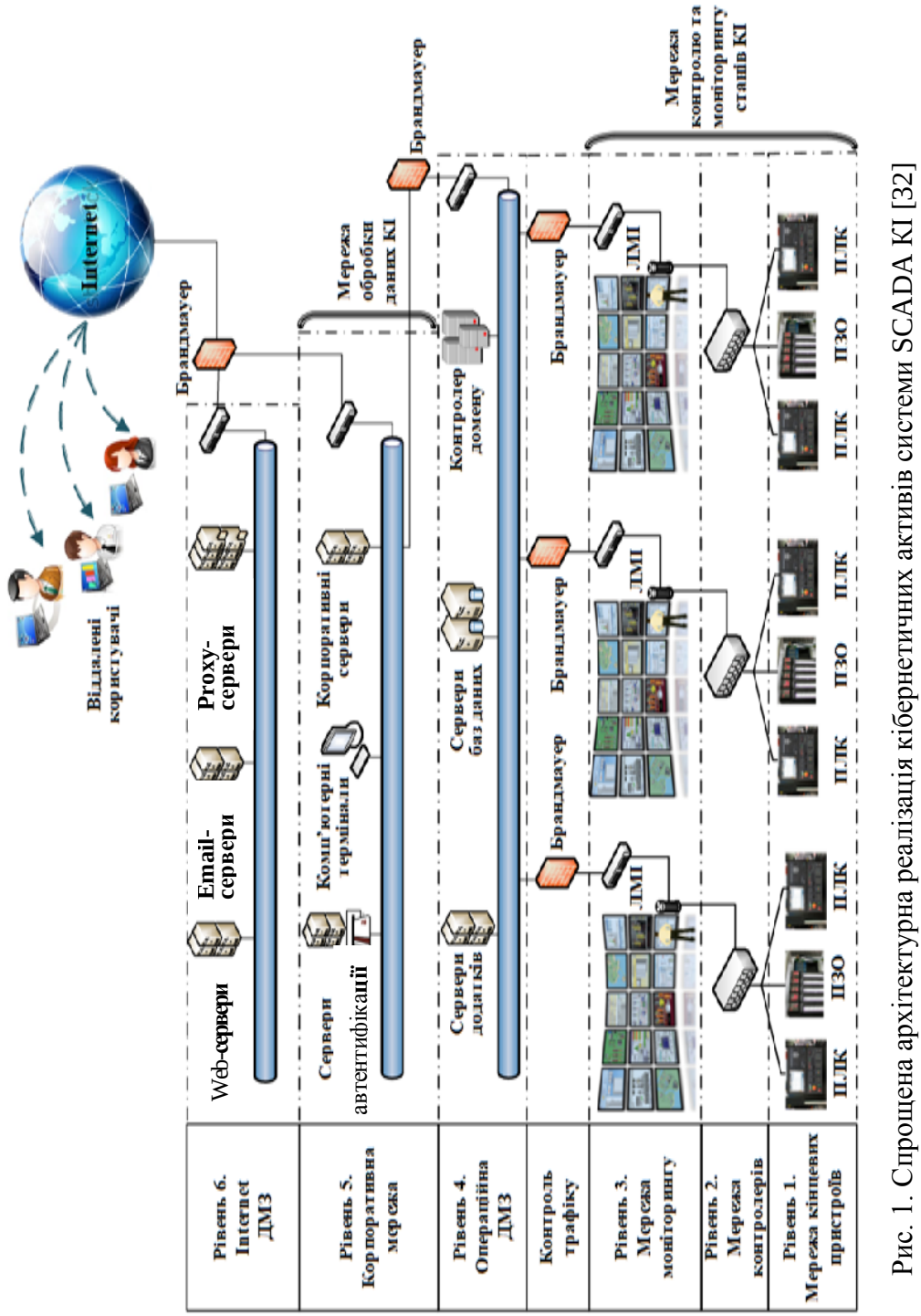


Рис. 1. Спрощена архітектурна реалізація кібернетичних активів системи SCADA КІ [32]

Детальний аналіз функціональних особливостей побудови мережних рівнів кібернетичних активів SCADA КІ (рис. 1) виконано в [32]. Зауважимо, що в розробці пропонованого методу було враховано негативні фактори, які впливають на рівень функціональної (ФБ) та інформаційної безпеки (ІБ) SCADA відповідно до вимог стандартів IEC 61508, ISA/IEC 62443 та рекомендацій, наведених у [39; 40]. Логічним завершенням виконаного аналізу є пропонований аналітико-стохастичний метод побудови ССБ кібернетичних активів системи SCADA КІ, який містить такі кроки.

Перший крок. Визначення кількості мережних рівнів згідно з архітектурною реалізацією кібернетичних активів SCADA КІ (рис. 1).

Другий крок. Побудова таксономічної схеми ризику негативного впливу на ФБ та ІБ системи SCADA КІ. На рис. 2 зображено таксономію виникнення ризику ФБ та ІБ системи SCADA КІ з урахуванням двох найбільш суттєвих негативних факторів впливу, а саме: зловмисних впливів на кібернетичні активи; відмов та збоїв комп'ютерного обладнання і відповідних програмних модулів. Фактично наведена таксономічна схема (рис. 2) пояснює природу виникнення загрози безпеці системи SCADA.

Відповідно до рис. 2 концепція безпеки полягає в зниженні ризику системи SCADA КІ за рахунок зменшення відмов та збоїв її комп'ютерного обладнання і програмного забезпечення, а також завдяки усуненню ЗЛВ на кібернетичні активи, які застосовуються в контурі управління інфраструктурою. Слід ще раз звернути увагу на те, що суттєвим обмеженням дії запропонованої концепції є врахування лише двох найбільш актуальних негативних факторів впливу.

Третій крок. Розробка логіко-ймовірнісної моделі ризику для ФБ та ІБ (далі – безпеки) системи SCADA КІ.

Згідно з таксономічною схемою (рис. 2) логіко-ймовірнісна модель ризику для безпеки (РБ) системи SCADA КІ з урахуванням факторів негативного впливу може бути записана у такому вигляді:

$$Risk = P\left\{\left[\left(SAF \cup INS\right) \cap FF\right] \cap \left[FF \cap DMI\right] \cap \left[\left(SAF \cup INS\right) \cap DMI\right]\right\}, \qquad (1)$$

де SAF – ФБ системи SCADA КІ;

INS – ІБ системи SCADA КІ;

FF – відмови та збої комп'ютерного обладнання і програмного забезпечення SCADA КІ; DMI – ЗЛВ на кібернетичні активи SCADA КІ.

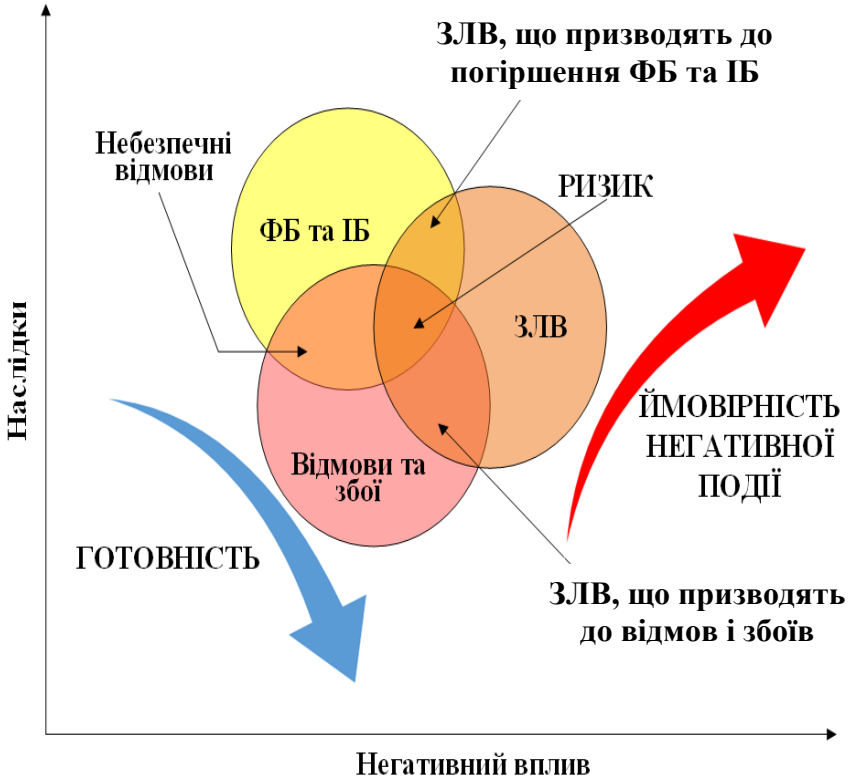


Рис. 2. Таксономія ризику для функціональної та інформаційної безпеки системи SCADA КІ

Четвертий крок. Побудова діаграми системної відмови (ДСВ) з урахуванням факторів негативного впливу на кібернетичні активи системи SCADA КІ.

На рис. 3 зображено ДСВ відповідно до отриманої логіко-ймовірнісної моделі РБ (1) системи SCADA КІ, яка враховує відмови комп'ютерного обладнання, збої програмного забезпечення та зловмисні впливи на кібернетичні активи. Пропозиції, наведені в [10; 11], були використані як теоретичне підґрунтя в побудові ДСВ.

Головна особливість отриманої ДСВ (рис. 3), на відміну від відомих, полягає у відображенні ЗЛВ (позначається як DMI) на сервери відповідного мережного рівня. Це дає можливість отримати комплексну ймовірнісну оцінку готовності (доступності) кіберактивів SCADA з урахуванням природи виникнення та механізмів дії ЗЛВ. Моделі ЗЛВ на кіберактиви системи SCADA КІ на основі НПММ перспективні з погляду подальших досліджень.

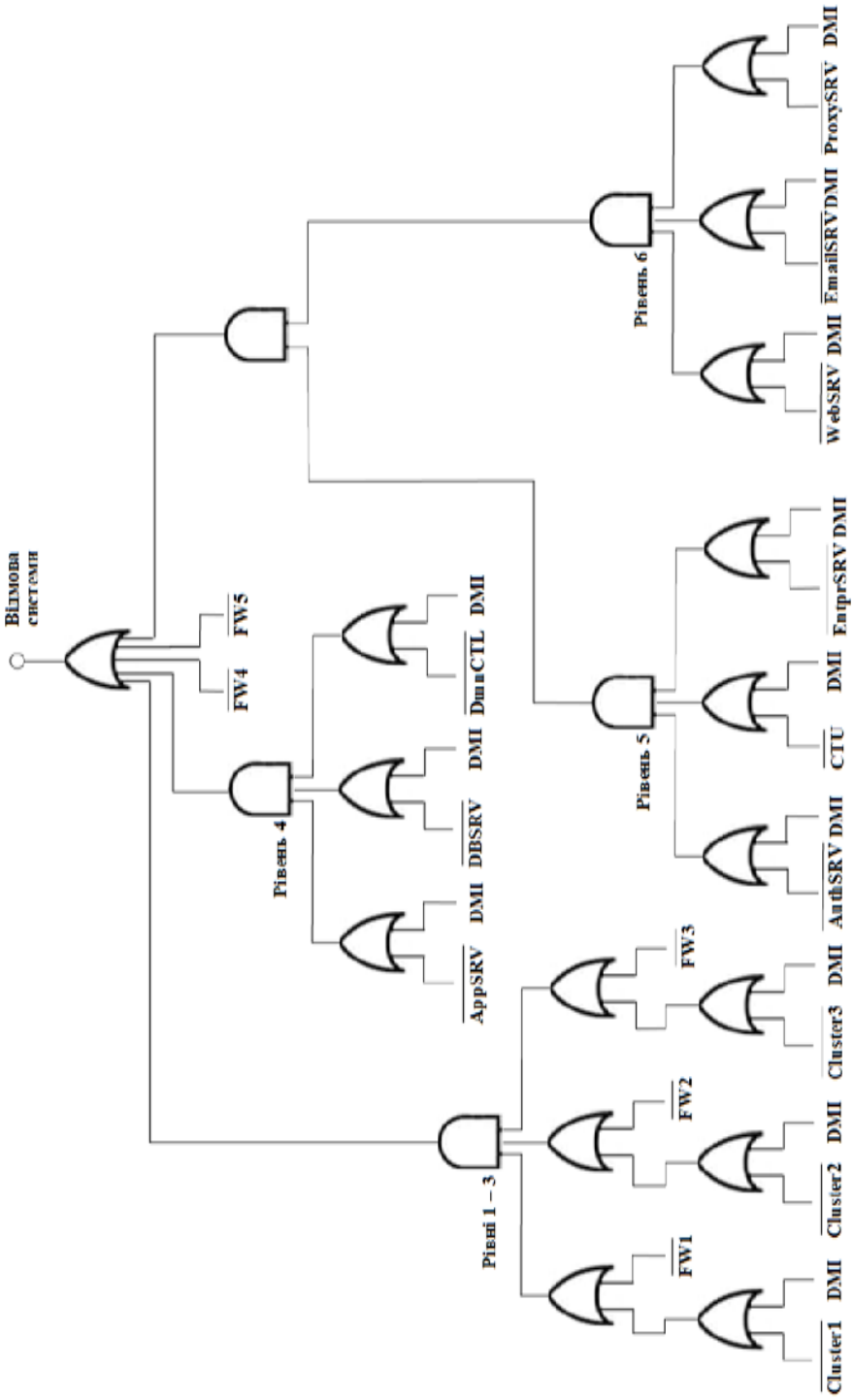


Рис. 3. Діаграма системної відмови кібернетичних активів системи SCADA КІ

Відображені на діаграмі (рис. 3) кластери $Cluster1,2,3$ утворені шляхом укрупнення та об'єднання елементів мережних рівнів 1, 2, 3, а саме: ПЛК, ПЗО, контролерів та людино-машинних інтерфейсів (ЛМІ).

П'ятий крок. Визначення комплексної ймовірнісної оцінки неготовності кіберактивів SCADA КІ.

Відповідно до зображеної рис. 3 ДСВ комплексна ймовірнісна оцінка готовності кіберактивів SCADA КІ може бути визначена так:

$$UnAvailability = P\left(\Phi\left(X\right)=0\right) = P\left\{UA_{1-3} \cup UA_4 \cup \left[UA_5 \cap UA_6\right] \cup \right.$$
$$\left. \cup \overline{FW4} \cup \overline{FW5} \right\}, \quad (2)$$

$$UA_{1-3} = \left\{\left[\overline{Cluster1} \cup DMI\right] \cup \overline{FW1}\right\} \cap \left\{\left[\overline{Cluster2} \cup DMI\right] \cup \overline{FW2}\right\} \cap$$
$$\cap \left\{\left[\overline{Cluster3} \cup DMI\right] \cup \overline{FW3}\right\}, \quad (3)$$

$$UA_4 = \left[\overline{AppSRV} \cup DMI\right] \cap \left[\overline{DBSRV} \cup DMI\right] \cap \left[\overline{DmnCTL} \cup DMI\right], \quad (4)$$

$$UA_5 = \left[\overline{AuthSRV} \cup DMI\right] \cap \left[\overline{CTU} \cup DMI\right] \cap \left[\overline{EntprSRV} \cup DMI\right], \quad (5)$$

$$UA_6 = \left[\overline{WebSRV} \cup DMI\right] \cap \left[\overline{EmailSRV} \cup DMI\right] \cap \left[\overline{Pr\,oxySRV} \cup DMI\right], \quad (6)$$

де $\overline{Cluster1}, \overline{Cluster2}, \overline{Cluster3}$ – події, які полягають у неготовності кластерів $Cluster1,2,3$;

$\overline{FW1}, \overline{FW2}, \overline{FW3}, \overline{FW4}, \overline{FW5}$ – події, які полягають у неготовності брандмауерів 1–5;

$\overline{AppSRV}$ – подія, яка полягає в неготовності серверів додатків;

$\overline{DBSRV}$ – подія, яка полягає в неготовності серверів баз даних;

$\overline{DmnCTL}$ – подія, яка полягає в неготовності контролера домену;

$\overline{AuthSRV}$ – подія, яка полягає в неготовності серверів автентифікації;

$\overline{CTU}$ – подія, яка полягає в неготовності комп'ютерних терміналів;

$\overline{EntprSRV}$ – подія, яка полягає в неготовності корпоративних серверів;

$\overline{WebSRV}$ – подія, яка полягає в неготовності web-серверів;

$\overline{EmailSRV}$ – подія, яка полягає в неготовності поштових серверів;

$\overline{Pr\,oxySRV}$ – подія, яка полягає в неготовності проксі-серверів.

Тоді ймовірність події, яка полягає в надійному функціонуванні кібернетичних активів SCADA КІ з урахуванням факторів їхньої готовності та захисту від ЗЛВ, записується у такому вигляді:

$$Availability = 1 - UnAvailability = 1 - P\left\{UA_{1-3} \cup UA_4 \cup \left[UA_5 \cap UA_6\right] \cup \right.$$
$$\left. \cup \overline{FW4} \cup \overline{FW5} \right\}. \quad (7)$$

Шостий крок. Побудова структурної схеми надійності кібернетичних активів SCADA КІ.

На рис. 4 зображена ССН, побудована відповідно до рекомендацій і вимог, розглянутих у [8; 9]. Процес розбудови ССН базується на реалізації попередніх кроків і враховує фактор забезпечення надійної роботи кіберактивів SCADA КІ.

Сьомий крок. Оцінка готовності (доступності) кібернетичних активів SCADA КІ із застосуванням їхньої ССН.

Використовуючи отриману ССН та відомі моделі [16], співвідношення для визначення показника готовності у вигляді стаціонарного коефіцієнта готовності (КГ) A_{SCADA} можна записати так:

$$A_{SCADA} = \left\{1 - \left[1 - A_{Cluster1}A_{FW1}\right] \times \left[1 - A_{Cluster2}A_{FW2}\right] \times \left[1 - A_{Cluster3}A_{FW3}\right]\right\} \times$$
$$\times \left\{1 - \left[1 - A_{AppSRV}\right] \times \left[1 - A_{DBSRV}\right] \times \left[1 - A_{DmnCTL}\right]\right\} \times \left\{1 - \left[1 - A_{AuthSRV}\right] \times \right.$$
$$\times \left[1 - A_{CTU}\right] \times \left[1 - A_{EntprSRV}\right] \times \left[1 - A_{WebSRV}\right] \times \left[1 - A_{EmailSRV}\right] \times \quad (8)$$
$$\left. \times \left[1 - A_{ProxySRV}\right]\right\} \times A_{FW4} \times A_{FW5}.$$

Складові A_{SCADA} у формулі (8) визначаються як значення стаціонарних КГ відповідних кластерів, серверів, комп'ютерних терміналів та брандмауерів.

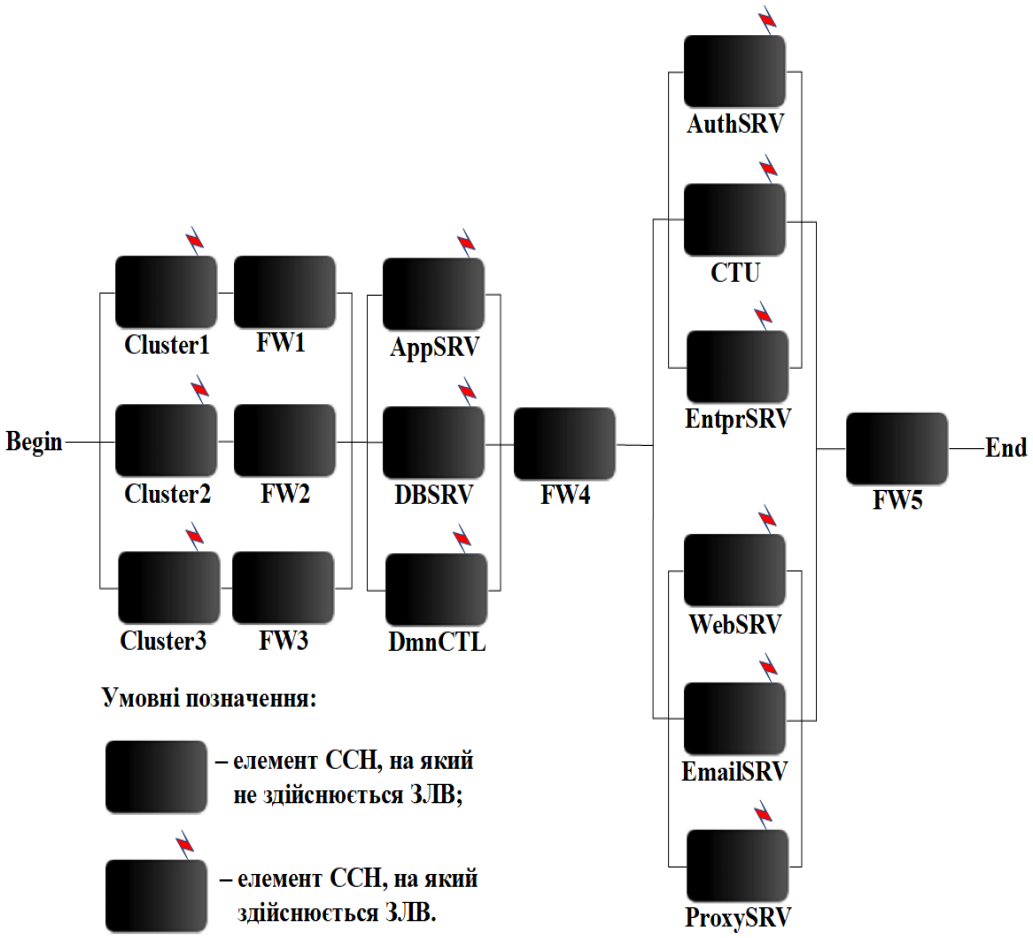


Рис. 4. Структурна схема надійності системи SCADA КІ
з урахуванням ЗЛВ на її кібернетичні активи

Восьмий крок. Параметризація вхідних даних компонентних складових ССН кібернетичних активів SCADA КІ для виконання аналітико-стохастичного моделювання.

Для обчислення загальної оцінки A_{SCADA} необхідно визначити значення складових, які входять у співвідношення (8). Розв'язати цю задачу можна шляхом виконання аналітико-стохастичного моделювання на основі застосування апарата НПММ [20–25] з метою отримання кількісних значень стаціонарних КГ компонентів, які входять до складу ССН (рис. 4). У табл. 1 наведено результати скороченого аналізу найбільш відомих джерел щодо проблематики НПММ.

Таблиця 1

Аналіз відомих наукових праць щодо застосування НПММ

Атрибути	Проблематика	Розв’язування
НПММ з виродженими станами [41]	Застосування процесу НПММ для моделювання деградаційних процесів промислової системи за умови виконання періодичних профілактичних ремонтів та контролю технічного стану	Обчислення динаміки зміни стаціонарного КГ на основі використання вкладених дискретних марковських ланцюгів (ВДМЛ)
НПММ з використанням стохастичних не експоненціальних розподілень [42]	Застосування процесу НПММ для моделювання поведінки системи енергоживлення з двома типами відключень	Визначення точкової оцінки стаціонарного КГ на основі використання ВДМЛ
НПММ з визначенням перехідних імовірностей для стохастичних псевдоекспоненціальних розподілень [43; 44]	Застосування процесу НПММ для моделювання процесів зміни готовності серверних систем з реалізацією режиму очікування (режим холодного резервування)	Визначення точкових оцінок стаціонарного КГ, середнього часу напрацювання до системної відмови на основі використання ВДМЛ

З погляду відповідності розв’язуваної задачі та зважаючи на мережний рівень забезпечення серверними системами, доцільно виконати параметризацію, застосувавши вхідні дані, які використовувались у працях [43; 44]. Певну зацікавленість викликає праця [45], яка присвячена моделюванню поведінки серверних систем хмарної інфраструктури з урахуванням кількості фізичних машин. Хоча обчислення були виконані на основі стохастичних мереж Петрі та марковських ланцюгів [13; 45], ці результати можуть бути використані для завдання вхідних даних з метою реалізації аналітико-стохастичного моделювання. В табл. 2, 3 подано результати параметризації з урахуванням виконаного аналізу.

Таблиця 2

Значення стаціонарного КГ компонентних складових ССН кібернетичних активів SCADA КІ за результатами НПММ [43, 44]

Типи серверів та іншого обладнання	Інтенсивність відмов кластерів SCADA КІ $\lambda_{Cluster1,Cluster2,Cluster3} = 0,1$ 1/год	
	Інтенсивність відмов серверів та іншого обладнання γ, 1/год	
	$\gamma = 0,3$	$\gamma = 0,5$
AppSRV	0,91 352	0,871 814
DBSRV	0,914 446	0,873 394
DmnCTL	0,915 307	0,874 806
AuthSRV	0,916 103	0,876 112
CTU	0,916 837	0,877 318
EntprSRV	0,917 514	0,878 431
WebSRV	0,918 138	0,87 946
EmailSRV	0,918 715	0,880 412
ProxySRV	0,919 248	0,881 294
FW	0,919 742	0,882 113

Таблиця 3

Значення показників надійності компонентних складових ССН кібернетичних активів SCADA КІ [45]

Показники надійності серверів та іншого обладнання	Кількісне значення
$1/\gamma_{SRV}$, $1/\gamma_{DmnCTL,CTU}$, $1/\gamma_{FW}$	500 год, 1750 год, 2500 год
$1/\mu$	3 год

Дев'ятий крок. Побудова структурної схеми ЗЛВ на кібернетичні активи SCADA КІ.

Для побудови структурної схеми (СС) ЗЛВ використовується ССН (рис. 4). Результати попереднього аналізу свідчать, що СС ЗЛВ є результатом трансформації ССН за умови, що на схемі відображаються тільки ком-

поненти, на які здійснюється зловмисний вплив або втручання в їхній контур управління. Схема будується з використанням факторного аналізу ЗЛВ на кібернетичні активи SCADA КІ.

До уваги також слід узяти обмеження, яке стосується дії ЗЛВ на всі сервери та комп'ютерне обладнання, крім брандмауерів, які виконують функції захисту і фільтрації інформаційних потоків SCADA КІ. На рис. 5 зображена СС ЗЛВ, отримана відповідним чином.

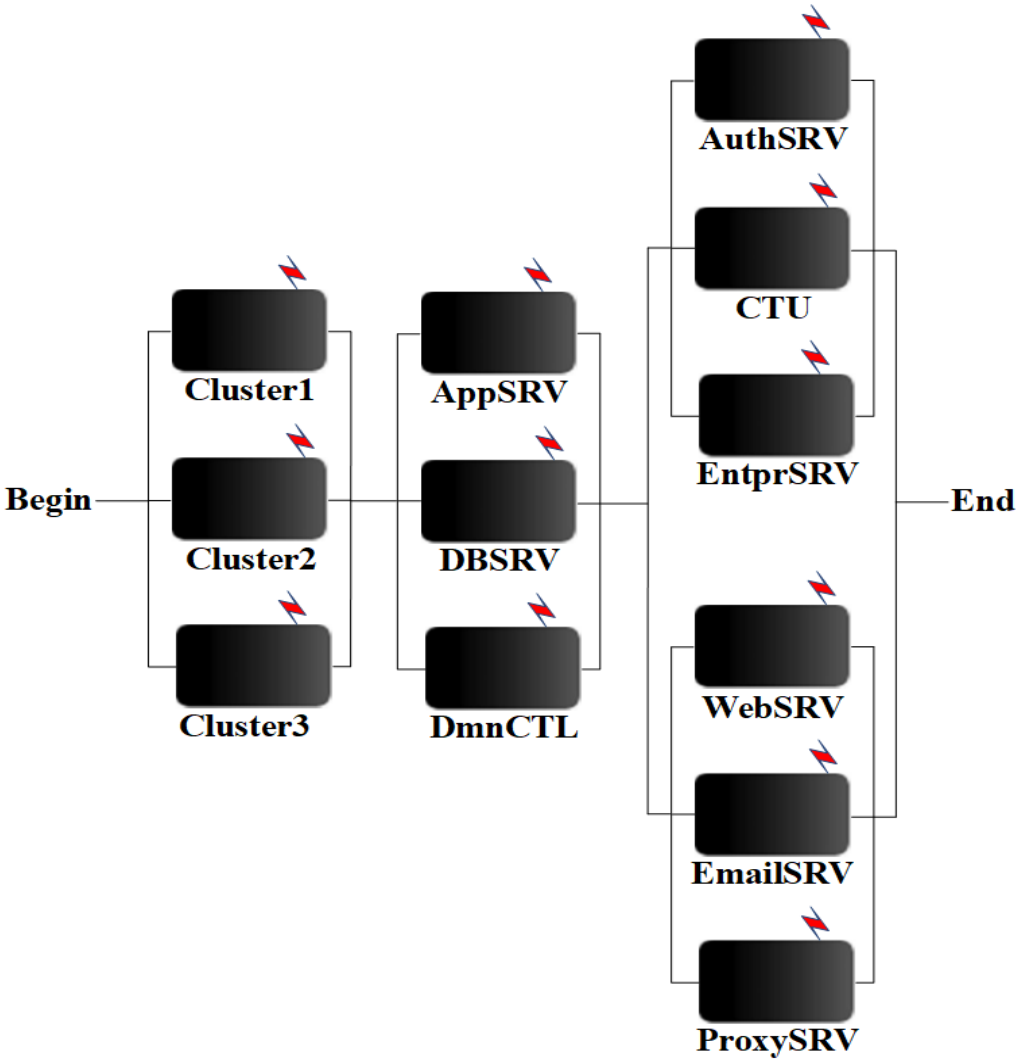


Рис. 5. Структурна схема ЗЛВ на кібернетичні активи SCADA КІ

Десятий крок. Оцінка ймовірності зловмисного впливу на кібернетичні активи SCADA КІ із застосуванням структурної схеми ЗЛВ.

Згідно з отриманою СС ЗЛВ співвідношення для визначення ймовірності ЗЛВ $P_{SCADA_{DMI}}$ може бути записано у такому вигляді:

$$P_{SCADA_{DMI}} = \left\{1-\left[1-P_{Cluster1_{DMI}}\right]\times\left[1-P_{Cluster2_{DMI}}\right]\times\left[1-P_{Cluster3_{DMI}}\right]\right\}\times$$
$$\times\left\{1-\left[1-P_{AppSRV_{DMI}}\right]\times\left[1-P_{DBSRV_{DMI}}\right]\times\left[1-P_{DmnCTL_{DMI}}\right]\right\}\times$$
$$\left\{1-\left[1-P_{AuthSRV_{DMI}}\right]\times\left[1-P_{CTU_{DMI}}\right]\times\left[1-P_{EntprSRV_{DMI}}\right]\times\left[1-P_{WebSRV_{DMI}}\right]\times\right. \quad (9)$$
$$\left.\times\left[1-P_{EmailSRV_{DMI}}\right]\times\left[1-P_{Pr oxySRV_{DMI}}\right]\right\},$$

де $P_{Cluster1_{DMI}}$, $P_{Cluster2_{DMI}}$, $P_{Cluster3_{DMI}}$ – ймовірність ЗЛВ на кластери $Cluster1,2,3$;

$P_{AppSRV_{DMI}}$ – ймовірність ЗЛВ на сервери додатків;

$P_{DBSRV_{DMI}}$ – ймовірність ЗЛВ на сервери баз даних;

$P_{DmnCTL_{DMI}}$ – ймовірність ЗЛВ на контролер домену;

$P_{AuthSRV_{DMI}}$ – подія, яка полягає в неготовності серверів автентифікації;

$P_{CTU_{DMI}}$ – ймовірність ЗЛВ на комп'ютерні термінали;

$P_{EntprSRV_{DMI}}$ – ймовірність ЗЛВ на корпоративні сервери;

$P_{WebSRV_{DMI}}$ – ймовірність ЗЛВ на web-сервери;

$P_{EmailSRV_{DMI}}$ – ймовірність ЗЛВ на поштові сервери;

$P_{Pr oxySRV_{DMI}}$ – ймовірність ЗЛВ на проксі-сервери.

Одинадцятий крок. Параметризація вхідних даних компонентних складових СС ЗЛВ на кібернетичні активи SCADA КІ для виконання аналітико-стохастичного моделювання.

Параметризація виконується для визначення ймовірності ЗЛВ $P_{SCADA_{DMI}}$ (9) шляхом виконання аналітико-стохастичного моделювання на основі застосування апарата НПММ [46]. Процедура аналогічна тій, що була

реалізована на восьмому кроці пропонованого методу. В табл. 4 наведено вхідні дані для виконання чергового етапу аналітико-стохастичного моделювання.

Таблиця 4

Значення параметрів для виконання НПММ ЗЛВ на кібернетичні активи SCADA КІ [46]

Параметр	Кількісне значення
Інтенсивність успішного злому контуру кіберзахисту γ_{break}, 1/год	0,5
Інтенсивність повернення системи в працездатний стан роботи зі стану ЦФ γ_{return}, 1/год	2
Середній час цільового фішингу (ЦФ) $1/\gamma_{fishing}$, год	0,5–1
Середній час зміни ключів кодування $1/\gamma_{rekeying}$, год	0,017–1

Числові результати НПММ ЗЛВ на кібернетичні активи SCADA КІ для вхідних даних згідно з табл. 4 зображено на рис. 6.

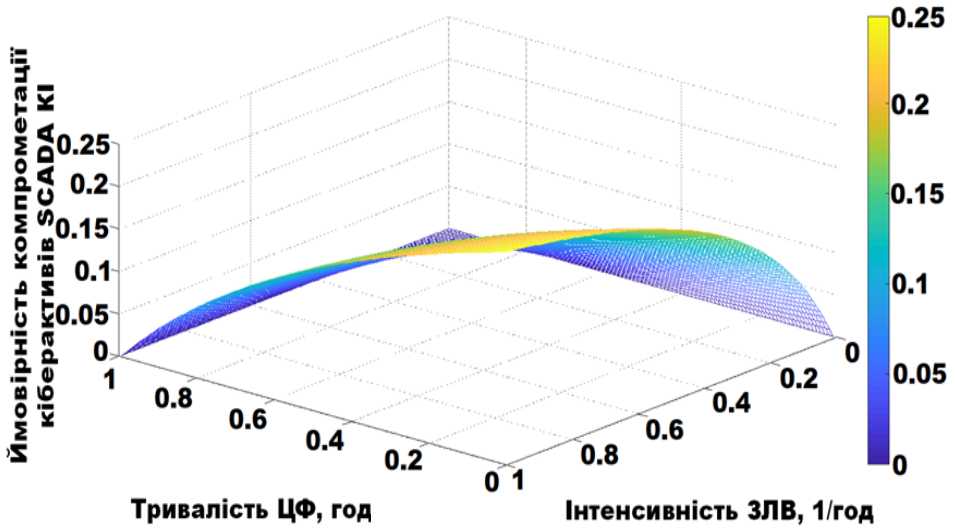


Рис. 6. Числові результати НПММ ЗЛВ на кіберактиви SCADA КІ

Отримані результати моделювання (рис. 6) у вигляді залежності ймовірності компрометації кібернетичних активів SCADA КІ від тривалості цільового фішингу та інтенсивності зловмисних впливів свідчать про досить високий рівень кіберзагроз і можуть бути використані для обґрунтування вимог щодо створення ефективної системи кіберзахисту.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. В досліджені розглянуто етапи побудови ССБ кібернетичних активів системи SCADA КІ з урахуванням аспектів, пов'язаних із забезпеченням необхідного рівня їхньої готовності (доступності) та захисту від кіберзагроз у вигляді зловмисних впливів і проникнень. Результати проведених досліджень у концентрованому вигляді сформульовані як відповідний метод.

Запропонований метод базується на таксономії виникнення ризику для функціональної та інформаційної безпеки системи SCADA КІ для мережного рівня її архітектурної реалізації. Проведений аналіз підтвердив доцільність застосування НПММ для отримання числових результатів моделювання поведінки компонентних складових як ССН, так і СС ЗЛВ, що дає можливість отримати кількісні оцінки загального рівня безпеки кіберактивів SCADA КІ. Результати моделювання можуть бути використані для розробки оптимізаційних процедур щодо побудови ефективної системи забезпечення функціональної та інформаційної безпеки КІ і системи SCADAяк важливої компонентної складової ІУС інфраструктури. Зокрема, за результатами НПММ ймовірність компрометації кібернетичних активів SCADA КІ залежно від тривалості цільового фішингу та інтенсивності зловмисних впливів становить 25 %.

Перспективи подальшого застосування цього методу пов'язані з розробкою концепції управління КІ за мегастаном на основі ризик-аналізу різноманітних факторів негативного впливу як на фізичні, так і на кібернетичні активи інфраструктури.

Список використаних джерел:

1. *Fairley P.* Cybersecurity at U.S. utilities due for an upgrade: Tech to detect intrusions into industrial control systems will be mandatory // Jornal IEEE Spectrum. 2016. Vol. 53(5). P. 11–13.

2. *Дрозд А. В., Харченко В. С.* Рабочее диагностирование безопасных информационно-управляющих систем. Харьков: Национальный аэрокосмический университет им. Н. Е. Жуковского "ХАИ", 2012. 614 с.

3. *Никул В. В., Дрозд А. В., Дрозд Ю. В., Озеранский В. С.* Эффективность поразрядной конвейеризации вычислений в FPGA-компонентах систем критического применения // Технология и конструирование в электронной аппаратуре. 2018. № 4. С. 3–13.

4. *Misbahuddin S.* Faulttolerant remote terminal units (RTUs) in SCADA systems : materials of the *International Symposium on Collaborative Technologies and Systems.* Chicago, 2010. P. 440–446.

5. A testbed for secure and robust SCADA systems / Giani A., Karsai G., Roosta T. and oth. : materials of the 14th Real-Time and Embedded Technology and Applications Symposium, SIGBED Review. 2008. St. Louis, USA. P. 93–96.

6. Unavailability of critical SCADA communication links interconnecting a power grid and a Telco network / Bobbio A., Bonanni G., Ciancamerla E. and oth. // Reliability Engineering & System Safety. 2010. № 95 (12). P. 1345–1357.

7. *Lipman Y., Funkhouser T.* Möbius voting for surface correspondence // ACM Transactions on Graphics (TOG). 2009. Vol. 28 (3). P. 1–12.

8. Hassan B. Diab, Albert Y. Zomaya. Dependable Computing Systems: Paradigms, Performance Issues, and Applications. New York: John Wiley & Sons, 2005. 688 p.

9. *Острейковский В. А.* Теория надёжности. Москва: Высшая школа, 2003. 463 с.

10. *Zang X., Wang D., Sun H., Trivedi K. A* BDD-based algorithm for analysis of multistate components // IEEE Transactions on Computers. 2003. Vol. 52 (12). P. 1608–1618.

11. *Kuo W., Zuo M.* Optimal reliability modeling: principles and applications. New York: John Wiley & Sons, 2003. 544 p.

12. CASE-оценка критических программных систем / Одарущенко О. Н., Харченко В. С., Маевский Д. А. и др. Том 2. Надёжность. Харьков: Национальный аэрокосмический университет им. Н. Е. Жуковского "ХАИ", 2012. 292 с.

13. *Bolch G., Greiner S., Hermann de Meer, Trivedi K.* Queueing Networks and Markov Chains: modeling and performance evaluation with computer science applications. New Jersey: John Wiley & Sons, 2006. 878 p.

14. *Patel A., Joshi A.* Modeling and Analysis of Stand by Redundancy System to Generate the Reachability Tree using Petri Net System // Asian Journal of current Engineering and Maths. 2013. Vol. 2 (3). P. 145–150.

15. *Dantas J., Matos R., Araujo J., Maciel P.* Eucalyptus-based private clouds: availability modeling and comparison to the cost of a public cloud // Computing. 2015. Vol. 97 (11). P. 1121–1140.

16. Sensitivity analysis of a hierarchical model of mobile cloud computing / Matos R., Araujo J., Oliveira D. and oth. // Simulation Modelling Practice and Theory. 2015. Vol. 50. P. 151–164.

17. *Kim D., Machida F., Trivedi K.* Availability modeling and analysis of a virtualized system: materials of the 2009 15th IEEE Pacific Rim International Symposium on Dependable Computing. Shanghai, China. 2009. P. 365–371.

18. *Changa X., Zhang Z., Li X., Trivedi K.* Model-Based Survivability Analysis of a Virtualized System: materials of the 2016 IEEE 41st Conference on Local Computer Networks. Dubai, 2016. P. 611–614.

19. Dynamically-Enabled Defense Effectiveness Evaluation in Home Internet Based on Vulnerability Analysis / Wang T., Lei M., Chen J. and oth. : materials of the *International Conference on Cloud Computing and Security.* Springer, 2017. P. 805–815.

20. Распределённые критические системы и инфраструктуры: практикум / О. В. Иванченко, Ловягин В. С., Мащенко Е. Н. и др. Харьков: Национальный аэрокосмический университет им. Н. Е. Жуковского "ХАИ", Севастопольский национальный технический университет, 2013. 179 с.

21. Иванченко О. В. Полумарковские модели мониторинга информационно-технического состояния критических інфраструктур // Радіоелектронні і комп'ютерні системи. 2010. № 7 (48). С. 219–224.

22. Ivanchenko O., Kharchenko V., Skatkov A. Management of Critical Infrastructures Based on Technical Megastate // Information and Security. Critical Infrastructures Safety and Security. 2012. Vol. 28 (1). P. 37–51.

23. *Яцек Я. Ф., Иванченко О. В., Войтюк А. В., Степанов В. А.* Комплексный подход к управлению критическими инфраструктурами по техническому мегасостоянию // Збірник наукових праць Академії Військово-морських сил ім. П. С. Нахімова. 2010. № 4 (4). С. 91–99.

24. *Иванченко О. В., Харченко В. С., Бирюков Д. Ю.* Полумарковская модель протекания аварии критической инфраструктуры // Радіоелектронні і комп'ютерні системи. 2013. № 5 (64). С. 45–51.

25. Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения: учеб. пособие / под ред. В. С. Харченко. Харьков: Национальный аэрокосмический университет им. Н. Е. Жуковского "ХАИ", 2011. 641 с.

26. *Sundararajan A., Khan T., Moghadasi A., Sarwat A.* Survey on synchrophasor data quality and cybersecurity challenges, and evaluation of their interdependencies. URL: https://doi.org/10.1007/s40565-018-0473-6

27. *Hentea M.* Improving security for SCADA control systems // Interdisciplinary Journal of Information, Knowledge, and Management. 2008. Vol. 3 (1). P. 73–86.

28. *Brandle M., Naedele M.* Security for Process Control systems: An Overview // IEEE Security & Privacy. 2008. Vol. 6 (6). P. 24–29.

29. *Chen T., Abu-Nimeh S.* Lessons from Stuxnet // IEEE Computer Magazine. 2011. Vol. 44 (4). P. 91–93.

30. *Keizer G.* Development timeline key to linking Stuxnet, Flame malware. 2012. URL: http://www.computerworld.com/s/article/9227580/ Development_timeline_key_to_linking_Stuxnet_Flame_ma lware

31. Centre for the Protection of National Infrastructure, Viewpoint // Securing the Move to IP-Based SCADAlPLC networks. URL: http://www.cpni.gov.ukldocuments/publications/2011/2011035-securing-move-to-ip-based-networks.pdf?epslanguageen-gb

32. *Ahmed I., Obermeier S., Naedele M., Richard III G. G.* Scada systems: Challenges for forensic investigators // Computer. 2012. Vol. 45 (12). P. 44–51.

33. *Pidikiti B., Kalluri R., Kumar R., Bindhumadhava B.* SCADA communication protocols: vulnerabilities, attacks and possible mitigations // CSITransactions on ICT. 2013. Vol. 1 (2). P. 135–141.

34. *Nazir S., Patel S., Patel D.* Assessing and augmenting SCADA cyber security: A survey of techniques // Computers & Security. 2017. Vol. 70. P. 436–454.

35. *Chen S., Wang Y., Pedram M.* A semi-markovian decision process based control method for offloading tasks from mobile devices to the cloud: materials of the *2013 IEEE Global Communications Conference (GLOBECOM)*. Atlanta, GA, USA, 2013. P. 2885–2890.

36. Juniper Networks // *Juniper connected security: dynamic, adaptive multicloud security*. 2019. URL: https://media.bitpipe.com/io_14x/io_146335/item_1879854/3510634-en.pdf

37. Cloud Data Sharing Platform (S-67G), Final Project Rep. / Hauser C., Bose A., Meng M. Cornell University and Washington State University, 2016. 29 p.

38. Smart Grids. Clouds, Communications, OpenSource, and Automation / Edited byBakken D. CRC. Taylor and Francis Group, New York, 2014. 468 p.

39. *Скляр В. В.* Функциональная безопасность. Часть 2 из 7. МЭК 61508: кем быть Шерлоком Холмсом или Дата Туташхиа? URL: https://habr.com/ru/post/309636

40. *Скляр В. В.* Информационная безопасность АСУ ТП: Дон Кихот в эру кибероружия. URL: https://habr.com/ru/post/316184

41. *Vinayk R., Dharmaraja S.* Semi-Markov Modeling Approach for Deteriorating Systems with Preventive Maintenance // International Journal of Performability Engineering. 2012. Vol. 8 (5). P. 515–526.

42. *Distefano S., Trivedi K.* Non-Markovian State-Space Models in Dependability Evaluation // Quality and Reliability Engineering International. 2013. Vol. 29 (2). P. 225–239.

43. *Bhardwaj R., Singh R.* Semi-Markov approach for asymptotic performance analysis of a standby system with server failure // International Journal of Computer Applications. 2014. Vol. 98 (3). P. 9–14.

44. *Bhardwaj R., Singh R.* A Cold-Standby System with Server Failure and Delayed Treatment // International Journal of Computer Applications. 2015. Vol. 124 (17). P. 31–36.

45. *Ghosh R.* Scalable stochastic models for cloud services: Doctoral dissertation. Duke University, 2012. 494 p.

46. *Meng T.* Security and Performance Tradeoff Analysis of Offloading Policies in Mobile Cloud Computing: Doctoral dissertation. Institute for Computer and Systems Engineering, 2017. 150 p.

References:

1. *Fairley P.* (2016), Cybersecurity at U.S. utilities due for an upgrade: Tech to detect intrusions into industrial control systems will be mandatory // Journal IEEE Spectrum. vol. 53(5), pp. 11–13.

2. Drozd A. V. and Kharchenko V. S. (2012), Rabocheye diagnostirovaniye bezopasnykh informatsionno-upravlyayushchikh sistem [Working diagnostics of secure management information systems], Natsional'nyy aerokosmicheskiy universitet im. N. Ye. Zhukovskogo «KHAI», Khar'kov, 614 p. [Ukraine].

3. Nikul V. V., Drozd A. V., Drozd Yu. V. and Ozeranskiy V. S. (2018), "Effektivnost' porazryadnoy konveyyerizatsii vychisleniy v FPGA-komponentakh sistem kriticheskogo primene-niya" ["Efficiency of bitwise pipelining of computations in FPGA components of critical application systems"], journal Tekhnologiya i konstruirovaniye v elektronnoy apparature [Technology and Electronic Design], vol. 4, pp. 3–13 [Ukraine].

4. Misbahuddin S. (2010), "Faulttolerant remote terminal units (RTUs) in SCADA systems", materials of the International Symposium on Collaborative Technologies and Systems, Press Chicago, pp. 440–446 [USA]

5. Giani A., Karsai G., Roosta T., Shah A. and oth. (2008),"A testbed for secure and robust SCADA systems", materials of the 14th Real-Time and Embedded Technology and Applications Symposium, SIGBED Review, St. Louis, pp. 93–96 [USA].

6. Bobbio A., Bonanni G., Ciancamerla E., Clemente R. and oth. (2010),"Unavailability of critical SCADA communication links interconnecting a power grid and a Telco network", journal Reliability Engineering & System Safety, vol. 95(12), pp. 1345–1357.

7. LipmanY., Funkhouser T. (2009), "Möbius voting for surface correspondence", journal ACM Transactions on Graphics (TOG), vol. 28(3), pp. 1–12.

8. Hassan B. Diab, Albert Y. Zomaya (2005), Dependable Computing Systems: Paradigms, Performance Issues, and Applications. New York: John Wiley& Sons, 688 p. [USA].

9. Ostreykovskiy V. A. (2003), Teoriya nadozhnosti. [Theory of Reliability], Press Vysshaya shkola [Higher School], Moscow, 463 p. [Russia].

10. Zang X., Wang D., Sun H. and Trivedi K. (2003),"A BDD-based algorithm for analysis of multistate components", journal IEEE Transactions on Computers, vol. 52(12), pp. 1608–1618.

11. Kuo W. and Zuo M. (2003), Optimal reliability modeling: principles and applications, John Wiley & Sons, New York, 544 p. [USA].

12. Odarushchenko O. N., Kharchenko V. S., Mayevskiy D. A., Ponochovnyy Yu. L. and oth. (2012), CASE-otsenka kriticheskikh programmnykh sistem [CASE-evaluation of critical software systems], Volume 2, Nadozhnost' [Reliability], Press National Aerospace University named after N. Ye. Zhukovskogo «KhAI», Khar'kov, 292 p. [Ukraine].

13. Bolch G., Greiner S., Hermann de Meer and Trivedi K. (2006), Queueing Networks and Markov Chains: modeling and performance evaluation with computer science applications. New Jersey: John Wiley & Sons, 878 p. [USA].

14. Patel A., Joshi A. (2013),"Modeling and Analysis of Stand by Redundancy System to Generate the Reachability Tree using Petri Net System", Asian Journal of current Engineering and Maths, vol. 2(3), pp. 145–150 [USA].

15. Dantas, J., Matos, R., Araujo, J., Maciel, P. (2015),"Eucalyptus-based private clouds: availability modeling and comparison to the cost of a public cloud", journal Computing, vol. 97(11), pp. 1121–1140.

16. Matos R., AraujoJ., Oliveira D., Maciel P., Trivedi K. (2015),"Sensitivity analysis of a hierarchical model of mobile cloud computing", journal Simulation Modelling Practice and Theory, vol. 50, pp. 151–164.

17. Kim D., Machida F., Trivedi K. (2009),"Availability modeling and analysis of a virtualized system", materials of the2009 15th IEEE Pacific Rim International Symposium on Dependable Computing, Shanghai, China. P. 365–371.

18. Changa X., Zhang Z., Li X., Trivedi K. (2016),"Model-Based Survivability Analysis of a Virtualized System", materials of the2016 IEEE 41st Conference on Local Computer Networks, Dubai, United Arab Emirates. P. 611-614.

19. Wang T., Lei M., Chen J., Deng S., Yang Y. (2017),"Dynamically-Enabled Defense Effectiveness Evaluation in Home Internet Based on Vulnerability Analysis", materials of the International Conference on Cloud Computing and Security, Springer, Cham. P. 805–815.

20.Распределённые критические системы и инфраструктуры: практикум / О. В. Иванченко, Ловягин В. С., Мащенко Е. Н., Скатков А. В., Шевченко В. И. Харків: Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ», Севастопольський національний технічний університет, 2013. 179 с.

21.Иванченко О. В. Полумарковские модели мониторинга информационно-технического состояния критических инфраструктур.Радіоелектронні і комп'ютерні системи. 2010. № 7(48). С. 219–224.

22. IvanchenkoO., KharchenkoV., Skatkov A. (2012), “Management of Critical Infrastructures Based on Technical Megastate”, International Journal Information and Security. Critical Infrastructures Safety and Security, vol. 28(1), pp. 37–51.

23.Яцек Я. Ф., Иванченко О. В., Войтюк А. В., Степанов В. А. Комплексный подход к управлению критическими инфраструктурами по техническому мегасостоянию. Збірник наукових праць Академії Військово-морських Сил ім. П.С. Нахімова. 2010. № 4(4). С. 91–99.

24. Иванченко О.В., Харченко В.С., Бирюков Д.Ю. Полумарковская модель протекания аварии критической инфраструктуры. Радіоелектронні і комп’ютерні системи. 2013. № 5(64). С. 45–51.

25. Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения: навчальний посібник / за ред. В.С. Харченка. Харків: Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», 2011. 641 с.

26. A. Sundararajan, T. Khan, A. Moghadasi, A. Sarwat (2018),Survey on synchrophasor data quality and cybersecurity challenges, and evaluation of their interdependencies, [Online], available at: https://doi.org/10.1007/s40565-018-0473-6.

27. Hentea, M. (2008),“Improving security for SCADA control systems”, Interdisciplinary Journal of Information, Knowledge, and Management, vol. 3(1), pp. 73–86.

28. BrandleM., NaedeleM. (2008),“Security for Process Control systems: An Overview”, in journal IEEE Security & Privacy, vol. 6(6), pp. 24–29.

29. ChenT., Abu-NimehS. (2011), “Lessons from Stuxnet”, in journal IEEE Computer Magazine, vol. 44(4), pp. 91–93.

30. Keizer G. (2012), “Development timeline key to linking Stuxnet, Flame malware”, Computerworld, official site, available at: http://www.computerworld. com/s/article/9227580/Development_timeline_key_to_linking_Stuxnet_Flame_m a lware.

31. Centre for the Protection of National Infrastructure, Viewpoint (2011), Securing the Move to IP-Based SCADAlPLC networks, [Online], available at: http://www.cpni.gov.ukldocuments/publications/2011/2011035-securing-move-to-ip-based-networks.pdf?epslanguageen-gb.

32. Ahmed, I., Obermeier, S., Naedele, M., Richard III, G. G. (2012),“Scada systems: Challenges for forensic investigators”, journal Computer, vol. 45(12), pp. 44–51.

33. PidikitiB., KalluriR., KumarR., BindhumadhavaB. (2013), “SCADA communication protocols: vulnerabilities, attacks and possible mitigations”, journal CSITransactions on ICT, vol. 1(2), pp. 135–141.

34. Nazir S., Patel S., Patel D. (2017),“Assessing and augmenting SCADA cyber security: A survey of techniques”, journal Computers & Security, vol. 70, pp. 436–454.

35. Chen S., Wang Y., Pedram M. (2013), “A semi-markovian decision process based control method for offloading tasks from mobile devices to the cloud”, materials of the 2013 IEEE Global Communications Conference (GLOBECOM), Atlanta, GA, USA. P. 2885–2890.

36. Juniper Networks (2019), Juniper connected security: dynamic, adaptive multicloud security, [Online], available at: https://media.bitpipe.com/io_14x/io_146335/item_1879854/3510634-en.pdf.

37. HauserC., BoseA., MengM., AndersonD., BirmanK., GkountouvasT., SongW. (2016), Cloud Data Sharing Platform (S-67G), Final Project Rep., Press Cornell University and Washington State University, 29 p. [the USA].

38. Edited byBakken D.(2014).Smart Grids. Clouds, Communications, OpenSource, and Automation,CRC Press Taylor and Francis Group, New York, 468 p. [the USA].

39. Скляр В.В. Функциональная безопасность. Часть 2 из 7. МЭК 61508: кем быть Шерлоком Холмсом или Дата Туташхиа? / habr: офіційний сайт. URL: https://habr.com/ru/post/309636/.

40. Скляр В.В.Информационная безопасность АСУ ТП: Дон Кихот в эру кибероружия/ habr: офіційний сайт. URL: https://habr.com/ru/post/316184/.

41. Vinayk R., Dharmaraja S. (2012),“Semi-Markov Modeling Approach for Deteriorating Systems with Preventive Maintenance”, International Journal of Performability Engineering, vol. 8(5), pp. 515–526

42. Distefano S., Trivedi K. (2013), “Non-Markovian State-Space Models in Dependability Evaluation”, journalQuality and Reliability Engineering International, vol. 29(2), pp. 225–239.

43. Bhardwaj R., Singh R. (2014), “Semi-Markov approach for asymptotic performance analysis of a standby system with server failure”, International Journal of Computer Applications, vol. 98(3), pp. 9–14.

44. Bhardwaj R., Singh R. (2015), “A Cold-Standby System with Server Failure and Delayed Treatment”, International Journal of Computer Applications, vol. 124(17), pp. 31–36.

45. Ghosh R. (2012), Scalable stochastic models for cloud services, Doctoral dissertation, Duke University, 494 p. [the USA].

46. Meng T. (2017), Security and Performance Tradeoff Analysis of Offloading Policies in Mobile Cloud Computing, Doctoral dissertation, Institute for Computer and Systems Engineering, 150 p. [Germany].

DOI: https://doi.org/10.32836/2521-6643-2019-1-57-7
УДК 004.056.55

Л. В. Кабак, кандидат технічних наук, доцент кафедри програмного забезпечення комп'ютерних систем Національного технічного університету "Дніпровська політехніка"
О. Н. Молотков, кандидат технічних наук, доцент кафедри інформаційних систем та технологій Університету митної справи та фінансів
О. П. Буланий, кандидат фізико-математичних наук, доцент кафедри інформаційних систем та технологій Університету митної справи та фінансів
В. В. Куц, студент Університету митної справи та фінансів

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ ВБУДОВАНИХ ПАКЕТІВ КРИПТОЗАХИСТУ ДАНИХ СЕРВЕРІВ MS SQL SERVER ТА ORACLE

Проведено дослідження, розглянуто можливості впровадження вбудованих у сервер Oracle та MS SQL Server алгоритмів криптозахисту даних у спеціалізовані інформаційні системи на прикладі інформаційної системи Державної фіскальної служби України. Досліджено швидкодію роботи алгоритмів, оцінено зростання завантаження серверів і навантаження на комп'ютерну мережу через збільшення обсягу даних, що передаються. Набув подальшого розвитку метод оцінювання роботи вбудованих симетричних алгоритмів шифрування даних. Запропоновано алгоритм універсальної функції, яка дає можливість шифрувати дані завдяки введеному ключеві та обраному алгоритму.

Ключові слова: *криптоалгоритми; захист даних; шифрування даних; бази даних; спеціалізовані інформаційні системи.*

Проведено исследование и рассмотрены возможности внедрения встроенных в сервер Oracle и MS SQL Server алгоритмов криптозащиты данных в специализированные информационные системы на примере информационной

системы Государственной фискальной службы Украины. Также исследовано быстродействие работы алгоритмов и проведена оценка роста загрузки серверов и нагрузка на компьютерную сеть за счет увеличения объемов передаваемых данных. Получил дальнейшее развитие метод оценки работы встроенных симметричных алгоритмов шифрования данных. Предложен алгоритм универсальной функции, которая позволяет проводить шифрованые данных благодаря введенному ключу и выбранному алгоритму.

Ключевые слова: *криптоалгоритмы; защита данных; шифрование данных; базы данных; специализированные информационные системы.*

At the present time Oracle and MS SQL Servers are used for datastorage in the information system of department of customs control organization and for processing of State Fiscal Service of Ukraine. Data cumulated during customs clearance which requires access from all users are spread among many databases located between various physical storages. Data is passed between servers using different types of computer networks. With development of ramified informational systems and networks become a topical issue of ensuring sustainability, confidentiality and authenticity of data in customs departments of fiscal service of Ukraine, which are transmitted through open data line, through usage of modern cryptography methods. It's important to know that there are different methods that help to choose such set of security tools that will provide maximum data security. To protect data from unauthorized access are used modern data encryption algorithms. At the present time data is transmitted over the computer network without usage of any crypt protection system which may give attacker opportunity to capture data. DBMS Oracle and MS SQL Server have standard built-in crypto data protection packets. The purpose of this article is to consider merits and demerits of using these packages and analyze possibility of their using in customs departments of fiscal service of Ukraine. According to research technique in this article following tasks were solved: analyzing of built-in crypto data protection packets, as in their cryptostability, speed and volume increase of transmitted data, developing of plug-in for speed test of existing methods for crypt protection, considering possibility of implementation built-in packets into informational system of fiscal service of Ukraine. In this article, the speed of algorithms work was investigated and an estimation of the growth of server loading and loading on the computer network was made due to the increase of data volumes being transmitted. In the article, the method for evaluating the work of embedded symmetric data encryption algorithms has been further developed.

Key words: *grid system; partitioning; data consolidation; data bases; specialized information systems.*

Постановка проблеми. Нині в інформаційній системі департаменту організації митного контролю та оформлення Державної фіскальної служби України для збереження даних використовують сервери Oracle та MS SQL Server. Дані, що накопичуються під час митного оформлення, до яких необхідний доступ усім користувачам, розкидані серед безлічі баз даних, розташованих у різних фізичних місцях зберігання. Дані передаються між серверами через різні типи комп'ютерних мереж. Із розвитком розгалужених інформаційних систем і мереж стало актуальним питання забезпечення цілісності, конфіденційності та достовірності даних в митних підрозділах Державної фіскальної служби України, які передаються через відкриті канали зв'язку, шляхом використання сучасних методів криптографії. Важливо знати, що існують різні методи, котрі допомагають обрати таку сукупність засобів захисту, яка забезпечить максимальну безпеку даних. Для захисту даних від несанкціонованого доступу використовують сучасні алгоритми шифрування даних. Деякі стандартні алгоритми у вигляді пакетів постачаються разом із СКБД Oracle та MS SQL Server. Для організації роботи сучасної Єдиної інформаційної системи фіскальної служби використовуються засоби Oracle, які називаються розподіленою базою даних і тиражуванням даних. Кожна база даних керується власною локальною системою керування базою даних (далі – СКБД). Усі сервери баз даних у розподіленій базі даних співпрацюють, щоб підтримувати погодженість глобальної бази даних. Однак нині дані передаються через комп'ютерну мережу без використання будь-яких систем криптозахисту, це уможливлює перехоплення даних зловмисниками. СКБД Oracle має утиліту Oracle Advanced Security, яку потрібно купувати за окремі кошти, але вона не придатна для роботи гетерогенних розподілених баз даних. СКБД Oracle та MS SQL Server мають стандартні вбудовані пакети криптозахисту даних. Мета дослідження – розглянути переваги та недоліки використання цих пакетів, а також можливість їх використання в митних підрозділах фіскальної служби України.

Відповідно до мети наукового дослідження слід виконати такі завдання:

– вивчити вбудовані пакети криптозахисту даних, а саме: їхню криптостійкість, швидкодію та збільшення обсягу даних, що передаються;

– розробити алгоритм тестування швидкодії наявних методів криптозахисту;

– розглянути можливість втілення убудованих пакетів в інформаційну систему Державної фіскальної служби України.

Аналіз останніх досліджень і публікацій. У СКБД Oracle та MS SQL Server наявні такі алгоритми шифрування даних: DES, DES3, AES.

DES (англ. Data Encryption Standard) – це симетричний алгоритм шифрування певних даних, стандарт шифрування прийнятий урядом США з 1976 р. до кінця 1990-х рр., із часом набув міжнародного застосування. Ще

після розроблення алгоритм викликав неоднозначні відгуки. Оскільки DES містив засекречені елементи своєї структури, то виникали побоювання щодо можливості контролю з боку Національного Агентства Безпеки США (англ. National Security Agency). Алгоритм піддавався критиці через малу довжину ключа, що, зрештою, після бурхливих обговорень і контролю академічної громадськості не завадило йому стати загальноприйнятим стандартом. DES дав поштовх сучасним уявленням про блокові алгоритми шифрування та криптоаналіз [1–3].

Нині DES вважається ненадійним, адже він має малу довжину ключа (56 біт) і розмір блоку (64 біти). У праці M. Mitsuru [4] подано методику криптоаналізу, завдяки якій у 1999 р. ключ DES було публічно дешифровано. Процес дешифрування тривав 22 год 15 хв. Нині цей алгоритм використовується в модифікації 3-DES, вважається, що в цій модифікації алгоритм досить надійний для застосування. DES поступово витісняється алгоритмом AES, що з 2002 р. є стандартом США [2; 4].

Робота над розробкою алгоритму шифрування AES почалась 1997 р. у NIST (National Institute of Standards and Technology). Співробітники цього інституту співпрацювали з промисловцями та вченою спільнотою, котра займалась криптозахистом інформації, й досліджували новітні методи для розробки сучасного більш надійного, вдосконаленого стандартного стандарту шифрування. Мета полягала в тому, щоб розробити алгоритм шифрування, який можна використовувати як стандартний алгоритм шифрування. І цей алгоритм було зараховано до Федерального стандарту обробки інформації (далі – FIPS). Вважається, що він має достатню криптостійкість і зможе добре захистити інформацію уряду та інших організацій упродовж досить тривалого проміжку часу. Нині цей алгоритм використовує уряд США та на добровільних засадах будь-які підприємства. Крім того, цей алгоритм реалізовує симетричну криптографію ключів як блоковий шифр, він підтримує розміри блоків 128 біт і розмір ключів 128, 192, 256 біт [5–8].

Мета статті – дослідження можливості використання вбудованих у СКБД Oracle та MS SQL Server криптографічних алгоримів захисту інформації на швидкодію, розмір даних, які отримуються після шифрування даних, і криптостійкість. Для тестування вбудованих алгоритмів розроблено спеціальний програмний додаток, за допомогою якого проводились експерименти.

Виклад основного матеріалу. В сучасній Єдиній автоматизованій інформаційній системі митних підрозділів Державної фіскальної служби України використовуються СКБД ORACLE та MS SQL Server.

У СКБД Oracle та MS SQL Server наявні такі алгоритми шифрування даних: DES, DES3, AES. Для реалізації цих алгоритмів використовується

пакет DBMS_CRYPTO. Опис функцій, що зараховуються до пакета, подано в табл. 1. Пакет DBMS_CRYPTO надає тільки одну функцію для шифрування даних, саме тому тип шифрування зазначається в параметрі. Алгоритми шифрування, що підтримуються, та відповідні їм функції подано в табл. 1. Необхідна константа задається у форматі *ім'я_пакета.ім'я_функції*. Наприклад, щоб обрати алгоритм Triple DES, слід використовувати функцію DBMS_CRYPTO.ENCRYPT_3DES.

Таблиця 1

Алгоритми шифрування пакета DBMS_CRYPTO

Ім'я_функції	Опис	Довжина ключа, Bit
ENCRYPT_DES	Data Encryption Standard (DES)	56
ENCRYPT_3DES_2KEY	Modified Triple Data Encryption Standard обробляє кожен блок тричі, використовуючи 2 ключі	112
ENCRYPT_3DES	Triple Data Encryption Standard (3DES); обробляє кожен блок тричі	156
ENCRYPT_AES128	Advanced Encryption Standard	128
NCRYPT_AES192	Advanced Encryption Standard	192
ENCRYPT_AES256	Advanced Encryption Standard	256
ENCRYPT_RC4	Потокове шифрування	

Під час застосування пакета слід обрати алгоритм шифрування, задавши відповідне значення параметра *typ*. Під час шифрування даних кожен блок, який зашифровується, може бути зашифрований незалежно від інших або зчеплений з іншими для створення більш надійної (з погляду криптографії) системи. В останньому випадку зашифроване значення краще захищено. Щоб обрати метод зчеплення, слід зазначити відповідну константу з табл. 2 у значенні параметра *typ*, наприклад DBMS_CRYPTO.CHAIN_OFB.

Під час використання алгоритмів шифрування слід явно доповнити дані так, щоб їхня довжина була кратна розміру блоку. Однак цей підхід не є криптографічно надійним. DBMS_CRYPTO дає змогу вказати необхідний тип доповнення. Більшість компаній використовує метод PKCS # 5 [9].

Щоб обрати метод доповнень, слід зазначити відповідну константу з табл. 3 у значенні параметра *typ*, DBMS_CRYP TO.PAD_PKCS5.

Таблиця 2

Типи зчеплень DBMS_CRYPTO

Константа	Опис
CHAIN_CBC	Зчеплення блоків шифротексту – Cipher Block Chaining
CHAIN_ECB	Електронна книга кодів – Electronic Code Book
CHAIN_CFB	Шифрування зі зворотним зв'язком від шифротексту – Cipher Feedback
CHAIN_OFB	Шифрування зі зворотним зв'язком за виходом – Output Feedback

Таблиця 3

Типи доповнення DBMS_CRYPTO

Константа	Опис
PAD_PKCS5	Доповнення засобами криптографічної системи із загальним ключем (Public Key Cryptography System # 5)
PAD_ZERO	Доповнення нулями
PAD_NONE	Відсутність доповнення. Використовується в разі впевненості в тому, що довжина даних уже кратна розміру блоку, що зашифровується (кратно 8)

Нині на митних постах для митного оформлення використовується ПІК "Інспектор 2006", тому дані зберігаються у СКБД MS SQL Server. У СКБД MS SQL Server для шифрування даних використовуються вбудовані процедури PL/SQL, які послуговуються такими ж алгоритмами, що й у СКБД Oracle (рис. 1).

Проаналізувавши інформаційну систему митних підрозділів, було виявлено, що незаконний доступ до даних може отримати зловмисник під час передання інформації до ЦБД, а також адміністратор БД, який має доступ до незашифрованих даних, що зберігаються в БД. Для захисту даних слід застосувати шифрування. Шифрування даних не розв'язує проблему контролю доступу, однак значно підвищує безпеку збереження даних, адже до них не матимуть доступу всі рівні адміністраторів (рис. 3). Наприклад, якщо сервер центральної бази даних було неправильно налаштовано, і хакер зміг отримати доступ до даних, то вкрадені дані не матимуть ніякої цінності, якщо вони зашифровані.

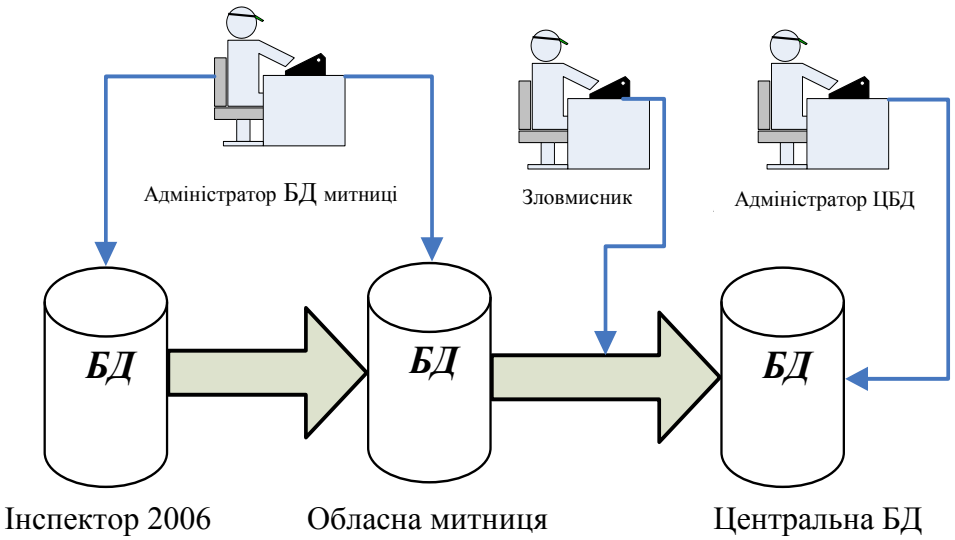


Рис. 1. Перехоплення секретної інформації зловмисником

Хоча шифрування – надійний засіб захисту даних, його не слід застосовувати щодо всіх даних, тому що під час шифрування суттєво збільшуються обсяг даних і навантаження на процесор сервера. Коли вирішується, чи потрібно шифрувати дані, слід оцінити, чи можуть отримати доступ до комп'ютерної мережі зловмисники. Якщо користувачі отримують доступ до даних через загальнодоступну мережу, для збільшення безпеки може знадобитися шифрування даних. Однак, якщо для доступу передбачено безпечну конфігурацію інтрамережі, шифрування може не знадобитися. Будь-яке використання шифрування також має містити стратегію обслуговування паролів, ключів і сертифікатів.

MS SQL Server дає змогу адміністраторам і розробникам обирати з декількох алгоритмів, зокрема DES, Triple DES, TRIPLE_DES_3KEY, RC2, RC4, RC4 зі 128-розрядним ключем, DESX, AES зі 128-розрядним ключем, AES зі 192-розрядним ключем і AES із 256-розрядним ключем [9].

Якщо для шифрування даних на митних постах використовується MS SQL Server, а в ЦБД Oracle 11g, то потрібно, щоб алгоритми шифрування збігалися. В Oracle 11g асиметричних алгоритмів шифрування немає, їх можна використовувати, якщо придбати утиліту Oracle Advanced Security. В табл. 4 відображено алгоритми шифрування, наявні в Oracle та в MS SQL Server.

Таблиця 4

Алгоритми шифрування, що збігаються

Алгоритм Oracle	Алгоритм MS SQL Server	Довжина ключа, Byte
DES	DES	4
Triple DES	Triple DES	20
3DES_2KEY	3DES_2KEY	14
AES 128	AES 128	8
AES 192	AES 192	12
AES 256	AES 256	16

Щоб виокремити алгоритми, які найдоцільніше використовувати в Єдиній інформаційній системі митної служби, маємо дослідити, як ці алгоритми працюють.

Для проведення порівняльного аналізу запропонованих шифрів розглянемо їхні основні параметри: довжина ключа, кількість раундів шифрування, довжина оброблюваного блоку, який зашифрується, криптостійкість.

Тепер визначимо, скільки часу забере спроба дібрати ключа до алгоритму. Спроба добору ключа розраховується за формулою:

$$T = \frac{P^L}{V \times n},$$

де P – потужність алфавіту ключа, $P = 2$ (0 або 1);

L – довжина ключа;

V – швидкість перенабору на комп'ютері Pentium I 5 із 4 ядрами і тактовою частотою 2,7 GHz – приблизно 2 700 000 000 операцій за секунду, якщо будуть задіяні всі чотири ядра, то швидкість перенабору буде в 4 рази більшою;

n – коефіцієнт переведення, секунд за дні, $n = 3\ 156\ 000$;

Значення розрахованих параметрів для криптоалгоритмів DES, AES подано в табл. 5.

Таблиця 5

Параметри криптостійкості алгоритмів

Алгоритм	Довжина ключа, Bit	Кількість перенаборів для розшифрування	Кількість років для добору ключа
DES	56	2^{56}	2,11
Triple DES	168	2^{168}	$1{,}1*10^{34}$
AES 128	128	2^{128}	$1*10^{22}$
AES 192	192	2^{192}	$1{,}8*10^{41}$
AES 256	256	2^{256}	$3{,}4*10^{64}$

Як бачимо з табл. 5, жоден із алгоритмів неможливо зламати шляхом добору ключа, однак найбільш незахищеними алгоритмами є DES та AES 128. Але й для цих алгоритмів спроба зламати алгоритм шляхом добору ключа забере дуже багато часу.

Для оцінювання швидкодії роботи алгоритмів було розроблено програмний додаток, що працює за певним алгоритмом (рис. 2).

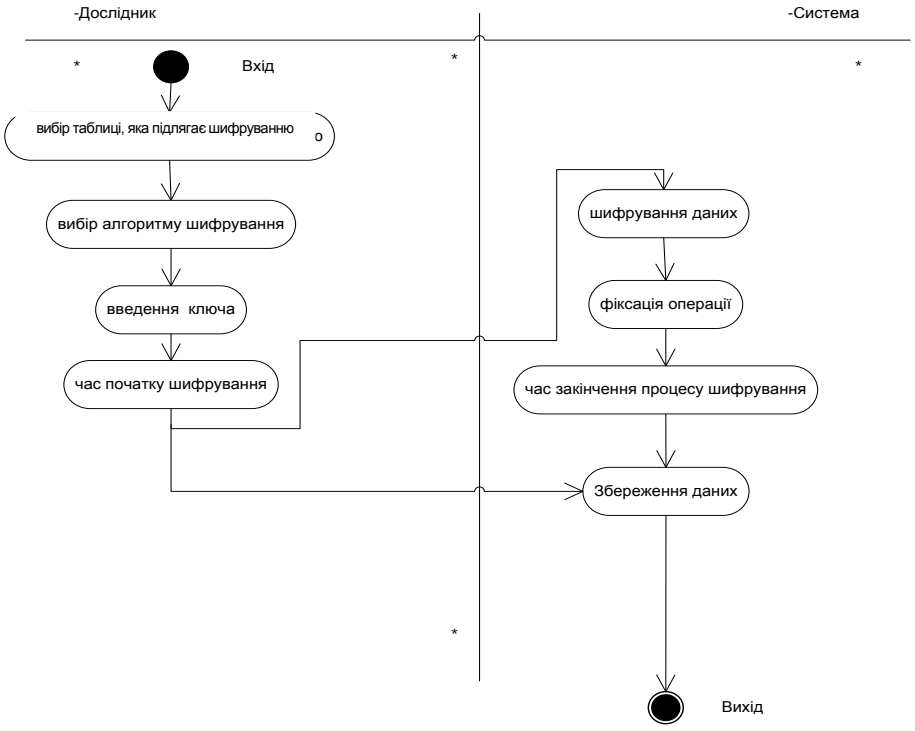


Рис. 2. Алгоритм роботи програмного додатка

Дослідник обирає таблицю, тип алгоритму, який застосовуватиметься для шифрування, потім генерується ключ, далі обирається для шифрування зазначений стовпець із певним типом даних, який потрібно зашифрувати. Під час роботи додатка запам'ятовується t_s – час початку шифрування, t_f – час закінчення шифрування. Різницю між часом початку та закінченням шифрування називаємо швидкодією обраного алгоритму: $T_{cr} = t_s - t_f$. Коли дані буде зашифровано за допомогою вбудованих алгоритмів, експортуємо таблицю, в якій шифрували дані, й оцінюємо, наскільки збільшився розмір таблиці після шифрування.

Для генерації ключів використовується така процедура над вхідними даними, що є довжиною ключа шифрування.

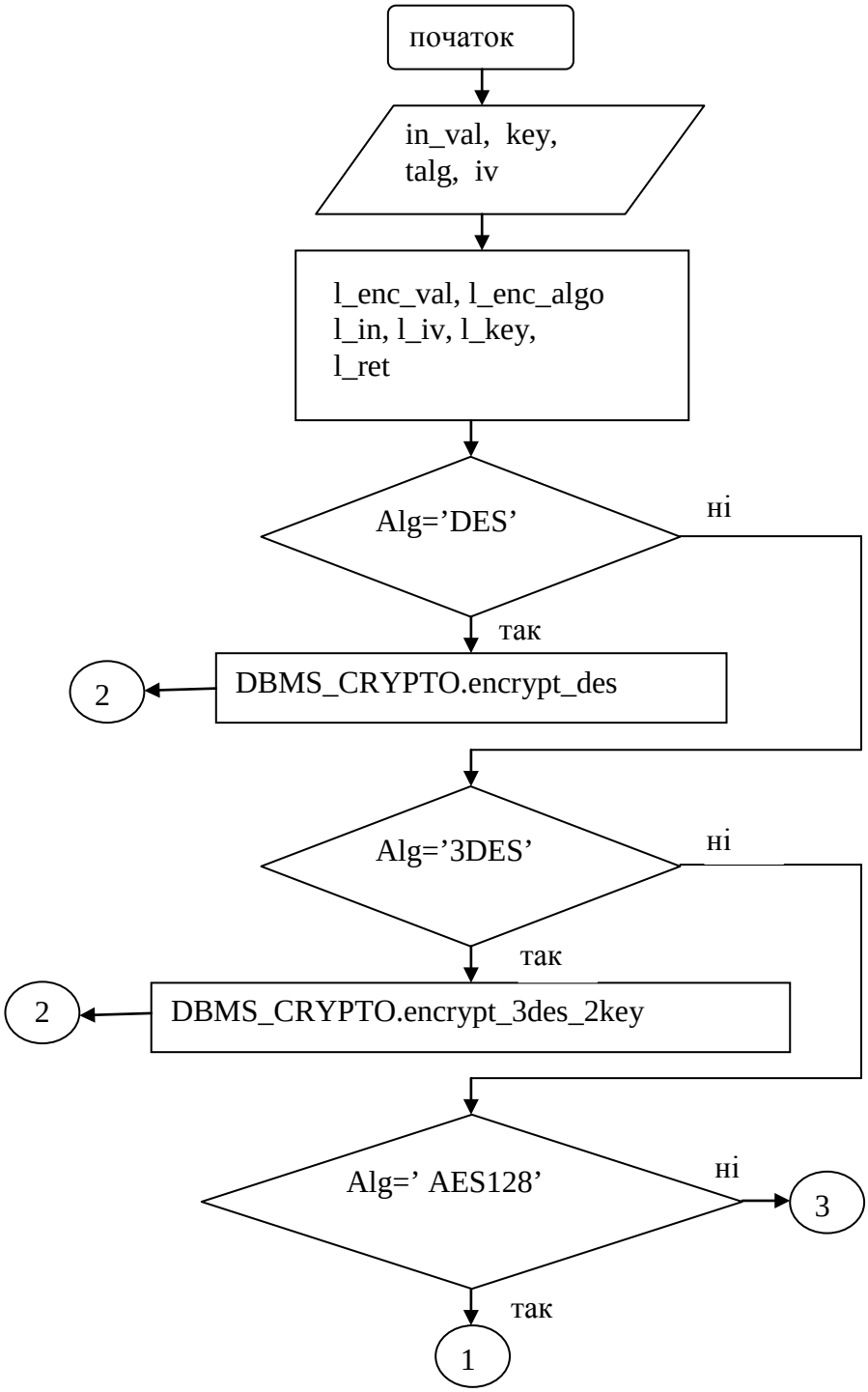
```
CREATE OR REPLACE procedure
 genkey (pl  IN PLS_INTEGER, key out raw)
IS
    BEGIN
    key := dbms_crypto.randombytes (pl);
END genkey;
```

Для генерації ключа застосовується функція `RANDOMBYTES` із пакета `DBMS_CRYPTO`.

Для шифрування даних у СКБД Oracle використовується пакет `DBMS_CRYPTO` з функціями для шифрування даних. Для зручності в роботі з цим пакетом розробляємо функцію шифрування, алгоритм якої зображено на рис. 3. Вхідні дані у функцію – це назва алгоритму шифрування і стовпець із таблиці, який підлягає шифруванню. Оскільки вбудовані в пакет функції шифрування працюють тільки з даними у форматі RAW, то спочатку функція дані зі стовпця перетворює на формат RAW, потім шифрує, після чого перетворює на формат CHAR і перезаписує вже зашифровані дані в таблицю. Функція для розшифрування даних працює аналогічно, тільки замість функції `DBMS_CRYPTO.encrypt` викликається функція `DBMS_CRYPTO.dencrypt` для розшифрування даних (рис. 3).

Для дослідження роботи системи створюємо програмний додаток на мові C#. У проведенні дослідження використовуватимемо таблицю, яка є в демо БД Oracle 11, – це таблиця користувача SH.CUSTOMER, вона має 55 000 записів.

Для шифрування даних обираємо три стовпці `CUST_FIRST_NAME, CUST_LAST_NAME, CUST_STREET_ADDRESS`. Щоб зашифровані дані потім можна було перезаписати в ту саму чарунку таблиці, збільшуємо розмір стовпця до VARCHAR2(4000).


початок
in_val, key,
talg, iv
l_enc_val, l_enc_algo
l_in, l_iv, l_key,
l_ret
Alg='DES'
ні
так
2
DBMS_CRYPTO.encrypt_des
Alg='3DES'
ні
так
2
DBMS_CRYPTO.encrypt_3des_2key
Alg=' AES128'
ні
3
так
1

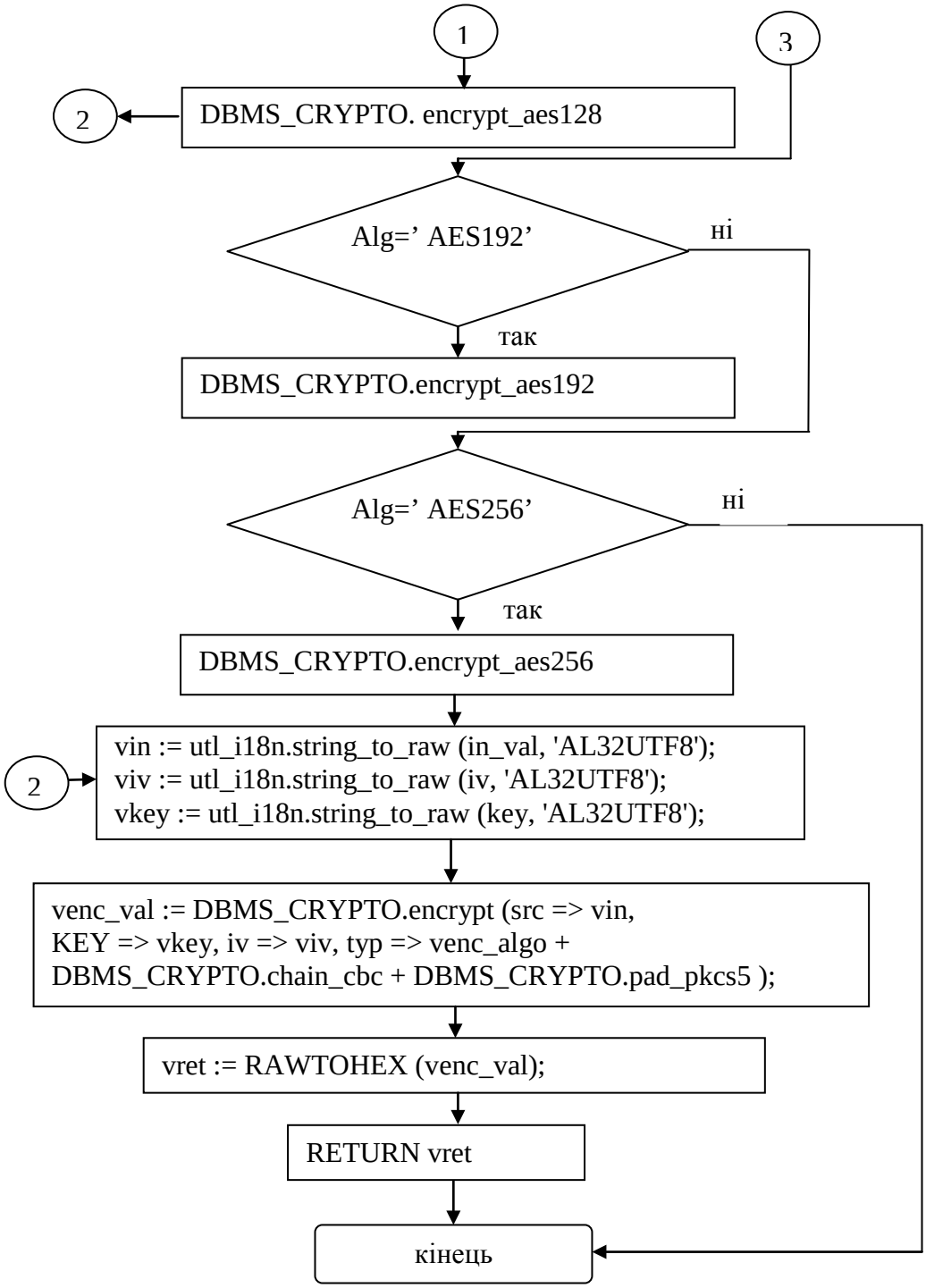


Рис. 3. Алгоритм роботи функції шифрування даних

За допомогою розробленого додатка (рис. 4) зобразимо головне вікно програми.

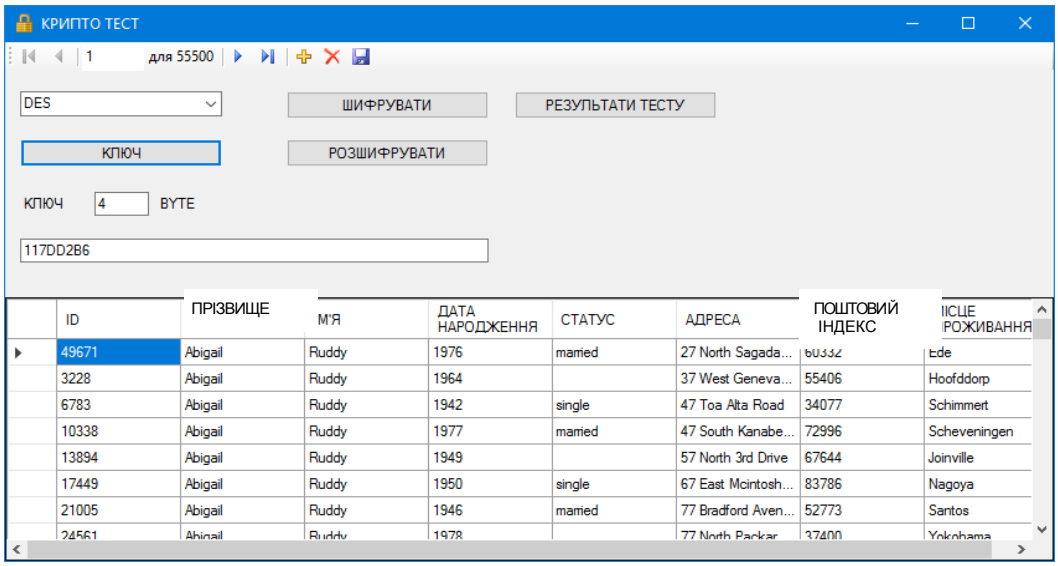


Рис. 4. Головне вікно програми

По черзі обираємо алгоритми шифрування, генеруємо для кожного алгоритму ключ, потім проводимо операції шифрування та розшифрування даних таблиці. Час роботи алгоритмів і розмір файла експорту таблиці заносимо в таблицю “TEST”. Після проведення тестів натискаємо кнопку “Результати тестів”. На рис. 5 зображено результати роботи системи шифрування даних. Час роботи алгоритмів відображається в секундах.

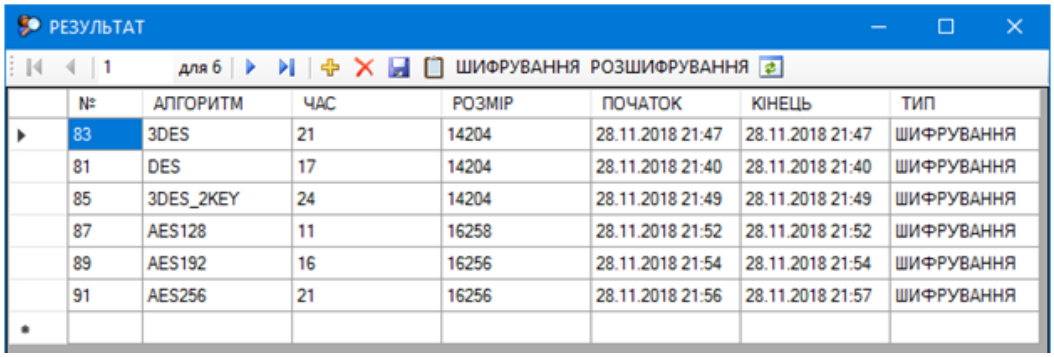
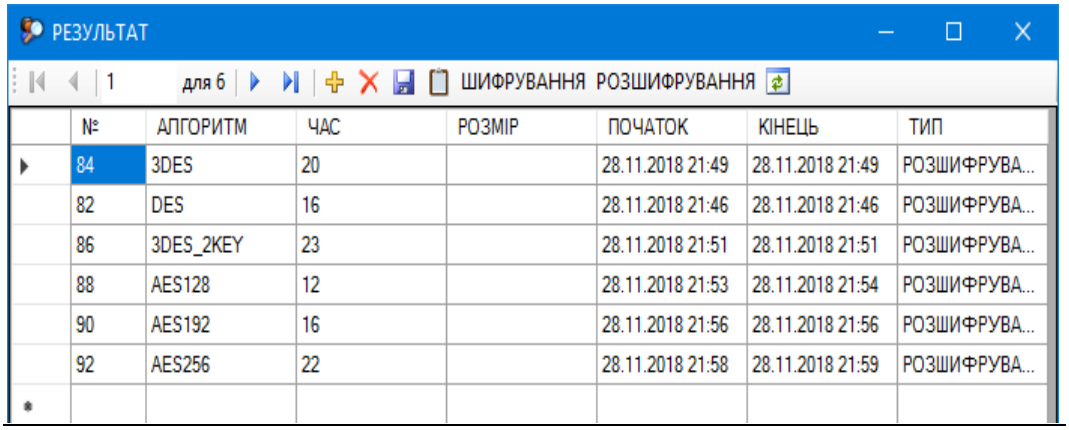


Рис. 5. Результати оцінювання роботи системи в режимі шифрування

Натиснемо на кнопку “РОЗШИФРУВАННЯ”, у вікні “РЕЗУЛЬТАТ ” буде виведено дані щодо результату роботи вбудованих алгоритмів у режимі розшифрування даних. На рис. 6 зображено результат роботи системи у режимі розшифрування даних. На рис. 7 – час роботи алгоритмів у вигляді графіка. На рис. 8 відображено залежність розміру зашифрованих даних від режимів шифрування .



№	АЛГОРИТМ	ЧАС	РОЗМІР	ПОЧАТОК	КІНЕЦЬ	ТИП
84	3DES	20		28.11.2018 21:49	28.11.2018 21:49	РОЗШИФРУВА...
82	DES	16		28.11.2018 21:46	28.11.2018 21:46	РОЗШИФРУВА...
86	3DES_2KEY	23		28.11.2018 21:51	28.11.2018 21:51	РОЗШИФРУВА...
88	AES128	12		28.11.2018 21:53	28.11.2018 21:54	РОЗШИФРУВА...
90	AES192	16		28.11.2018 21:56	28.11.2018 21:56	РОЗШИФРУВА...
92	AES256	22		28.11.2018 21:58	28.11.2018 21:59	РОЗШИФРУВА...

Рис. 6. Результат роботи алгоритмів у режимі розшифрування

Рис. 7. Результат роботи алгоритмів шифрування у вигляді графіка

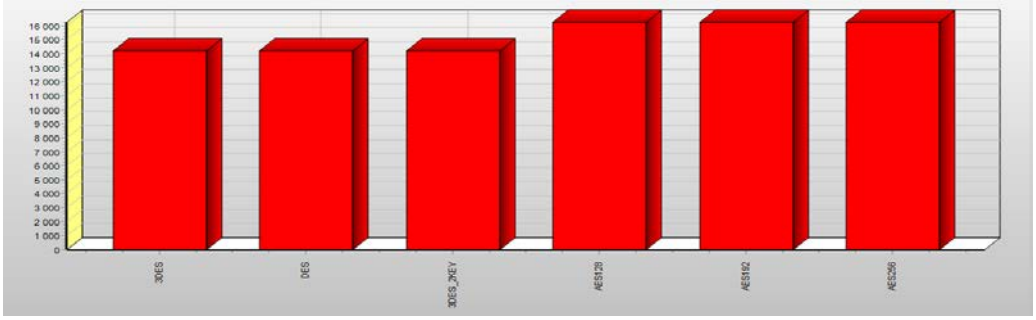


Рис. 8. Залежність обсягу зашифрованих даних від режимів шифрування

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Набув подальшого розвитку метод оцінювання роботи вбудованих симетричних алгоритмів шифрування даних. Запропоновано алгоритм універсальної функції, яка дає змогу шифрувати дані завдяки введеному ключеві та обраному алгоритму. У результаті досліджень роботи вбудованих алгоритмів шифрування отримано такі результати:

1. Найшвидший алгоритм шифрування з вбудованих алгоритмів – AES 128, найповільніший – 3DES_2KEY, але різниця незначна – 5 секунд на 55 500 записів.

2. Під час шифрування даних їхній обсяг збільшується для алгоритмів серії DES удвічі, для алгоритмів AES – утричі.

3. Від довжини ключа залежить швидкодія роботи алгоритму.

4. Обсяг зашифрованих даних не залежить від довжини ключа, він залежить тільки від типу алгоритму (рис. 8).

5. Ресурси, що споживають алгоритми, не залежать ні від довжини ключа, ні від типу алгоритму навантаження на процесор комп'ютера (за всіх видів шифрування – приблизно 30 %).

6. Застосування вбудованих алгоритмів шифрування доцільне лише тоді, коли використовується швидкісна комп'ютерна мережа. Наприклад, в митних підрозділах можливо використовувати цей метод тільки у разі передачі інформації через кручену пару чи оптоволокно. Якщо ми застосуємо цю криптосистему для захисту інформації на митних постах, де використовується супутниковий зв'язок із технологією VSAT, то в пікові години система не зможе передавати збільшений унаслідок шифрування обсяг інформації, це спричинить затори на митниці.

7. Якщо обирати метод шифрування з погляду можливого криптоаналізу та швидкодії, то оптимальним є метод AES 128, він найшвидший.

8. Якщо обирати щодо збільшення обсягу інформації, можливо застосовувати метод 3DES_2KEY. Він хоча й забирає більше часу (як було показано, під час шифрування 55 000 записів спрацював повільніше на 3 с), однак цей метод досить криптостійкий і зашифровані дані збільшуються тільки вдвічі.

Список використаних джерел:

1. *Семенов Ю. А.* Алгоритм DES. URL: http://book.itep.ru/6/des_641.htm
2. *Ходаковський О. С., Літнарович Р. М.* Криптографічний захист інформації. Рівне: МЕГУ, 2012. 108 с.
3. *Mitsuru M.* Linear Cryptanalysis of DES Cipher. URL: https://www.cs.bgu.ac.il/~ beimel/Courses/crypto2001/Matsui.pdf
4. *Ruohonen K.* Mathematical Cryptology. Tampere: Tampere University of Technology. 2010. 136 p.
5. *Daemen J., Rijmen V.* AES – The Advanced Encryption Standard. Berlin: Springer–Verlag. 2002. 238 p.
6. *Dudykevych V., Bakay O., Lakh Y.* Investigation of Payment Cards Systems Information Security Control // Proceedings of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), (September 12–14, 2013, Berlin, Germany). 2013. P. 651–654. DOI: 10.1109/IDAACS.2013.6663005
7. *Bawna Bhat, Abdul Wahid Ali, Apurva Gupta* DES and AES performance evaluation // International Conference on Computing, Communication & Automation, 15–16 May, 2015. P. 887–890. DOI: 10.1109/CCAA.2015.7148500
8. *Reatrey Pich, Sorawat Chivapreecha, Jaruwit Prabnasak* A single, triple chaotic cryptography using chaos in digital filter and its own comparison to DES and triple DES // 2018 International Workshop on Advanced Image Technology (IWAIT). P. 1–4. DOI:10.1109/IWAIT.2018.8369682
9. *Dilna V., Babu C.* Area optimized and high throughput AES algorithm based on permutation data scramble approach // 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT). P. 3056–3060. DOI: 10.1109/ICEEOT.2016.7755263
10. *Akash Kumar Mandal, Chandra Parakash, Archana Tiwari* Performance evaluation of cryptographic algorithms: DES and AES // 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science. P. 1–5. DOI: 10.1109/SCEECS.2012.6184991
11. Using the DBMS_CRYPTO Subprograms. UPL: https://docs.oracle.com/database/121/ARPLS /d_crypto.htm#ARPLS664
12. Choose an Encryption Algorithm. UPL: https://docs.microsoft.com/ru-ru/sql/relational-databases/security/encryption/choose-an-encryption-algorithm?view=sql-server-2017

References:

1. Semenov Yu. A. Alhorytm DES, available at: http://book.itep.ru/6/des_641.htm
2. Khodakovs'kyy O. S. and Litnarovych R. M. (2012), *Kryptohrafichnyy zakhyst informatsiyi* [Cryptographic protection of information], press International Economic-Humanities University, Rivne, 108 p.

3. Mitsuru M. Linear Cryptanalysis of DES Cipher, available at: https://www.cs.bgu.ac.il/ ~beimel/Courses/crypto2001/Matsui.pdf]

4. Ruohonen K. (2010), Mathematical Cryptology, press Tampere University of Technology, Tampere, 136 p.

5. Daemen J. and Rijmen V. (2002), AES – The Advanced Encryption Standard, Springer–Verlag, Berlin, 238 p. [Germany].

6. Dudykevych V., Bakay O. and Lakh Y. (2013), Investigation of Payment Cards Systems Information Security Control // Proceedings of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), vol. 2, (September 12–14, 2013, Berlin, Germany), pp. 651–654. DOI: 10.1109/IDAACS.2013.6663005 [Germany].

7. Bawna Bhat, Abdul Wahid Ali, Apurva Gupta (2015), DES and AES performance evaluation // International Conference on Computing, Communication & Automation, 15-16 May 2015, pp. 887–890. DOI: 10.1109/CCAA.2015.7148500

8. Reatrey Pich, Sorawat Chivapreecha, Jaruwit Prabnasak (2018), A single, triple chaotic cryptography using chaos in digital filter and its own comparison to DES and triple DES // International Workshop on Advanced Image Technology (IWAIT), pp. 1–4. DOI:10.1109/IWAIT.2018.8369682

9. Dilna V. and Babu C. (2016), Area optimized and high throughput AES algorithm based on permutation data scramble approach // 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), pp. 3056–3060. DOI: 10.1109/ICEEOT.2016.7755263

10. Akash Kumar Mandal, Chandra Parakash and Archana Tiwari (2012), Performance evaluation of cryptographic algorithms: DES and AES // 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science P. 1-5. DOI: 10.1109/SCEECS.2012.6184991

11. Using the DBMS_CRYPTO Subprograms, available at: https://docs.oracle.com/database/121/ARPLS /d_crypto.htm#ARPLS664

12. Choose an Encryption Algorithm, available at: https://docs.microsoft.com/ru-ru/sql/relational-databases/security/encryption/choose-an-encryption-algorithm? view=sql-server-2017

DOI: https://doi.org/10.32836/2521-6643-2019-1-57-8
УДК 656.022

А. М. Пасічник, доктор фізико-математичних наук, професор кафедри транспортних систем та технологій Університету митної справи та фінансів
І. Г. Лебідь, кандидат технічних наук, доцент кафедри міжнародних перевезень та митного контролю Національного транспортного університету
С. В. Мірошніченко, старший інспектор енергетичної митниці Державної фіскальної служби України

НАПРЯМИ ОРГАНІЗАЦІЇ ШВИДКІСНОГО АВТОТРАНСПОРТНОГО СПОЛУЧЕННЯ КИЇВ–ДНІПРО

Наведено результати аналізу стану автомобільних доріг, придатних для організації швидкісного сполучення за маршрутом Київ–Дніпро, та визначено основні напрями його реалізації. Проведено розрахунки допустимих технічних параметрів руху транспортних засобів за визначеними маршрутами. Показано, що в складі транспортних потоків зростає частка великовагових і великогабаритних транспортних засобів, що призводить до швидкого руйнування автомобільних доріг і мостів, які розраховані на значно менші обсяги й навантаження. Для впровадження швидкісного руху запропоновано заходи підвищення технічного рівня наявних доріг. Обґрунтовано потребу інтенсифікації проведення модернізації та ремонтних робіт автомобільних доріг в Україні шляхом застосування сучасних технологій. Це дасть змогу створити необхідні умови для впровадження швидкісних автотранспортних перевезень.

Ключові слова: *автомобільні дороги; швидкісний рух; маршрути руху.*

Приведены результаты анализа состояния автомобильных дорог, пригодных для организации скоростного движения по маршруту Киев–Днепр, и определены основные направления его реализации. Проведены расчеты допустимых технических параметров движения транспортных средств на определенных маршрутах. Показано, что в составе транспортных потоков увеличивается доля тяжеловесных и крупногабаритных

транспортных средств, что приводит к быстрому разрушению автомобильных дорог и мостов, которые рассчитаны на значительно меньшие объемы и нагрузки. Для внедрения скоростного движения предложены мероприятия по повышению технического уровня существующих дорог. Обоснована необходимость интенсификации проведения модернизации и ремонта автомобильных дорог в Украине на основе применения современных технологий. Это позволит создать необходимые условия для внедрения скоростных автотранспортных перевозок.

Ключевые слова: *автомобильные дороги; скоростное движение; маршруты движения.*

The article shows that the availability of modern transport infrastructure is a prerequisite for sustainable economic development of the state. Consequently, the development of transport infrastructure is planned taking into account strategic goals and is based on the realization of a sufficient level of mobility of transportation using modern highways. The substantiation of the relevance of the improvement and development of the methodology for the development of various elements of the transport infrastructure, rolling stock and technologies for the organization of high-speed traffic was made.

As a result of the study it was found that almost half of the population's needs in passenger and freight transportation are provided by road transport. According to expert estimates the problem of restoring and modernizing the Ukrainian road network to ensure high-speed transportation is of strategic importance, since their condition is generally unsatisfactory. Thus, according to the results of the analysis, it was established that the Ukrainian public highways have more than 3 million square meters. m yam, about 56 thousand km of roads that require updating of road markings, more than 20 thousand km of roads, where it is necessary to remove natural landfills and on most roads it is necessary to cut down overgrowths. In addition, a separate more than 50 % of the roads do not meet the requirements for equality, and about 40 % – for strength. Accordingly, the average speed on Ukrainian roads is 2–3 times lower than in Western European countries.

The results of the analysis of the condition of highways suitable for organizing high-speed traffic on the Kyiv–Dnipro route are presented and the main directions for its implementation are identified. The calculations of the permissible technical parameters of the movement of vehicles on certain routes. It is shown that the proportion of heavy and large-sized vehicles grows in the transport flows, which leads to the rapid destruction of roads and bridges, which are designed for much smaller volumes and loads. For the introduction of high-speed traffic proposed measures to improve the technical level of existing roads. The necessity of intensifying the modernization and repair of roads in Ukraine based on the use of

modern technologies, which will create the necessary conditions for the introduction of high-speed road transport.
Key words: *roads; highways; high-speed traffic; traffic routes.*

Постановка проблеми. Розбудова сучасної транспортної системи створює сприятливі умови для сталого розвитку різних галузей економіки держави. У міжнародній практиці планування транспортної інфраструктури здійснюється з урахуванням стратегічних цілей і базується на реалізації достатнього рівня мобільності перевезень. При цьому одним із основних чинників забезпечення мобільності перевезень є наявність сучасних транспортних магістралей [1].

Нині автомобільний транспорт забезпечує майже половину потреб громадян у пасажирських і вантажних перевезеннях. За експертними оцінками проблема відновлення та модернізації української мережі автомобільних доріг для забезпечення швидкісних перевезень має стратегічне значення, оскільки їхній стан незадовільний, зокрема більше 50 % доріг не відповідають вимогам щодо рівності, майже 40 % – щодо міцності. Відповідно середня швидкість руху на українських автомобільних дорогах у 2–3 рази нижча, ніж у західноєвропейських країнах. Отже, для розвитку та впровадження швидкісних автотранспортних перевезень слід визначити перспективні напрями розбудови, модернізації та проведення ремонтних робіт українських автомобільних доріг. Тому розробка методології розвитку різних елементів транспортної інфраструктури, рухомого складу, технологій організації швидкісних перевезень є актуальними завданнями [2].

Аналіз останніх досліджень і публікацій. Теоретичні й практичні аспекти транспортних проблем за наявних умов розвитку національної та міжнародної економіки стали предметом численних наукових досліджень. Так, у праці [3] проаналізовано структуру вантажних перевезень і головних чинників падіння обсягів перевезень, визначено складові елементи транспортного процесу в Україні. Наведено показники оцінки ефективності діяльності транспортної галузі, що відображають необхідність реформування й оновлення підходів до управління транспортною галуззю. Дослідження й оцінювання стану та напрямів розвитку мережі автомобільних доріг проведено в праці [1]. Стан і проблеми організації швидкісних пасажирських перевезень залізничним транспортом розглянуто у статті [4], в якій встановлено, що ситуація з пасажирськими залізничними перевезеннями в Україні задовільна, але суттєво відстає від міжнародних показників таких перевезень. Результати аналізу рівня розвитку автотранспортної інфраструктури в Україні наведено в публікації [5]. Аналіз підходів до оцінювання транзитного потенціалу і пропускної спроможності української транспортної системи й напрямів модернізації

мережі автомобільних доріг в Україні проведено в праці [6]. Дослідження напрямів формування транспортно-логістичної інфраструктури та основних чинників її визначення проведено в дослідженні [7]. Аналіз сучасного стану та рівня розвитку автотранспортної інфраструктури України розглянуто у [8]. Основні перспективні напрями модернізації та розвитку транспортної системи України досліджено в [9]. Аналіз сучасного стану транспортної інфраструктури України та шляхи її вдосконалення розглянули автори праці [10]. У монографії [11] подано результати аналізу впливу ринкових трансформацій на розвиток технологій вантажних і пасажирських перевезень, визначено основні тенденції їхнього розвитку.

Проблеми підвищення ефективності реалізації транзитного потенціалу, аналіз пропускної спроможності української мережі міжнародних транспортних коридорів і перспективні напрями розвитку відповідної інфраструктури розглянуто в [12]. У праці [13] з урахуванням стану розвитку української економіки проведено обґрунтування потреби підвищення якості автомобільних доріг відповідно до технічних стандартів розвинених країн світу, а також розширення їхньої мережі та протяжності.

Сучасні тенденції розвитку транспортної галузі України, шляхи її подальшого розвитку та можливі проблеми реалізації інфраструктурних проектів, зважаючи на регіональні особливості, наведено в праці [14].

Так, за даними комісійного огляду [15], виявлено понад 3 млн кв. м ямковості на українських дорогах загального користування. Крім того, виявлено близько 56 тис. км доріг, що потребують оновлення дорожньої розмітки, більше 20 тис. км доріг, де необхідно прибрати стихійні звалища, а на більшості доріг потрібно здійснити вирубку порослі.

Мета статті – аналіз стану й можливих напрямів удосконалення транспортної інфраструктури й мережі автомобільних доріг для організації швидкісних перевезень автомобільним транспортом відповідно до світових стандартів за маршрутом Київ–Дніпро. Для досягнення поставленої мети слід виконати такі завдання:

- проаналізувати класифікацію та наявний стан автомобільних доріг за напрямком сполучення Київ–Дніпро;
- розробити критерії оцінювання й визначити найефективніші напрями організації швидкісного автомобільного сполучення Київ–Дніпро.

Виклад основного матеріалу. За експертними оцінками [6; 12; 16; 17], Україна має досить високий транспортно-транзитний рейтинг 3,75 бала (до 2002 р. – 3,11). Це найвищий показник у Європі. В сусідній Польщі цей показник становить 2,92 бала (до 2002 р. – 2,72). Транзитний рейтинг території тієї або іншої країни враховує розвиненість розміщених у ній транспортних систем і мереж, а також рівень розвитку їхньої інфраструктури. Схему української мережі міжнародних транспортних коридорів зображено на рис. 1 [18].

Із сукупної довжини доріг загального користування з твердим покриттям в Україні лише 1,7 % припадає на дороги 1-ї категорії, дороги 2-ї категорії становлять 7,7 %, дороги 3-ї – 16,6 %, дороги 4-ї – 65,3 %, дороги 5-ї – 8,7 %.

Рис. 1. Схема української мережі
автомобільних міжнародних транспортних коридорів

Найбільше доріг 1-ї категорії в Київській, Дніпропетровській, Донецькій, Житомирській і Харківській областях, найменше – в Сумській, Закарпатській і Чернівецькій областях [15].

Слід зауважити, що за аналогічних кліматичних умов автомобільні дороги європейських країн мають значно кращий стан та якість. В Україні, порівняно з Польщею, протяжність мережі автомобільних доріг у 2,5 раза менша, а інтенсивність руху – майже в 4 рази більша. Це свідчить про недостатню якість доріг і недосконаліть технологічних рішень під час їх будівництва [13].

Згідно з обстеженням дорожньої мережі України більшість українських доріг становить загрозу для водіїв через поганий стан дорожнього покриття. Більше 21 тис. км доріг державного значення має незадовільний стан, а це 46 % від їхньої загальної протяжності. Складна ситуація у кількох областях, де більшість доріг державного значення вкрита ямами: у Волинській області – 55 %, Дніпропетровській – 66 %, Запорізькій – 51 %, Миколаївській – 67 %, Одеській – 56 %, Харківській – 89 %, Хмельницькій – 65 %, Чернігівській – 58 % [15]. Такий стан автодоріг не дає можливості реалізувати нормативно встановлені швидкісні режими руху автотранспорту. Згідно з правилами дорожнього руху, транспортним засобам (крім автобусів, мікро-

автобусів, вантажних автомобілів та автомобілів, якими керують водії зі стажем до 2 років) на автодорозі, позначеній знаком “Автомагістраль”, можна їхати зі швидкістю до 130 км/год, на автодорозі з окремими проїзними частинами, що відокремлені одна від одної розділювальною смугою, – до 110 км/год, на інших автошляхах – не більше 90 км/ч. Середня швидкість руху на дорогах України у 2–3 рази нижча, ніж у європейських країнах, відповідно, ефективність і швидкість переміщення автотранспорту не відповідають сучасним вимогам.

На європейських швидкісних автомагістралях немає загальних обмежень, але рекомендована швидкість – 130 км/год. Загальне європейське обмеження швидкості на сільських дорогах (українським аналогом є термін “автомобільні дороги місцевого значення”) – 80–90 км/год, а на міських – 50 км/год. У Німеччині понад 30 % загального обсягу перевезень автотранспортом здійснюється автобанами, де немає загальних обмежень швидкості. Тільки на окремих ділянках для особистої безпеки водіїв і довкілля встановлюється обмеження від 80 до 130 км/год. Нідерланди також мають ділянки автошляхів із постійно зниженою максимальною швидкістю 80, 100 км/год для зменшення шуму та забруднення повітря в місцях, що прилягають до густонаселених районів.

Аналіз досвіду європейських країн показує, що стан дорожньої мережі та транспортної інфраструктури – одна з найважливіших умов успішного економічного розвитку країни. Порівняння транспортної забезпеченості України та деяких європейських країн подано в табл. 1.

Україна займає найбільшу територію серед європейських країн, але довжина автошляхів у нашій державі – менша в кілька разів. Площі території України та Франції майже однакові, але довжина автошляхів в Україні у 5,6 раза менша, ніж у Франції.

Таблиця 1

Порівняння транспортної забезпеченості України та деяких європейських країн

Країна	Площа, тис. кв. км	Довжина автошляхів, тис. км	Щільність автошляхів, км/тис. кв. км	Довжина залізниць, тис. км	Щільність залізниць, км/тис. кв. км
Україна	603,7	169,4	280,6	21,7	35,9
Польща	312,6	424,0	1355,9	22,3	71,4
Франція	551,6	951,2	1749,1	29,2	53,7
Німеччина	357,0	644,5	1805,3	41,9	117,4
Іспанія	307,6	681,2	1349,5	15,3	30,3
Італія	301,2	487,7	1618,7	19,7	65,5

Одне з перших місць за щільністю транспортної мережі займає Німеччина. Загальна протяжність автомобільних доріг у цій країні перевищує 11 тис. км. На вантажообіг автомобільним транспортом припадає 60 %, пасажирообіг становить 90 %. При цьому, незважаючи на наявність Міністерства транспорту, Німеччина має децентралізовану систему управління дорогами. Відповідно питаннями утримання та експлуатації автомобільних доріг займаються Дорожні адміністрації земель, а регіональні та місцеві дороги будуються і утримуються за рахунок регіонального бюджету. Експлуатація швидкісних автомагістралей супроводжується спеціальними заходами, а також своєчасним проведенням ремонтних робіт. Середня вартість будівництва одного кілометра автомагістралі в Німеччині становить 27 млн євро, а витрати безпосередньо на будівництво дорожнього полотна – 25,3 % загальної вартості автомагістралі.

Нині в Європі ставляться такі основні вимоги до швидкісних автомагістралей:

- не менше двох смуг руху в одному напрямку;
- повне розділення зустрічних і пересічних транспортних потоків у різних рівнях;
- наявність розділової смуги завширшки 3,5–4 м із розділовими неглухими загородженнями між зустрічними потоками руху;
- несуча поверхня полотна дороги – бетон із асфальтовим покриттям;
- обладнання дороги рефлекторними покажчиками, встановленими з інтервалом не більше 50 м, зонами відпочинку з парковками, сервісними станціями, заправними станціями, підприємствами громадського харчування, телефонами для виклику допомоги на кожних двох кілометрах дороги, стандартизованими знаками та покажчиками, захисними засобами, що перешкоджають доступу тварин на проїжджу частину, протишумовими захисними спорудами;
- забезпечення автоматизованого трафіку та динамічного визначення рекомендованої швидкості руху транспортних засобів залежно від завантаженості дороги, погодних умов та інших об’єктивних умов і обставин.

Планування та подальше будівництво доріг у Німеччині реалізується відповідно до так званого принципу гравітації, згідно з яким “ступінь транспортних відносин прямо пропорційний обсягу економічної активності в різних пунктах і обернено пропорційний квадрату відстані між ними”.

Першочергове значення для розбудови транспортного та промислового комплексів України має міжнародний транспортний коридор Європа–Азія.

Транспортний коридор Європа–Кавказ–Азія пов’язує регіони з розвинутою промисловістю та сільським господарством через регіональні промислово-економічні вузли: Київський, Луганський, Донецький, Дніпропетровський, Черкаський, Кіровоградський, Житомирський, Рівненський, Вінни-

цький, Тернопільський, Хмельницький, Львівський, а також великі центри: Львів, Київ, Дніпро. Коридор відповідає центральному широтному ходу Донбас–Кривбас–Карпати й надважливий для розбудови транспортного комплексу України.

Дніпро – одне з найбільших міст України, але не має сучасного швидкісного автомобільного сполучення з Києвом. Тож розглянемо можливі варіанти організації швидкісних маршрутів Дніпро–Київ:

- траса Дніпро–Олександрія–Київ;
- траса Дніпро–Решетилівка–Київ;
- траса Дніпро–Кременчук–Київ.

Проаналізуємо кожний із наведених маршрутів за швидкістю руху, відстанню, типом дороги та часом переміщення.

Результати розрахунків за критерієм швидкості руху, відстанню, типом дороги та часом у дорозі відображено в табл. 2–4.

Таблиця 2

Маршрут по трасі Дніпро–Кременчук–Київ

Назва населеного пункту	Відстань від м. Дніпра, км	Назва дороги	Швидкість, км/год	Час, хв
1	2	3	4	5
Дніпро	0	М-04, міська дорога	30	0:00
Дніпро (виїзд)	11	М-04, міська дорога	30	0:25
М-04 × Н-08	21	Н-08, автомагістраль	85	0:31
Дніпродзержинськ (в'їзд)	34	Н-08, автомагістраль	85	0:37
Дніпродзержинськ (виїзд)	42	Н-08, міська дорога	30	0:54
Н-08 × Т-04-23	108	Н-08, головна дорога регіону	60	2:54
Кіровоградська область	130	Н-08, головна дорога регіону	60	2:54
Н-08 × Т-12-03	131	Н-08, головна дорога регіону	60	2:54
Полтавська область	152	Н-08, головна дорога регіону	60	2:54
Кременчук (в'їзд)	153	Н-08, головна дорога регіону	60	3:10

Закінчення табл. 2

1	2	3	4	5
Кременчук (М-22 × Н-08)	158	Н-08, міська дорога	30	3:10
Кременчук (виїзд)	167	Н-08, міська дорога	30	3:10
Градизьк (в'їзд)	192	Н-08, головна дорога регіону	60	3:34
Градизьк (виїзд)	194	Н-08, міська дорога	30	3:39
Н-08 × Т-17-21	219	Н-08, головна дорога регіону	60	4:02
Черкаська область	291	Н-08, головна дорога регіону	60	5:12
Н-08 × Н-16 × × Золотоноша	292	Н-08, головна дорога регіону	60	5:13
Золотоноша (в'їзд)	295	Н-08, дорога міського призначення	50	5:15
Золотоноша (виїзд)	300	Н-08, міська дорога	30	5:25
Н-08 × Золотоноша	304	Н-08, дорога міського призначення	50	5:30
Н-08 × Гельм'язів	326	Н-08, головна дорога регіону	60	5:51
Київська область	357	Н-08, головна дорога регіону	60	6:25
Н-08 × Переяслав-Хмельницький	358	Н-08, міська дорога	30	6:26
Бориспіль (в'їзд)	410	Н-08, головна дорога регіону	60	6:37
Бориспіль (М-03 × Н-08)	411	М-03, міська дорога	30	6:38
Бориспіль (виїзд)	416	М-03, міська дорога	30	6:40
М-03 × Бориспіль	417	М-03, магістральна дорога	85	6:41
Київ (в'їзд)	433	М-03, автомагістраль	85	6:46
Київ	451	міська дорога	30	6:48

За результатами табл. 2, маршрут по трасі Дніпро–Кременчук–Київ становить 451 км. Приблизний час у дорозі – 6 год 48 хв. Цей маршрут – оптимальний за критерієм відстані.

Таблиця 3

Маршрут по трасі Дніпро–Олександрія–Київ

Назва населеного пункту	Відстань від м. Дніпра, км	Назва дороги	Швидкість, км/год	Час, хв
1	2	3	4	5
Дніпро	0	М-04, міська дорога	30	0:00
Дніпро (виїзд)	11	М-04, міська дорога	30	0:22
М-04 × Н-11	54	М-04, автомагістраль	85	0:53
П’ятихатки (в’їзд)	109	М-04, магістральна дорога	70	1:41
П’ятихатки (виїзд)	113	М-04, міська дорога	30	1:48
Кіровоградська область	164	М-04, магістральна дорога	70	2:31
Олександрія (в’їзд)	165	М-04, магістральна дорога	70	2:32
Олександрія (виїзд)	171	М-04, міська дорога	30	2:46
Знам’янка (в’їзд)	200	М-04, магістральна дорога	70	3:11
Знам’янка (виїзд)	205	М-04, міська дорога	30	3:22
М-12 × Н-01	207	М-12, магістральна дорога	70	3:23
Н-01 × Н-14	250	Н-01, головна дорога регіону	60	4:04
Черкаська область	284	Н-01, головна дорога регіону	60	4:36
Сміла (в’їзд)	285	Н-01, головна дорога регіону	60	4:37
Н-01 × Н-16	297	Н-01, міська дорога	30	5:02
Корсунь-Шевченківський (в’їзд)	349	Н-01, головна дорога регіону	60	5:32
Корсунь-Шевченківський (виїзд)	351	Н-01, міська дорога	30	5:36
Н-01 × Корсунь-Шевченківський	352	Н-01, головна дорога регіону	60	5:37

Закінчення табл. 3

1	2	3	4	5
Київска область	412	Н-01, головна дорога регіону	60	6:04
Н-01 × Р-32	413	Н-01, головна дорога регіону	60	6:05
Кагарлик (в'їзд)	414	Н-01, міська дорога	30	6:06
Кагарлик (виїзд)	416	Н-01, міська дорога	30	6:08
Н-01 × Обухів	443	Н-01, головна дорога регіону	60	6:29
Н-01 (проміжна)	474	Н-01, автомагістраль	85	6:40
Київ (Н-01 × вул. Академіка Заболотнього)	478	Н-01, магістральна дорога	70	6:46
Р-01 × Н-01	479	Н-01, автомагістраль	85	6:47
Київ (Столичне шосе × Південний міст)	485	Н-01, головна дорога регіону	60	6:55
Київ	493	міська дорога	30	7:00

За даними табл. 3, маршрут по трасі Дніпро–Олександрія–Київ становить 493 км. Наближений розрахунок часу в дорозі – 7 год.

Таблиця 4

Маршрут по трасі Дніпро–Решетилівка–Київ

Назва населеного пункту	Відстань від м. Дніпра, км	Назва дороги	Швидкість, км/год	Час, хв
1	2	3	4	5
Дніпро	0	М-04, міська дорога	30	0:00
Дніпро (виїзд)	18	М-04, міська дорога	30	0:25
Р-52 × Т-04-14	42	Р-52, автомагістраль	85	0:37
Петриківка	52	Р-52, головна дорога регіону	70	0:54
Царичанка (в'їзд)	79	Р-52, головна дорога регіону	70	1:06
Царичанка	83	Р-52, міська дорога	30	1:35
Царичанка (виїзд)	86	Р-52, міська дорога	30	1:42
Полтавська область	114	Р-52, головна дорога регіону	60	1:50
Кобеляки (в'їзд)	115	Р-52, міська дорога	30	2:16
Кобеляки	116	Р-52, міська дорога	30	2:17

Закінчення табл. 4

1	2	3	4	5
Кобеляки (в'їзд)	115	Р-52, міська дорога	30	2:16
Кобеляки	116	Р-52, міська дорога	30	2:17
Кобеляки (виїзд)	118	Р-52, міська дорога	30	2:20
М-22 × Р-52	130	Р-52, головна дорога регіону	60	2:24
Р-52 × Т-17-36	155	Р-52, головна дорога регіону	60	2:35
Решетилівка (в'їзд)	167	Р-52, головна дорога регіону	60	3:10
Решетилівка (Сені × Ганжі)	168	Р-52, міська дорога	30	3:11
Решетилівка (виїзд)	169	Р-52, міська дорога	30	3:14
М-03 × Р-52	175	Р-52, головна дорога регіону	60	3:20
М-03 (проміжна)	182	М-03, автомагістраль	85	3:25
М-03 × Лубни	291	М-03, магістральна дорога	70	4:00
М-03 × Т-17-01	348	М-03, автомагістраль	85	4:30
Київська область	349	М-03, автомагістраль	85	4:31
М-03 (проміжна)	434	М-03, автомагістраль	85	5:10
М-03 × Р-03	437	М-03, магістральна дорога	70	5:15
Р-03 × Т-10-26	453	Р-03, головна дорога регіону	60	5:35
М-03 × Р-03	457	Т-10-26, дорога міського значення	50	5:40
Київ (в'їзд)	470	М-03, автомагістраль	85	5:55
Київ	482	міська дорога	30	6:16

За даними табл. 4, маршрут по трасі Дніпро–Решетилівка–Київ становить 482 км, приблизний час у дорозі – 6 год 16 хв. Цей маршрут – оптимальний за критерієм швидкості та часу перебування на маршруті. Перевірку наведених даних проведено з використанням інтернет-ресурсу [19].

За результатами в табл. 2–4, маємо:

- траса Дніпро–Кременчук–Київ, відстань за маршрутом становить 451 км. Приблизний час у дорозі – 6 год 48 хв. Це найкоротший шлях із Дніпра до Києва;
- траса Дніпро–Олександрія–Київ становить 493 км. Приблизний час у дорозі – 7 год;
- траса Дніпро–Решетилівка–Київ, відстань становить 482 км, приблизний час у дорозі – 6 год 16 хв. Це найбільш швидкісний маршрут із Дніпра до Києва.

Узагальнені результати розрахунків характеристик маршрутів з Дніпра до Києва подано в табл. 5.

Таблиця 5

Характеристика маршрутів руху з Дніпра до Києва

Маршрут	Довжина, км	Час руху, год	Швидкість руху, км/год
Дніпро–Олександрія–Київ	493	7	70
Дніпро–Кременчук–Київ	451	6,8	69
Дніпро–Решетилівка–Київ	482	6,27	78

Проаналізувавши дані, бачимо, що швидкість руху автомобіля по трасі Дніпро–Решетилівка–Київ – найвища й дорівнює 78 км/год. Це найбільший показник середньої швидкості, тому нині оптимальний за критерієм швидкості переміщення й часу перебування на маршруті. Тож тривають роботи з реконструкції дороги Дніпро–Царичанка–Кобеляки–Решетилівка із застосуванням сучасних технологій будівництва залізобетонних і залізофібробетонних доріг [2; 13]. Класифікація даної дороги у 2015 р. підвищена до рівня національної Н-31 [20], вона має протяжність 157,9 км і проходить по території Полтавської і Дніпропетровської областей. Цей статус підтверджено у 2019 р. [21].

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Результати проведеного дослідження свідчать, що якість проектів ремонту та реконструкції на багато років визначають основні транспортно-експлуатаційні ознаки автомобільної дороги. Одне із основних завдань цих проектів – визначити та забезпечити перспективну інтенсивність руху транспортних потоків між кореспондуючими пунктами. Середньорічне підвищення рівня інтенсивності дорожнього руху на основних автомобільних дорогах країни останнім часом становить до 20 відсотків. У складі транспортних потоків зростає частка великовагових і великогабаритних транспортних засобів, це призводить до швидкого руйнування автомобільних доріг і мостів, що розраховані на значно менші обсяги навантаження. Тому підвищення технічного рівня наявних доріг має стати пріоритетним напрямом розвитку дорожньої галузі України. Активізація проведення ремонтних робіт і модернізації автомобільних доріг в Україні шляхом застосування сучасних технологій дасть можливість створити необхідні умови для впровадження швидкісних автотранспортних перевезень.

Подальші дослідження можуть бути спрямовані на пошук нових напрямів і сучасних технологій розбудови швидкісних магістралей української мережі міжнародних транспортних коридорів.

Список використаних джерел:

1. *Дмитрієв І. А., Бурмака М. М.* Сучасний стан та перспективи розвитку мережі автомобільних доріг загального користування // Проблеми і перспективи розвитку підприємництва. 2013. № 1 (4). С. 64–72.

2. Про затвердження Державної цільової економічної програми розвитку автомобільних доріг загального користування державного значення на 2018–2022 роки: Постанова КМУ від 21 березня 2018 р. № 382. URL: https://zakon.rada.gov.ua/laws/show/382-2018-%D0%BF

3. *Веприцький Р. С., Ейтутіс Г. Д., Артем'єва С. В.* Аналіз та оцінка обсягів транзитних перевезень залізничним транспортом України // Вісник економіки транспорту і промисловості. 2018. № 62. С. 53–63.

4. *Божок Н. О., Булгакова Ю. В., Пуларія А. Л.* Дослідження сучасного стану парку пасажирських вагонів // Проблеми економіки транспорту. 2014. Вип. 8. С. 78–87.

5. *Doroshchuk V.* Transport system and transit potential of the state System transportowy Ukrainy i możliwości przewozów tranzytowych // Zeszyty Naukowe Wyższej Szkoły Ekonomii i Innowacji w Lublinie. Seria: "Transport i informatyka". 2016. (6/1). P. 5–17.

6. *Пасічник А. М., Клен О. М., Мірошніченко С. В.* Аналіз та оцінка ефективності використання транзитного потенціалу української транспортної системи // Електромагнітна сумісність та безпека на залізничному транспорті. 2016. Вип. 12. С. 88–97.

7. *Pasichnyk A., Vitruh I., Kutyrev V.* Factors that influence the formation of the transport-logistics networks // Systemy i srodki transportu samohodowego. Rzeszow: Politechnika Rzeszowska, 2013. P. 517–526.

8. *Мікловда В. П., Шевчук Я. В.* Сучасний стан та рівень розвитку автомобільної інфраструктури України // Науковий вісник Ужгородського університету. Серія "Економіка". 2011. Вип. 32. С. 6–13.

9. *Логвинова Н. В.* Шляхи розвитку транспортної системи України. 2016. URL: http://www.dspace.onua.edu.ua/bitstream/handle/11300

10. *Логутова Т. Г., Полторацький М. М.* Сучасний стан транспортної інфраструктури України // Теоретичні і практичні аспекти економіки та інтелектуальної власності. 2015. Вип. 2 (2). С. 8–14.

11. *Пасічник А. М.* Сучасні транспортно-митні технології міжнародних перевезень товарів : монографія / за ред. А. М. Пасічника. – Дніпропетровськ : АМСУ, 2012. 288 с.

12. *Пасічник А. М., Клен О. М.* Міжнародні транспортні коридори як основа реалізації транзитного потенціалу України // Вісник СНУ ім. В. Даля. 2011. № 5 (159). Ч. 1. С. 218–223.

13. *Пасічник А. М., Лебідь Є. М., Клен О. М., Мірошніченко С. В.* Проблеми оцінки транспортно-експлуатаційного стану та напрямки

модернізації мережі автомобільних доріг в Україні // Вісник СНУ ім. В. Даля. 2017. № 3 (233). С. 150–158.

14. *Якименко Н. В.* Пріоритетні напрямки розбудови міжнародних транспортних коридорів на території України (з точки зору Харківського регіону // Науково-техн. зб. 2007. № 78. С. 381–386.

15. Технічний стан автомобільних доріг загального використання. URL: http://mtu.gov.ua/content

16. *Біла С. О.* Удосконалення державного управління ринку транспортно-транзитних послуг в Україні // Держава та регіони. Сер. Державне управління. 2007. № 1. С. 16–19.

17. *Дикань В. Л.* Повышение транзитности Украины через интеграцию в мировую транспортную систему // Вісник економіки транспорту і промисловості. 2005. Вип. № 9–10. С. 13–18.

18. Мережа міжнародних транспортних коридорів. URL: http://www. mintrans.gov.ua/uk/transports/ print/42.html

19. Розрахунок відстаней між містами. URL: https://flagma.ua

20. Про затвердження переліку автомобільних доріг загального користування державного значення : Постанова КМУ від 16 вересня 2015 р. № 712. URL: https://zakon.rada.gov.ua/laws/show/712-2015-%D0%BF

21. Про затвердження переліку автомобільних доріг загального користування державного значення : Постанова КМУ від 30 січня 2019 р. № 55. URL: https://zakon.rada.gov.ua/laws/show/55-2019-%D0%BF

References:

1. Dmitriev I. A. and Burmaka M. M. (2013), *"Suchasnyy stan ta perspektyvy rozvytku merezhi avtomobil'nykh dorih zahal'noho korystuvannya"* ["Current situation and prospects of the development of a network of highways of general use"], Journal *Problemy i perspektyvy rozvytku pidpryyemnytstva* [Problems and prospects of entrepreneurship development] Collection of scientific works of KHNADU, vol. 1 (4), pp. 64–72 [Ukraine].

2. KMU (2018), *Pro zatverdzhennya Derzhavnoyi tsil'ovoyi ekonomichnoyi prohramy rozvytku avtomobil'nykh dorih zahal'noho korystuvannya derzhavnoho znachennya na 2018–2022 roky* [On approval of the State Target Economic Program for the development of public roads of state importance for 2018-2022 years]. Resolution of the Cabinet of Ministers of Ukraine dated March 21, 2018 No. 382, available at: https://zakon.rada.gov.ua/ laws / show / 382-2018-% D0% BF [Ukraine].

3. Vepritsky R.S., Aitutis G. D. and Artemyev S. V (2018), *"Analiz ta otsinka obsyahiv tranzytnykh perevezen' zaliznychnym transportom Ukrayiny"* ["Analysis and estimation of volumes of transit transportations by railway of

Ukraine"], *Visnyk ekonomiky transportu i promyslovosti* [Bulletin of the Economy of Transport and Industry], vol. 62, pp. 53–63 [Ukraine].

4. Bozhok N. O., Bulgakov Yu. V. and Pularijia A. L. (2014), *"Doslidzhennya suchasnoho stanu parku pasazhyrs'kykh vahoniv"* ["Research of the modern state of the park of passenger cars"], Journal *Problemy ekonomiky transportu* [Problems of Transport Economics], vol. 8, pp. 78–87 [Ukraine].

5. Doroshchuk V. (2016), Transport system and transit potential of the state transport system for Ukraine in transit traffic transit // Zeszyty Naukowe Wyższej Szkoły Ekonomii i Innowacji w Lublinie. Seria: Transport and Information, vol. 6/1, pp. 5–17 [Poland].

6. Pasichnik A. M., Klen O. M. and Miroshnichenko S. V. (2016), *"Analiz ta otsinka efektyvnosti vykorystannya tranzytnoho potentsialu ukrayins'koyi transportnoyi systemy"* ["Analysis and evaluation of the efficiency of the transit potential of the Ukrainian transport system"], Journal *Elektromahnitna sumisnist' ta bezpeka na zaliznychnomu transporti* [Electromagnetic compatibility and safety in railway transport], vol. 12, pp.88–97 [Ukraine].

7. Pasichnyk A., Vitruh I., Kutyrev V. (2013), "The Factors That Affect the Formation of the Transport-Logistics Networks" // Systemy i srodki transportu samohodowego, Rzeszow: Politechnika Rzeszowska, pp. 517–526 [Poland].

8. Miklovoda V. P. and Shevchuk Ya. V. (2011), *"Suchasnyy stan ta riven' rozvytku avtomobil'noyi infrastruktury Ukrayiny"* ["Modern state and level of development of automobile infrastructure of Ukraine"], Collection of scientific works *Naukovyy visnyk Uzhhorods'koho universytetu. Seriya "Ekonomika"* [Scientific Bulletin of Uzhgorod University. The series "Economics"], vol. 32. pp. 6–13 [Ukraine].

9. Logvinova N. V. (2016), *Shlyakhy rozvytku transportnoyi systemy Ukrayiny* [Ways of development of the transport system of Ukraine], available at: http://www.dspace.onua.edu.ua/ bitstream/handle/11300 [Ukraine]/

10. Logutova T. G. and M. M Poltoratsky (2015), *"Suchasnyy stan transportnoyi infrastruktury Ukrayiny"* ["Modern state of transport infrastructure of Ukraine"], Journal *Teoretychni i praktychni aspekty ekonomiky ta intelektual'noyi vlasnosti* [Theoretical and practical aspects of economy and intellectual property], vol. 2 (2). pp. 8–14 [Ukraine].

11. Pasichnyk A. M. (2012), *Suchasni transportno-mytni tekhnolohiyi mizhnarodnykh perevezen' tovariv* [Modern transportation and customs technologies of international goods transportation], monograph, Press AMSU, Dnipropetrovsk, 288 p. [Ukraine]

12. Pasichnyk A. M. and Klen O. M. (2011), *"Mizhnarodni transportni kor-ydory yak osnova realizatsiyi tranzytnoho potentsialu Ukrayiny"* ["International transport corridors as the basis for the implementation of the transit potential of

Ukraine"], Collection of scientific works *Visnyk SNU im. V. Dalya*, vol. 5 (159), part 1, pp. 218–223 [Ukraine].

13. Pasichnyk A. M., Lebid' Ye. M., Klen O. M. and Miroshnichenko S. V. (2017), *"Problemy otsinky transportno-ekspluatatsiynoho stanu ta napryamky modernizatsiyi merezhi avtomobil'nykh dorih v Ukrayini"* ["Problems of estimation of transport and operational condition and directions of modernization of the network of highways in Ukraine"], Bulletin of the SNU named after V. Dal', vol. 3 (233), pp. 150–158 [Ukraine].

14. Yakimenko N. V. (2007), *"Priorytetni napryamky rozbudovy mizhnarodnykh transportnykh korydoriv na terytoriyi Ukrayiny (z tochky zoru Kharkivs'koho rehionu"* ["Priority directions of development of international transport corridors on the territory of Ukraine (from the point of view of Kharkiv region"], *Naukovo-tekhnichnyy zbirnyk* [Scientific and Technical Collection], vol. 78, pp. 381–386 [Ukraine].

15. *Tekhnichnyy stan avtomobil'nykh dorih zahal'noho vykorystannya* [Technical condition of highways of general use], available at: http://mtu.gov.ua/content [Ukraine].

16. Bila S. O. (2007), *"Udoskonalennya derzhavnoho upravlinnya rynku transportno-tranzytnykh posluh v Ukrayini"* ["Improvement of state administration of the market of transport-transit services in Ukraine"], Journal *Derzhava ta rehiony. Ser. Derzhavne upravlinnya* [State and Regions. Series. Governance], vol. 1, pp. 16–19 [Ukraine].

17. Dikan' V. L. (2005), *"Povysheniye tranzitnosti Ukrainy cherez integratsiyu v mirovuyu transportnuyu sistemu"* [Increase of transit of Ukraine through integration into the world transport system], Bulletin of the Economy of Transport and Industry (a collection of scientific and practical articles), vol. 9-10, pp. 13–18 [Ukraine].

18. *Merezha mizhnarodnykh transportnykh korydoriv* [The network of international transport corridors], available at: http://www.mintrans.gov.ua/ uk/transports/print/42.html [Ukraine].

19. *Rozrakhunok vidstaney mizh mistamy* [Calculation of distances between cities, available at: https://flagma.ua [Ukraine].

20. CMU (2015), *Pro zatverdzhennya pereliku avtomobil'nykh dorih zahal'noho korystuvannya derzhavnoho znachennya* [On approval of the list of public roads of state importance], CMU Resolution dated September 16, 2015, No. 712, available at: https://zakon.rada.gov.ua/ laws/show/712-2015-%D0%BF [Ukraine].

21. CMU (2019), *Pro zatverdzhennya pereliku avtomobil'nykh dorih zahal'noho korystuvannya derzhavnoho znachennya* [On approval of the list of public roads of state importance], CMU Resolution dated January 30, 2019, No. 55, available at: https://zakon.rada.gov.ua/laws/show/55-2019-%D0%BF [Ukraine].

DOI: https://doi.org/10.32836/2521-6643-2019-1-57-9
УДК 004.942:004.55:519.17

Т. В. Січко, кандидат технічних наук,
доцент кафедри прикладної математики
і теорії систем управління Донецького
національного університету
імені Василя Стуса
К. В. Смоктій, кандидат економічних наук,
доцент кафедри прикладної математики
і теорії систем управління Донецького
національного університету
імені Василя Стуса
А. О. Ткачук, студент Донецького
національного університету
імені Василя Стуса

ПРИКЛАДНІ АСПЕКТИ РОЗРАХУНКУ СТРУКТУРНО-ТОПОЛОГІЧНИХ ХАРАКТЕРИСТИК СИСТЕМ

Розроблено односторінковий веб-додаток для обчислення структурно-топологічних характеристик систем, які впливають на різноманітні аспекти розвитку суспільства. Наведено програмну реалізацію алгоритмів обчислень структурно-топологічних характеристик систем, представлено стартовий інтерфейс розробленого додатка. Роботу додатка продемонстровано на прикладі розрахунку структурно-топологічних характеристик організаційної структури компанії, яка розробляє ігри. Окреслено перспективи подальшого вдосконалення розробленого веб-додатка.

Ключові слова: *графові моделі; структурний аналіз; структурно-топологічні характеристики; односторінковий веб-додаток.*

Разработано одностраничное веб-приложение для вычисления структурно-топологических характеристик систем, которые влияют на различные аспекты развития общества. Приведена программная реализация алгоритмов вычисления структурно-топологических характеристик систем, представлено стартовый інтерфейс разработанного приложения. Работу приложения продемонстрировано на примере расчета структурно-топологических характеристик организационной структуры компании, ко-

торая разрабатывает игры. Определены перспективы дальнейшего совершенствования разработанного веб-приложения.

Ключевые слова: *графовые модели; структурный анализ; структурно-топологические характеристики; одностраничное веб-приложение.*

Often happens that for the analysis of the system structural properties on a graphmetric characteristics are inconsequential, at the same such topological nature parametersas connectivity, compactness and continuity are valuable. These characteristics allow optimizing structural links between elements of any system according to different criteria using structural-topological analysis of systems, which play important role for social and economic development of any country.

In this paper we analyzed the existing applications for graph processing and took into account purchasing costs (that can be licensed use) and concluded that it isadvisable to develop a web application that would be an open source code (free to use) and to perform the calculation of the basic characteristics for the structural analysis of the systems that are described by the graph model, for instance: connectivity, continuity, redundancy, compactness, hierarchy, diameter, uneven distribution of bonds.

Applied aspects of the calculation of systems structural-topological characteristics are considered and an approach as for the automation of systems structural-topological characteristics calculations is developed. This approach allows to synthesize the corresponding web application with its publication in the Internet for further use for the decision-making process concerning the optimization of the structural relations of the investigated system.

Single-page format was chosen as one of the most widespread and most convenient to use for the web-application. A single-page application is a web application that uses a single HTML document as a shell for all web pages and organizes user interaction through HTML, CSS, and JavaScript files that are dynamically loaded. Developed application is connected to the version control system Git, downloaded to Git Hub and connected to Git Hub Pages. As an example, the organizational structure of the game developing company is considered and needed calculations of the system characteristics are done. The conclusions from this research and the prospects for further improvement of the developed one-page application are presented.

Key words: *graphmodels; structural analysis; structuraltopo logical characteristics; one-pageapplication.*

Постановка проблеми. Питання управління складними системами обумовлюють дослідження, в яких використовується математична теорія, що дає

можливість поєднати математичні властивості соціально-економічних систем та їх економічний зміст. Такою теорією є теоретико-графове моделювання економічних об'єктів і процесів виробництва до якого останнім часом виявляється більша зацікавленість. Так, теоретико-графові моделі не лише відображають структуру системи та зв'язки між елементами, але й використовуються для прийняття оптимальних управлінських рішень у моделюванні соціально-економічних системи різної складності.

Аналіз останніх досліджень і публікацій. Графовий підхід до моделювання складних систем розглядається у працях І. М. Мельника, О.М. Парубця, О. Г. Климко, С. П. Кобця, І. І. Скрильник, А. А. Кочкарова, А. М. Штангрета, К. В. Ніколаєва, В. В. Кобійчука та ін.

Теоретико-графові моделі застосовуються для розв'язання великого класу оптимізаційних задач, а саме: задачі розподілу ресурсів, задачі управління запасами, задачі планування та розміщення тощо. Розв'язанню таких задач присвячено дослідження провідних українських учених І. В. Сергієнка, Н. З. Шора, Ю. Г. Стояна, О. О. Ємця, І. М. Ляшенка, С. В. Яковлева.

Алгоритмам розв'язання цих задач та їх програмній реалізації різними мовами програмування (від VBA до C++) присвячено фундаментальні праці Г. А. Черноморова [*1,* 28–73] та Р. Седжвика [*2,* 231–304], проте більшість вітчизняних авторів спрямовують свої дослідження на підтримку розв'язання екстремальних задач на графах за допомогою надбудови Solver (Пошук рішення) MS Excel [3–6].

Для розв'язання задач, об'єктами яких є графи, використовують пакети аналітичних обчислень: Mathematica, MATLAB, Mathcad, Maple, що дають можливість виконувати аналітичні символьні перетворення [7].

Існують також готові програмні рішення, які реалізують безліч **алгоритмів** для обробки графів: пошук мінімального шляху різними способами, пошук ейлеревих і гамільтонових маршрутів, визначення хроматичного числа, пошук мінімального остовного дерева, визначення максимального потоку, перевірка на зв'язність, пошук радіуса і діаметра графа, перевірка чи є граф деревом, перевірка на планарність, пошук критичного шляху, пошук циклів, пошук максимального повного підграфа [8–10].

Виникають ситуації під час аналізу структурних властивостей системи на графі, коли метричні характеристики несуттєві, а важливими є характеристики зв'язності, компактності та неперервності, тобто характеристики топологічного характеру. Ці характеристики уможливлюють оптимізацію структурних зв'язків між елементами будь-якої системи за різними критеріями з використанням структурно-топологічного аналізу систем.

Автори проаналізували наявні додатки для обробки графів і дійшли висновку, що з урахуванням вартості покупки (ліцензійного використання)

доцільно здійснити розробку веб-додатка, який буде з відкритим програмним кодом (безкоштовним для використання) і реалізує розрахунок базових характеристик для структурного аналізу систем, що описуються графовою моделлю, а саме: зв'язності, неперервності, надмірності, компактності, ієрархічності, діаметра, нерівномірності розподілу зв'язків.

Мета статті – розглянути прикладні аспекти розрахунку структурно-топологічних характеристик систем і визначити підхід до автоматизації обчислень структурно-топологічних характеристик систем, що, зі свого боку, дає можливість синтезувати відповідний веб-додаток із його публікацією для подальшого використання в мережі Internet та приймати рішення щодо оптимізації структурних зв'язків досліджуваної системи.

Виклад основного матеріалу. Для реалізації веб-додатка було обрано односторінковий ормат як один із найпоширеніших та найзручніших у використанні. Односторінковий додаток – це веб-додаток, який використовує єдиний HTML-документ як оболонку для всіх веб-сторінок і організовує взаємодію з користувачем через HTML, CSS, Java Script файли, що динамічно завантажуються.

Перевагами односторінкових веб-додатків є:

– висока швидкість роботи, оскільки додаток не оновлює всю сторінку, а тільки потрібну частину, що істотно підвищує швидкість;

– висока швидкість розробки, оскільки готові бібліотеки і фреймворки дають потужні інструменти для розробки веб-додатків. Над проектом можуть паралельно працювати back-end і front-end розробники. Завдяки чіткому поділу вони не заважатимуть один одному;

– мобільність, оскільки додаток дає змогу легко розробити мобільний додаток на основі готового коду [11].

Архітектурно розроблений односторінковий додаток є сторінкою html з одним контейнером div, логікою відображення контенту, в якому керує скрипт мовою javascript:

```
<body>
  <div id="root">
      <script src="Topological_characteristics.js"></script>
  </div>
</body>
```

Рис. 1. Місце підключення керуючого скрипту до html сторінки

Це дає можливість установлювати розміри всіх елементів сторінки відповідно до розміру вікна.

Скрипт може змінювати зміст html-сторінки завдяки використанню об'єктної моделі документа (DOM). Об'єктна модель документа – специфікація прикладного програмного інтерфейсу для роботи зі структурованими документами (як правило, документами XML). Визначається ця специфікація консорціумом W3C.

Разом із поширенням та розвитком веб-технологій і веб-переглядачів почали з'являтись різні, часто несумісні інтерфейси роботи із HTML-документами в інтерпретаторах Java Script, вбудованих у веб-переглядачі. Це спонукало World Wide Web Consortium (W3C) узгодити та визначити низку стандартів, які отримали назву W3C Document Object Model (W3C DOM). Специфікації W3C не залежать від платформи або мови програмування [12].

Логіка обчислень структури реалізована у класі MyGraph (рис. 2). Структура зберігається у вигляді незваженого неорієнтованого графа.

```
class MyGraph{
    constructor(n) {
        this.n=n;//Кількість вершин
        this.adjacency=create2DimArray([this.n,this.n]);//Матриця суміжності
        this.distance=create2DimArray([this.n,this.n]);//Матриця відстаней
        this.connection=create2DimArray([this.n,this.n]);//Матриця зв'язності
        for(var i=0;i<n;i++)
            for(var j=0;j<n;j++){
                this.adjacency[i][j]=0;
                this.distance[i][j]=0;
                this.connection[i][j]=0;
            }
        this.redundancy=0;//Збитковість
        this.redundancy2=0;//Квадратне відхилення заданого розподілу вершин від рівномірного
        this.Q=0;//Абсолютна компактність
        this.compactness=0;//Відносна компактність
        this.d=0;//Діаметр системи
        this.sigma=0;//Ступінь централізації
    }
```

Рис. 2. Структура класу, що зберігає граф

Відповідні змінні зберігають показники графа. Кількість вершин і матриця суміжності вводяться користувачем, а всі інші показники обчислюються у процесі роботи. Наведемо назви й деякі реалізації методів для обчислення структурно-топологічних характеристик систем.

Обчислення структурної надлишковості (надмірності, збитковості), яка показує перевищення загальної кількості зв'язків над мінімально необхідною, використовується для непрямої оцінки економічності й надійності досліджуваних систем. Реалізацію зображено на рис. 3 у методі calc_redundancy.

Нерівномірність розподілу зв'язків, що характеризує недовикористання можливостей заданої структури в досягненні максимальної зв'язності, реалізовано в методі calc_redundadncy2.

```
calc_redundadncy(){
    var R=0;
    for (var i = 0; i <this.n; i++)
    for (var j = 0; j < this.n; j++)
        R += this.adjacency[i][j];
R=R*0.5/(this.n-1)-1;
    this.redundancy=R;
}
```

Рис. 3. Фрагмент обчислення структурної надлишковості

Обчислення матриці зв'язності реалізовано в методі calc_connection (рис. 4).

```
calc_connection(){
    if (this.n > 0){
        var Ak=createNDimArray([this.n,this.n,this.n]);
        for (var i = 0; i < this.n; i++)
            for (var j = 0; j < this.n; j++)
                Ak[0][i][j] = this.adjacency[i][j];
        for (var k = 1; k < this.n; k++){
            for (var i = 0; i < this.n; i++)
                for (var j = 0; j < this.n; j++){
                    Ak[k][i][j] = 0;
                    for (var m = 0; m < this.n; m++)
                        Ak[k][i][j] += Ak[k - 1][i][m]*this.adjacency[m][j];
                }
    }
    for (var i = 0; i < this.n; i++)
        for (var j = 0; j < this.n; j++)
            this.connection[i][j] = 0;
    for (var k = 0; k < this.n; k++){
        for (var i = 0; i < this.n; i++)
            for (var j = 0; j < this.n; j++)
                this.connection[i][j] += Ak[k][i][j];
    }

    for (var i = 0; i < this.n; i++)
        for (var j = 0; j < this.n; j++)
            if (this.connection[i][j] >= 1)this.connection[i][j]=1;
    }
}
```

Рис. 4. Фрагмент обчислення матриці зв'язності

Обчислення абсолютної та відносної структурної компактності реалізовано у методі calc_compactness. Наприклад, структурна компактність транспортних систем дає можливість отримати інформацію про ступінь використання дорожніх зв'язків за повного навантаження на систему (одночасне перевезення вантажу з усіх елементів системи в усі напрямки).

Обчислення діаметра структури реалізовано в методі calc_d. Діаметр структури визначає найкоротшу відстань між найвіддаленішими вершинами.

```
calc_compactness(){
    var Q=0;
    var Qmin=this.n*(this.n-1);
    for(var i=0;i<this.n;i++)
        for(var j=0;j<this.n;j++){
            Q=Q+this.distance[i][j];
        }
    this.Q=Q;
    var Qrel=(Q/Qmin)-1;
    this.compactness=Qrel;
}
```

Рис. 5. Фрагмент обчислення абсолютної та відносної структурної компактності

Значення діаметра структури може характеризувати, скажімо, пропускну здатність системи. Економічний зміст даної характеристики виявляється під час оптимізації інформаційних, матеріальних, фінансових потоків.

```
calc_d(){
    var max=this.distance[0][0];
    var size = this.n;
    for (var i = 0; i < size; i += 1)
        for (var j = 0; j < size; j += 1)
            if(max<this.distance[i][j])max=this.distance[i][j];
    this.d=max;
}
```

Рис. 6. Фрагмент обчислення діаметра структури

Обчислення ступеня централізації структури реалізовано в методі calc_sigma. Цей показник змінюється в діапазоні від 0 до 1. Нуль відповідає абсолютно децентралізованій системі, одиниця – абсолютно централізованій.

Матриця відстаней обчислюється за допомогою алгоритму Флойда–Воршела, який являє собою динамічний алгоритм для знаходження найкоротших відстаней між усіма вершинами графа [13]. Він реалізований у методі класу calc_distancematr (рис. 8).

В додатку передбачено дві можливості введення матриці суміжності графа: з клавіатури та з файлу. Можливість уведення матриці суміжності з файлу реалізована з допомогою FileAPI. FileAPI – це набір інструментів Java Script для роботи з файлами, він підтримується більшістю сучасних браузерів [14].

```
calc_sigma(){
    var size = this.n;
    var Z=new Array(size);
    for(var i=0;i<size;i++){
        var tmp=0;
        for(var j=0;j<size;j++){
            if(isFinite(this.distance[i][j])==false){
                tmp=Infinity;
                break;
            }
            tmp=tmp+this.distance[i][j];
        }
        Z[i]=this.Q/(2*tmp);
    }
    var Zmax=Z[0];
    for(var i=1;i<size;i++)
        if(Z[i]>Zmax)Zmax=Z[i];
    this.sigma=((size-1)*(2*Zmax-size))/(Zmax*(size-2))
}
```

Рис. 7. Фрагмент обчислення ступеня централізації структури

Можливість уведення з клавіатури реалізована в 2 етапи: введенням кількості вершин та введенням матриці суміжності. Поле для введення матриці реалізовано як таблиця select-елементів, у кожному з яких є тільки два варіанти 0 або 1 (оскільки граф незважений). За замовчуванням усі елементи заповнюються нулями. За зміною будь-якого елемента змінюється елемент, симетричний йому відносно головної діагоналі (оскільки граф є неорієнтованим). Реалізовано можливість зберегти введену матрицю у файл, що дає можливість її змінити і знову завантажити для подальших розрахунків.

```
calc_distancematr(){
  var size = this.n;
  for (var i = 0; i < size; i += 1) {
    for (var j = 0; j < size; j += 1) {
      if (i === j) {
        this.distance[i][j] = 0;
      } else if (this.adjacency[i][j]==0) {
        this.distance[i][j] = Infinity;
      } else {
        this.distance[i][j] = this.adjacency[i][j];
      }
    }
  }
  for (var k = 0; k < size; k += 1) {
    for (var i = 0; i < size; i += 1) {
      for (var j = 0; j < size; j += 1) {
        if (this.distance[i][j] > this.distance[i][k] + this.distance[k][j])
          this.distance[i][j] = this.distance[i][k] + this.distance[k][j];
        }
      }
    }
  }
}
```

Рис. 8. Фрагмент обчислення матриці відстаней

Розроблений додаток підключено до системи контролю версій git, завантажено на Git Hub [15] та підключено до Git Hub Pages.

Для прикладу розглянемо організаційну структуру компанії, яка розробляє ігри.

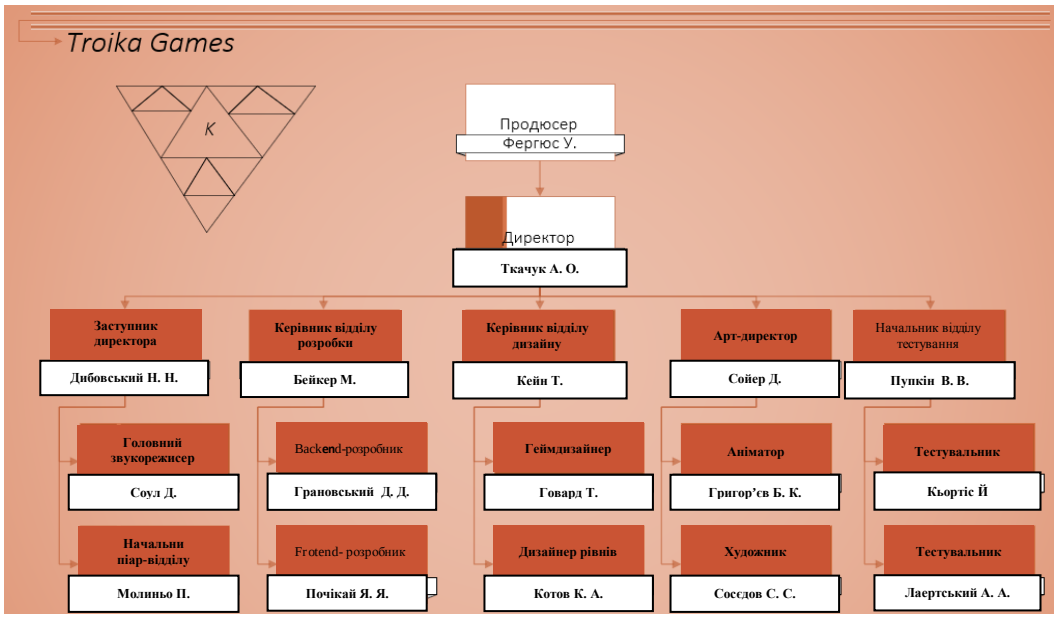


Рис 9. Організаційна структура управління компанії, яка розробляє ігри

Створимо текстовий файл, у першому рядку якого буде кількість вершин структури, а в наступних – матриця суміжності структури.

```
17
0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
1 0 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0
0 1 0 0 0 0 0 1 1 0 0 0 0 0 0 0 0
0 1 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0
0 1 0 0 0 0 0 0 0 0 0 1 1 0 0 0 0
0 1 0 0 0 0 0 0 0 0 0 0 0 1 1 0 0
0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1
0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0
```

Рис. 10. Вміст файлу з матрицею суміжності структури

Запустимо на виконання розроблений односторінковий додаток. Стартовий інтерфейс додатка зображено на рис. 12.

Оберіть спосіб уведення структури

Увести матрицю суміжності структури з клавіатури
Завантажити матрицю суміжності структури з файлу

Рис. 12. Стартовий інтерфейс розробленого односторінкового додатка

Оберемо варіант завантаження матриці суміжності структури з файлу.

Формат файлу:
Кількість вершин
Матриця суміжності

Приклад файлу:
5
0 1 1 1 0
1 0 1 1 1
1 1 0 1 0
1 1 1 0 1
0 1 0 1 0

Завантажити файл

Рис. 13. Інтерфейс для завантаження файлу

Натиснемо кнопку “Завантажити файл”. У наступному вікні оберемо файл, який було створено раніше, й натиснемо “відкрити”. Отримали розраховані топологічні характеристики організаційної структури компанії, яка розробляє ігри. Наведемо нижче деякі з них:

Надлишковість структури $(R)=0$

Квадратне відхилення заданого розподілу вершин від рівномірного $(\varepsilon^2)\approx 31.765$

Абсолютна компактність структури $(Q)=772$

Відносна компактність структури $(Q_{відн})\approx 1.838$

Діаметр структури $(d)=4$

Рис. 14. Результати роботи розробленого односторінкового додатка

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Запропонований підхід дає можливість автоматизувати проведення аналізу організаційної структури управління та розрахунку структурно-топологічних характеристиках, що, зі свого боку, дає змогу приймати рішення з оптимізації структурних зв’язків досліджуваної системи.

Перспективи подальшого вдосконалення розробленого односторінкового додатка автори вбачають у розробці більш лаконічного дизайну та розширенні підтримки мобільних платформ, чого можна досить швидко досягти завдяки застосуванню мови дизайну Material Design [16]. Material Design використовує більше макетів на основі сітки, адекватних анімацій і переходів, доповнення та ефектів глибини, таких як освітлення й тіні.

Доцільно було б реалізувати можливість уведення структури шляхом її зображення у вигляді графа й можливість автоматичного зображення структури відповідно до її матриці суміжності. Цього можна швидко досягти завдяки бібліотеці з відкритим вихідним кодом, написаній на JS – cytoscape.js [17]. Cytoscape.js дає можливість легко відображати та маніпулювати детальними інтерактивними графами. Cytoscape.js легко інтегрується та підтримує мобільні версії браузерів.

Список використаних джерел:

1. *Черноморов Г. А.* Теория принятия решений. Новочеркасск: Известия вузов: Электромеханика, 2002. 276 с.

2. *Седжвик Р.* Фундаментальные алгоритмы на С++. Алгоритмы на графах. Санкт-Петербург : ООО “Диа Софт ЮП”, 2002. 496 с.

3. *Гліненко Л. К., Яковенко Є. І.* Розв'язання задач на графах за допомогою надбудови Solver MS Excel // Вісник Хмельницького національного університету. Технічні науки. 2013. № 5. С. 176–184.

4. *Гліненко Л. К., Фаст В. М.* Розв'язання задач комбінаторної оптимізації радіоелектронних систем у середовищі MSExcelSolver. URL: http://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/5120/ 25glinenkofast. pdf (дата звернення: 8.04.2019).

5. *Кузьмичов А. І.* Математичне програмування в Excel: навч. посіб. Київ: Вид-во Європ. Ун-ту, 2005. 320 с.

6. Гліненко Л. К., Фаст В. М. Автоматизація розв'язання екстремальних задач на графах у конструкторському проектуванні РЕА // Вісник НТУУ "КПІ". Серія "Радіотехніка", Радіоапаратобудування. 2013. № 54. С. 90–101.

7. *Кирсанов М. Н.* Графы в Maple. Задачи, алгоритмы, программы. М.: ФИЗМАТЛИТ, 2007. 168 с.

8. Сайт программы для визуализации графов "Графоанализатор". URL: http://grafoanalizator.unick-soft.ru (дата звернення: 8.04.2019).

9. Cytoscape: An Open Source Platform for Complex Network Analysis. URL: https: //cytoscape.org (дата звернення: 10.04.2019).

10. Gephi – The Open Graph Viz Platform. URL: https://gephi.org (дата звернення: 10.04.2019).

11. Single Page Application (SPA) и Multi Page Application (MPA): преимущества и недостатки. URL: https://merehead.com/ru/blog/single-page-application-vs-multi-page-application/ (дата звернення: 10.04.2019).

12. Об'єктна модель документа. URL: https://uk.wikipedia.org/wiki/Об%27єктна_модель_документа (дата звернення: 10.04.2019).

13. Floyd–Warshallal gorithm. URL: https://en.wikipedia.org/wiki/Floyd%E2%80%93Warshall_algorithm (дата звернення: 10.04.2019).

14. FileAPI. URL: https://javascript.ru/blog/brmaley-ee/fileapi (дата звернення: 10.04.2019).

15. Репозиторій розробленого додатка на GitHub. URL: https://github.com/ArtiomTkachuk1/Topological_characteristics (дата звернення: 12.04.2019).

16. Material_Design. URL: https://en.wikipedia.org/wiki/Material_Design (дата звернення: 12.04.2019).

17. Cytoscape.js. URL: http://js.cytoscape.org (дата звернення: 12.04.2019).

References:

1. Chernomorov H. A. Teoryia pryniatyia reshenyi. Novocherkassk: Yzvestyiavuzov: Elektromekhanyka, 2002. 276 s.

2. Sedzhvyk R. Fundamentalnyie alhorytmyina S++. Alhorytmyi na hrafakh. SPb. : OOO "DyaSoftIuP", 2002. 496 s.

3. Hlinenko L. K., Yakovenko Ye. I. Rozviazannia zadach na hrafakh za dopomohoiu nadbudovy Solver MS Excel // Visnyk Khmelnytskoho natsionalnoho universytetu. Tekhnichni nauky. 2013. № 5. S. 176–184.

4. Hlinenko L. K., Fast V. M., Rozviazannia zadach kombinatornoi optymizatsii radioelektronnykh system u seredovyshchi MSExcelSolver. URL: http://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/5120/25glinenkofast.pdf (date of the application:8.04.2019).

5. Kuzmychov A. I. Matematychne prohramuvannia v Excel: navch. posib. Kyiv: Vyd-voYevrop. un-tu, 2005. 320 s.

6. Hlinenko L. K., Fast V. M. Avtomatyzatsiia rozviazannia ekstremalnykh zadach na hrafakh u konstruktorskomu proektuvanni REA // Visnyk NTUU “KPI”. Seriia Radiotekhnika, Radioaparatobuduvannia. 2013. № 54. S. 90–101.

7. Kyrsanov M. N. Hrafyi v Maple. Zadachy, alhorytmyi, prohrammyi. Moskva: FYZMATLYT, 2007. 168 s.

8. Sait prohrammyi dlia vyzualyzatsyy hrafov “Hrafoanalyzator”. URL: http://grafoanalizator.unick-soft.ru (date of the application:8.04.2019).

9. Cytoscape: An Open Source Platform for Complex Network Analysis.URL:https://cytoscape.org (date of the application:10.04.2019).

10. Gephi – The Open Graph Viz Platform.URL: https://gephi.org (date of the application: 10.04.2019).

11. Single Page Application (SPA) и Multi Page Application (MPA): preimuschestva i nedostatki. URL: https://merehead.com/ru/blog/single-page-application-vs-multi-page-application (date of the application:10.04.2019).

12. Obiektna model dokumenta. URL: https://uk.wikipedia.org/wiki/Об%27єктна_модель_документа (date of the application:10.04.2019).

13. Floyd–Warshall algorithm. URL: https://en.wikipedia.org/wiki/Floyd%E2% 80%93Warshall_algorithm (date of the application:10.04.2019).

14. FileAPI. URL: https://javascript.ru/blog/brmaley-ee/fileapi (date of the application:10.04.2019).

15. Repozitorii rozroblenoho dodatka na GitHub. URL: https://github.com/ArtiomTkachuk1/Topological_characteristics (date of the application:12.04.2019).

16. Material_Design. URL: https://en.wikipedia.org/wiki/Material_Design (date of the application:12.04.2019).

17.Cytoscape.js. URL: http://js.cytoscape.org (date of the application:12.04.2019).

DOI: https://doi.org/10.32836/2521-6643-2019-1-57-10
УДК 004.912

В. В. Костенко, старший викладач кафедри комп'ютерних наук та інженерії програмного забезпечення Університету митної справи та фінансів
Д. Є. Костенко, старший викладач кафедри комп'ютерних наук та інженерії програмного забезпечення Університету митної справи та фінансів
Є. Д. Замотаєв, студент Університету митної справи та фінансів
В. О. Широченко, студент Університету митної справи та фінансів

ВИЯВЛЕННЯ ПРОБЛЕМ СТРУКТУРИ ІНФОРМАЦІЙНИХ РЕСУРСІВ ПІД ЧАС ОБРОБКИ ТА ПОШУКУ ІНФОРМАЦІЇ

Досліджено одну з важливих проблем процесу пошуку інформації. Виявлено основні відмінності між пошуком (як автоматизованою процедурою) і виділенням потрібної інформації. Визначено питання, які доцільно аналізувати під час розв'язання проблеми пошуку або виділення необхідної інформації. Створено тестовий програмний модуль, який розв'язує частину описаних у статті проблем. Розкрито основні моменти реалізації механізму виділення потрібної інформації. Надано рекомендації та пропозиції щодо розв'язання проблеми отримання необхідної для користувача інформації серед великої кількості "інформаційного шуму".

Ключові слова: *інформація; дані; інформаційний пошук; фільтрація інформації; сортування інформації.*

Исследована одна из важных проблем процесса поиска информации. Выявлены основные различия между поиском (как автоматизированной процедурой) и выделением нужной информации. Определены вопросы, которые целесообразно анализировать при решении проблемы поиска или выделения необходимой информации. Создан тестовый программный модуль, который решает часть описанных в работе проблем. Раскрыты основные моменты реализации механизма выделения нужной информации. Даны реко-

мендации и предложения по решению проблемы нахождения необходимой для пользователя информации среди большого количества "информационного шума".

Ключевые слова: *информация; данные, информационный поиск; фильтрация информации; сортировка информации.*

There are investigated important problems of the information search process. Long-term accumulation of information has its negative sides. The main problem is the glut of so-called "digital noise". "Digital noise" is information which doesn't assist the user in information searching process. "Digital noise" makes it difficult to find the right answer. At the same time there is another problem – the number of materials that are freely available is constantly growing, doubling on average once every 2 years. Sometimes – more often. In this growth there are hidden one of the main problems. Finding the right information often turns into a difficult problem that takes time and effort. There are shown the main differences between the search (as an automatical procedure) and the necessary information allocation. Identified some questions which appropriate to analyze when solving a search problem or highlighting the necessary information (site content, data storage and processing methods, site values for information support of the relevant type of activity). The main idea of this article is in optimize the filtering and retrieving information process for users. It is necessary to hide from the user information which doesn't solve his problems.

There are create a test-software module which solve some problems described in this article. Revealed the main points of implementation the selection mechanism of the necessary information. The idea is in allocate absolutely or most useful answers. It wouldn't be necessary to re-read or scroll through the whole discussion board to find out what is the ultimate correct answer or the right decision. Recommendations and suggestions are given to solve the problem of finding the necessary information for the user among a large amount of "information noise". It is necessary to create the more specialized and thematic resources with high-quality content. Using this portals, the information searching will be faster and better. It's necessary to develop comparison services. If it possible, there are necessary to use geolocation services and base searching process on user's location. It is necessary to emphasize the quality of information and divide it according to the tasks.

Key words: *information; data; information search; information filtering, information sorting*.

Постановка проблеми. Нині в глобальній мережі Інтернет існує інформація щодо будь-якого аспекту, будь-якої галузі.

Також існують розвинені (не завжди повною мірою) пошукові системи, які не тільки знаходять інформацію, пов'язану із пошуковим запитом, але й мають досить потужні фільтри та ключові слова, завдяки яким пошук проходить, наприклад, з точною відповідністю запиту і лише серед документів зазначеного формату. Але це працює, якщо проводиться пошук інформації загального спрямування.

Багаторічне накопичення інформації має і також свої негативні аспекти, головним із яких є перенасичення так званим "цифровим шумом".

Під "цифровим шумом" розуміють інформацію, яка під час пошуку жодним чином не допомагає користувачу, а дуже часто навіть заважає знайти потрібну відповідь серед усієї маси цього самого "шуму".

Розглянемо проблему на прикладі двох абстрактних сервісів для розробників програмного забезпечення: Сервіс № 1 та Сервіс № 2.

Нехай обидва сервіси мають численну аудиторію, яка безперервно ставить питання щодо виконання різноманітних завдань та зазвичай отримує робочі рішення від інших користувачів.

Таким чином, коли у нового користувача виникає питання, яке вже було обговорено, він з великою вірогідністю натрапить на відповідь. Сервіс № 2 має структуру звичайного "діалогу", всі коментарі додаються у нижню частину сайту лише з розподілом за сторінками. Простіше кажучи, довге "полотно" повідомлень (розташованих за датою додавання).

Але в усіх сервісів, які мають таку ж структуру, як і Сервіс № 2, є велика проблема: після того, як користувач знайшов своє питання, яке хтось уже ставив, йому доводиться прокручувати сотні відповідей, у яких інші користувачі пишуть: "Маю таку ж проблему …" або дають неправильні відповіді. А дочитавши до кінця цієї гілки відповідей, майже завжди бачить повідомлення: "Робоче рішення знаходиться за таким посиланням ..." з переходом на іншу гілку відповідей. Не виключено, що з десяток наступних гілок будуть з такими ж посиланнями в кінці. Отже, процес стає нескінченним.

При цьому зазвичай у разі переходу в іншу гілку дещо змінюється і проблема, розв'язання якої шукають. Таким чином, виявляється, що розробник, якому необхідно отримати відповідь, втрачає великий обсяг робочого часу, даремно витрачає свої сили на перечитування сотень непотрібних відповідей. Це і є "інформаційний шум".

На відміну від Сервісу № 2, Сервіс № 1 менш популярний, але він частково позбавлений цієї проблеми. Реалізовано це завдяки винесенню робочого рішення на самий верх сторінки одразу ж під питанням. Правильною вважається та відповідь, яку або позначив такою автор самого питання, або яка набрала максимальну кількість позначок "правильності" від усіх користувачів. Виникає питання щодо "професійної адекватності" тих, хто вважає відповідь правильною.

Та факт залишається фактом: відкривши сторінку з питанням, користувач одразу ж бачить відповідь, яка є правильною на 100 %, або ту, яка допомогла найбільшій кількості користувачів.

Роблячи висновок з вищезазначеної проблеми, нескладно дійти до розв'язання проблеми для всіх сервісів, що працюють за типом Сервіс № 2. Беручи до уваги надлишкову кількість інформації, вважаємо обов'язковим додавання алгоритму "рейтингів" відповідей до кожного подібного сервісу.

Аналіз останніх досліджень і публікацій. Інформаційний пошук – процес пошуку неструктурованої документальної інформації, що задовольняє інформаційні потреби [1].

Головне завдання інформаційного пошуку – допомогти користувачеві задовольнити його інформаційну потребу.

Здавалося б, в епоху інформаційних технологій, Інтернету і пошукових систем стало набагато простіше знайти потрібну інформацію. Але чи дійсно це так?

Чим більший обсяг інформації, тим більша можливість використання корисної її частини для прийняття рішень [2].

Сучасні технічні засоби (комп'ютери, мережа Інтернет) значно спрощують доступ до величезної кількості матеріалів, що перебувають у вільному доступі. Причому ця величезна кількість постійно зростає, подвоюючись у середньому раз на 2 роки. Саме в такому зростанні й приховано "підводне каміння": пошук потрібної інформації часто перетворюється на досить непросту проблему [2].

У роботі з інформаційними потоками діє закон Парето. Згідно зі статистичними дослідженнями, якщо інформація збільшується вдвічі, її корисність становить не більше 20 %, а 80 %, які залишилися, не мають корисного характеру [2; 3].

Не зайво нагадати, що однією з ознак інформаційного суспільства є розвинута інфраструктура, що забезпечує створення достатньої кількості інформаційних ресурсів [4].

Інформація стає предметом масового використання. Інформаційне суспільство забезпечує індивіду доступ до будь-якого джерела інформації, що гарантується законом і технічними можливостями [4].

Закладені в працях К. Муерса і Дж. Солтона фундаментальні основи пошуку інформації актуальні й донині. Однак тут є невеликий нюанс у використанні термінології цих праць [5].

Слід підкреслити відмінність між пошуком як автоматизованою процедурою і виділенням потрібної інформації в знайдених документах [5].

Суть відмінностей полягає в такому [5]:

1) виділення інформації – це діяльність людини, яка використовує пошукову машину. Вона є інтерактивною, ітераційною і пов'язана з іншими видами інтелектуальної діяльності людини;

2) користувач шукає не документи як такі, а інформацію, що міститься в них для яких-небудь власних цілей (навчання, прийняття рішень тощо.);

3) користувач потребує доступу до різних джерел даних, щоб отримати всеосяжне уявлення про об'єкт пошуку;

4) якими б досконалими не були апаратне і програмне забезпечення, що використовуються людиною, вони залишаються інструментами, а інтелект – це атрибут користувача.

Однак інтернет-сайт являє собою не просто набір документів, а досить складну систему, вивчаючи яку доцільно аналізувати такі питання [5]:

а) інформаційне наповнення сайту;

б) методи зберігання й обробки даних (що розглядаються разом з програмними засобами);

в) значення сайту для інформаційного забезпечення відповідного виду діяльності.

Ці питання тісно взаємопов'язані.

Згадаємо, як проходить процес пошуку. Вводиться запит у пошуковий рядок і в результаті ми отримуємо занадто багато відповідей (інколи – тисячі або десятки тисяч, а інколи більше). Тут можна поставити такі досить актуальні питання: що зі знайденого було корисним? як швидко була знайдена відповідь на поставлене питання?

Формування результатів пошуку (наприклад, в Інтернеті) проходить у кілька етапів.

1. Спочатку потрібно визначити, які є сторінки. Оскільки їх офіційного реєстру не існує, доводиться постійно шукати нові сторінки й додавати їх до списку вже відомих. Цей процес називається скануванням.

2. Після виявлення сторінки потрібно визначити, які темі присвячено її зміст. Цей процес називається індексацією. Він полягає в тому, що відбувається аналіз контенту сторінки і проводиться систематизація знайдених на ній зображень і вбудованих відео. Отримана інформація зберігається у величезній базі даних, яка розміщена на багатьох комп'ютерах.

3. Коли користувач уводить запит, відбувається пошук найбільш відповідних результатів за низкою факторів. До таких факторів належать розташування, мова, тип пристрою користувача тощо.

Ніби то ідеальний механізм. Але тут є свої проблеми, що стосуються пошуку інформації.

1. Накопичення "порожньої" і застарілої інформації.

2. Ресурси та сервіси з невеликою кількістю інформації.

3. "Чорний" копірайтинг.

Мета статті – вдосконалення процесу фільтрації та пошуку інформації для користувачів. Тобто надання максимально корисної для користувача інформації.

Виклад основного матеріалу. Зазвичай на форумах, де обговорюється та чи інша проблема, доводиться читати всі повідомлення, щоб знайти хоча б невеличку частину потрібної інформації. А коли потрібне посилання знайдено, виявляється, що ресурс уже закритий або не працює. Тут потрібно було б ввести більш чітку модерацію або адміністраторами, або користувачами. Або зробити її автоматичною. Адміністратори відбиратимуть теми, які протягом тривалого часу перебувають без відповіді і можуть їх закривати. На великих порталах це буде неефективно і витратно, тому що за це треба платити, а ентузіазм зазвичай не оплачується. Користувачі за бажанням могли б відправити свою тему у розділ актуальних або видалити її, якщо на цьому порталі вже була дана відповідь на подібне питання, але тут можна зіштовхнутися із проблемою під назвою "війна за місце" [6].

До подібних сайтів можна зарахувати сайти для дизайнерів, ілюстраторів, фотографів або, наприклад, сервіси, що містять корисні функції, та не мають на своїх сторінках хороших текстів, щоб їх знайшли пошукові роботи. У більшості випадків, такі сайти знаходиш випадково й заносиш їх у закладки, щоб "потім, коли-небудь" ними скористатися. Із розв'язанням цієї проблеми нам має допомогти або пошукова система, або якийсь ресурс, який збиратиме такі сайти в один список. В обох випадках доведеться вводити теги для більш зручного пошуку. Найцікавіше починається з цього моменту: кількість і рівень SEO-оптимізаторів збільшується щороку, разом з ними зростає кількість сайтів для пошукових роботів з метою заробітку на рекламі.

Завдання полягає в тому, щоб звертаючись, скажімо, до теми з заголовком "Яка мінімальна версія підтримки N-го софту", користувач бачив напис "Версія 7 і вище" замість п'ятисторінкового чату, в самому кінці якого розміщена потрібна відповідь.

При цьому немає необхідності знищувати всю інформацію з коментарями. Серед усіх коментарів для кого-небудь іншого знайдеться і своя потрібна інформація.

Ідея полягає у так званому виділенні абсолютно або максимально корисної відповіді, щоб тисячам нових відвідувачів не треба було б перечитувати-перегортати всю стрічку обговорення, щоб дізнатися, що ж у підсумку є правильною відповіддю/правильним рішенням?.

Реалізація цього механізму така.

Кожному з коментарів в обговоренні присвоюється особливе число – рейтинг (рис. 1, табл. 1). Спочатку воно дорівнює нулю.

id	message	rating	owner
1.	Як цьому запобігти?	0	11
2.	В мене не виходить	−5	43
3.	Треба оновити ядро	7	76
4.	Мені це допомогло!	−2	54

Рис. 1. Фрагмент таблиці з бази коментарів

Таблиця 1

Властивості коментарів, які зберігаються в базі для можливості розподілу їх за рейтингом

Стовпець	Пояснення
id	Унікальний ключ ідентифікації коментаря
message	Текст коментаря
rating	За цим полем відбувається сортування
owner	Ключ власника коментаря: він необхідний для того, щоб коментарі могли видаляти ті, хто їх створив

Будь-який користувач має право один раз або підвищити рейтинг будь-якого з коментарів на 1 одиницю значення, або знизити (за принципом “лайків” у соціальних мережах). При цьому обов’язково проводиться перевірка коментаря на “порожність”.

$$message = \begin{cases} null, \textit{ то вивести помилку} \\ not\ null, \textit{ то додати коментар.} \end{cases}$$

Через деякий час у кожного коментаря обговорення сформується певний рейтинг. В одних коментарів він буде негативним, що свідчить про його непотрібність, оскільки максимальна кількість користувачів забажала відняти бал рейтингу, натиснувши кнопку “непотрібний коментар”. Процедура обробки зниження рейтингу аналогічна до процедури збільшення.

В інших записів, навпаки, рейтинг буде високим. На цьому етапі стає зрозуміло, що коментарі з найвищим рейтингом найбажаніші. Отже, необхідно якомога швидше показати цю інформацію всім наступним користувачам. Таким чином, згодом під час виведення діалогу обговорення повідомлення з найвищим рейтингом просто виводяться у верхню частину обговорення.

Тобто змінна сортування дорівнює SQL-запиту, в якому зазначено: “вибрати все з таблиці, відсортувати рейтинг за зменшенням”.

На рис. 2 наведено фрагмент програмного коду тестового модуля.

```
// insert a quote if submit button is clicked
if (isset($_POST['submit']))                                    // якщо натиснута кнопка submit
{
        if (empty($_POST['task']))                              // якщо поле порожнє
        {
                $errors = "Порожній коментар  .";               // якщо порожнє, вивести помилку
        }
        else                                                    // в іншому випадку
        {
                $task = $_POST['task'];
                $query = "INSERT INTO `data` (`message`) VALUES ('$task')";// змінна query = цьому SQL-запиту
                mysqli_query($db, $query);                      // звертаємося до бази db за допомогою змінної query
                header('location: index.php');                  // відкрити index.php
        }
}
```

Рис. 2. Фрагмент програмного коду тестового модуля

На рис. 3 зображено діаграму варіантів використання, яка відображає дії користувачів

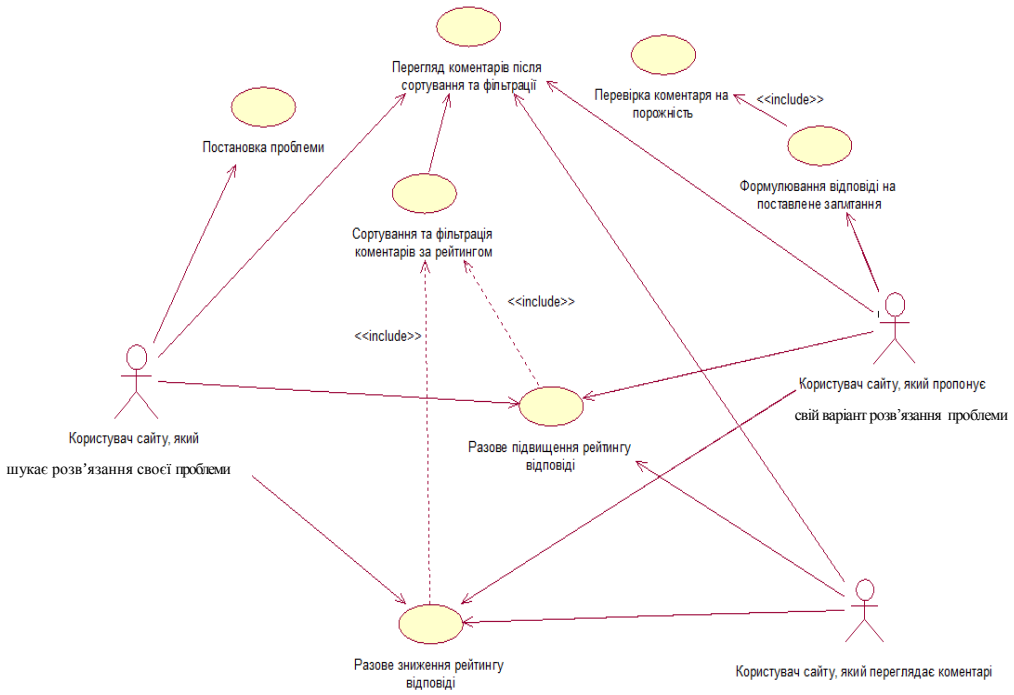


Рис. 3. Діаграма варіантів використання

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Інтернет – це “звалище даних”, у якому легко знайти розважальний матеріал, творчість різних людей тощо. Знайти це інколи легше, ніж потрібну робочу інформацію. Особливо, якщо вона вузькоспрямованого характеру. Ідеальним було б проводити повну модерацію у всесвітній мережі, але ресурсів зараз стільки, що таке завдання буде занадто проблематичним.

У статті досліджено важливу проблему пошуку інформації. Створено тестовий програмний модуль, який розв’язує проблему фільтрації й пошуку інформації для користувачів. Пропонується продовжити проект і вдосконалити цей модуль для простішого інтегрування в будь-які системи серверів.

Не зайве нагадати, що потрібно створювати більше спеціалізованих і тематичних ресурсів з якісним контентом. Чим більше таких порталів, тим швидше і якісніше триватиме пошук інформації.

Необхідно розвивати так звані сервіси порівняння. Це сервіси, що надають зведену таблицю за певною проблемою, ґрунтуючись на результатах, отриманих з багатьох сайтів і сервісів. Як наприклад, конкретні сервіси порівняння цін на товари. Користувач пише назву товару і такий сервіс видає порівняльну таблицю цін і відгуків з усіх можливих магазинів. ІТ-сфера значною мірою потребує подібного сервісу. Вводячи проблему, користувач отримував би звіт готових рішень за всіма ІТ-сайтами без необхідності заходити на кожен із сайтів і перечитувати масу інформації. Але тут з’являється ще одна необхідність: за можливості потрібно використовувати сервіси геолокації і засновувати пошукові видачі на основі місця розташування користувача. Це робиться, на жаль, рідко.

Зараз необхідно робити акцен на якості інформації і розподіляти її залежно від завдань. Якщо користувач налаштований на роботу і йому необхідно максимально швидко знайти потрібний контент, то слід прибирати з пошуку розважальні ресурси. А коли користувач хоче відпочити, то навпаки.

Список використаних джерел:

1. *Маннинг К. Д., Рагхаван П., Шютце Х.* Введение в информационный поиск / пер. с англ. Д. А. Клюшин. М.: Вильямс, 2011. 528 с.

2. *Поташова А. В.* Проблеми пошуку інформації в глобальній мережі Інтернет // Науковий огляд. № 5 (48). 2018. С. 130–139.

3. *Лук’янчикова Ю. В., Попова Ю. М.* Інформаційні потоки в системі управління організацією. URL: https://conferdsum.ucoz.ua/_fr/0/7120405.pdf

4. *Пожуєв В. І.* Глобальне інформаційне суспільство як новий соціальний та економічний феномен XXI століття // Гуманітарний вісник Запорізької державної інженерної академії. 2013. Вип. 52. С. 5–14.

5. *Шокин Ю. И., Федотов А. М., Барахнин В. Б.* Проблемы поиска информации. Новосибирск: Наука, 2010. – 220 с.

6. *Карпенко О.* Эпическая битва за пиксели: как участники Reddit воевали за место на графическом полотне. URL: https://ain.ua/2017/04/10/bitva-za-pikseli

References:

1. Manning C.D., Raghavan P., Schütze H. (2011), *Vvedenie v informazionnyi poisk* [Introduction to Information Retrieval], translated from english D.A.Klushin, Williams, Moscow, Russia, 528p. [Rus.]

2. Potashova A.V. (2018), *"Problemy poshuku informacii v globalniy merezhi Internet"* [Problems of searching information in the Internet], journal *Naukovyi Oglyad* [The Scientific Screening], vol. 5(48), pp. 130-139. [Ukr.]

3. Lukyanchikova Y.V., Popova Y.M., *Informaciyni potoki v sisteme upravlinnya organizaciey* [The information flows in the management system organization], available at: https://conferdsum.ucoz.ua/_fr/0/7120405.pdf. [Ukr.]

4. Poghuev V.I. (2013), *"Globalne informaciyne suspilstvo yak novyi socialnyi ta ekonomichnyi fenomen 21 stolittya"* [Global information society as new social and economic phenomenon of the 21st century], journal *Gumanitarnyi visnyk Zaporizhskoi derghavnoi ingenernoi akademii* [The Humanities Bulletin of Zaporizhzhe State Engineering Academy], vol. 52, pp. 5-14. [Ukr.]

5. Shokin Y.I., Fedotov A.M., Barahnin V.B. (2010), *Problemy poiska informacii* [The problems of information searching], Nauka, Novosibirsk, Russia, 220 p. [Rus.]

6. Karpenko O. (2017), *Epicheskaya bitva za pikseli: kak uchastniki Reddit voevali za mesto na graficheskom poligone* [Epic battle for Pixels: how Reddit participants fought for a place on a graphic canvas], available at: https://ain.ua/2017/04/10/bitva-za-pikseli/ [Rus.]