

ISSN 2521-6643

Системи та технології



№ 1 (56)

2018

Системи та технології

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

№ 1 (56)

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

Дніпро
Університет митної справи та фінансів
2018

УДК 62

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

Рекомендовано до друку та до поширення через мережу Інтернет вченою радою
Університету митної справи та фінансів (протокол № 11 від 25.03.2019 р.)

Редакційна колегія:

Кабак Л. В. – к.т.н., доц.
(*головний редактор*);
Іванченко О. В. – к.т.н., доц.
(*заступник головного редактора*);
Прокопович-Ткаченко Д. І. – к.т.н.
(*заступник головного редактора*);
Дерев’янка Т. П. (*відповідальний секретар*)
Акуловський В. Г. – к.т.н., доц.;
Бабенко В. Г. – к.т.н., доц.;
Богданов О. М. – д.т.н., проф.;
Гордєєв О. О. – к.т.н., доц.;
Доценко С. І. – д.т.н., доц.;
Дрозд О. В. – д.т.н., проф.;
Защолкін К. В. – к.т.н., доц.;

Зверєв В. П. – к.т.н., с.н.с.;
Змисний М. М. – к.т.н.;
Колісник М. О. – к.т.н., доц.;
Мартинюк О. М. – к.т.н., доц.;
Пасічник А. М. – д.ф.-м.н., проф.;
Поночовний Ю. Л. – к.т.н., с.н.с.;
Смірнов В. В. – к.т.н., доц.;
Смоктій К. В. – к.е.н., доц.;
Сохацький А. В. – д.т.н., проф.;
Стелюк Б. Б. – к.т.н., доц.;
Тарасенко Ю. С. – к.ф.-м.н., доц.;
Фесенко Г. В. – к.т.н., доц.;
Шапорін Р. О. – к.т.н., доц.;
Шкілюк О. П. – к.т.н.

DOI: <https://doi.org/10.32836/2521-6643-2018-1-56>
ISSN 2521-6643

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

Свідоцтво про державну реєстрацію: серія КВ № 21857-11757ПР від 21.12.2015 р.
Тираж 300 прим. Замовлення № 49.

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 27.12.2018. Формат 60×84/16. Папір офсетний.
Гарнітура Таймс. Ум. друк. арк. 15,00. Обл.-вид. арк. 13,33.

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

© Університет митної справи та фінансів, 2018

ЗМІСТ

Защелкин К. В., Дрозд А. В., Сулима Ю. Ю., Иванова Е. Н. Метод формирования стега-пути при решении задачи контроля целостности программного кода FPGA-базированных устройств	5
Шапорин В. О., Тишин П. М., Шапорина Е. Л. Онтология уязвимости в системах SCADA	18
Мартинюк О. М., Тамім Ахмеш, Дрозд О. В., Степова Г. С. Контролепридатність ієрархічних переходів у поведінковому контролі	30
Халіпова Н. В., Леснікова І. Ю., Шингур В. О. Розробка моделі управління якістю транспортно-логістичних процесів підприємств	41
Антонюк В. В., Дрозд М. О., Дрозд О. В., Кабак Л. В. Контролепридатність FPGA-проектів за розсіюваною потужністю	64
Yakovenko V. O., Ulianovska Yu. V., Kaliaka O. O. Software implementation of neural network technologies for automated textual information classification	75
Кузьменко А. І., Трофімов О. В. Удосконалення транспортно-логістичних процесів обслуговування вантажопотоків на території річкового порту	89

CONTENTS

Zashcholkin K. V., Drozd O. V., Sulima J. Y., Ivanova O. M. The method for stego-path formation in solving the problem of monitoring the integrity of the program code of FPGA-based devices	5
Shaporin V. O., Tishin P. M., Shaporina O. L. Vulnerability ontology in SCADA systems	18
Martynyuk O. N., Tamim Ahmesh, Drozd O. V., Stepova H. S. Checkability of hierarchical transmissions for behavioral check	30
Khalipova N. V., Lesnikova I. Y., Shingur V. A. Quality management model development for transport-logistic processes of enterprises	41
Antoniuk V. V., Drozd M. O., Drozd O. V., Kabak L. V. Checkability of FPGA projects by power-dissipation	64
Yakovenko V. O., Ulianovska Yu. V., Kaliaka O. O. Software implementation of neural network technologies for automated textual information classification	75
Kuzmenko A. I., Trofimov A. V. Transportation-logistic processes of cargo flow treatment improvement at the territory of the river port	89

DOI: <https://doi.org/10.32836/2521-6643-2018-1-56-1>

УДК 004.056.53

К. В. Защелкин, кандидат технических наук, доцент кафедры компьютерных интеллектуальных систем и сетей Одесского национального политехнического университета

А. В. Дрозд, доктор технических наук, профессор кафедры компьютерных интеллектуальных систем и сетей Одесского национального политехнического университета

Ю. Ю. Сулима, кандидат технических наук, заведующий электронно-холодильным отделением Одесского технического колледжа Одесской национальной академии пищевых технологий

Е. Н. Иванова, старший преподаватель кафедры компьютерных систем Одесского национального политехнического университета

МЕТОД ФОРМИРОВАНИЯ СТЕГО-ПУТИ ПРИ РЕШЕНИИ ЗАДАЧИ КОНТРОЛЯ ЦЕЛОСТНОСТИ ПРОГРАММНОГО КОДА FPGA-БАЗИРОВАННЫХ УСТРОЙСТВ

Рассмотрены вопросы контроля целостности программного кода FPGA-базированных компонентов компьютерных систем. В качестве эффективного отмечен подход к контролю целостности, в рамках которого контрольная хэши-сумма внедряется в контролируемый информационный объект в виде цифрового водяного знака. Предлагается метод формирования в пространстве LUT-контейнера микросхемы FPGA стеганографического пути (стего-пути) внедрения цифрового водяного знака. Стего-путь представляет собой упорядоченное множество элементарных вычислительных блоков LUT, в программные коды которых выполняется непосредственное внедрение разрядов контрольного цифрового водяного знака. В статье обосновываются основные теоретические положения предлагаемого метода и формулируется последовательность этапов его выполнения.

Ключевые слова: контроль целостности; FPGA; LUT; цифровой водяной знак; стеганографический путь; программируемые вычислительные блоки.

© К. В. Защелкин, А. В. Дрозд, Ю. Ю. Сулима, Е. Н. Иванова, 2018

Розглянуто питання контролю цілісності програмного коду FPGA-базованих компонентів комп'ютерних систем. В якості ефективного відзначено підхід до контролю цілісності, в рамках якого контрольна хеш-сума вбудовується в контрольований інформаційний об'єкт у вигляді цифрового водяного знака. Пропонується метод формування в просторі LUT-контейнера мікросхеми FPGA стеганографічного шляху (стего-шляху) вбудовування цифрового водяного знака. Стего-шлях являє собою впорядковану множину елементарних обчислювальних блоків LUT, у програмні коди яких виконується безпосереднє вбудовування розрядів контрольного цифрового водяного знака. В дослідженні обґрунтовуються основні теоретичні положення запропонованого методу, формулюється послідовність етапів його виконання.

Ключові слова: контроль цілісності; FPGA; LUT; цифровий водяний знак; стеганографічний шлях; програмовані обчислювальні блоки.

Issues of program code integrity monitoring of the FPGA-based components of computer systems is considered. As the most effective, the approach is chosen in which the control hash sum is embedded in the monitored information object as a digital watermark. This makes it possible to hide the fact that integrity monitoring is performed, as well as to hide the hash sum by which integrity is monitored. The disadvantage of the existing methods is that they do not specify the way of forming in the informational object a sequence of elementary units into which the digits of the digital watermark are embedded.

A method for forming in the space of a LUT-container (LUT – Look Up Table) the FPGA chip of a steganographic path (stego-path) of embedding the digital watermark is proposed. Stego-path is an ordered set of elementary computational LUT units, into the program codes of which the direct embedding of the digits of the digital watermark is performed. The paper substantiates the basic theoretical propositions of the proposed method, and formulates a sequence of stages for its implementation. The method determines the way and source of the ordering of the set of LUT units. The method also formalizes the natural constraints on the choice of LUT units for the stego-path. These natural constraints are due to the structure of the LUT-container. The method also defines artificial constraints on the choice of LUT units, which are caused by the bounding components of the stego-key. A rule is established that makes it possible to decide on the inclusion of a LUT unit in the stego path, depending on the connections with the blocks already included in the stego path. The theoretical positions of the method form a cyclic sequence of actions for choosing LUT units from the available set of LUT-container units.

A software implementation of the method is proposed, based on the analysis of the information model of the LUT-container obtained using the CAD system Intel

Quartus Prime. The implementation of the proposed method can be used as part of software systems that perform automated monitoring of the integrity of the program code of FPGA-based components.

Key words: *integrity monitoring; FPGA; LUT; digital watermark; steganographic path; programmable computing units.*

Постановка проблемы. Важной составляющей безопасности компьютерных систем является обеспечение их целостности, которое состоит в исключении непредусмотренных изменений системы или предоставляемых ею сервисов [1]. Большинство современных компьютерных систем содержат в своем составе программируемые компоненты: микропроцессоры, микроконтроллеры, программируемые логические интегральные схемы (далее – ПЛИС) [2]. Функционирование систем такого рода обеспечивается как физическими связями компонентов, так и совокупностью программных кодов, настраивающих компоненты на решение требуемых задач. В отличие от компонентов с жесткой логикой функционирования обеспечение целостности программируемых компонентов усложняется в силу двух факторов:

- 1) относительной простоты процесса внесения изменений в программный код компонентов;
- 2) необходимости внесения легитимных (разрешенных) изменений программного кода, которые выполняются на всех этапах жизненного цикла системы.

В этих условиях нарушение целостности программного кода компонентов может быть замаскировано под его легитимное изменение или входить в состав легитимного изменения как закамouflированная часть [3].

В работе [4] рассматривается проблема обеспечения целостности программного кода микросхем типа FPGA (Field Programmable Gate Array), которые являются наиболее современной и часто используемой разновидностью ПЛИС. Структура таких микросхем представляет собой двухмерную матрицу элементарных программируемых блоков нескольких видов: настраиваемых и специализированных вычислителей, блоков распределенной и сосредоточенной памяти, блоков ввода-вывода. Программный код микросхем FPGA задает настройку каждого из блоков матрицы на выполнение конкретной функции, а также формирует систему связей между блоками.

Несмотря на наличие во многих микросхемах FPGA встроенных механизмов защиты программного кода от перезаписи [5], существуют способы обхода такой защиты [6], позволяющие вносить в программный код нелегитимные изменения. В силу этого наиболее распространенным подходом к обеспечению целостности программного кода FPGA-базированных компонентов вы-

ступают приемы, основанные на использовании блоков дополнительной контрольной информации, которые позволяют сделать выводы о целостности кода.

Анализ последних исследований и публикаций. Наиболее часто применяемые подходы к контролю целостности программного кода основаны на применении контрольных хэш-сумм [7]. Хэш-суммы для этих целей вычисляются при помощи криптографических хэш-функций [8], основная особенность которых состоит в необратимости, то есть относительной простоте получения значения функции по ее аргументу, но крайней вычислительной сложности получения аргумента по значению функции. Все практически используемые подходы к контролю целостности базируются на двукратном вычислении хэш-суммы с последующим сравнением результатов этих вычислений [9]. Последовательность действий относительно контроля целостности при этом образует две стадии: стадию подготовки программного кода к контролю и непосредственно стадию контроля.

Стадия подготовки программного кода P к контролю:

1) для информационного объекта программного кода P при помощи заданной хэш-функции вычисляется хэш-сумма SP ;

2) полученная хэш-сумма некоторым оговоренным образом присоединяется к информационному объекту P или сопоставляется с ним. В результате формируется информационный объект $CP = (P, SP)$, включающий в себя программный код и его хэш-сумму.

Стадия контроля целостности информационного объекта CP^* :

1) информационный объект $CP^* = (P^*, SP_1^*)$ разделяется на составляющие его программный код P^* и хэш-сумму SP_1^* .

2) для информационного объекта программного кода P^* при помощи заданной хэш-функции вычисляется хэш-сумма SP_2 ;

3) вновь вычисленная хэш-сумма SP_2 сравнивается с хэш-суммой SP_1^* , извлеченной из проверяемого объекта. В случае несовпадения этих хэш-сумм целостность считается нарушенной.

Недостаток традиционных методов контроля целостности программных кодов заключается в том, что контрольная хэш-сумма SP , сформированная на стадии подготовки информационного объекта к контролю, хранится либо полностью открыто, либо может быть найдена в структуре информационного объекта в результате его анализа. Так, известен подход [10], в рамках которого контрольная хэш-сумма размещается в памяти рядом с контролируемым программным кодом. Другой часто используемый подход [11] предполагает включение хэш-суммы в информационный объект программного кода в качестве одного из его полей. Указанные подходы не позволяют скрыть факт того, что контроль целостности выполняется и не дают возможности скрыть контрольную информацию, на основании которой этот

контроль проводится. Существует также подход [12], в рамках которого контрольная хэш-сумма присоединяется к информационному объекту программного кода не в открытом, а в зашифрованном виде при помощи оговоренного криптографического алгоритма. Такой подход скрывает контрольную информацию, но оставляет открытым для внешнего наблюдателя сам факт того, что контроль целостности производится. Это приводит к возможности применения достаточно большого спектра приемов (от полного перебора до методов социальной инженерии) для открытия и фальсификации хэш-суммы.

Перспективный подход к хранению контрольной хэш-суммы, устраняющий приведенные выше недостатки, заключается в том, что хэш-сумма не присоединяется к информационному объекту P программного кода, а погружается в него в виде цифрового водяного знака (далее – ЦВЗ) [13–15]. Достоинства такого подхода состоят в том, что:

- 1) ЦВЗ не увеличивает объем информационного объекта на размер хэш-суммы;
- 2) отсутствует возможность для внешнего наблюдателя выявить факт того, что программный код контролируется, а также выделить часть информационного объекта, которая содержит полезный программный код и часть, которая содержит хэш-сумму;
- 3) внедрение ЦВЗ в программный код выполняется таким образом, что функционирование микросхемы FPGA не претерпевает изменений.

Методы [13–15], реализующие концепцию применения ЦВЗ для контроля программного кода FPGA-базированных компонентов, предполагают использование программных кодов блоков LUT (Look Up Table) в качестве среды, в которую погружается ЦВЗ. Блоки LUT являются наиболее массовыми элементарными вычислительными единицами FPGA. Их количество в современных микросхемах FPGA может варьироваться от десятков тысяч до нескольких миллионов. Блок LUT представляет собой программируемый вычислитель логической функции от n -аргументов (обычно от 4 до 8). Настройка блока LUT на реализацию конкретной логической функции производится при помощи 2^n -разрядного программного кода. В соответствии с положениями методов [13–15] совокупность программных кодов блоков LUT используется в качестве среды внедрения контрольного ЦВЗ. Внедрение в рамках указанных методов выполняется с использованием эквивалентных преобразований [16; 17], которые не изменяют реализуемые блоками LUT логические функции и не влияют на функционирование микросхемы FPGA. Методы [13–15] определяют, что для внедрения ЦВЗ из множества блоков LUT формируется упорядоченное множество блоков,

каждый элемент которых однозначно соответствует разряду ЦВЗ и используется для внедрения этого разряда. Указанное упорядоченное множество называется стеганографическим путем (стего-путем) в среде LUT-ориентированного информационного объекта. При этом правило формирования стего-пути выступает частью стего-ключа – совокупности секретной информации, определяющей формальные правила извлечения ЦВЗ из программных кодов блоков LUT. Методы [13–15] не конкретизируют способ формирования стего-пути и не определяют возможные ограничения, накладываемые на его элементы.

Целью статьи является формализация метода формирования стего-пути как части задачи внедрения ЦВЗ в программный код FPGA-базированных компонентов в процессе контроля целостности.

Изложение основного материала. Предлагаемый метод выполняет формирование стего-пути в LUT-контейнере. Под LUT-контейнером микросхемы FPGA понимается совокупность: а) блоков LUT этой микросхемы; б) связей между этими блоками; в) связей между блоками LUT и выводами микросхемы FPGA; г) программных кодов, поставленных в соответствие каждому из блоков LUT. LUT-контейнер является частью структуры микросхемы FPGA, непосредственно задействованной в процессе внедрения ЦВЗ.

Входные данные метода:

а) информационная модель LUT-контейнера [18], содержащая структурированную информацию о его компонентах;

б) контрольный ЦВЗ, предназначенный для внедрения в LUT-контейнер – двоичная последовательность $W = \langle w_1, \dots, w_n \rangle$, содержащая хэш контролируемого программного кода;

в) стего-ключ – секретный набор формально заданных правил внедрения ЦВЗ в LUT-контейнер.

Задача метода: получить упорядоченное множество (последовательность) блоков LUT, предназначенных для непосредственного внедрения разрядов ЦВЗ.

Выходные данные метода (результаты): стего-путь в LUT-контейнере, представляющий собой упорядоченное множество элементов:

$$P = \langle p_1, \dots, p_n \rangle, \quad (1)$$

в котором каждый элемент p_i описывает отдельный блок LUT микросхемы FPGA, а также содержит информацию, необходимую для внедрения одного разряда ЦВЗ в программный код этого блока; каждый элемент p_i однозначно соответствует разряду ЦВЗ w_i при $i = 1 \dots n$; p_i представляет собой тройку элементов:

$$p_i = \langle id_{LUT_i}, code_{LUT_i}, DList_{LUT_i} \rangle, \quad (2)$$

где id_{LUT_i} – идентификатор блока LUT;

$code_{LUT_i}$ – программный код блока LUT id_{LUT_i} ;

$DList_{LUT_i}$ – список блоков LUT, источником входных данных для которых является блок с идентификатором id_{LUT_i} .

Первое положение метода заключается во введении отношения порядка на множестве элементов стега-пути за счет использования: а) уникальных идентификаторов блоков LUT, заданных информационной моделью LUT-контейнера; б) правила упорядочивания элементов, заданных стега-ключом.

Информационная модель [18] LUT-контейнера формируется как результат получения данных о FPGA-проекте при помощи соответствующей системы автоматизированного проектирования (далее – САПР) и программного обеспечения, выполняющего построение информационной модели. САПР-производители микросхем FPGA идентифицируют блоки LUT в матрице микросхемы при помощи числового идентификатора. Этот идентификатор представляет собой натуральное число, сопоставленное блоку LUT и являющееся уникальным в пределах матрицы FPGA. Наличие такого идентификатора дает возможность ввести отношение порядка на множестве блоков LUT-контейнера.

Правило упорядочивания блоков LUT-контейнера задается одним из компонентов стега-ключа. Этот компонент формально описывает порядок обхода блоков LUT-контейнера в процессе внедрения ЦВЗ.

Второе положение метода заключается в том, что при формировании стега-пути учитываются *естественные* ограничения, накладываемые структурой LUT-контейнера на выбор блоков, включаемых в стега-путь.

Указанные ограничения обусловлены спецификой эквивалентных преобразований [16; 17] программных кодов блоков LUT, в результате выполнения которых осуществляется внедрение разрядов ЦВЗ в эти программные коды. При внедрении разряда ЦВЗ в программный код некоторого блока LUT_k производится условное инвертирование разрядов программного кода для достижения требуемого значения в заданном его разряде. Для компенсации этого инвертирования выполняется модификация программных кодов всех блоков LUT, входы которых подключены к выходу блока LUT_k (далее – блок LUT_k), в который выполняется внедрение разряда ЦВЗ, будет называться *целевым блоком*, а множество блоков LUT, получающих входные данные с выхода целевого блока LUT_k , *компенсирующим множеством блоков для блока LUT_k* . Если же блок LUT_k подключен к выходу микросхемы FPGA, то компенсирующая модификация программных кодов становится невозможной из-за отсутствия блоков LUT, находящихся между выходом блока LUT_k и выходом микросхемы FPGA. В силу этого данное

положение метода определяет ограничение, заключающееся в невозможности использования в качестве элементов стега-ключа блоков LUT, выходы которых непосредственно подключены к выходам микросхемы FPGA.

Третье положение метода заключается в том, что при формировании стега-пути учитываются *искусственные* ограничения, накладываемые стега-ключом на выбор блоков, включаемых в стега-путь.

Эквивалентные преобразования [16; 17], реализующие непосредственное внедрение разрядов ЦВЗ, требуют модификации программного кода как целевого блока, так и программных кодов всех компенсирующих блоков, относящихся к данному целевому блоку. В этих условиях может быть нецелесообразным внедрение разряда ЦВЗ в целевой блок, выход которого подключен к большому количеству компенсирующих блоков. Для управления возможностью внедрения разряда ЦВЗ в подобные целевые блоки стега-ключ может содержать компонент, задающий ограничивающий порог количества элементов компенсирующего множества блоков. Все целевые блоки LUT, у которых количество подключенных к их выходу компенсирующих блоков превышает ограничивающее значение, не включаются в состав стега-пути. Указанное искусственное ограничение, задаваемое компонентом стега-ключа, не является единственно возможным. Метод допускает наличие иных подобных ограничений, применяемых в соответствии с данным положением метода.

Четвертое положение метода заключается в том, что в процессе формирования стега-пути в его состав не может быть включен блок LUT, выход которого подключен к входу хотя бы одного блока LUT, ранее включенного в стега-путь.

Обоснование данного положения состоит в следующем. Пусть некоторый блок LUT_a включен в состав стега-пути. Пусть также выход другого блока LUT_b подключен к одному из входов блока LUT_a . Необходимо принять решение о возможности включения блока LUT_b в состав стега-пути. На этапе внедрения ЦВЗ в программный код блока LUT_a будет встроен один из разрядов ЦВЗ. В этом случае при внедрении разряда ЦВЗ в блок LUT_b потребуется выполнить модификацию программного кода, как самого блока LUT_b , так и всех его компенсирующих блоков, принимающих данные с выхода блока LUT_b . В число таких блоков, по условию описываемой ситуации, входит и блок LUT_a , в программный код которого уже внедрен разряд ЦВЗ. Модификация программного кода блока LUT_a приведет к искажению ранее внедренного в него разряда ЦВЗ. Для предотвращения такого искажения блок LUT_b не должен входить в состав блоков, в которые внедряются разряды ЦВЗ. Следовательно, в заданной ситуации блок LUT_b не может входить в состав стега-пути.

Предлагаемый метод включает следующую последовательность действий.

Этап 1. Из множества L идентификаторов блоков LUT-контейнера формируется упорядоченное множество идентификаторов:

$$L_{order} = \langle id_1, id_2, \dots, id_m \rangle.$$

Правило упорядочивания задается компонентом стега-ключа, определяющего порядок обхода блоков LUT-контейнера в процессе внедрения ЦВЗ (первое положение метода).

Далее этапы 2–5 выполняются последовательно для каждого из элементов множества L_{order} .

Этап 2. Для текущего блока LUT с идентификатором id_j , где $j = 1 \dots m$, выполняется проверка естественных ограничений, накладываемых структурой LUT-контейнера на возможность использования этого блока в составе стега-пути (второе положение метода). Для этого производится проверка того, не имеет ли выход блока LUT с идентификатором id_j непосредственных подключений к выводам микросхемы FPGA? Если такие подключения имеются, то блок id_j в состав стега-пути не включается, и выполняется переход к анализу следующего блока из множества L_{order} (возвращение на этап 2). Иначе, осуществляется переход к этапу 3.

Этап 3. Для текущего блока LUT с идентификатором id_j , где $j = 1 \dots m$, выполняется проверка искусственных ограничений, накладываемых стега-ключом на возможность использования этого блока в составе стега-пути (третье положение метода). Если блок id_j не удовлетворяет ограничивающее условие стега-ключа, то этот блок в состав стега-пути не включается, а выполняется переход к анализу следующего блока из множества L_{order} (возвращение на этап 2). Иначе, осуществляется переход к этапу 4.

Этап 4. Для текущего блока LUT с идентификатором id_j , где $j = 1 \dots m$, выполняется проверка того, имеются ли в LUT-контейнере блоки, подключенные к выходу блока id_j и при этом уже включенные в состав стега-пути (четвертое положение метода)? Если такие блоки имеются, то блок id_j в состав стега-пути не включается, а выполняется переход к анализу следующего блока из множества L_{order} (возвращение на этап 2). Иначе, осуществляется переход к этапу 5.

Этап 5. Идентификатор блока id_j включается в состав стега-пути (включается в упорядоченное множество $P(1)$, описывающее стега-путь). Если id_j – последний обработанный элемент множества L_{order} , то стега-путь сформирован и полное его описание содержится во множестве $P(1)$. Иначе, выполняется переход к обработке следующего элемента множества L_{order} (переход на этап 2).

Предлагаемый в данной статье метод формирования стега-пути в пространстве LUT-контейнера был реализован программно. Реализация выполнялась на языке C# в рамках программной платформы Net. В среде разработанного программного обеспечения выполнено тестирование предлагаемого метода. В качестве целевых микросхем использовались микросхемы FPGA Intel (Altera) Cyclone II–IV [19]. Для получения информационной модели LUT-контейнера была применена САПР Intel Quartus Prime [20] совместно с разработанными собственными программными модулями. Результаты тестирования свидетельствуют о целесообразности использования реализации предлагаемого метода в составе системы контроля целостности программного кода FPGA-базированных компонентов.

Выводы по данному исследованию и перспективы дальнейших исследований в данном направлении. Предложенный в статье метод позволяет выполнить построение стега-пути в пространстве LUT-контейнера. Метод позиционируется как составная часть решения задачи контроля целостности программных кодов FPGA-базированных компонентов путем использования ЦВЗ. В исследовании обоснованы основные положения метода и сформулированы этапы его выполнения. Предложена программная реализация метода, основанная на анализе информационной модели LUT-контейнера, получаемой при помощи САПР Intel Quartus Prime. Реализация метода может найти применение в составе программных систем, выполняющих автоматизированный контроль целостности программного кода FPGA-базированных компонентов.

Дальнейших исследований требует вопрос построения в пространстве LUT-контейнера оптимального в соответствии с заданными параметрами стега-пути. Например, построения стега-пути, обеспечивающего для заданного LUT-контейнера внедрение ЦВЗ максимального объема, или стега-пути, использующего минимальное количество блоков LUT (целевых и компенсирующих) для внедрения ЦВЗ фиксированного объема.

Список использованных источников:

1. Бохмач Е. С., Герасименко А. Д., Головир В. А. Отказобезопасные информационно-управляющие системы на программируемой логике / под ред. В. С. Харченко, В. В. Склера. Харьков : НАУ “ХАИ”, НПП “Радий”, 2008. 380 с.
2. Vanderbauwhede W., Benkrid K. High-performance computing using FPGAs. New-York: Springer, 2016. 525 p.
3. Mishra P., Bhunia S., Tehranipoor M. Hardware IP Security and Trust. New-York: Springer, 2017. 353 p.

4. *Rodriguez Andina Juan Jose, Torre Arnanz Eduardo de la, Dolores Valdes Maria* FPGAs: Fundamentals, Advanced Features, and Applications in Industrial Electronics. CRC Press, 2017. 450 p.

5. Using the Design Security Features in Intel FPGAs. URL: <https://www.intel.com/content/dam/www/programmable/us/en/pdfs/literature/an/an556.pdf>

6. Handbook of FPGA design security / T. Huffmire, C. Irvine, T. D. Nguyen, T. Levin, R. Kastner, T. Sherwood. Dordrecht: Springer, 2013. 178 p.

7. *Vacca J.* Computer and information security, 2nd edition. USA, Waltham: Morgan Kaufmann Publishers, 2013. 1280 p.

8. *Stallings W.* Cryptography and Network Security: Principles and Practice, 7th Edition. United Kingdom, Harlow: Pearson Education Limited, 2017. 768 p.

9. *Kleidermacher D., Kleidermacher M.* Embedded Systems Security: Practical Methods for Safe and Secure Software and Systems Development. Boston: Newnes, 2012. 416 p.

10. *Katz J., Lindell Y.* Introduction to Modern Cryptography, Second Edition Hall/CRC, 2014. 554 p.

11. *Ferguson N., Schneier B., Kohno T.* Cryptography engineering. Hoboken: Wiley, 2013. 354 p.

12. *Katz J.* Digital signatures. New York: Springer, 2010. 192 p.

13. *Zashcholkin K., Ivanova O.* The Control Technology of Integrity and Legitimacy of LUT-Oriented Information Object Usage by Self-Recovering Digital Watermark // CEUR Workshop Proceedings. 2015. Vol. 1356. P. 486–497.

14. *Zashcholkin K., Ivanova O.* LUT-object integrity monitoring methods based on low impact embedding of digital watermark // Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET-2018): Proceedings of the 14th International Conference. Lviv-Slavske, 2018. P. 519–523.

15. Checkable FPGA Design: Energy Consumption, Throughput and Trustworthiness / A. Drozd, S. Antoshchuk, J. Drozd, K. Zashcholkin, M. Drozd, N. Kuznietsov, M. Al-Dhabi, V. Nikul // In book: Green IT Engineering: Social, Business and Industrial Applications, Studies in Systems, Decision and Control / V. Kharchenko, Y. Kondratenko, J. Kacprzyk (Edits). Berlin, Heidelberg: Springer International Publishing, 2018. P. 73–94, DOI: 10.1007/978-3-030-00253-4_4.

16. *Drozd A., Drozd M., Kuznietsov M.* Use of natural LUT redundancy to improve trustworthiness of FPGA design // CEUR Workshop Proceedings. 2016. Vol. 1614. P. 322–331.

17. *Drozd O., Drozd M., Martynyuk O., Kuznietsov M.* Improving of a circuit checkability and trustworthiness of data processing results in LUT-based FPGA components of safety-related systems // CEUR Workshop Proceedings. 2017. Vol. 1844. P. 654–661.

18. Защелкин К. В., Иванова Е. Н. Поиск целевых блоков LUT в информационной модели FPGA-устройства в рамках задачи контроля целостности программного кода // *Електротехнічні та комп'ютерні системи*. 2018. № 28 (104). С. 215–222.

19. Intel Cyclone IV Device Handbook. URL: <https://www.intel.com/content/dam/www/programmable/us/en/pdfs/literature/hb/cyclone-iv/cyclone4-handbook.pdf>

20. Intel Quartus Prime Standard Edition Handbook. URL: <https://www.intel.com/content/dam/www/programmable/us/en/pdfs/literature/hb/qts/archives/qts-qps-handbook-16.0.pdf>

References:

1. Bokhmach E.S., Gerasimenko A.D. and Golovir V.A. (2008), *Otkazobezopasnyye informatsionno-upravlyayushchiye sistemy na programmiruyemoy logike* [Fail-safe information control systems on programmable logic] / ed. by V. S. Kharchenko, V. V. Sklyar. Press NAU “KhAI”, NPP “Radiy”, Kharkov. 380 p. [Ukraine].

2. Vanderbauwhede W. and Benkrid K. (2016), *High-performance computing using FPGAs*. New-York: Springer, 525 p. [USA].

3. Mishra P., Bhunia S. and Tehranipoor M. (2017), *Hardware IP Security and Trust*. New-York: Springer, 353 p. [USA].

4. Rodriguez Andina Juan Jose, Eduardo de la Torre Arnanz and Dolores Valdes Maria (2017), *FPGAs: Fundamentals, Advanced Features, and Applications in Industrial Electronics*. CRC Press, 450 p.

5. *Using the Design Security Features in Intel FPGAs* (2019), available at: <https://www.intel.com/content/dam/www/programmable/us/en/pdfs/literature/an/an556.pdf>

6. Huffmire T., Irvine C., Nguyen T. D. and Levin T. et al (2013), *Handbook of FPGA design security*, Sherwood, Dordrecht: Springer, 178 p.

7. Vacca J. (2013), *Computer and information security*, 2nd edition. USA, Waltham: Morgan Kaufmann Publishers, 1280 p.

8. Stallings W. (2017), *Cryptography and Network Security: Principles and Practice*, 7th Edition. United Kingdom, Harlow: Pearson Education Limited, 768 p.

9. Kleidermacher D. and Kleidermacher M. (2012), *Embedded Systems Security: Practical Methods for Safe and Secure Software and Systems Development*. Boston: Newnes, 416 p.

10. Katz J. and Lindell Y. (2014), *Introduction to Modern Cryptography*, Second Edition Hall/CRC, 554 p.

11. Ferguson N., Schneier B. and Kohno T. (2013), *Cryptography engineering*. Hoboken: Wiley, 354 p.

-
12. Katz J. (2010), Digital signatures. New York: Springer, 192 p.
 13. Zashcholkin K. and Ivanova O. (2015), “The Control Technology of Integrity and Legitimacy of LUT-Oriented Information Object Usage by Self-Recovering Digital Watermark” // CEUR Workshop Proceedings, vol. 1356, pp. 486–497.
 14. Zashcholkin K. and Ivanova O. (2018), “LUT-object integrity monitoring methods based on low impact embedding of digital watermark” // Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET-2018), Proceedings of the 14th International Conference. Lviv-Slavske, pp. 519–523.
 15. Drozd A., Antoshchuk S., Drozd J. and Zashcholkin K. et al (2018), Checkable FPGA Design: Energy Consumption, Throughput and Trustworthiness // In book: Green IT Engineering: Social, Business and Industrial Applications, Studies in Systems, Decision and Control / V. Kharchenko, Y. Kondratenko, J. Kacprzyk (Edits). Berlin, Heidelberg: Springer International Publishing, pp. 73–94, DOI: 10.1007/978-3-030-00253-4_4.
 16. Drozd A., Drozd M. and Kuznietsov M. (2016), “Use of natural LUT redundancy to improve trustworthiness of FPGA design” // CEUR Workshop Proceedings, vol. 1614, pp. 322–331.
 17. Drozd O., Drozd M., Martynyuk O. and Kuznietsov M. (2017), “Improving of a circuit checkability and trustworthiness of data processing results in LUT-based FPGA components of safety-related systems” // CEUR Workshop Proceedings, vol. 1844, pp. 654–661.
 18. Zashcholkin K. V. and Ivanova E. N. (2018), “*Poisk tselevykh blokov LUT v informatsionnoy modeli FPGA-ustroystva v ramkakh zadachi kontrolya tselostnosti programmogo koda*” [“Search for target LUT blocks in the information model of an FPGA device as part of the task of monitoring the integrity of a program code”] // Journal *Elektrotekhnichni ta komp'yuterni systemy* [Electronic Systems and Computer Systems], vol. 28(104), pp. 215–222 [Ukraine].
 19. Intel Cyclone IV Device Handbook (2019), available at: <https://www.intel.com/content/dam/www/programmable/us/en/pdfs/literature/hb/cyclone-iv/cyclone4-handbook.pdf>
 20. Intel Quartus Prime Standard Edition Handbook (2019), available at: <https://www.intel.com/content/dam/www/programmable/us/en/pdfs/literature/hb/qts/archives/qts-qps-handbook-16.0.pdf>

DOI: <https://doi.org/10.32836/2521-6643-2018-1-56-2>

УДК 004.056.5

В. О. Шапорин, кандидат технических наук, доцент кафедры компьютерных интеллектуальных систем и сетей Одесского национального политехнического университета

П. М. Тишин, кандидат физико-математических наук, доцент кафедры компьютерных интеллектуальных систем и сетей Одесского национального политехнического университета

Е. Л. Шапорина, старший преподаватель кафедры компьютерных интеллектуальных систем и сетей Одесского национального политехнического университета

ОНТОЛОГИЯ УЯЗВИМОСТИ В СИСТЕМАХ SCADA

Статья представляет исследование в области построения онтологических моделей уязвимости систем SCADA. Метод проектирования онтологии базируется на языке описания онтологии OWL и на использовании базы данных известных типов уязвимостей. При построении онтологии уязвимости учитывается иерархичность влияния параметров модели, что позволяет описывать унифицированные модели уязвимости с повышением детализации общего описания уязвимости. Предложенная онтологическая модель реализована в системе моделирования Protégé.

Ключевые слова: управление уязвимостями; SCADA системы; Common Weakness Enumeration; дескриптивная логика; Web Ontology Language.

Стаття подає дослідження у сфері побудови онтологічних моделей вразливості систем SCADA. Метод проектування онтології базується на мові опису онтології OWL і на використанні бази даних відомих типів вразливостей. У побудові онтології вразливості враховується ієрархічність впливу параметрів моделі, що дає можливість описувати уніфіковані моделі вразливості з підвищенням деталізації загального опису вразливості. Запропонована онтологічна модель реалізована в системі моделювання Protégé.

Ключові слова: управління вразливостями; SCADA системи; Common Weakness Enumeration; дескриптивна логіка; Web Ontology Language.

© В. О. Шапорин, П. М. Тишин, Е. Л. Шапорина, 2018

The main feature of information security is that it is not a state, but a continuous process of analyzing the security of computer systems and networks and their components. Modern information systems are often the part of public services, what make a large number of challenges for system and security administrators. The main problem is that the all hardware and software of this systems has a many vulnerabilities, because it's a complex, modular and multi-vendor tools and devices. So it's important to have an opportunity to manage the weakness of this tools and decrease the probability of network attack, using this vulnerabilities. This article presents a study in the field of building ontological models of vulnerability of SCADA systems. The ontology design method is based on the OWL ontology description language and on the use of a database of known types of vulnerabilities. The paper proposes a system of axioms and related classes describing the vulnerability of hardware and software. This system is allowed security engineers to have a tool for flexible and effective representation of systems weakness and vulnerabilities. When constructing an ontology of vulnerability, the hierarchy of the influence of model parameters is taken into account, which makes it possible to describe unified vulnerability models with increased detail in the general description of vulnerability. The proposed ontological model is implemented in the Protégé modeling system.

Testing of this method was carried out in the university laboratory. Testing was perform during regular inventory of the classroom and troubleshooting current network infrastructure. The implementing of this method is make possible to decrease a time of analyzing the state of the target system. Also this method provide a decreasing of the risk of injection types of attacks in networks. The proposed method allows the use of not only external sources of information about vulnerabilities, but also the knowledge and experience gained during the operation of the target system by administrators and analysts in the processes of analyzing systems and networks.

Key words: vulnerability management; SCADA systems; Common Weakness Enumeration; descriptive logic; Web Ontology Language.

Постановка проблемы. В условиях интеграции автоматизированных систем управления технологическим процессом с корпоративными сетями и Internet все чаще возникают вопросы обеспечения сетевой безопасности, устойчивости сети предприятия к внутренним и внешним угрозам, а также к обеспечению антивирусной защиты.

Независимо от направления деятельности организации, от простой автоматизации рутинных механизмов к системам критического применения (энергетика, транспорт, медицина), большинство процессов управления свя-

заны с системами SCADA, которые реализуют диспетчеризацию, сбор и обработку данных.

С ростом популярности технологий Интернета вещей такие системы все чаще подвергаются вирусным и целенаправленным атакам, целью которых является как замедление или остановка производственных процессов, так и разрушение систем или же нанесение вреда людям и окружающей среде. Вместе с этим до сих пор такие атаки редко диагностируются в связи с отсутствием или ограниченностью механизмов определения уязвимости и вредоносных процессов в системах. Поэтому сбои, вызванные вирусами и злоумышленниками, расцениваются как ошибки оборудования или программного обеспечения.

Цели атак на промышленные информационно-управляющие системы, как правило, схожи с атаками на корпоративные системы – доказательство возможности проникновения, кража информации или разрушение системы. Однако существуют некоторые отличия в методах атак на такие системы. Например, простая задержка в передаче информации, которая не приводит к существенным потерям в корпоративных сетях, может оказаться фатальной в промышленных системах в связи с потерей актуальности информации или ее несвоевременностью.

Также могут отличаться и уязвимости промышленных систем. На волне популярности многие производители промышленных систем, стремясь вывести продукт раньше конкурентов, не уделяют должного внимания безопасности программного или аппаратного обеспечения. Это приводит к тому, что простую атаку типа “отказ в обслуживании” осуществляют с использованием интеллектуальных лампочек, чайников и т. п.

Беря во внимание рассмотренные проблемы, в данной работе было поставлено решение следующих задач:

- с помощью семантических технологий формально и точно описать структуру внешних и внутренних уязвимостей;
- введение совокупности понятий, отношений и аксиом предметной области управления уязвимостями;
- построение онтологии уязвимости в системах SCADA, которая определяет ключевые концепции управления уязвимостью и их отношение.

Анализ последних исследований и публикаций. Основная особенность информационной безопасности заключается в том, что это не состояние, а непрерывный процесс анализа защищенности компьютерных систем, сетей, и их компонентов. Базовым семейством стандартов в области информационной безопасности является ISO 27000 [1] и его дополнения, в которых описываются терминология, методы защиты, методы контроля безопасности и т. д. Одним из основных элементов, которому уделяется внимание

в данных документах, является управление уязвимостью. Национальным институтом стандартов и технологий США предложен общий подход к описанию уязвимости системы [2] с использованием инструментов баз знаний [3], который дает общее понимание того, как идентифицировать уязвимость и какие элементы могут выступать в качестве определяющих параметров данного описания. При этом документ не регламентирует, какие именно инструментальные средства следует использовать и какие именно параметры уязвимости выделять как ключевые. Вместе с тем широкую популярность приобретают подходы к информационной безопасности с использованием различных методов и разделов искусственного интеллекта [4–6]. Учитывая такую тенденцию, авторами было проведено исследование, которое позволяет оценить использование OWL онтологии как способа хранения знаний [7; 8] об уязвимости, что позволит использовать накопленный опыт анализа защищенности систем для сокращения временных затрат на повторный анализ или портирования знаний для анализа других систем.

Цель статьи – развитие методов анализа уязвимостей в информационных системах и компьютерных сетях за счет построения онтологий, использующихся в области информационной безопасности. Ожидается, что применение онтологий уязвимости позволит сократить время, необходимое для анализа защищенности систем и сетей, а также поддержания актуальности их программного и аппаратного обеспечения.

Изложение основного материала. Для создания онтологии уязвимости в системах SCADA необходимо ввести совокупность понятий, отношений и аксиом предметной области. За основу для представления в общем виде множества понятий и отношений между классами взята работа [2].

Общий вид описания уязвимости и взаимосвязей ее элементов представлен на рис. 1.

Для построения онтологии уязвимости в статье использовались базы данных известных уязвимостей Common Vulnerability and Exposures и Common Weakness Enumeration. Данные источники позволяют описывать как основные характеристики уязвимости, так и способствуют определению специфических понятий, введенных в [1]. В качестве инструментального средства построения онтологии использовался прикладной пакет Protege [9].

Учитывая, что одна уязвимость может порождаться использованием иной уязвимости, необходимо также определить структуру взаимодействия между ними. Таким образом можно устанавливать родственные уязвимости и отношения между ними, как правило, типа Child Of, Parent Of или Member Of.

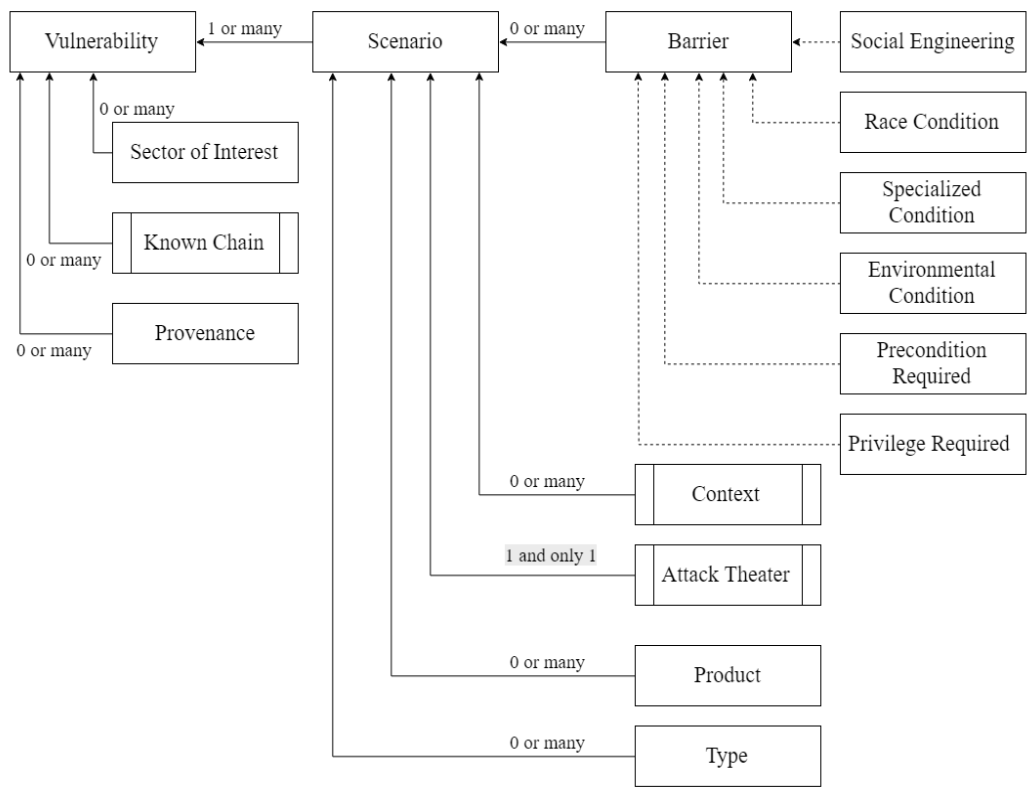


Рис. 1. Онтология уязвимости в системах SCADA

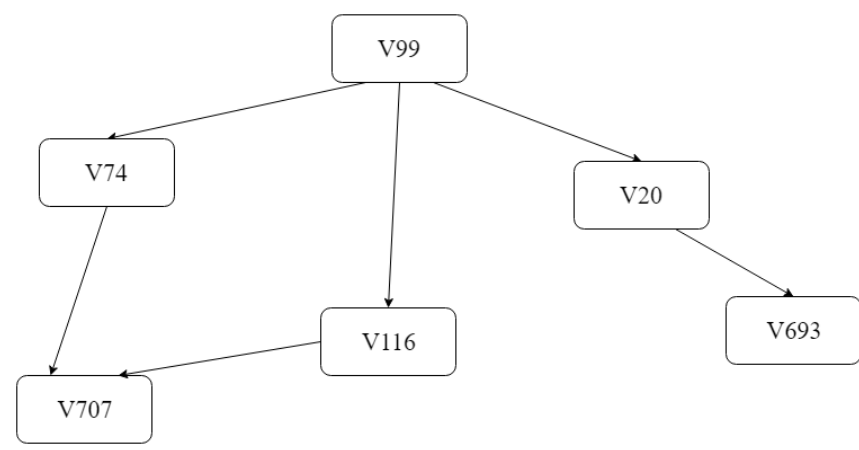


Рис. 2. Структурная сеть взаимосвязей уязвимости

Для описания классов и отношений между ними в качестве примера использовалась уязвимость CWE-99 Improper Control of Resource Identifiers ('Resource Injection').

Класс VULNERABILITY. Класс “уязвимость” вводится для идентификации выявленной уязвимости. Каждой уязвимости должен быть присвоен свой уникальный идентификатор, который имеет функцию упрощения системы поиска и препятствование неправильному восприятию информации. Поскольку собственный идентификатор задается численным значением, это препятствует пониманию того, что имеется в виду под идентификатором. Для этого необходимо ввести название уязвимости. Название уязвимости должно содержать общую краткую информацию об уязвимости. Название должно быть согласовано на международном уровне для исключения возможных неточных или ошибочных утверждений, которые могут привести к тому, что эксперты не смогут в полном объеме, или вообще, правильно понять содержание уязвимости. Необходимо отметить дату создания и дату модификации информации для отображения актуальности информации о данной уязвимости. Также необходимо ввести поле, которое предоставит дополнительную информацию об уязвимости, если в этом может возникнуть необходимость. Дополнительная информация может дать эксперту больше понимания об уязвимости. Исследовав необходимые параметры к этому классу, можно выделить следующие свойства у класса “уязвимость”:

- has_vulnerability_id – это уникальный идентификатор, определяющий уязвимость;

- has_vulnerability_name – это атрибут, который является текстовым описанием уязвимости;

- has_vulnerability_version – определяет номер версии уязвимости;

- has_vulnerability_creation_date – определяет дату, когда была создана уязвимость (для этой версии);

- has_vulnerability_modification_date – определяет дату, когда уязвимость была последний раз модифицирована (для этой версии);

- has_vulnerability_documentation – может быть добавлена дополнительная информация об уязвимости.

Относительно этого класса и его свойств можно сформулировать следующие аксиомы. Данные аксиомы являются утверждениями, справедливыми для данной предметной области:

Аксиома 1. Областью значений (range) свойства has_vulnerability_id является xsd: int.

Это означает, что данное свойство будет определяться численным значением, которое будет задавать эксперт при создании уязвимости.

Аксиома 2. Областью определения (domain) свойства has_vulnerability_id является класс VULNERABILITY.

Это означает, что вся полученная информация, которая была введена экспертом, будет храниться в классе VULNERABILITY (уязвимость).

Для свойства `has_vulnerability_id` выполняется следующее ограничение:
Аксиома 3.

$$\text{VULNERABILITY} \subseteq (= 1)\text{has_vulnerability_id}, \quad (1)$$

где VULNERABILITY – класс уязвимости;

`has_vulnerability_id` – имя свойства класса “уязвимость”.

Ограничение (1) утверждает, что каждой уязвимости, которая задается в базу знаний, должен быть поставлен в соотношение один и только один объект, предоставляющий уязвимости уникальный идентификатор.

Для уязвимости “V99” уникальным идентификатором в рамках онтологии уязвимости, согласно базе данных CWE, является численное значение “99”. Численное значение “99” не может быть предоставлено более ни одной другой уязвимости в рамках данной онтологии и делает этот идентификатор уникальным.

Аксиома 4. Областью значений (range) свойства `has_vulnerability_name` является `xsd:string`.

Это означает, что данное свойство определяется строчным значением, которое предоставляет эксперт при создании уязвимости.

Аксиома 5. Областью определения (domain) свойства `has_vulnerability_name` является класс VULNERABILITY.

Из этого следует, что значение, которое предоставил эксперт, будет храниться в классе VULNERABILITY (уязвимость).

Для свойства `has_vulnerability_name` выполняется следующее ограничение:

Аксиома 6.

$$\text{VULNERABILITY} \subseteq (= 1)\text{has_vulnerability_name}, \quad (2)$$

где VULNERABILITY – это класс уязвимости;

`has_vulnerability_name` – это имя свойства класса “уязвимость”.

Ограничение (2) утверждает, что в каждой уязвимости, которая задается в базу знаний, должен быть поставлен в соотношение один и только один объект, предоставляющий уязвимости имя.

Для уязвимости “V99” названием в рамках онтологии уязвимости, согласно базе данных CWE, является строчное значение “неправильный кон-

троль идентификаторов ресурсов (“Вливание ресурсов”). Строчное значение является кратким описанием уязвимости в рамках данной онтологии, которое было согласовано между экспертами этой предметной области, что позволит избежать вероятных неточных или ошибочных утверждений, могущих привести к тому, что эксперты не смогут в полном объеме, или вообще, правильно понять содержание уязвимости.

Последующие классы и уязвимости описываются по тому же принципу, и общая схема примет вид, как на рис. 3.

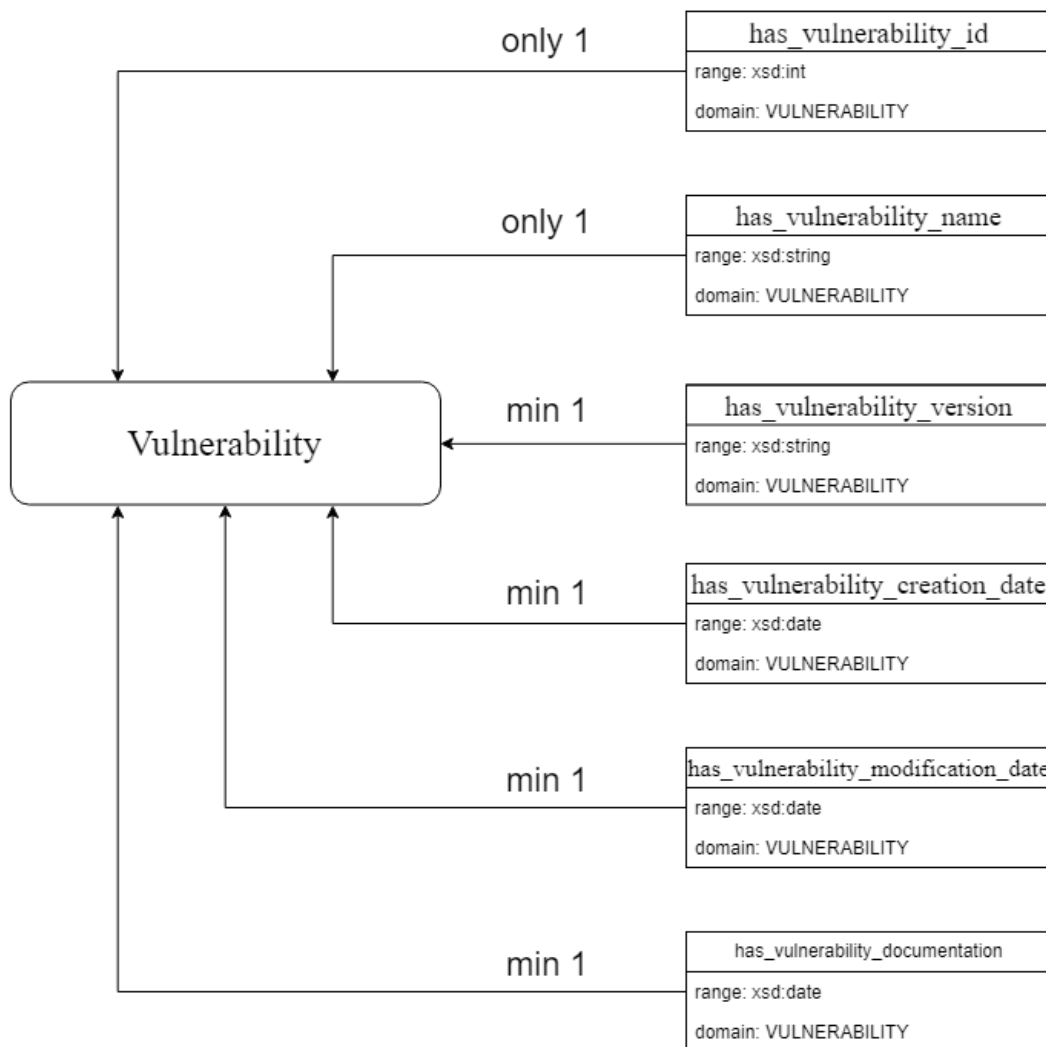


Рис. 3. Класс уязвимости с его свойствами

Отдельное внимание стоит уделить связям между классами. После создания классов онтологии уязвимости в системах SCADA необходимо установить отношение между классами. В рамках данной предметной области отношение между классами строится по особой процедуре.

Было решено ввести специализированные классы-отношения, которые предоставили бы возможность увеличить эффективность онтологии уязвимости.

Если между двумя классами необходимо задать отношение, то вводится дополнительный класс, имеющий свойства, которые связывают его с исходными классами. Схема данного строительства отображена на рис. 4.

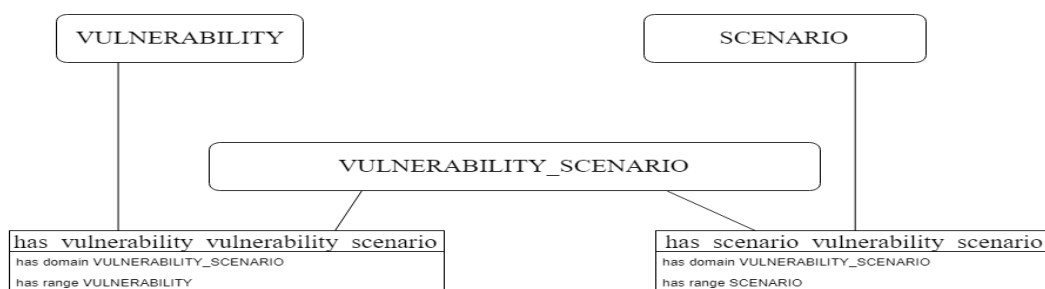


Рис. 4. Схема класса-отношения “уязвимость-сценарий”

Ниже приведена структура создания классов-отношений для онтологии уязвимости в системах SCADA.

Класс-отношение VULNERABILITY_SCENARIO. Класс-отношение “уязвимость-сценарий” введено для того, чтобы установить отношение между классом “уязвимость” и классом “сценарий”. Этому классу необходимо установить минимум два свойства, каждое из которых должно иметь способность установить связь между этими двумя классами. Проанализировав все требования к этому классу, можно установить следующие свойства:

- has_vulnerability_vulnerability_scenario – свойство, которое связывает с классом уязвимость;
- has_scenario_vulnerability_scenario – свойство, которое связывает с классом сценарий.

Относительно этого класса и его свойств можно сформулировать следующие аксиомы.

Аксиома 7. Областью значений (range) свойства has_vulnerability_vulnerability_scenario является класс VULNERABILITY.

Это означает, что связь будет установлена от класса VULNERABILITY (уязвимость).

Аксиома 8. Областью определения (domain) свойства `has_vulnerability_vulnerability_scenario` является класс `VULNERABILITY_SCENARIO`.

Это означает, что связь от класса `VULNERABILITY` (уязвимость) будет храниться в классе `VULNERABILITY_SCENARIO` (уязвимость-сценарий).

Для свойства `has_vulnerability_vulnerability_scenario` выполняется следующее ограничение:

Аксиома 9

$$\text{VULNERABILITY}_{\text{SCENARIO}} \subseteq (\geq 1)\text{has_vulnerability_vulnerability_scenario}, \quad (3)$$

где `VULNERABILITY_SCENARIO` – класс-отношение;

`has_vulnerability_vulnerability_scenario` – имя свойства класса “уязвимость-сценарий”.

Ограничение (3) утверждает, что к каждому объекту класса-отношение “уязвимость-сценарий”, задаваемый в базу знаний, должен быть поставлен в соотношение один или более объектов, который предоставляет отношение к классу “уязвимость”.

Этим было изображено, как устанавливается связь между классом “уязвимость” и классом-отношением “уязвимость-сценарий”.

Аксиома 10. Областью значений (range) свойства `has_scenario_vulnerability_scenario` является класс `SCENARIO`.

Это означает, что связь будет установлена от класса `SCENARIO` (сценарий).

Аксиома 11. Областью определения (domain) свойства `has_scenario_vulnerability_scenario` является класс `VULNERABILITY_SCENARIO`.

Это означает, что связь от класса `SCENARIO` (сценарий) будет храниться в классе `VULNERABILITY_SCENARIO` (уязвимость-сценарий).

Для свойства `has_scenario_vulnerability_scenario` выполняется следующее ограничение:

Аксиома 12.

$$\text{VULNERABILITY}_{\text{SCENARIO}} \subseteq (> 1)\text{has_scenario_vulnerability_scenario}, \quad (4)$$

где `VULNERABILITY_SCENARIO` – класс-отношение;

`has_scenario_vulnerability_scenario` – имя свойства класса “уязвимость-сценарий”.

Ограничение (4) утверждает, что к каждому объекту класса-отношения “уязвимость-сценарий”, который задается в базу знаний, должен быть по-

ставлен в соотношение один или более объектов, предоставляющих отношение к классу “сценарий”.

Этим было продемонстрировано, как устанавливается связь между классом “сценарий” и классом-отношением “уязвимость-сценарий”.

Таким образом была установлена связь между двумя уязвимостями, что, как ожидается, обеспечит преимущество перед другими способами, с помощью оптимизации онтологии. Этот класс будет не столько информативным, сколько инструментом оптимизации. Для установления связи необходимо в класс занести объект с названием, созданным от первых букв названий классов, которые необходимо соединить, и порядкового номера. В уязвимости “V99” объектом связи является “vs1”.

Выводы из данного исследования и перспективы дальнейших исследований в данном направлении. Скорость реакции на киберугрозы и ошибки в промышленных системах на сегодняшний день играют ключевую роль в стабильности работы систем критического применения. Поэтому существует необходимость в разработке технологий, методов и подходов, которые реализуют автоматизированный или автоматический поиск проблемных и уязвимых мест в сетях и системах, с целью снижения вероятности проникновения в систему или утечек информации.

Предложенный в работе метод позволяет использовать в процессах анализа систем и сетей не только внешние источники информации об уязвимостях, такие как mitre.org или другие ресурсы, но и знания, опыт, накопленные в процессе эксплуатации целевой системы администраторами и аналитиками.

Применение данного метода при анализе состояния системы в испытательной лаборатории позволили сократить время, затраченное на поиск уязвимости в компьютерной сети и ее элементах, приблизительно на 8 %. Также использование данного подхода снизило риск внедрения посторонних программных объектов в рассматриваемой сети приблизительно на 14 %.

Список использованных источников:

1. ISO/IEC 27000:2016. Information technology. Security techniques. Information security management systems. Overview and vocabulary. URL: <https://www.iso.org/standard/66435.html>. ISO/IEC. Geneva, Switzerland, 2016. 41 p.

2. Booth H., Turner Chr. Vulnerability Description Ontology. A Framework for Characterizing Vulnerabilities. Gaithersburg: NIST, 2016. 45 p.

3. Antoniou G., Harmelen Frank van. OWL Web Ontology Language Overview // Handbook on Ontologies. Springer, Berlin, Heidelberg, 2004. P. 67–92. DOI.ORG/10.1007/978-3-540-24750-0_4

4. *Uschold M.* Building Ontologies: Towards a Unified Methodology // 16th Annual Conference of the British Computer Society Specialist Group on Expert Systems 16–18 December 1996. Cambridge, UK. 20 p.

5. *Tuzovsky A. F., Chirikov S. V., Yampolsky V. Z.* Knowledge management systems (methods and technologies) // NTL, Tomsk, 2005. 260 p.

6. *Brown K.* Encyclopedia of Language & Linguistics, Second Edition // Elsevier Science. Oxford, United Kingdom, 2006. P. 665–670.

7. *Konstantinova N. S., Mitrofanov O. A.* Ontologies as a knowledge storage system // SPDU, Saint Petersburg, 1990. 54 p.

8. *Thomas R. Gruber.* Toward Principles for the Design of Ontologies Used for Knowledge Sharing SKSL. Padowa, Italy, 1993. 602 p.

9. *Dosin D. G., Darevich R. R., Shkutyak N. V.* The opening of the ontology of materialism in Protégé-OWL artefacts // Artificial Intelligence, Lviv, Ukraine, 2008. 70–77 pp.

References:

1. ISO/IEC 27000:2016 (2016), Information technology. Security techniques. Information security management systems. Overview and vocabulary. Geneva, Switzerland, 41 p., available at: <https://www.iso.org/standard/66435.html>. ISO/IEC.

2. Booth H. and Turner Chr. (2016), Vulnerability Description Ontology. A Framework for Characterizing Vulnerabilities. Gaithersburg: NIST, 45 p.

3. Antoniou G. and Harmelen Frank van (2004), OWL Web Ontology Language Overview // Handbook on Ontologies. Springer, Berlin, Heidelberg, pp. 67–92. DOI.org/10.1007/978-3-540-24750-0_4

4. *Uschold M.* (1996) “Building Ontologies: Towards a Unified Methodology” // 16th Annual Conference of the British Computer Society Specialist Group on Expert Systems 16-18 December, Cambridge, UK, 20 p.

5. *Tuzovsky A. F., Chirikov S. V. and Yampolsky V. Z.* (2005), Knowledge management systems (methods and technologies) // NTL, Tomsk, 260 p.

6. *Brown K.* (2006), Encyclopedia of Language & Linguistics, Second Edition // Elsevier Science. Oxford, United Kingdom, 665–670 p.

7. *Konstantinova N. S. and Mitrofanov O. A.* (1990), Ontologies as a knowledge storage system // SPDU, Saint-Petersburg, 54 p.

8. *Thomas R. Gruber* (1993), Toward Principles for the Design of Ontologies Used for Knowledge Sharing SKSL. Padowa, Italy, 602 p.

9. *Dosin D. G., Darevich R. R. and Shkutyak N. V.* (2008), The opening of the ontology of materialism in Protégé-OWL artefacts // Artificial Intelligence. Lviv, Ukraine, pp. 70–77.

DOI: <https://doi.org/10.32836/2521-6643-2018-1-56-3>

УДК 004.738:004.94

О. М. Мартинюк, кандидат технічних наук,
доцент кафедри комп'ютерних
інтелектуальних систем та мереж
Одеського національного політехнічного
університету

Ахмеш Тамім, аспірант Одеського
національного політехнічного університету

О. В. Дрозд, доктор технічних наук,
професор кафедри комп'ютерних
інтелектуальних систем та мереж
Одеського національного політехнічного
університету

Г. С. Степова, кандидат технічних наук,
ст. викладач кафедри комп'ютеризованих
систем управління мереж Одеського
національного політехнічного університету

КОНТРОЛЕПРИДАТНІСТЬ ІЄРАРХІЧНИХ ПЕРЕХОДІВ У ПОВЕДІНКОВОМУ КОНТРОЛІ

Засоби робочого контролю складних розподілених інформаційних систем (РІС), що часто володіють властивостями критичності застосування, мають забезпечувати їх повну перевірку в реальному часі. Контроль слід виконувати не тільки для статичних апаратної, програмної та інформаційної складових РІС, але й для динамічних інформаційно-керуючих потоків, що відповідають основним функціям і сценаріям роботи та встановлюють поведінку РІС. Розглянуто спадкування контролепридатності для переходів ієрархічних поведінкових моделей РІС, суттєвої у часовій декомпозиції робочого контролю. Спадкування ґрунтується на використанні в ієрархічних переходах відносин сумісності та квазіпорядку для умов, подій, дій, функцій, відповідних їм вхідних-вихідних сигналів у процесі організації фонового розпізнавання поведінки ієрархічних мереж Петрі.

Ключові слова: робочий поведінковий контроль; контролепридатність; ієрархічна модель; розпізнавання поведінки; ієрархічні мережі Петрі.

Средства рабочего контроля сложных распределенных информационных систем (РИС), часто обладающих свойствами критичности применения, должны обеспечивать их полную проверку в реальном времени. Контроль

© **О. М. Мартинюк, Ахмеш Тамім, О. В. Дрозд, Г. С. Степова, 2018**

должен выполняться не только для статических аппаратной, программной и информационной составляющих РИС, но и для динамических информационно-управляющих потоков, соответствующих основным функциям и сценариям работы и составляющих поведение РИС. Рассмотрено наследование контролепригодности для переходов иерархических поведенческих моделей РИС, существенной при временной декомпозиции рабочего контроля. Наследование основано на использовании в иерархических переходах отношений совместимости и квазипорядка для условий, событий, действий, функций, соответствующих им вход-выходных сигналов при организации фонового распознавания поведения иерархических сетей Петри.

Ключевые слова: рабочий поведенческий контроль; контролепригодность; иерархическая модель; распознавание поведения; иерархические сети Петри.

The means of on-line testing of complex distributed information systems (DIS), often possessing criticality properties, must ensure their complete verification in real time. The high structural-functional and combinatorial complexity of modern DIS translates most of the tasks of their construction and analysis into the NP-hard class. To a large extent, this refers to the design and analysis stages of the system-architectural, structural-functional, and especially behavioral levels. This state is even more aggravated by the dynamism, non-determinism, intelligence of situational component interactions of DIS. In designing DIS, the issues of ensuring the reliability of their functioning play a crucial role. Existing and promising models and methods for checking and diagnosing DIS, providing their solution, inherit these features, in addition, they can often exceed the complexity of the corresponding models and design methods. These circumstances necessitate the use of decomposition, network and hierarchical models, multi-level, incremental and parallel methods that reduce the dimensionality of the tasks of building and analyzing DIS, in particular, behavioral check and diagnosis. This reduction is particularly significant with operational behavioral on-line testing performed in real-time DIS operation. The article discusses certain aspects of decomposition hierarchical models of behavioral on-line testing - formal models of inheritance of testability in the hierarchical transitions of a multi-level behavioral check model of DIS based on hierarchical Petri nets. This model provides a definition of the mechanisms for interlevel inheritance of the identified check behavior, which is essential for the hierarchical temporal decomposition of on-line testing. Inheritance is based on the use in hierarchical transitions of compatibility and quasi-order relations for alphabets of positions, transitions, input-output alphabets and associated conditions, events, actions, functions of hierarchical Petri nets when organizing reference recognition of their behavior.

Key words: on-line testing; checkability; hierarchical model; behavior recognition; Petri hierarchical networks.

Постановка проблеми. Перспективні розподілені інформаційні системи (далі – РІС) [1], зокрема системи Internet of Things та GRID-системи [2], характеризуються ускладненням, розширенням застосування, критичністю застосування [3]. Такі властивості, набуваючи постійності, визначають динамічні системи, в яких оперативно формуються розподілені структури взаємодіючих процесів обробки, комунікацій, зберігання з підвищеними ризиками доступу, невизначеності, функціональної інвалідації, помилок, хибних дій [3; 4].

Актуальність статті викликана необхідністю вдосконалення ієрархічних, компонентно-часових композицій для відомих моделей поведінкового робочого контролю РІС [5; 6; 7], що подаються, зокрема, ієрархічними мережами Петрі (МП). Пропонований підхід ґрунтується на декомпозиційних, асинхронно-подієвих властивостях у спадкуванні контрольної поведінки [8; 9] ієрархічних мереж Петрі [10].

Розмірність, динамічність, недетермінізм, інтелектуальність і комбінаторність ситуативних компонентних взаємодій сучасних РІС ускладнює моделі та методи контролю й діагнозу, а також часто обмежує їх застосування системами середньої складності.

Аналіз останніх досліджень і публікацій. Як правило, ризики доступу, помилок, хибних дій знімаються, по-перше, комплексом заходів безпеки і систем захисту інформації РІС [3; 4], до яких можна зарахувати засоби авторизації/аутентифікації, цифрового підпису, шифрування, прав доступу/довіри і багаторівневого екранування, предметно-логічної віртуалізації, по-друге, їх формальним контролем і діагнозом [4–8].

Для аналізу РІС застосовуються методи евристичного, детермінованого, імовірнісного, нечіткого, інтелектуального контролю, діагнозу і тестування їх структурних, функціональних та інформаційних властивостей і механізмів [5–11], що характеризуються прийнятними значеннями вірогідності й витрат.

Водночас компонентна й системна автономність, мобільність, інтелектуалізація [1, 2], кооперація все більше набувають властивостей складних РІС і надають їм ознаки мультиагентних систем. Отже, для РІС необхідним є аналіз (часто NP-складний), проектування, супровід із застосуванням багатьох технологій, – й усе це в умовах зростання оперативності розробки й перевірки, зокрема поведінкового робочого контролю.

У процесі підвищення ефективності виконання контрольних діагностичних завдань розвиваються апаратні засоби [5–7; 12; 13], методи декомпозиції й розпаралелювання, складні формальні моделі аналізованих властивостей і механізмів [8; 9; 14; 15]. Подальше вдосконалення оперативного робочого контролю на основі динамічних, мережних та ієрархічних,

подійно-часових, поведінкових моделей і методів може підвищити оперативність аналізу, перевірки та відновлення працездатності складних РІС.

Мета статті – розвиток контролепридатності ієрархічних переходів у багаторівневій поведінковій контрольній моделі РІС на основі ієрархічних мереж Петрі за рахунок визначення моделей і механізмів міжрівневого упадкування ідентифікованої контрольної поведінки.

Виклад основного матеріалу. У багаторівневому поведінковому робочому контролі РІС за вхідну модель компонента *SI* прийнято розширену МП [12]:

$$S(f) = (P, T, X, Y, In, Pb, Ep, Et, F, S, M_0, L, K), \quad (1)$$

де P, T – множини позицій і переходів;

X, Y – множини відповідно вхідних і вихідних сигналів для умов, подій (як структур умов), дій (як структур функцій) і функцій, що виникають та розміщені у позиціях і переходах;

$In \subset N$ – множина цілочислових часових інтервалів переходів;

$Pb \subset [0; 1] \subset D$ – множина коефіцієнтів імовірності в діапазоні $[0; 1]$;

$Ep \subset N$ – множина цілочислових енерговитрат формування умов, подій і виконання функцій для позицій з P ;

$Et \subset N$ – множина цілочислових енерговитрат виконання дій і функцій для переходів з T ;

$F: (P \times X \times In \times Pb \times Ep) \cup (T \times Y \times In \times Pb \times Et \rightarrow P)$ – розширене умовне відношення інцидентності позицій-переходів;

$S: (P \rightarrow X \times In \times Pb \times Ep) \cup (T \rightarrow Y \times In \times Pb \times Et)$ – розширена відповідність значень змінних для умов, подій, дій, функцій, часових інтервалів, коефіцієнтів імовірності в позиціях і переходах;

$M_0: P \rightarrow N$ – початкова розмітка, ($M: P \rightarrow N$ – функція поточної розмітки);

$L: (T \times Y \times In \times Pb \times Et \rightarrow \{0, 1\})$ – предикат спрацьовування переходів;

$K: (((P \times X \times In \times Pb \times Ep) \rightarrow (P \times X \times In \times Pb \times Ep)) \cup ((T \times Y \times In \times Pb \times Et) \rightarrow (T \times Y \times In \times Pb \times Et)))$ – функція модифікації значень змінних для умов, подій, дій, функцій, часових інтервалів, коефіцієнтів імовірності для позицій і переходів.

У зв'язку з цим за базовий елемент багаторівневої ієрархії прийнято дворівневу ієрархічну розширену МП *IS*. Дворівнева ієрархія МП – це шістька виду:

$$IS = (S(f), \cup_{i \in I} S(f)_i^p, \cup_{j \in J} S(f)_j^t, S_{gis}), \quad (2)$$

де $S(f)$ – старша МП з верхнього рівня ієрархії;

$S(f)^p = \cup_{i \in I} S(f)_i^p$ – множина підмереж Петрі (ПМП) нижнього рівня ієрархії, що заміщають (із синхронізацією, трансляцією) макропозиції з $P' = \cup_{i \in I} p_i'$, де $P' \subseteq P$ для МП $S(f)$ верхнього рівня через підстановку з ієрархічних відображень $\chi^{\rightarrow p}, \chi^{p \rightarrow}$;

$S(f)^t = \cup_{j \in J} S(f)_j^t$ – множина ПМП нижнього рівня ієрархії, що заміщають макропереходи з $T' = \cup_{j \in J} t_j'$ (де $T' \subseteq T$) для МП $S(f)$ верхнього рівня через підстановку з ієрархічних відображень $\nu^{\rightarrow t}, \nu^{t \rightarrow}$;

$Sg_{IS} = \{ \chi^{\rightarrow p}, \chi^{p \rightarrow}, \nu^{\rightarrow t}, \nu^{t \rightarrow} \}$ – сигнатура самих ієрархічних відображень.

Сигнатура Sg_{IS} описується наступною п'ятіркою:

– $\chi^{\rightarrow p}$ – часткове відображення заміщення входів у макропозиції з P' ,

що розщеплюються, для МП $S(f)$ верхнього рівня на входи в нові початкові позиції із множини $\cup_{i \in I} p_{S(f)i}$ для ПМП $S(f)^p = \cup_{i \in I} S(f)_i^p$ нижнього рівня;

– $\chi^{p \rightarrow}$ – часткове відображення заміщення виходів у макропозиції з P' ,

що розщеплюються, для МП $S(f)$ верхнього рівня на виходи з нових кінцевих позицій із множини $\cup_{i \in I} p_{S(f)i}$ для ПМП $S(f)^p = \cup_{i \in I} S(f)_i^p$ нижнього рівня;

– $\nu^{\rightarrow t}$ – часткове відображення заміщення входів у макропереходи з T' ,

що розщеплюються, для МП $S(f)$ верхнього рівня на входи в нові початкові переходи з множини $\cup_{j \in J} t_{S(f)j}$ для ПМП $S(f)^t = \cup_{j \in J} S(f)_j^t$ нижнього рівня;

– $\nu^{t \rightarrow}$ – часткове відображення заміщення виходів з макропереходів із T' ,

що розщеплюються, для МП $S(f)$ верхнього рівня на виходи з нових кінцевих переходів з множини $\cup_{j \in J} t_{S(f)j}$ для ПМП $S(f)^t = \cup_{j \in J} S(f)_j^t$ нижнього рівня.

Дворівнева ієрархія IS об'єднує множини простих ієрархічних переходів двох основних типів між двома безпосередньо суміжними рівнями моделі. Результатом застосування такої наскрізної часової декомпозиції є деталізована молодша МП $S(f)^+ = S(f) \setminus ((\cup_{i \in I} p_i) \cup (\cup_{j \in J} t_j)) \cup (\cup_{i \in I} S(f)_i^p) \cup (\cup_{j \in J} S(f)_j^t)$, що отримується зі старшої МП $S(f)$ в результаті виконання заміщень, отриманих із підстановок і відображень $Sg_{IS} = \{ \chi^{\rightarrow p}, \chi^{p \rightarrow}, \nu^{\rightarrow t}, \nu^{t \rightarrow} \}$, усіх позицій P' і переходів T' старшої МП $S(f)$ відповідними ПМП із множин $\cup_{i \in I} S(f)_i^p, \cup_{j \in J} S(f)_j^t$, що й деталізують оці позиції і переходи.

Моделлю довільної МП або ПМП з $S(f)$, або $\cup_{i \in I} S(f)_i^p$ і $\cup_{j \in J} S(f)_j^t$ в ієрархії IS прийнята МП, достатня в задачах поведінкового контролю функціональних дефектів. Асинхронно-подієва МП $S(f)$ організовує свою внутрішню синхронізацію відповідно до відносин сумісності ξ та квазіпорядку ψ для алфавітів умов, подій, дій, функцій, а також їх вхід-вихідних сигналів.

Відносини сумісності ξ і квазіпорядку ψ також успадковуються у синхронізації відносин сумісності та квазіпорядку для ієрархії IS і молодшої МП $S(f)^+$, зводячи їх до єдиних відносин сумісності $\xi^+ = \xi \cup (\cup_{i \in I} \xi_i) \cup (\cup_{j \in J} \xi_j)$ і квазіпорядку $\psi^+ = \psi \cup (\cup_{i \in I} \psi_i) \cup (\cup_{j \in J} \psi_j)$ для об'єднаних алфавітів умов, подій,

дій, функцій, а також їх вхід-вихідних сигналів, пов'язаних із ними за часовими інтервалами для $S(f)^+$.

Таким чином, дворівнева ієрархія IS накладає на $S(f)$, $\cup_{i \in I} S(f)_i^c$, $\cup_{j \in J} S(f)_j^t$, які входять до її складу, умову синхронізації алфавітів. Дискретний асинхронно-подієвий час для ψ поширюється на IS і $S(f)^+$ під час успадкування часових умов ψ старшої МП $S(f)$ у часових умовах $\cup_{i \in I} \psi_i$, $\cup_{j \in J} \psi_j$ для ПМП з $(\cup_{i \in I} S(f)_i^c) \cup (\cup_{j \in J} S(f)_j^t)$. Єдиний асинхронно-подієвий час IS передбачає, що інтервали будь-якої ПМП з $(\cup_{i \in I} S(f)_i^c) \cup (\cup_{j \in J} S(f)_j^t)$ квазівпорядковані за ψ^+ і сумісні за ξ^+ як з інтервалами старшої МП $S(f)$, так і з інтервалами будь-якої іншої ПМП з $(\cup_{i \in I} S(f)_i^c) \cup (\cup_{j \in J} S(f)_j^t)$.

Без втрати спільності для поведінкового робочого контролю в рамках відносин квазівпорядку ψ і сумісності ξ властивості поведінки для ієрархій IS обмежені синхронізацією для умов, подій, дій, функцій, їх вхід-вихідних сигналів у відображеннях з Sg_{IS} для ієрархічних переходів з IS . Тобто для ієрархічного переходу ієрархії IS для МП з $S(f)^+$, згідно з відносинами ψ і ξ старшої МП $S(f)$ і відносинами ξ^+ та ψ^+ молодшої МП $S(f)^+$, виконуються такі умови:

– миттєве виникнення умови, події, дії, функції, їх вхід-вихідного сигналу для старшої МП $S(f)$ у певний відповідний до відносин ξ^+ і ψ^+ момент асинхронно-подієвого часу успадковується у миттєвих виникненнях відповідних структур умов, подій, дій, функцій, їх вхід-вихідних сигналів для $S(f)^+$;

– єдиність виникнення умови, події, дії, функції, їх вхід-вихідного сигналу для старшої МП $S(f)$ у певний, відповідний до відносин ξ^+ і ψ^+ , момент асинхронно-подієвого часу успадковується в єдиності виникнення відповідних структур умов, подій, дій, функцій, їх вхід-вихідних сигналів для $S(f)^+$;

– виникнення умови, події, дії, функції, їх вхід-вихідні сигнали для старшої МП $S(f)$ у певний, відповідний до відносин ξ^+ і ψ^+ , момент асинхронно-подієвого часу ϖ з можливістю його збереження до деякого відповідного до відносин ξ і ψ моменту $\varpi + \zeta$, де $\zeta = 0, 1, 2, \dots$ – номери наступних відповідних структур умов, подій, дій, функцій, їх вхід-вихідних сигналів, пов'язаних із початковою подією виникнення при $\zeta = 0$, успадковується у виникненнях відповідних структур умов, подій, дій, функцій, їх вхід-вихідних сигналів для $S(f)^+$ із загальними початковими моментами часу $\varpi^+ = \varpi \cup (\cup_{i \in I} \varpi_i) \cup (\cup_{j \in J} \varpi_j)$ та можливістю їх збереження до деяких загальних (сумарних) для всіх множин граничних моментів:

$$\varpi^+ + \zeta^+ = (\varpi + \zeta) \cup (\varpi' + \zeta') \cup (\cup_{i \in I} \varpi_i + \zeta_i) \cup (\cup_{j \in J} \varpi_j + \zeta_j),$$

де ϖ' , $\varpi' + \zeta'$ – заміщені інтервали; $(\cup_{i \in I} \varpi_i)$, $(\cup_{j \in J} \varpi_j)$, $(\cup_{i \in I} \varpi_i + \zeta_i)$, $(\cup_{j \in J} \varpi_j + \zeta_j)$ – нові інтервали, якими заміщують старі інтервали ϖ' , $\varpi' + \zeta'$ відповідно $S(f)^+$;

– виникнення умов, подій, дій, функцій, їх вхід-вихідних сигналів, що не зберігаються (на один момент асинхронно-подієвого часу), і умов, подій, дій, функцій, їх вхід-вихідних сигналів, що зберігаються (на більш ніж один момент асинхронно-подієвого часу).

Згідно з цим для робочого контролю ієрархія IS накладає на ПСП з множин $\cup_{i \in I} S(f)_i^c$, $\cup_{j \in J} S(f)_j^t$, що входять до неї, умови успадкування контрольної поведінки в ієрархічних переходах із IS у разі заміщення обраних макропозицій і макропереходів системної МП $S(f)$ відповідними ПМП із множин $\cup_{i \in I} S(f)_i^c$, $\cup_{j \in J} S(f)_j^t$ відповідно до відображень Sg_{is} .

Так, організація ієрархії контрольних примітивів і, як наслідок, виконаного під час їх покриття поведінкового робочого контролю можлива за умови збереження сигнатурою Sg_{is} контрольованих властивостей та ідентифікаторів позицій у $S(f)^+$. Ця умова обмежує множини $\cup_{i \in I} S(f)_i^c$, $\cup_{j \in J} S(f)_j^t$ молодших ПМП із множин $\cup_{i \in I} S(f)_i^c$, $\cup_{j \in J} S(f)_j^t$ допустимими для збереження контрольованих властивостей та ідентифікаторів. У цьому випадку множина ієрархічних переходів формує четвірку сумісних ієрархій, похідних від початкової ієрархії $IS = (S(f), \cup_{i \in I} S(f)_i^c, \cup_{j \in J} S(f)_j^t, Sg_{is})$, – еталонних властивостей iPr , ідентифікаторів позицій iCi , контрольних примітивів iCp , фрагментів зафіксованої реальної поведінки iW^{\wedge} :

$$\begin{aligned} iPr &= (Pr, \cup_{i \in I} Pr_i^c, \cup_{j \in J} Pr_j^t, Sg_{iP}), \\ iCi &= (Ci, \cup_{i \in I} Ci_i^c, \cup_{j \in J} Ci_j^t, Sg_{iId}), \\ iCp &= (Cp, \cup_{i \in I} Cp_i^c, \cup_{j \in J} Cp_j^t, Sg_{iEx}), \\ iW^{\wedge} &= (W^{\wedge}, \cup_{i \in I} W_i^{\wedge c}, \cup_{j \in J} W_j^{\wedge t}, Sg_{iW}) \end{aligned} \quad (3)$$

для обумовленої дворівневої контрольної ієрархії

$$iCS = (cS, \cup_{i \in I} cS_i^c, \cup_{j \in J} cS_j^t, Sg_{cS}). \quad (4)$$

Таким чином, для ієрархії IS формується ієрархічна модель багаторівневого поведінкового робочого контролю iCS . У робочому контролі аналіз ієрархічних відображень із Sg_{is} старшої МП $S(f)$ і будь-якої компонентної ПМП з $S(f)^+$ ієрархії IS виконується для відносин квазіпорядку ψ^+ і сумісності ξ^+ , що представляють старший і молодший рівні синхронізації поведінки ієрархічного переходу для $S(f)^+$ у загальній асинхронно-подієвій ієрархії IS .

Синхронізація відносин ψ^+ і ξ^+ в ієрархічних переходах ієрархії IS для $S(f)^+$ визначає різні класи старшого й молодшого рівнів синхронізації для множин вхідних $X \cup (\cup_{i \in I} X_i^c) \cup (\cup_{j \in J} X_j^t)$, вихідних $Y \in (\cup_{i \in I} Y_i^c) \cup (\cup_{j \in J} Y_j^t)$ алфавітів і алфавітів позицій $P \cup (\cup_{i \in I} P_i^c) \cup (\cup_{j \in J} P_j^t)$ та переходів $T \cup (\cup_{i \in I} T_i^c) \cup (\cup_{j \in J} T_j^t)$, а через них і умов, подій, дій та функцій для $S(f)^+$. Отже, ці класи передбачають класифікацію алфавітів у їх конкретній інцидентності всім МП і ПМП із $S(f)^+$.

У довільному ієрархічному переході ієрархії IS для старшої МП $S(f)$ і молодших ПМП з $(\cup_{i \in I} S(f)_i^p) \cup (\cup_{j \in J} S(f)_j^t)$ для будь-якої з двох ПМП, що деталізують позицію з P' або перехід з T' для $S(f)$ (наприклад, ПМП $S(f)_i^c$ для позиції з МП $S(f)$), для вхідного алфавіту можливі три випадки: а) $X \cap X_i^p = \emptyset$, б) $X \cap X_i^p \neq \emptyset$ при $P \cap P_i^p = \emptyset$ і $T \cap T_i^p = \emptyset$, в) $X \cap X_i^p \neq \emptyset$ при $P \cap P_i^p \neq \emptyset$ або $T \cap T_i^p \neq \emptyset$. Решта випадків зводиться до їх комбінацій, тому без втрати спільності досить розглянути їх для вхідного, вихідного алфавітів, алфавітів позицій і переходів. Для цього прикладу алфавіти МП $S(f)$ і ПМП $S(f)_i^p$ відповідно мають такі можливості.

Перша можливість. Нехай $X \cap X_i^p = \emptyset$. У цьому випадку МП $S(f)$ і ПМП $S(f)_i^p$ отримуються в результаті деталізації. Еквівалентна по відношенню до IS молодша МП $S(f)^+$ не знижує детермінованість відносин суміжності позицій і переходів (у межах її попереднього ієрархічним переходу існування). Як наслідок попередній контрольний аналіз старшої МП не руйнується. Надалі на молодшому рівні для повного $S(f)^+$ контрольний аналіз зводиться до аналізу організації, не потребуючи будь-яких спеціальних дій. Відносини вихідних алфавітів Y і Y_i^p на виконаний раніше контрольний аналіз не впливають.

Друга можливість. Нехай $X \cap X_i^p \neq \emptyset$. При $P \cap P_i^p = \emptyset$ і $T \cap T_i^p = \emptyset$ МП $S(f)$ і ПМП $S(f)_i^p$ також отримуються в результаті деталізації. Еквівалентна по відношенню до IS повна молодша МП $S(f)^+$ не знижує детермінованість відносин суміжності позицій і переходів. Попередній контрольний аналіз не руйнується, але еквівалентна молодша МП $S(f)^+$ може потребувати аналізу мінімальності або дії за низхідного проектування, що її забезпечують, за участю вихідних алфавітів Y і Y_i^p та відносин квазіпорядку ψ^+ сумісності ξ^+ .

Третя можливість. Нехай $X \cap X_i^p \neq \emptyset$. При $P \cap P_i^p \neq \emptyset$ або $T \cap T_i^p \neq \emptyset$ МП $S(f)$ і ПМП $S(f)_i^p$ також отримуються в результаті деталізації. Еквівалентна щодо IS повна молодша МП $S(f)^+$ може знизити детермінованість відносин суміжності позицій і переходів. Попередній контрольний аналіз старшої МП $S(f)$ може зруйнуватися, тому для молодшої МП $S(f)^+$ слід дотримуватися контрольного перепроєктування і повторного аналізу мінімальності у його складі або дій за низхідного проектування, які її забезпечують, за участю вихідних алфавітів Y і Y_i^p та відносин квазіпорядку ψ^+ і сумісності ξ^+ .

У реальному проектуванні наявні всі три можливості. Контролепридатною для наскрізного проектування можна вважати першу можливість. Умовно контролепридатною з мінімальним рівнем перевірок і відсутністю контрольного перепроєктування – другу можливість. Умовно не контролепридатною є третя можливість, де може губитися деякий попередній контрольний аналіз старшого рівня і в цьому разі потрібно виконувати контрольне перепроєктування.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. У статті розглянуто властивості спадкування контроле-

придатності для переходів ієрархічної моделі поведінкового робочого контролю розподілених інформаційних систем, що ґрунтується на ієрархічних мережах Петрі. Спадкування істотне у разі часової декомпозиції робочого контролю, воно ґрунтується на перевірці виконання в ієрархічних переходах відносин сумісності та квазіпорядку для умов, подій, дій, функцій, відповідних їм вхід-вихідних сигналів у ієрархічних мережах Петрі під час організації фонового розпізнавання еталонної поведінки. Застосування ієрархічної моделі дає можливість не лише визначити умови побудови наскрізного методу контролю, що застосовується на системному і компонентному рівні, але й у цілому знизити розмірність виконання поведінкового робочого контролю.

Список використаних джерел:

1. *Coulouris G., Dollimore J., Kindberg T., Blair G.* Distributed Systems: Concepts and Design, 5th ed. Boston: Addison-Wesley, 2011. 1067 p.
2. *Hahanov V., Litvinova E., Chumachenko S.* Cyber Physical Computing for IoT-driven Services. Springer, 2017. 279 p.
3. *Kharchenko V., Gorbenko A., Sklyar V., Phillips C.* Green Computing and Communications in Critical Application Domains: Challenges and Solutions // IX International Conference of Digital Technologies. Zhilina, Slovak Republic, 2013. P. 191–197.
4. *Romankevich V. A.* Self-testing of multiprocessor systems with regular diagnostic connections // Automation and Remote Control. 2017. Vol. 78, Issue 2. P. 289–299.
5. *Drozd O., Antoshchuk S., Rucinski A., Martinuk A.* Parity prediction method for on-line testing A Barrel-shifter // Proc. IEEE East-West Design & Test Symposium. Lviv, Ukraine, 2008. P. 208–213. DOI: 10.1109/EWDTS.2008.5580162.
6. *Drozd O., Antoshchuk S., Martinuk A., Drozd J.* Increase in reliability of on-line testing methods using natural time redundancy // Proc. IEEE East-West Design & Test Symposium. Moscow, Russia, 2010. P. 223–229.
7. *Hahanov V., Litvinova E., Obrizan V., Gharibi W.* Embedded method of SoC diagnosis // Elektronika in Elektrotechn. 2008. № 8. P. 3–8.
8. *Kudryavtsev V. B., Grunskii I. S., Kozlovskii V. A.* Analysis and synthesis of abstract automata // Journal of Mathematical Sciences. 2010. Vol. 169. Issue 4. P. 481–532.
9. *Gomes L., Fernandes J. M.* Behavioral Modeling for Embedded Systems and Technologies: Applications for Design and Implementation. 2010. 494 p. DOI: 10.4018/978-1-60566-750-8.
10. *Zaitsev D. A.* Toward the Minimal Universal Petri Net // IEEE Transactions on Systems, Man, and Cybernetics: Systems. 2013. P. 1–12.

11. *Martynyuk O., Sugak A., Martynyuk D., Drozd O.* Evolutionary Network Model of Testing of the Distributed Information Systems // Proc. 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. Bucharest, Romania, 2017. P. 888–893. DOI: 10.1109/IDAACS.2017.8095215.

12. *Мартынюк А. Н., Тамим А., Мартынюк Д. А., Дрозд А. В.* Поведенческий рабочий контроль сетевых компьютерных систем // Электротехнические и компьютерные системы. 2018. № 28 (104). С. 201–207. DOI: <http://dx.doi.org/10.15276/eltecs.28.104.2018.24>.

13. *Skobtsov Yu. A., Skobtsov V. Yu.* Evolutionary test generation methods for digital devices // Design of Digital Systems and Devices / [eds.: M.Adamski et al.]. Berlin: Springer-Verlag, 2011. P. 331–361 (Lecture Notes in Electrical Engineering. Vol. 79).

14. *Drozd O., Drozd M., Martynyuk O., Kuznietsov M.* Improving of a Circuit Checkability and Trustworthiness of Data Processing Results in LUT-based FPGA Components of Safety-Related Systems // CEUR Workshop Proceedings. 2017. Vol. 1844. P. 654–661.

15. *Sugak H., Martynyuk O., Drozd A.* Models of the Mutation and Immunity in Test Behavioral Evolution // Proc. 8th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Warsaw, Poland, 2015. P. 790–795.

References:

1. Coulouris G., Dollimore J., Kindberg T. and Blair G. (2011), Distributed Systems: Concepts and Design, 5th ed. Boston : Addison-Wesley, 1067 p.

2. Hahanov V., Litvinova E. and Chumachenko S. (2017), Cyber Physical Computing for IoT-driven Services. Springer, 279 p.

3. Kharchenko V., Gorbenko A., Sklyar V. and Phillips C. (2013), “Green Computing and Communications in Critical Application Domains: Challenges and Solutions” // IX International Conference of Digital Technologies, Zhilina, Slovak Republic, pp. 191–197.

4. Romankevich V. A. (2017), “Self-testing of multiprocessor systems with regular diagnostic connections” // Automation and Remote Control, vol. 78, issue 2, pp. 289–299.

5. Drozd O., Antoshchuk S., Rucinski A. and Martinuk A. (2008), Parity prediction method for on-line testing A Barrel-shifter // Proc. IEEE East-West Design & Test Symposium, Lviv, Ukraine, pp. 208–213. DOI: 10.1109/EWDTS.2008.5580162.

-
6. Drozd O., Antoshchuk S., Martinuk A. and Drozd J. (2010), Increase in reliability of on-line testing methods using natural time redundancy // Proc. IEEE East-West Design & Test Symposium. Moscow, Russia, pp. 223–229.
 7. Hahanov V., Litvinova E., Obrizan V. and Gharibi W. (2008), “Embedded method of SoC diagnosis” // Elektronika in Elektrotechn, vol. 8, pp. 3–8.
 8. Kudryavtsev V. B., Grunskii I. S. and Kozlovskii V. A. (2010), “Analysis and synthesis of abstract automata” // Journal of Mathematical Sciences, vol. 169, issue 4, pp. 481–532.
 9. Gomes L. and Fernandes J. M. (2010), Behavioral Modeling for Embedded Systems and Technologies: Applications for Design and Implementation, 494 p. DOI: 10.4018/978-1-60566-750-8.
 10. Zaitsev D. A. (2013), Toward the Minimal Universal Petri Net // IEEE Transactions on Systems, Man, and Cybernetics: Systems, pp. 1–12.
 11. Martynyuk O., Sugak A., Martynyuk D. and Drozd O. (2017), “Evolutionary Network Model of Testing of the Distributed Information Systems” // Proc. 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Bucharest, Romania, pp. 888–893. DOI: 10.1109/IDAACS.2017.8095215.
 12. Martynyuk A. N., Tamim A., Martynyuk D. A. and Drozd A. V. (2018), “*Povedencheskiy rabochiy kontrol' setevykh komp'yuternykh sistem*” [“Behavioral Working Control of Network Computer Systems”] // Journal *Elektrotekhnicheskkiye i komp'yuternyye sistemy* [Electrotechnical and Computer Systems], vol. 28 (104), pp. 201–207. DOI: <http://dx.doi.org/10.15276/eltecs.28.104.2018.24> [Russia].
 13. Skobtsov Yu. A. and Skobtsov V. Yu. (2011), Evolutionary test generation methods for digital devices // Design of Digital Systems and Devices / [eds.: M.Adamski et al.], Berlin: Springer-Verlag, pp. 331–361 (Lecture Notes in Electrical Engineering, vol. 79).
 14. Drozd O., Drozd M., Martynyuk O. and Kuznietsov M. (2017), “Improving of a Circuit Checkability and Trustworthiness of Data Processing Results in LUT-based FPGA Components of Safety-Related Systems” // CEUR Workshop Proceedings, vol. 1844, pp. 654–661.
 15. Sugak H., Martynyuk O. and Drozd A. (2015), “Models of the Mutation and Immunity in Test Behavioral Evolution” // Proc. 8th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Warsaw, Poland, pp. 790–795.

DOI: <https://doi.org/10.32836/2521-6643-2018-1-56-4>
УДК 656:51-74

Н. В. Халіпова, кандидат технічних наук,
доцент кафедри транспортних систем
та технологій Університету митної справи
та фінансів

І. Ю. Леснікова, кандидат технічних наук,
доцент кафедри транспортних систем
та технологій Університету митної справи
та фінансів

В. О. Шингур, студент Університету
митної справи та фінансів

РОЗРОБКА МОДЕЛІ УПРАВЛІННЯ ЯКІСТЮ ТРАНСПОРТНО- ЛОГІСТИЧНИХ ПРОЦЕСІВ ПІДПРИЄМСТВ

Сформовано модель для обґрунтування ефективних заходів управління якістю транспортно-логістичних процесів підприємства, що передбачає впровадження та розвиток процесного підходу в діяльності компанії, подальше статистичне управління якістю процесів шляхом оцінки параметрів та їх моніторингу. Запропоновано алгоритм, в основу якого покладено застосування механізму покращання процесів на основі повного циклу Демінга (PDCA). Проведено моделювання статистичного управління якістю транспортно-логістичних процесів та запропоновано шляхи вдосконалення роботи логістичного підприємства на основі стабілізації процесів поставок.

Ключові слова: моделювання транспортно-логістичних процесів; статистичне управління процесами; показники якості; контрольні карти; стабілізація процесів поставок.

Сформирована модель для обоснования эффективных мероприятий управления качеством транспортно-логистических процессов предприятия, предусматривающая внедрение и развитие процессного подхода в деятельности компании, последующее статистическое управление качеством процессов путем оценки параметров и их мониторинга. Предложен алгоритм, в основу которого положено применение механизма улучшения процессов на основе полного цикла Деминга (PDCA). Проведено моделирование статистического управления качеством транспортно-логистических процессов, а также предложены пути совершенствования работы логистического предприятия на основе стабилизации процессов поставок.

© Н. В. Халіпова, І. Ю. Леснікова, В. О. Шингур, 2018

Ключевые слова: моделирование транспортно-логистических процессов; статистическое управление процессами; показатели качества; контрольные карты; стабилизация процессов поставок.

Formed the two-phase model for the substantiation of effective measures in quality management of transport-logistic processes of the enterprises'. The first phase involves implementation and development of the process approach in the organization. BPMS-system supports business at all stages of the formation and improvement of the process approach, continuous processes improvement mechanism allows you to develop a company management model. The use of BPMS system capabilities allows to not only collect and organize statistical information of existing business processes, but also to monitor their strict implementation. The second phase is based on the usage of the process approach and includes statistical quality management of processes by measuring and monitoring of parameters. It is expected to receive information on the variation of the process, achievement of the state of statistical stability and obtaining estimates of the process parameters in this state, with subsequent control of the stability of processes.

Proposed the algorithm for revealing unstable processes of the enterprise and determination of their stabilization ways based on statistical management of quality indicators and improvement of transport-logistic processes by means of control cards. The algorithm is based on the usage of a mechanism for improving processes that affects the development of the enterprise management model based on the complete Deming cycle (PDCA). The control function represents the necessary attribute of management, which allows to identify problems and adjust the organization accordingly, before these problems turn into a crisis. The control is carried out by means of preliminary analysis of executable processes.

For statistical management of logistics enterprise's supply processes, performed simulation using one of the Statistica software package's main modules – Industrial Statistics and Six Sigma. Simulation using control cards allowed detecting a violation of the processes stability beyond the control limits. Result of the calculations: the construction of a medium-sized map, a multidimensional flow of X-bar and R maps identified the causes of instability. The analysis allowed to suggest ways of the logistics enterprise work improvement through the stabilization of supply processes.

Key words: modeling of transport-logistic processes; statistical processes management; quality indicators; control maps; stabilization of supply processes.

Постановка проблеми. Важливою умовою успішного розвитку сучасної економіки є виробництво конкурентних продукції та послуг, що неможливо без підвищення стандартів якості. У зв'язку з цим останнім часом

активно розвиваються системи, методи та інструменти менеджменту якості, розширюється сфера їх застосування. В умовах швидкого зростання на ринку кількості логістичних підприємств проблема якісного обслуговування клієнтів набуває особливої актуальності.

Визначення закономірностей ефективного функціонування логістичного підприємства ґрунтується на дослідженні великої кількості факторів і потребує застосування методів управління якістю процесів за кількісними ознаками. Використання статистичного моделювання та оптимізація ознак якості допомагає як виявляти закономірності та оцінювати рівень стабільності процесів на основі вихідної статистичної інформації, так і безпосередньо управляти якістю транспортно-логістичних процесів підприємства.

Аналіз світового досвіду впровадження систем менеджменту якості свідчить, що в сучасних умовах прискорення науково-технічного прогресу, глобалізації економіки, загострення конкуренції виробників актуальність проблем якості постійно зростає.

Аналіз останніх досліджень і публікацій. Аналізу застосування статистичних методів у процесі управління якістю присвячено [1]. Методологічні принципи статистичного моделювання та прогнозування соціально-економічних явищ процесів, аналітичні можливості та межі застосування конкретних моделей наведено в праці [2].

Обґрунтування сучасних концепцій менеджменту якості, питання ефективності впровадження систем управління якістю розглянуто в [3], аналіз методів оптимізації витрат на забезпечення якості продукції, особливостей сертифікації послуг, що впливає на якість і конкурентоспроможність промислового підприємства висвітлено в підручнику [4]. Теоретичні, методичні й практичні аспекти застосування статистичних методів регулювання технологічних процесів на підприємстві наведено в дослідженні [5].

Новітні системи менеджменту якості й методи підвищення ефективності організацій на основі покращання якості, такі як система продуктивного обслуговування обладнання за участю всього персоналу (TPM), система економного виробництва (Lean Production), методологія “Шість сигм”, бенчмаркінг, реінжиніринг, реструктуризація підприємства, економіка якості, проаналізовано в [6].

Управління ланцюгом поставок являє собою комплексний і системний підхід, який потребує одночасного розгляду й обліку багатьох операцій з постачання та збуту. У [7; 8] розглянуто етапи управління ланцюгами постачання й можливості підвищення його ефективності та якості.

Різновиди управлінських інновацій, що можуть бути використані в різних підсистемах підприємства залежно від необхідності розв’язання порушених проблем та напряму інноваційного розвитку підприємства, досліджено в [9].

Застосування стратегічного менеджменту на основі принципів синергії, об'єктно-цільового та процесного підходів, використання яких забезпечує стійкі конкурентні переваги підприємства на ринку продукції, подано в [10].

Аналіз сучасних концепцій, методів та стратегій удосконалення управління якістю процесів свідчить про актуальність даного напрямку. Проте покращання конкурентоспроможності й здатності динамічно реагувати на вимоги ринку, ефективне використання внутрішніх ресурсів транспортно-логістичних компаній неможливе без розвитку і впровадження процесного підходу в діяльності організації та застосування методів для статистичного управління якістю поставок.

Мета статті. Удосконалення якості транспортно-логістичних процесів на основі розвитку процесного підходу в діяльності організації та застосування методів для статистичного управління якістю процесів. Для досягнення мети необхідно виконати такі завдання:

- сформулювати модель для обґрунтування ефективних заходів управління якістю транспортно-логістичних процесів підприємства на основі застосування процесного підходу та статистичного управління якістю поставок;
- запропонувати алгоритм виконання завдань управління показниками якості транспортно-логістичних процесів підприємства;
- провести моделювання із застосуванням контрольних карт для виявлення нестабільних транспортно-логістичних процесів підприємства та запропонувати шляхи їх стабілізації.

Виклад основного матеріалу. Якість постачання продукції від виробників до торговельних фірм, а від них через дилерів і філії кінцевому споживачеві має особливо велике значення для підтримання іміджу торговельної компанії та задоволення вимог і потреб споживачів. Потреба організації в побудові ефективного ланцюга постачання обумовлена необхідністю доставки товару кінцевому споживачеві краще, швидше й дешевше від конкурентів [7].

Формування моделі управління якістю транспортно-логістичних процесів підприємства

Пропонуємо двофазну модель для обґрунтування ефективних заходів управління якістю транспортно-логістичних процесів підприємства на основі застосування процесного підходу та статистичного управління якістю поставок.

Перша фаза включає впровадження й розвиток процесного підходу в транспортно-логістичній компанії.

Для підвищення рівня зрілості підприємств, що характеризує керованість та передбачуваність процесів, керівники впроваджують системи автоматизації діяльності компанії (бізнес-процесів, документообігу тощо). Шкала зрілості процесів визначає п'ять градацій (рис. 1) [11]. Щодо рівня зрі-

лості бізнес-процесів, то навіть повний опис і регламентація всіх процесів дає можливість компанії піднятися максимум до третього рівня зрілості [11–13].

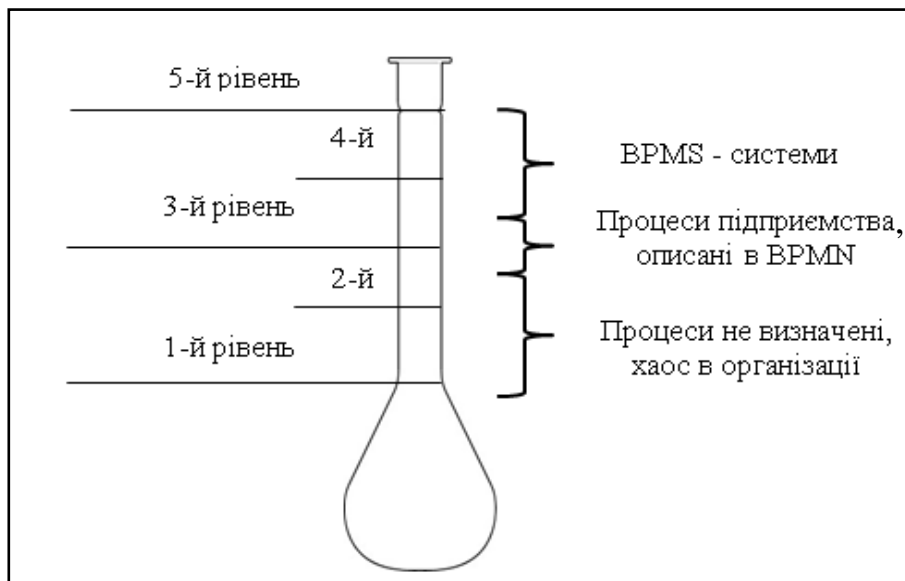


Рис. 1. Шкала рівня зрілості підприємства

Четвертий рівень передбачає, що процеси на практиці здійснюються в запропонованих рамках для досягнення певних цілей. Результати процесів збираються й аналізуються, що дозволяє зробити кількісну оцінку можливостей процесу, його прогнозування та управління продуктивністю.

Для досягнення п'ятого рівня процеси мають бути повністю визначені, їх цілі та завдання синхронізовані з загальними стратегічними цілями бізнесу, тобто вони стають невід'ємною частиною повсякденної діяльності кожного учасника процесу. Самостійне безперервне вдосконалення стає частиною процесів [11].

Ефективним засобом автоматизації бізнес-процесів є BPMS-система, яка дозволяє перейти від інструкцій до автоматичного виконання і контролю процесів, допомагає керувати ефективністю діяльності компанії. Механізм постійного поліпшення процесів дає можливість розвивати модель управління в компанії. BPMS-система дозволяє супроводжувати бізнес на всіх етапах становлення та вдосконалення процесного підходу в управлінні компанією. Але тільки за використання повного циклу Демінга “Plan-Do-Check-Act” (PDCA) в діяльності компанії слід очікувати розвитку та вдосконалення бізнесу, підвищення конкурентоздатності й управління “майбутнім” цієї компанії. Застосування можливостей BPMS-системи дозволяє не

тільки збирати та впорядковувати статистичну інформацію за наявних бізнес-процесів, але й контролювати чітко їх виконання [11; 12].

Друга фаза включає статистичне управління якістю транспортно-логістичних процесів і має два етапи: оцінка параметрів та їх моніторинг [1].

Метою першого етапу є отримання інформації про варіацію процесу, досягнення ним стану статистичної стабільності та одержання оцінок параметрів процесу в цьому стані.

Мета другого етапу – підтримка процесу в стабільному стані.

Виконання завдання статистичного управління якістю транспортно-логістичних процесів підприємства пропонуємо здійснювати за таким алгоритмом:

Крок 1. Визначення ключових бізнес-процесів для забезпечення успішного розвитку компанії.

Крок 2. Виявлення факторів, що впливають на якість транспортно-логістичних процесів та їх систематизація.

Крок 3. Ідентифікація основних проблем, існування яких стримує розвиток компанії.

Зручним інструментом для виявлення ключових взаємозв'язків між різними факторами в технічній, організаційній, технологічній, економічній, соціальній та інших сферах є причинно-наслідкова діаграма (діаграма Ісікави), яка одержала назву “риб'ячий кістяк”, або “риб'яча кістка” [14]. Діаграма має структуру у вигляді “ялинки”, в якій проблемна характеристика якості є стовбуром, а основні фактори (матеріали, методи, персонал, технічні засоби), які спричиняють проблему, подані у вигляді стрілок, розташованих під нахилом від стовбура. Діаграма Ісікави допомагає виявити та систематизувати різні фактори й умови, що впливають на досліджувану проблему, краще зрозуміти досліджуваний процес. Аналіз сприяє визначенню головних чинників негативного впливу та формуванню запобіжних заходів для усунення наявних проблем.

Крок 4. Аналіз та обґрунтування застосування методів управління показниками якості транспортно-логістичних процесів підприємства на основі кількісних оцінок.

Забезпечення відповідного рівня якості товарів або послуг потребує впровадження в діяльність підприємств статистичного управління процесами. Статистичне управління процесами – заснована на статистичному оцінюванні й теорії варіабельності методологія постійного вдосконалення процесів, що використовує відповідний статистичний інструментарій збору, обробки, оцінки та аналізу даних [15].

Ефективними методами контролю якості різноманітних процесів вважаються контрольні карти Шухарта. Дані для побудови карт отримують із процесу вибірково через приблизно рівні інтервали, які можуть бути задані

або за часом (наприклад, щогодини), або за кількістю продукції (кожна партія). Карта Шухарта – це графік значень певних характеристик підгруп залежно від їх номерів (рис. 2). Центральна лінія (CL) відповідає еталонному значенню характеристики [16]. Для оцінки перебування процесу в статистично керованому стані еталонним, зазвичай, служить середнє арифметичне розглянутих даних. Карта Шухарта має дві статистичні контрольні межові лінії, що розташовані по обидва боки від центральної лінії (CL) і називаються верхньою контрольною межею (UCL) і нижньою контрольною межею (LCL).

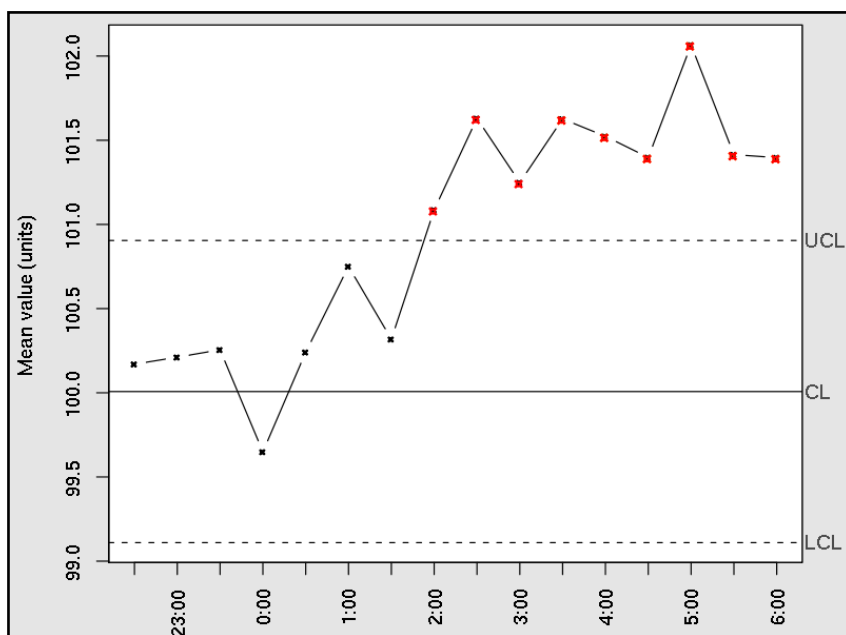


Рис. 2. Контрольні карти Шухарта

Контрольні лінії на карті Шухарта розміщено на відстані 3σ від центральної лінії, де σ – генеральне стандартне відхилення. Межі $\pm 3\sigma$ вказують, що близько 99,7 % значень характеристики підгруп потраплять у ці межі за умови, що процес перебуває в статистично керованому стані. Іншими словами, є ризик, який дорівнює приблизно 0,3 %, що нанесена точка опиниться поза контрольними межами (при стабільному процесі). Якщо процес статистично керований, контрольні карти реалізують метод безперервної статистичної перевірки нульової гіпотези про те, що процес не змінився й залишається стабільним. Коли значення параметра виходить за будь-яку з контрольних меж або серія значень виявляє незвичайні структури, стан статистичної керованості піддається сумніву. В цьому випадку потрібно

дослідити й виявити невідповідності (особливі) причини, а процес можна зупинити або скорегувати. Для виявлення причини відхилення досліджують вплив якості вихідного матеріалу або деталей, методів, операцій, умов проведення технологічних операцій, обладнання. Як тільки особливі причини знайдено й вилучено, процес знову готовий до продовження роботи [17]. У виробничій практиці застосовуються різні види контрольних карт. Наприклад, для контролю за кількісною ознакою показників якості процесів використовують карту середніх арифметичних і розмахів (X-R).

Крок 5. Застосування механізму покращання процесів, який впливає на розвиток моделі управління підприємством на основі повного циклу Демінга (PDCA).

Призначенням контрольних карт є подання сигналів про невідповідності, до яких можна зарахувати зсуви в рівні процесу. Спроможність контрольної карти віднаходити зміни в рівні якості визначається її операційною характеристикою [18; 19].

Цикл удосконалення якості на основі цілеспрямованого впливу на параметри процесу зображено на рис. 3 [1]. При зміні параметрів процесу впевненість у результаті змін через здійснений вплив, а не в результаті випадкової варіації через дію невідомих факторів, маємо наявності стану статистичної стабільності.

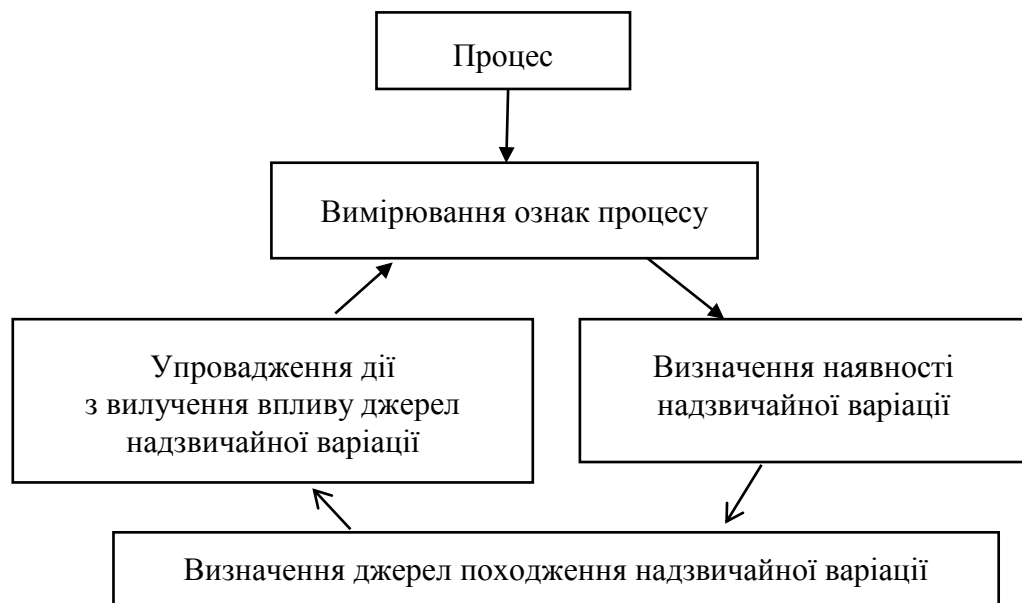


Рис. 3. Удосконалення процесів з використанням контрольних карт

Крок 6. Вибір інструмента для статистичного моделювання та проведення розрахунків.

Для моделювання обрано технології статистичного аналізу та обробки даних пакета програм Statistica, зокрема, модуль промислової статистики (Statistica Quality Control) та інструменти Шість сигм [20].

Крім одновимірних контрольних карт (стандартні карти Шухарта), пакет Statistica розширює можливості використання багатовимірних карт [21]. Багатовимірні карти дозволяють стежити за декількома процесами, що є надзвичайно ефективною функцією. Всі карти можуть бути побудовані як на основі наданих користувачем специфікацій, так і з використанням показників (вибіркове середнє, розмахи, частки тощо), які розраховуються з даних [22].

Використання контрольних карт дозволить виявляти нестабільні процеси транспортно-логістичних підприємств, усувати причини відхилення від норми й підвищувати якість та ефективність таких процесів. Це, зі свого боку, дає можливість підвищувати якість обслуговування клієнтів і покращувати імідж логістичного підприємства.

Крок 7. Аналіз результатів моделювання. Виявлення нестабільних процесів на логістичному підприємстві.

Крок 8. Формування пропозицій щодо покращання показників якості на основі стабілізації транспортно-логістичних процесів підприємства.

Крок 9. Перевірка ефективності заходів стабілізації процесів транспортно-логістичного підприємства за допомогою моделювання вдосконалених процесів. Якщо мети не досягнуто, переходимо до виконання кроку 8, доки процеси не стабілізуються.

Моделювання транспортно-логістичних процесів підприємства із застосуванням контрольних карт

Розглянемо модельний приклад для вдосконалення діяльності логістичної фірми. Функція контролю дозволяє виявити проблеми шляхом попереднього аналізу та вчасного коригування виконуваних процесів, щоб уникнути кризового стану. За результатами аналізу статистики виконання завдань можна приймати управлінські рішення щодо зміни ходу виконання процесу стосовно перерозподілу функцій між співробітниками (відділами), заохочення та мотивації персоналу тощо. Починаємо моделювання з аналізу напрямів покращання процесів, що розвиває модель управління підприємством.

Проаналізуємо основні фактори, які впливають на розвиток ланцюгів постачання на логістичному підприємстві. Результати систематизації факторів подано на рис. 4.

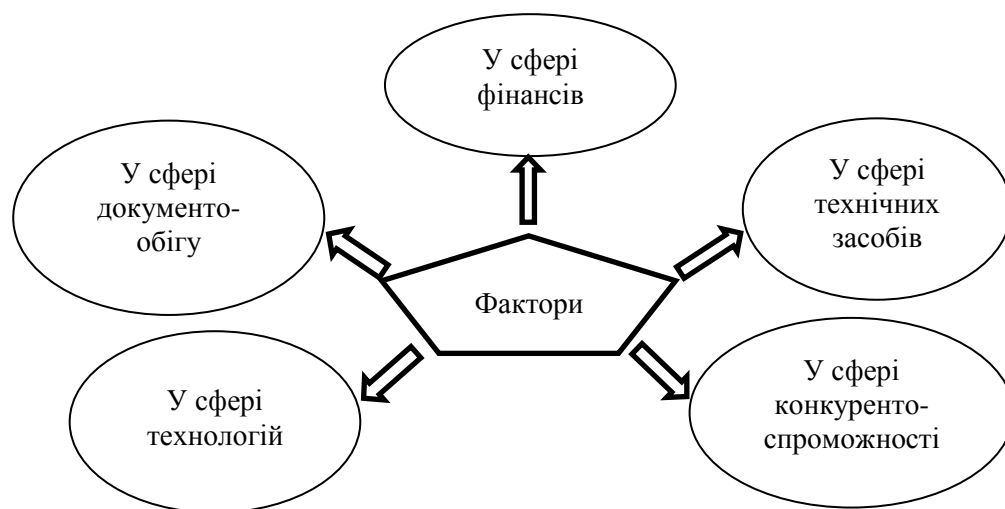


Рис. 4. Систематизація факторів, що визначають розвиток ланцюгів постачання на підприємстві

Можливі причини, що стримують розвиток підприємства, можна умовно поділити на групи:

- у сфері технологій: брак комплексного підходу до наскрізного транспортування (відсутність новітніх логістичних технологій перевезення); незадовільний наскрізний термін доставки і ритм поставок; низька надійність поставки за принципом “точно в строк”; недостатня взаємодія з органами державного контролю; низький рівень взаємодії з операторами-власниками рухомого складу [8];

- у сфері конкурентоспроможності: недостатній рівень сервісу; недостатній рівень інформаційного обміну між усіма учасниками процесу товароруку; складні митні і прикордонні процедури; відсутність наскрізної тарифної ставки;

- у сфері документообігу: відносно застаріла система ведення документації; низький рівень ознайомлення і впровадження новітніх систем електронного документообігу; великі затрати часу на заповнення паперових бланків;

- у сфері фінансів: непослідовність тарифної політики логістичного підприємства; відносно велика частка невчасно сплачених рахунків перевізників;

- у сфері технічних засобів: недостатній розвиток спеціалізованого технічного забезпечення вантажних перевезень; відсутність достатньої кількості спеціальних пунктів прийому вантажів, складів тимчасового зберігання, обладнання для завантаження-вивантаження товару.

Результати аналізу факторів, що стримують розвиток якості ланцюгів постачання, зображено за допомогою діаграми Ісікави (рис. 5).

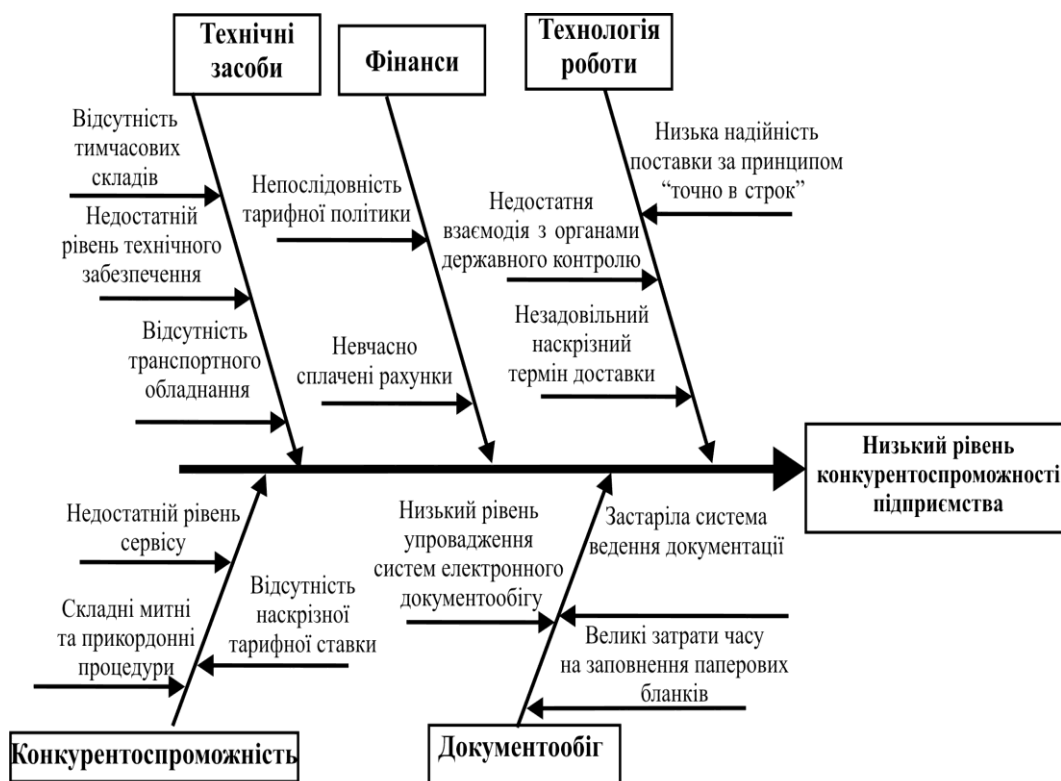


Рис. 5. Основні причини, що стримують розвиток якості ланцюгів постачання (діаграма Ісікави)

Механізм постійного поліпшення процесів на основі впровадження BPMS-системи дозволяє не лише спостерігати статистичні дані за наявними бізнес-процесами, але й контролювати чітко їх виконання. Моніторинг процесів показує характер реалізації як поточних процесів, так і завершених або перерваних. Якщо у процесів визначені планові показники (тимчасові, технічні й т. п.), то за допомогою BPMS-системи можна відстежувати, чи досягнуто цих показників у рамках процесу, чи ні. Тобто отримується корисна інформація для прийняття правильних управлінських рішень [12].

За результатами аналізу операційних процесів логістичного підприємства (рис. 6) визначено напрями вдосконалення якості поставок. Обрані напрями, а саме забезпечення вчасної і якісної обробки заявок та доставки вантажів, виділено на схемі прямокутниками із заливкою.



Рис. 6. Операційні процеси логістичного підприємства

Модельовання проводиться на основі зібраних статистичних даних з інформаційної бази підприємства. Необхідні дані для побудови контрольних карт упорядковуємо в середовищі Excel (табл. 1). Вихідні дані є вибірками з одинадцяти окремих партій поставок вантажів по 5 серій кожна. У кожній серії представлено дані про загальну кількість рахунків, кількість невчасно сплачених рахунків та кількість невчасно опрацьованих заявок. Також наведено дані за днями тижня щодо неопрацьованих заявок.

Фрагмент вихідних даних для побудови контрольних карт

Партія поставок	Дата	Загальна кількість рахунків	Кількість несплачених рахунків	Кількість неопрацьованих заявок	Пн	Вт	Ср	Чт	Пт	Сб	Н
21	01.09.2018	75	10	0	0	1	2	3	2	1	0
21	01.09.2018	68	2	1	0	0	2	0	0	0	0
21	01.09.2018	68	13	1	0	0	0	0	0	0	0
21	02.09.2018	71	3	0	0	0	0	2	2	0	0
21	02.09.2018	70	6	0	0	0	0	0	0	3	0
...
31	24.09.2018	72	8	0	3	0	0	0	0	2	0
31	25.09.2018	54	8	10	0	0	0	0	2	7	2
31	25.09.2018	56	13	9	0	2	0	0	0	4	6
31	26.09.2018	70	14	0	1	3	1	2	1	0	0
31	27.09.2018	68	3	0	0	0	2	1	2	0	2

Моделювання статистичного управління якістю транспортно-логістичних процесів проведено з використанням програмного пакета Statistica [20]. Вихідні дані у вікні Statistica зображено на рис. 7.

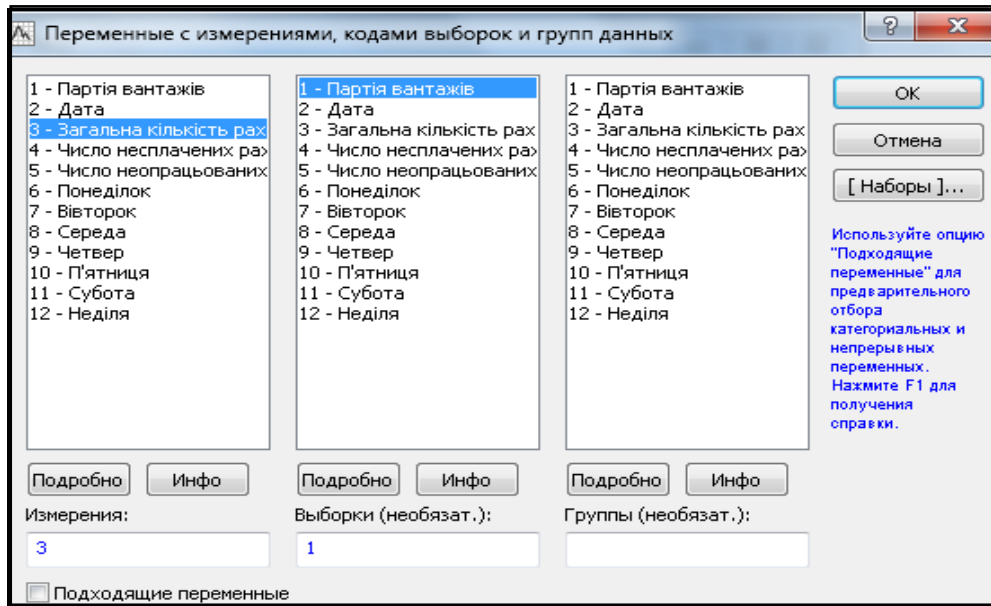


Рис. 7. Вікно змінних із вимірами, кодами вибірок і групами даних

Для проведення розрахунків файли вихідних даних імпортується в систему Statistica. Далі переходимо в меню Аналіз => Промислова статистика і Шість сигм => модуль Карти контролю якості. За допомогою контрольних карт можна виявити нестабільні процеси перевезення та усунути причини надзвичайної варіації.

Для характеристики якості процесу перевезення вантажу за вихідними даними побудовано карти Шухарта середніх значень (рис. 8) та розмахів варіації (рис. 9). Отримані діаграми використовуються для статистичного контролю стабільності досліджуваних процесів.

Перша точка на карті розмаху варіації (рис. 9) дорівнює 7. Це розмах варіації даних 21-ї партії першої вибірки, аналогічні дані подано для всіх партій перевезених вантажів.

На карті Шухарта зображено контрольні межі. Точка, що вийшла за контрольні межі, називається викидом. Це означає, що процес нестабільний, треба шукати шляхи для подолання такої ситуації та стабілізації процесу [1]. Центральна лінія та контрольні межі розраховуються таким чином: оцінюється розмах варіації R_i кожної підгрупи; потім знаходиться середній розмах варіації для всіх підгруп:

$$R = \sum R/k, \quad (1)$$

де k – кількість груп.

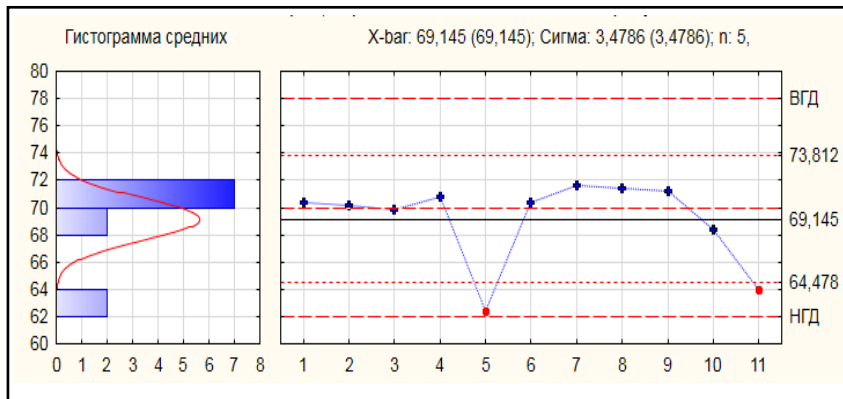


Рис. 8. Карта Шухарта середніх значень з X-bar

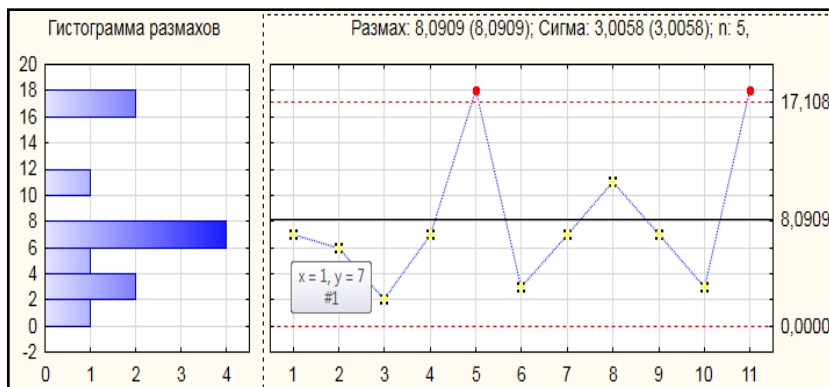


Рис. 9. Карта Шухарта розмахів варіації

Для побудови карти необхідно розрахувати центральну лінію (CL), що відповідає еталонному значенню характеристики, а також верхню (UCL) і нижню (LCL) контрольні лінії контрольної карти середніх значень (X -карти), які розраховуються так:

$$CL = \bar{R}, \quad (2)$$

$$UCL = \bar{R} + 3\sigma, \quad (3)$$

$$LCL = \bar{R} - 3\sigma. \quad (4)$$

Між вибірковими розмахами і стандартним відхиленням нормального розподілу існує залежність, яка має назву відносного розмаху [22]. Параметри розподілу цієї випадкової змінної $W = R/\sigma$ визначаються розмахом ви-

бірки n . Середнім значенням цієї змінної є величина d_2 , а середньоквадратичним відхиленням d_3 . Оскільки значення середньої величини процесу та її середньоквадратичного відхилення стандартні, параметри карти середніх значень будуть такими:

$$UCL = \mu + 3 \frac{\sigma}{\sqrt{n}}, \quad (5)$$

$$CL = \mu, \quad (6)$$

$$LCL = \mu - 3 \frac{\sigma}{\sqrt{n}}, \quad (7)$$

де μ – сума фіксованого середнього.

Так як $3/\sqrt{n} = A$, де A – множник, який визначається лише обсягом вибірки n , то параметри карти середніх із заданими значеннями матимуть такий вигляд:

$$UCL = \mu + A\sigma, \quad (8)$$

$$CL = \mu, \quad (9)$$

$$LCL = \mu - A\sigma. \quad (10)$$

Для створення карти розмахів R зі стандартними значеннями (враховуючи, що $\sigma = R/d_2$), значення параметрів будуть такі:

$$UCL = d_2 + 3d_3\sigma; \quad (11)$$

$$CL = d_2; \quad (12)$$

$$LCL = d_2 - 3d_3\sigma, \quad (13)$$

де d_2 і d_3 – константи, що залежать лише від обсягу вибірки n .

Нехай:

$$D_1 = d_2 - 3d_3, \quad (14)$$

$$D_2 = d_2 + 3d_3. \quad (15)$$

Тоді матимемо:

$$UCL = D_2 \sigma; \quad (16)$$

$$LCL = D_1 \sigma. \quad (17)$$

Отримані дані зображено червоною товстою штриховою лінією (рис. 8) на карті Шухарта: центральна лінія – це номінал, знизу – нижня межа допуску, зверху – верхня межа допуску. Треба підкреслити, що межі допуску визначають факт вчасної чи невчасної доставки вантажів, а контрольні межі вираховуються зі складової процесу опрацювання нових заявок на перевезення та вчасного сплатення рахунків перевізників. Завдання контрольних меж полягає в тому, щоб показати, що на процес перевезення впливають деякі конкретні причини та зміщують його або приводять до того, що мінливість процесу стає занадто великою.

Статистичний контроль під час керування процесом застосовується для своєчасного введення коригувальних дій. Найчастіше в багатопараметричному процесі існує декілька якісних показників, які необхідно контролювати й регулювати. Побудуємо карти Хотеллінга T^2 (рис. 10), що є багатовимірним аналогом карт Шухарта середніх значень і стандартних відхилень. Використовуємо дані спостережень по днях тижня. Значення T^2 , які перевищують розраховані, характеризують порушення контрольних умов [20]

Аналіз розрахунку стабільності процесів перевезення, результати якого наведено на контрольних картах (рис. 8–10), свідчить, що дані на карті Шухарта середніх значень (рис. 8) вказують на те, що процес доставки вантажу погано керований, вибірккові середні значення 5 і 11-ої вибірок розташовані поза контрольними межами. Розладнання перевізного процесу засвідчує також гістограма розподілу вибірккових середніх значень (графік зліва), демонструючи явну відмінність їх розподілу від нормального. Також на карті розмахів варіації (рис. 9) спостерігаємо 2 викиди (розмах п'ятої та одинадцятої вибірок вищий від верхньої контрольної межі).

Наведений на рис. 10 багатовимірний потік відображає всі сім потоків на одній карті. Дві точки перебувають поза контрольними межами, що характеризує нестабільність процесу.

Проаналізувавши результати моделювання процесів, що характеризують якість поставки вантажу, бачимо порушення їх стабільності. Аналіз інформації щодо точок, які містяться поза контрольними межами, засвідчив, що дні спостережень припадають на вихідні. Тому частина рахунків невчасно сплачується, що призводить до невчасної доставки вантажів.

Побудовані карти Хотеллінга T^2 вказують на те, що процес став статистично некерованим ще й з іншої причини. Найбільша кількість неопрацьованих заявок припадала на вихідні дні. Через очікування своєї черги на опрацювання заявок виникають затримки щодо оплати рахунків і вчасного перевезення вантажу. Це впливає не лише на якість перевезення, але й на репутацію компанії. Щоб усунути зазначені проблеми, компанія залучила до роботи співробітника для опрацювання таких заявок у вихідні. Після опрацювання заявок, які надійшли у вихідні, процес стабілізується (рис. 11–13).

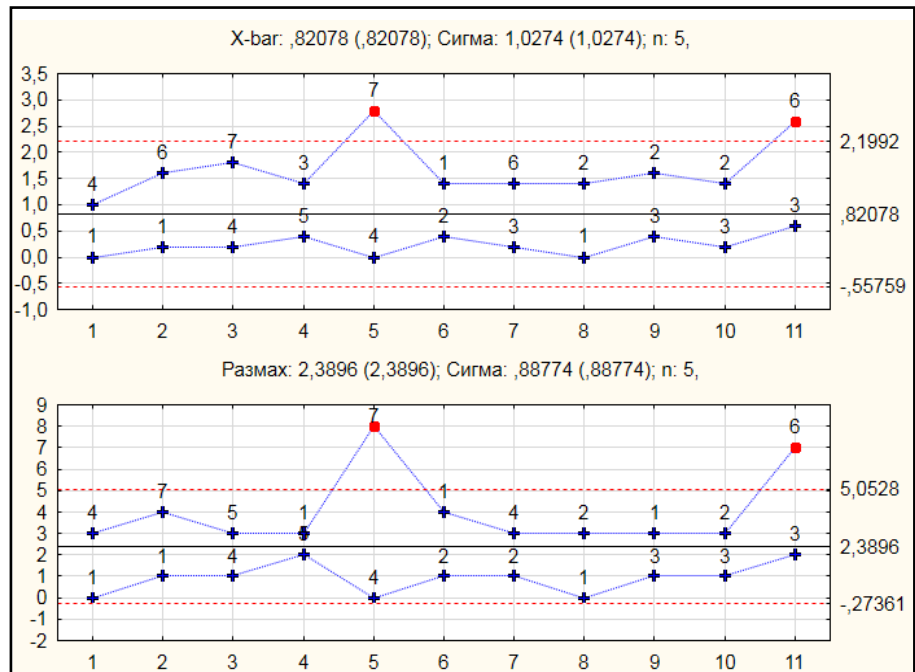


Рис. 10. Багатовимірний потік з X-bar і R-картами

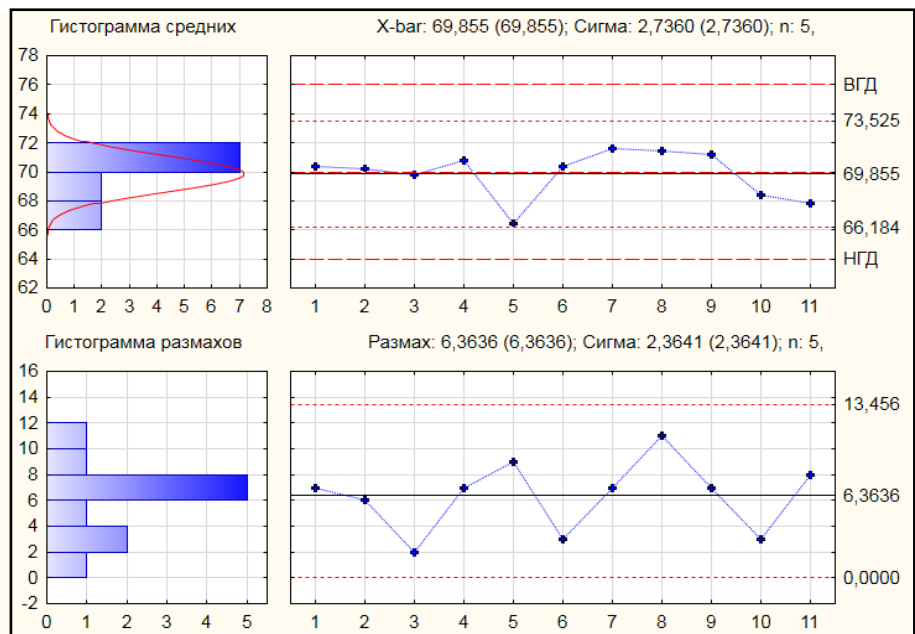


Рис. 11. Карти Шухарта для вдосконаленого процесу



Рис. 12. Карта Хотеллінга T² для окремих спостережень удосконаленого процесу

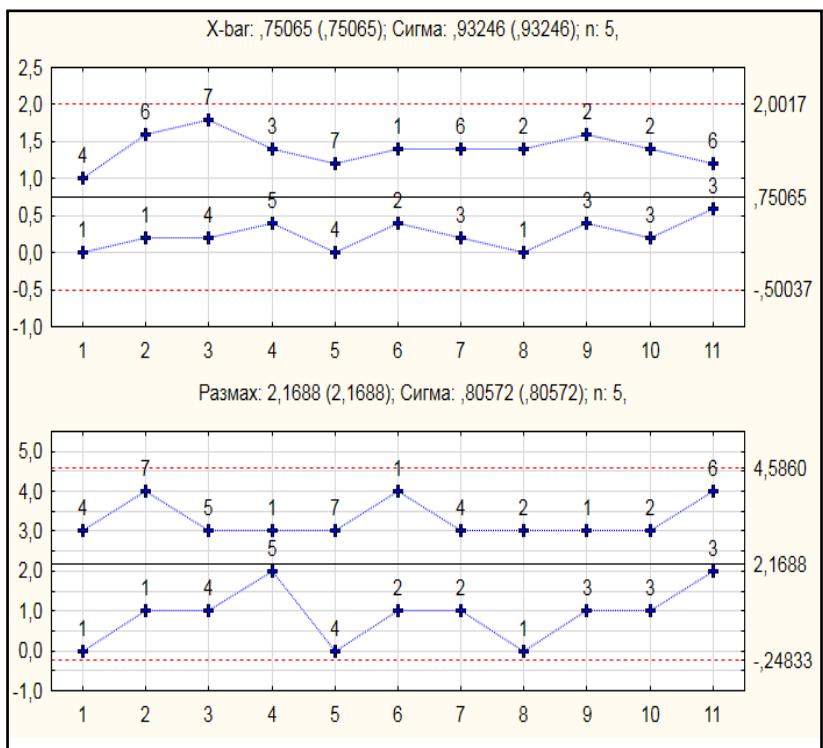


Рис. 13. Багатовимірний потік з X-bar та R-картами вдосконаленого процесу
Аналіз контрольних карт показує, що процес стає статистично стабільним.

Висновки з даного дослідження та перспективи подальших розвідок у даному напрямі. Сформовано двофазну модель для обґрунтування ефективних заходів управління якістю транспортно-логістичних процесів підприємства. Перша фаза передбачає впровадження та розвиток процесного підходу в організації. Супроводжувати бізнес на всіх етапах становлення та вдосконалення процесного підходу дозволяє BPMS-система, механізм постійного поліпшення процесів якої дає можливість розвивати модель управління в компанії. Застосування можливостей BPMS-системи дає можливість не лише збирати й упорядковувати статистичну інформацію за наявними бізнес-процесами, але й контролювати чітко їх виконання. Друга фаза ґрунтується на застосуванні процесного підходу та включає статистичне управління якістю процесів шляхом оцінки параметрів і їх моніторингу. Передбачається отримання інформації про варіацію процесу, досягнення стану його статистичної стабільності й одержання оцінок параметрів у цьому стані з подальшим контролюванням стабільності цих процесів.

Запропоновано алгоритм для виявлення нестабільних процесів підприємства й визначення шляхів їх стабілізації на основі статистичного управління показниками якості та вдосконалення транспортно-логістичних процесів за допомогою контрольних карт. В основу алгоритму покладено застосування механізму покращання процесів, який впливає на розвиток моделі управління підприємством на основі повного циклу Демінга (PDCA). Функція контролю – необхідний атрибут управління, який дає можливість виявити проблеми і скорегувати відповідно діяльність організації до того, як ці проблеми переростуть у кризу. Контроль здійснюється за допомогою попереднього аналізу виконуваних процесів.

Для статистичного управління процесами поставок логістичного підприємства проведено моделювання з використанням одного з головних модулів програмного пакета Statistica – промислова статистика та Шість сигм. На основі проведених розрахунків побудовано карти Шухарта середніх значень та розмахів варіації, карти багатовимірною потоку Хотеллінга T^2 . Моделювання із застосуванням контрольних карт дозволило виявити порушення стабільності процесів. На основі проведеного аналізу запропоновано шляхи стабілізації процесів поставок для вдосконалення діяльності логістичного підприємства.

Такий підхід сприятиме прийняттю ключових для успіху підприємства управлінських рішень. Результати можуть бути використані для подальших досліджень у напрямі вдосконалення якості роботи логістичних підприємств.

Список використаних джерел:

1. Чорний А. Ю., Захожай В. Б. Статистика якості. Київ : МАУП, 2011. 263 с.

-
2. *Єріна А. М.* Статистичне моделювання та прогнозування. Київ : КНЕУ, 2001. 172 с.
 3. *Беляев С. Ю., Забродин Ю. Н., Шапиро В. Д.* Управление качеством. Москва : Омега-Л, 2014. 381 с.
 4. *Глухов В. В., Гасюк Д. П.* Управление качеством : учебник. Москва : Омега-Л, 2005. 321 с.
 5. *Ефимов В. В., Барт Т. В.* Статистические методы в управлении качеством продукции. Москва : КНОРУС, 2006. 147 с.
 6. *Кане М. М., Иванов Б. В., Корешков В. Н., Схиртлатзе А. Г.* Системы, методы и инструменты менеджмента качества : учеб. пособие. Санкт-Петербург : Питер, 2008. 560 с.
 7. *Овчаренко Г. С., Рудківський О. А.* Управління ланцюгами постачання підприємства на основі системи SCM. Київ : КНЕУ, 2011. 145 с.
 8. *Костюк О. С.* Стратегічне управління ланцюгом поставок. Київ : МАУП, 2006. 56 с.
 9. *Шацька З. Я.* Управлінські інновації в системі підприємства // Актуальні проблеми економіки. 2012. № 1. С. 176–182.
 10. *Ігнат'єва І. А.* Стратегічний менеджмент. Київ : Каравелла, 2018. 464 с.
 11. Практический курс BPMN / сайт компанії ELMA. URL: https://www.elma-bpm.ru/journal/index.php?ELEMENT_ID=2900
 12. Сайт компанії ELMA. URL: <https://www.elma-bpm.ru>
 13. *Халіпова Н. В.* Щодо формування культури використання передових технологій управління компанією на основі автоматизованих бізнес-процесів // Формування сучасної моделі управління та підвищення якості менеджменту в системі вищої освіти : матеріали Міжнар. наук.-практ. конф. Дніпро: УМСФ, 2018. С. 224–226.
 14. *Исикава К.* Японские методы управления качеством. Москва : Экономика, 1988. 215 с.
 15. *Казинцев В. А.* Шесть Сигм в России. Методика снижения потерь, дефектов, издержек. Киев : Основа, 2009. 368 с.
 16. *Николаева Э. К.* Семь инструментов качества в японской экономике. Москва : Издательство стандартов, 1990. 88 с.
 17. *Бичківський Р. В., Столярчук П. Г., Сопільник Л. І., Каменський О. О.* Управління якістю. Сертифікація. Київ : Школа, 2005. 432 с.
 18. Контрольные карты. Контроль качества по непрерывному признаку / сайт Statistica. URL: <http://statistica.ru/local-portals/quality-control/kontrolnye-karty>
 19. Карты контроля качества / сайт StatSoft. URL: <http://statsoft.ru/home/textbook/modules/stquacon.html>

20. Боровиков В. П. *Statistica: искусство анализа данных на компьютере* / 2-е изд. Санкт-Петербург : Питер, 2003. 688 с.

21. Карты контроля качества. Многомерные карты / сайт StatSoft. URL: http://statsoft.ru/products/STATISTICA_QC/qcc.php

22. ДСТУ ISO 8258-2001. Статистичний контроль. Контрольні карти Шу-харта : національний стандарт України. URL: [http:// dnaop.com/html/34003/doc-ДСТУ_ISO_8258-2001](http://dnaop.com/html/34003/doc-ДСТУ_ISO_8258-2001)

References:

1. Chornyj A. Yu. and Zaxozhaj V. B. (2011), *Statystyka yakosti* [Quality statistics], Press MAUP, Kyiv, 263 p. [Ukraine].

2. Yerina A. M. (2001), *Statystychne modelyuvannya ta prohnozuvannya* [Statistical modeling and forecasting]. Press KNEU, Kyiv, 172 p. [Ukraine].

3. Belyaev S. Yu., Zabrodin Yu. N. and Shapiro V. D. (2014), *Upravlenie kachestvom* [Quality control], Press Omega-L, Moscow, 381 p. [Russia].

4. Gluhov V. V. and Gasyuk D. P. (2005), *Upravlenie kachestvom* [Quality control], Tutorial, Press Omega-L, Moscow, 321 p. [Russia].

5. Efimov V. V. and Bart T. V. (2006), *Statisticheskie metody v upravlenii kachestvom produkcii* [Statistical methods in product quality management], Press KNORUS, Moscow, 147 p. [Russia].

6. Kane M. M., Ivanov B. V., Koreshkov V. N. and Shirlatze A. G. (2008), *Sistemy, metody i instrumenty menedzhmenta kachestva* [Quality management systems, methods and tools], Tutorial, Press Piter, Sankt-Peterburg, 560 p. [Russia].

7. Ovcharenko G. S. and Rudkiv's'kyj O. A. (2011), *Upravlinnya lantsyuhamy postachannya pidpryyemstva na osnovi systemy SCM* [Management of the supply chain of the enterprise based on the SCM system], Press KNEU, Kyiv, 145 p. [Ukraine].

8. Kostyuk O. S. (2006), *Strategichne upravlinnya lancyugom postavok* [Strategic management of the supply chain], Press MAUP, Kyiv, 56 p. [Ukraine].

9. Shacz'ka Z. Ya. (2012), "Upravlinski innovatsiyi v systemi pidpryyemstva" ["Administrative innovations in the enterprise system"], journal *Aktual'ni problemy ekonomiky* [Current problems of the economy], vol. 1, pp. 176–182 [Ukraine].

10. Ignat'yeva I. A. (2018), *Strategichnyj menedzhment* [Strategic management], Press Karavella, Kyiv, 464 p. [Ukraine].

11. *Prakticheskij kurs BPMN* [BPMN practical course], ELMA company site, available at: https://www.elma-bpm.ru/journal/index.php?ELEMENT_ID=2900 [Russia].

12. Sajt kompanii ELMA, ELMA company site, available at: <https://www.elma-bpm.ru> [Russia].

13. Xalipova N. V. (2018), “*Shhodo formuvannya kultury vykorystannya peredovyx texnologij upravlinnya kompaniyeyu na osnovi avtomatyzovanyx biznes-procesiv*” [“Concerning the formation of the culture of using advanced technologies of company management on the basis of automated business processes”] // Materials of the International Practical Conference “*Formuvannya suchasnoyi modeli upravlinnya ta pidvyshhennya yakosti menedzhmentu v systemi vyshhoyi osvity*” [“Formation of a modern management model and improvement of management quality in the system of higher education”], Press UMSF, Dnipro, pp. 224–226 [Ukraine].

14. Isikava K. (1988), *Yaponskie metody upravleniya kachestvom* [Japanese quality management methods], Press Ekonomika, Moscow, 215 p. [Russia].

15. Kazincev V. A. (2009), *Shest' Sigm v Rossii. Metodika snizheniya poter', defektov, izderzhek* [Six Sigma in Russia. Methods of reducing losses, defects, costs], Press Osnova, Kyiv, 368 p. [Ukraine].

16. Nikolaeva Eh. K. (1990), *Sem' instrumentov kachestva v yaponskoj ehkonomike* [Seven quality tools in the Japanese economy], Press Izdatel'stvo standartov, Moscow, 88 p. [Russia].

17. Bychkivskiy R. V., Stoliarchuk P. H., Sopilnyk L. I. and Kalynskiy O. O. (2005), *Upravlinnya yakisty. Sertyfikaciya* [Quality management. Certification], Tutorial, Press Shkola, Kyiv, 432 p. [Ukraine].

18. *Kontrol'nye karty. Kontrol' kachestva po nepreryvnomu priznaku* [Control charts. Continuous quality control] / Statistica site, available at: <http://statistica.ru/local-portals/quality-control/kontrolnye-karty> [Russia].

19. *Karty kontrolya kachestva* [Quality control cards] / StatSoft site, available at: <http://statsoft.ru/home/textbook/modules/stquacon.html> [Russia].

20. Borovikov V. P. (2003), *Statistitica: iskusstvo analiza dannyh na komp'yutere* [Statistitica : art of analyzing data on a computer], Press Piter, Sankt-Peterburg, 688 p. [Russia].

21. *Karty kontrolya kachestva. Mnogomernye karty* [Quality control cards. Multidimensional maps] / StatSoft site, available at: http://statsoft.ru/products/STATISTICA_QC/qcc.php [Russia].

22. DSTU ISO 8258-2001. *Statystychnyj control'. Kontrol'ni karty Shuxarta : Nacional'nyj standart Ukrayiny* [DSTU ISO 8258-2001. Statistical control. Shukhart control Cards: National Standard of Ukraine], available at: http://dnaop.com/html/34003/doc-ДСТУ_ISO_8258-2001 [Ukraine].

DOI: <https://doi.org/10.32836/2521-6643-2018-1-56-5>

УДК 004.315

В. В. Антонюк, старший викладач кафедри комп'ютерних інтелектуальних систем та мереж Одеського національного політехнічного університету

М. О. Дрозд, кандидат технічних наук, старший викладач кафедри інформаційних систем Одеського національного політехнічного університету

О. В. Дрозд, доктор технічних наук, професор кафедри комп'ютерних інтелектуальних систем та мереж Одеського національного політехнічного університету

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

КОНТРОЛЕПРИДАТНІСТЬ FPGA-ПРОЕКТІВ ЗА РОЗСІЮВАНОЮ ПОТУЖНІСТЮ

Розглянуто розвиток контролепридатності схем для цифрових компонентів систем критичного застосування. Наголошено на важливості контролепридатності для забезпечення функціональної безпеки систем та їхніх компонентів у частині критичних додатків. Аргументовано потребу подальшого розвитку контролепридатності за межі логічної форми. Запропоновано розвиток контролепридатності цифрових компонентів за ознакою розсіюваної потужності. Отримано формулу для оцінювання контролепридатності схем за розсіюваною потужністю для FPGA-проектів. Проведено експерименти, виконано розрахунки контролепридатності схем за розсіюваною потужністю для матричних помножувачів, що імплементовані в FPGA-проекти.

Ключові слова: система критичного застосування; цифровий компонент; FPGA-проект; загальний сигнал; прихована несправність; контролепридатність; розсіювана потужність.

Рассмотрено развитие контролепригодности схем для цифровых компонентов систем критического применения. Отмечено важность контролепригодности для обеспечения функциональной безопасности систем и их компонентов в области критических приложений. Аргументована необхо-

© **В. В. Антонюк, М. О. Дрозд, О. В. Дрозд, Л. В. Кабак, 2018**

димось дальнейшего развития контролепригодности за пределы логической формы. Предлагается развитие контролепригодности цифровых компонентов по признаку рассеиваемой мощности. Получена формула для оценки контролепригодности схем по рассеиваемой мощности для FPGA-проектов. Проведены эксперименты и выполнены расчеты контролепригодности схем по рассеиваемой мощности для матричных умножителей, имплементированных в FPGA проекты.

Ключевые слова: система критического применения; цифровой компонент; FPGA-проект; общий сигнал; скрытая неисправность; контролепригодность; рассеиваемая мощность.

The issue is devoted to development of a checkability of the circuits for digital components of instrumentation and control safety-related systems, which operate objects of the increased risk, such as power grids and power plants, high-speed transport and aircraft. Importance of a checkability of the circuits for ensuring functional safety of systems and their components in the field of critical applications where the operating mode is divided into normal and an emergency is noted. In these conditions, there is a problem of the hidden faults which can be accumulated throughout the long normal mode and reduce fault tolerance of schemes in the most responsible emergency operation. The most studied logical form of a checkability of the digital circuits determines efficiency of on-line testing of the digital components. Need of further development of a checkability of the circuits out of limits of its logical form as it does not solve a problem of the common signals, such as signals of reset and synchronization signals is shown. The faults arising in chains of the common signals can remain hidden, by blocking schemes of on-line testing is able which demonstrates the correct functioning of on-line testing means. For the solution of this problem, development of a checkability of the digital components on the basis of the power-dissipation is offered. The formula for analytical assessment of a checkability of the circuits by the power-dissipation for FPGA projects is received. The experiments directed to studying of a checkability of the digital circuits by the power-dissipation for the iterative array multipliers implemented in FPGA projects with the help of a CAD of Quartus Prime 17.1 Lite Edition (Intel of FPGA) are made. By means of the PowerPlay Power Analyzer utility, values of the power-dissipation for all FPGA project and for its input/output system and also dynamic and static components of the power-dissipation in core are received. On these data obtained at various activity of the input signals, calculations of a checkability of the circuits for the power-dissipation of iterative array multipliers with various word size from 16 to 64 bits are executed.

Key words: critical application system; digital component; FPGA-project; common signal; hidden fault; checkability; power-dissipation.

Постановка проблеми. Системи критичного застосування – це розвиток комп’ютерних систем у напрямі керування об’єктами підвищеного ризику, до яких належать енергомережі, електростанції, швидкісний наземний і повітряний транспорт тощо [1; 2]. Керування спрямоване на забезпечення функціональної безпеки та системи, а також об’єкта для запобігання виникненню аварій і зниження їхніх наслідків. Удосконалення об’єктів за потужністю спричиняє їхнє ускладнення, а зростання потужності разом зі складністю та кількістю підвищують критичність очікуваних наслідків аварій. За таких обставин стримування ризиків потребує зниження ймовірності виникнення аварій, що стосується насамперед виконання вимог міжнародних стандартів щодо систем критичного застосування.

За цими стандартами основою в забезпеченні функціональної безпеки систем критичного застосування визначається використання відмовостійких рішень, що поширюються і на систему, і на її компоненти. Утім, на практиці використання відмовостійких рішень не дає повної впевненості щодо забезпечення функціональної безпеки, це засвідчує наявність імітаційних режимів, які для перевірки системи відтворюють умови аварії, що не раз призводили до аварійних наслідків.

Дійсно, системи критичного застосування не гарантують і не можуть гарантувати функціональну безпеку ані власну, ані об’єктів керування лише за рахунок відмовостійких рішень. Такі рішення стануть достатніми тільки для контролепридатних систем та їхніх компонентів, оскільки за браку контролепридатності кількість відмов завжди може перевищити закладену відмовостійкість рішення. Використання небезпечних імітаційних режимів вказує на наявність проблеми недостатньої контролепридатності систем критичного застосування та їхніх компонентів і потребу проведення досліджень у напрямі її підвищення.

Аналіз останніх досліджень і публікацій. Особливістю систем критичного застосування є їхня дворежимність: вони проектуються для роботи в нормальному й аварійному режимах. Вимоги до функціональної безпеки систем критичного застосування регламентуються стандартом ІЕС 61508 щодо електричних, електронних і програмованих компонентів [3]. Він є базовим для стандартів з функціональної безпеки у різних галузях, зокрема EN 50126 для залізничного транспорту й ІЕС 61513 для атомних електростанцій [4; 5].

Зазвичай контролепридатність розуміють як її логічну форму, тобто придатність до виявлення несправностей за помилками результату. Контролепридатність цифрових схем у тестовому режимі – тестопридатність, тобто придатність схем до написання для них тестів з виявлення несправностей. Вона структурна, бо повністю визначається самою схемою. В робочому режимі контролепридатність стає структурно-функціональною, оскільки залежить також від вхідних даних. У системах критичного застосування цифрові

компоненти працюють у нормальному та аварійному режимах зазвичай на різних вхідних даних. Це робить структурно-функціональну контролепридатність також дворежимною, тобто різною в нормальному та аварійному режимах [6]. Як наслідок, виникає проблема прихованих несправностей, що можуть накопичуватись упродовж довготривалого нормального режиму та виявляться в аварійному режимі зниженням відмовостійкості схемних рішень [7].

На практиці проблема прихованих несправностей розв'язується шляхом використання небезпечних імітаційних режимів, що вже мають певну історію несанкціонованого втручання людського фактора, та несправністю [8]. Імітація аварійних умов, як правило, потребує блокування засобів аварійного захисту, що стало однією з причин Чорнобильської катастрофи.

Для розв'язання проблеми прихованих несправностей запропоновано методи підвищення контролепридатності цифрових компонентів у нормальному режимі та вирівнювання контролепридатності обох режимів, що має певні наслідки [9]. Водночас обмеження розвитку контролепридатності схем тільки її логічною формою стикається з проблемами робочого діагностування, можливості якого вона визначає. До таких проблем належить проблема загальних сигналів, зокрема сигналів скидання та синхронізації. Загальні сигнали можуть блокувати не тільки роботу цифрових компонентів, але й засобів робочого діагностування, причому у стані, що ідентифікує правильне функціонування схем. Ці несправності також можна зарахувати до множини прихованих, однак їхньою особливістю є прихованість у виявленому стані.

На контролепридатність схем також суттєво впливають особливості цифрових компонентів. Високі технології, що задіяні в критичних ділянках застосування, визначають для їхньої розробки сучасні системи проектування, зокрема проектування на FPGA (Field Programmable Gate Array) [10; 11].

Мета статті – розвиток контролепридатності компонентів за межі її логічної форми на підставі можливостей, які надаються FPGA-проектуванням і можуть слугувати для оцінювання придатності схеми до контролю за розсіюваною потужністю. Запропоновано низку експериментів з FPGA-проектами щодо визначення їхньої контролепридатності за потужністю, що має ними розсіюватися за правильного функціонування.

Виклад основного матеріалу. Контролепридатність схеми за розсіюваною потужністю можна визначити відношенням обсягів діапазонів значень розсіюваної потужності за межами можливого за умов правильного функціонування до загального обсягу, що включає можливі та неможливі значення. Діапазон можливих значень виокремлює в загальному діапазоні два діапазони неможливих значень: нижній (від нуля до мінімального можливого значення) та верхній (від максимального можливого значення до межі вимірювання). Для цих діапазонів неможливих значень відповідно визначається нижня та верхня контролепридатність схеми.

Нижня контролепридатність корисна для виявлення несправностей, що значно зменшують розсіювану потужність, наприклад, призводять до блокування тактових сигналів, а верхня контролепридатність – навпаки, суттєво збільшує розсіювану потужність, що може трапитись за умови короткого замикання.

Далі розглядається нижня контролепридатність, яка дає можливість виявляти несправності, що спотворюють загальні сигнали, внаслідок чого зменшується динамічний складник розсіюваної потужності. Тому нижню контролепридатність можна визначити за мінімальним відношенням обсягів діапазонів мінімального $N_{D\text{MIN}}$ і максимального $N_{D\text{MAX}}$ значень динамічного складника розсіюваної потужності, тобто за такою формулою: $K_H = \text{MIN}(N_{D\text{MIN}} / N_{D\text{MAX}})$.

Контролепридатність K_H схеми залежить від умов її проектування. Розглянуто систему автоматизованого проектування Quartus Prime 17.1 Lite Edition від Intel FPGA [12].

Для моделювання параметрів енергоспоживання та розсіюваної потужності використовується утиліта PowerPlay Power Analyzer, що входить до складу Quartus Prime [13].

Контролепридатність K_H визначається для схем матричних помножувачів двійкових чисел за результатами моделювання, що проводилось на FPGA Intel Max 10 10M50DAF672I7G. У цій програмованій логічній інтегральній схемі (ПЛІС) розміщено 288 9-бітних апаратних блоків множення, котрі, крім власних помножувачів, містять буферні вхідні регістри операндів і вихідний регістр результату [14].

Апаратні блоки множення в Quartus Prime проектуються на основі інтелектуального модуля (Intellectual Property Core – IP-Core) помножувача LPM_MULT із бібліотеки параметризованих модулів (Library of Parameterized modules – LPM), що постачається разом із Quartus Prime [15].

Під час введення IP-Core до проекту майстер налаштування дає можливість задати основні характеристики помножувача (розрядність операндів, знакова або беззнакова операція, наявність або брак буферизації операндів і результату), що відповідають характеристикам убудованих блоків множення.

У результаті моделювання оцінюються значення загальної розсіюваної потужності ПЛІС N , системи введення/виведення N_{IO} , а також динамічного N_D і статичного N_S складників ядра ПЛІС.

Оскільки контролепридатність визначається через посередників, слід зважати на похибки вимірювання й оцінювання. Для утиліти PowerPlay Power Analyzer похибки оцінювання становлять 5 % в один бік зменшення, або збільшення – 2,5 %. Теплові датчики також працюють на рівні похибки 5 %. Тоді мінімальне значення знаходимо за формулою:

$$N_{D\text{MIN}} = N_D - 0.025 N_D.$$

Максимальне значення $N_{D\text{MAX}}$ визначається за вимірюванням N загальної розсіюваної потужності ПЛІС під час розрахунку оцінених значень розсіюваної потужності системи введення/виведення N_{IO} , а також статичного складника ядра N_S та їхніх похибок за формулою:

$$N_{D\text{MAX}} = N - N_{IO} - N_S + 0.025 N + 0.025 N_{IO} + 0.025 N_S,$$

або за умови, що $N - N_{IO} - N_S = N_D$,

$$N_{D\text{MAX}} = N_D + 0.025 N + 0.025 N_{IO} + 0.025 N_S.$$

Для знаходження мінімального значення $\text{MIN}(N_{D\text{MIN}}/N_{D\text{MAX}})$ необхідно зважати на коливання значень $N_{D\text{MIN}}$ і $N_{D\text{MAX}}$ залежно від активності сигналів, які подаються на входи до схеми, тобто моделювання слід виконувати за різної активності вхідних сигналів і далі обрати результати з мінімальним значенням обчисленої контролепридатності.

У ході експериментів було реалізовано FPGA-проекти знакових помножувачів із регістрами операндів і результату та розрядністю $n = 16, 32, 48, 64$. За допомогою утиліти PowerPlay Power Analyzer активність A вхідних сигналів задавалася від 0 до 100 % щодо сигналу синхронізації регістрів помножувача з кроком збільшення на 12,5 %.

Результати моделювання та розрахунку контролепридатності помножувачів подано в табл. 1–4 відповідно, якщо n – від 16 до 64 бітів.

Таблиця 1

Результати оцінювання контролепридатності помножувача, $n = 16$

$A, \%$	N_D, mW	N_S, mW	N_{IO}, mW	N, mW	$K_H, \%$
0	7,62	89,94	73,07	170,63	46,55
12,5	8,46	89,95	74,42	172,83	48,84
25	9,31	89,95	75,76	175,02	50,91
37,5	10,15	89,96	77,11	177,22	52,76
50	10,99	89,96	78,46	179,41	54,43
62,5	11,83	89,97	79,81	181,61	55,95
75	12,67	89,98	81,16	183,80	57,34
87,5	13,51	89,98	82,50	186,00	58,62
100	14,36	89,99	83,85	188,19	59,81

Таблиця 2

Результати оцінювання контролепридатності помножувача, $n = 32$

$A, \%$	N_D, mW	N_S, mW	N_{IO}, mW	N, mW	$K_H, \%$
0	15,83	90,17	153,70	259,71	54,31
12,5	19,04	90,19	156,40	265,63	58.29
25	22,25	90,21	159,10	271,55	61.51
37,5	25,45	90,22	161,79	277,47	64.14
50	28,66	90,24	164,49	283,38	66.35
62,5	31,86	90,25	167,18	289,30	68.23
75	35,07	90,27	169,88	295,22	69.85
87,5	38,27	90,28	172,58	301,14	71.25
100	41,48	90,30	175,27	307,05	72.48

Таблиця 3

Результати оцінювання контролепридатності помножувача, $n = 48$

$A, \%$	N_D, mW	N_S, mW	N_{IO}, mW	N, mW	$K_H, \%$
0	35,38	90,42	225,95	351,75	66,23
12,5	41,49	90,45	230,00	361,93	69.09
25	47,59	90,47	234,04	372,11	71.38
37,5	53,70	90,50	238,08	382,29	73.26
50	59,81	90,53	242,13	392,47	74.82
62,5	65,91	90,56	246,17	402,64	76.15
75	72,02	90,58	250,22	412,82	77.28
87,5	78,13	90,61	254,26	423,00	78.27
100	84,23	90,64	258,31	433,18	79.13

Таблиця 4

Результати оцінювання контролепридатності помножувача, $n = 64$

$A, \%$	N_D, mW	N_S, mW	N_{IO}, mW	N, mW	$K_H, \%$
0	64,97	90,69	297,99	453,66	73,63
12,5	76,04	90,74	303,38	470,16	75.93
25	87,10	90,78	308,77	486,66	77.73
37,5	98,16	90,83	314,17	503,16	79.18
50	109,23	90,87	319,56	519,66	80.39
62,5	120,29	90,92	324,95	536,16	81.40
75	131,35	90,96	330,34	552,66	82.25
87,5	142,41	91,01	335,74	569,16	82.99
100	153,48	91,05	341,13	585,66	83.63

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Контролепридатність цифрових компонентів систем критичного застосування – необхідний складник для забезпечення функціональної безпеки не тільки системи, але й об'єкта управління.

Розвиток моделей контролепридатності в її логічній формі від тестопридатності до структурно-функціональної та дворежимної сприяв усвідомленню проблеми прихованих несправностей і визначенню шляхів її розв'язання, покращивши ефективність робочого діагностування цифрових схем.

Водночас логічна форма контролепридатності обмежена у виявленні несправностей загальних сигналів, що можуть блокувати роботу засобів робочого діагностування у стані індикації правильного функціонування. Це потребує розвитку контролепридатності схем в інших формах, зокрема енергетичного складника, за яким найбільш забезпечені засоби (температурні датчики) – це придатність до контролю тепловиділення шляхом вимірювання розсіюваної потужності.

Оцінювання контролепридатності схем за розсіюваною потужністю, проведене для FPGA-проектів з урахуванням сучасних викликів, мають подальший розвиток щодо елементної бази ПЛІС у розробці цифрових компонентів систем критичного застосування.

Експерименти з оцінювання контролепридатності схем за розсіюваною потужністю здійснено на системі автоматизованого проектування Quartus Prime 17.1 Lite Edition (Intel FPGA) з використанням інтелектуального модуля LPM_MULT для низки значень розрядності матричних помножувачів і рівнів активності вхідних сигналів схеми.

Результати моделювання визначили вихідні дані для розрахунку контролепридатності, а саме: значення загальної розсіюваної потужності ПЛІС, її системи введення/виведення та динамічного N_D і статичного N_S складників ядра.

За отриманими результатами контролепридатність схеми оцінюється за мінімальним відношенням мінімального та максимального значень динамічного складника розсіюваної потужності ПЛІС, що визначаються, зважаючи на похибки вимірювання та оцінювання вихідних даних для різних рівнів активності вхідних сигналів.

Обчислені оцінки контролепридатності засвідчують досить високий рівень, який зростає зі збільшенням розрядності помножувачів та активності вхідних сигналів, тобто мінімальні значення контролепридатності відповідають найменшій (нульовій) активності вхідних сигналів, що для розрядності 16, 32, 48 і 64 становить відповідно 46,55 %, 54,31 %, 66,23 % та

73,63 %. Рекомендований рівень активності вхідних сигналів 12,5 % створює для вказаної розрядності матричних помножувачів резерв контролепридатності у 2,29 %, 3,98 %, 2,86 % та 2,30 % відповідно.

Подальші дослідження доцільно спрямувати на розвиток і використання нових форм контролепридатності схем з метою підвищення функціональної безпеки систем критичного застосування.

Список використаних джерел:

1. *Kharchenko V., Gorbenko A., Sklyar V., Phillips C.* Green Computing and Communications in Critical Application Domains: Challenges and Solutions // Digital Technologies: Proceedings of the 9th International Conference, Zhilina, Slovak Republic. 2013. P. 191–197.
2. *Brezhnev E., Kharchenko V.* Approach for formalization of influences in critical infrastructure // Critical Infrastructure Safety and Security (CrISSDESSERT): proceedings of I Int. Workshop, Kirovograd (Ukraine), 10–11 May. 2011. Kirovograd. 2011. P. 216–226.
3. IEC 61508-1:2010. Functional safety of electrical / electronic / programmable electronic safety related systems. Part 1: General requirements. Geneva: International Electrotechnical Commission. 2010.
4. EN 50126 / IEC 62278. Quick Guide to safety Management based on EN 50126 / IEC 62278 // Blogspot. 2008. URL: <http://en50126.blogspot.com>
5. IEC 61513:2001. Nuclear power plants – Instrumentation and control systems important to safety – General requirements for systems. Geneva: International Electrotechnical Commission. 2001.
6. *Drozd M., Drozd A., Kharchenko V., Antoshchuk S., Sulima J.* Checkability of the digital components in safety-critical systems: problems and solutions // IEEE East-West Design & Test: Proceedings of the IEEE Symposium, Sevastopol, Ukraine. 2011. P. 411–416.
7. *Drozd M., Drozd A.* Safety-Related Instrumentation and Control Systems and a Problem of the Hidden Faults // Digital Technologies : Proceedings of the 10th International Conference, Zhilina, Slovak Republic. 2014. P. 137–140.
8. *Gillis D.* The apocalypses that might have been // DAMN Interesting. 2007. № 298. URL: <http://www.popmech.ru/go.php?url=http%3A%2F%2Fwww.damninteresting.com%2F%3Fp%3D913>
9. Evolution of a Problem of the Hidden Faults in the Digital Components of Safety-Related Systems / *Drozd A., Kuznietsov M., Antoshchuk S., Martynyuk A., Drozd M., Sulima J.* // East-West Design & Test : Proceedings of the 16th IEEE Symposium. P. 1–5. 2018. DOI: 10.1109/EWDTS. 2018.8524806.

10. *Kharchenko V. S., Sklyar V. V. (edits) FPGA-based NPP I&C Systems: Development and Safety Assessment.* Kharkiv. RPC Radiy, National Aerospace University “KhAI”, SSTC on Nuclear and Radiation Safety. 2008. 188 p.

11. *Kharchenko V. S., Siora A. A., Bakhmach E. S. Diversity-Scalable Decisions for FPGA-based Safety-Critical I&Cs: from Theory to Implementation // Sixth ANS International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPI-HMIT 2009) April 5–9. 2009. Knoxville, Tennessee, USA.*

12. Intel Quartus Prime Standard Edition User Guide: Getting Started. URL: <https://www.intel.com/content/www/us/en/programmable/documentation/yoq1529444104707.html>

13. Intel Quartus Prime Standard Edition User Guide: Power Analysis and Optimization. URL: <https://www.intel.com/content/www/us/en/programmable/documentation/xhv1529966780595.html>

14. MAX 10 FPGA Device Architecture. URL: <https://www.intel.com/content/www/us/en/programmable/documentation/sss1397439908414.html>

15. Intel FPGA Integer Arithmetic IP Cores User Guide. URL: <https://www.intel.com/content/www/us/en/programmable/documentation/sam1395330298052.html>

References:

1. Kharchenko V., Gorbenko A., Sklyar V. and Phillips C. (2013), “Green Computing and Communications in Critical Application Domains: Challenges and Solutions” // *Digital Technologies: Proceedings of the 9th International Conference, Zhilina*, pp. 191–197 [Slovak Republic].

2. Brezhnev E. and Kharchenko V. (2011), Approach for formalization of influences in critical infrastructure // *Critical Infrastructure Safety and Security (CrISSDESSERT): proceedings of I Int. Workshop, Kirovograd, 10–11 May, Kirovograd*, pp. 216–226 [Ukraine].

3. IEC 61508-1:2010 (2010), Functional safety of electrical / electronic / programmable electronic safety related systems. Part 1: General requirements. Geneva: International Electrotechnical Commission.

4. EN 50126 / IEC 62278 (2008), Quick Guide to safety Management based on EN 50126 / IEC 62278 // Blogspot, available at: <http://en50126.blogspot.com>

5. IEC 61513:2001 (2001), Nuclear power plants – Instrumentation and control systems important to safety – General requirements for systems. Geneva: International Electrotechnical Commission.

6. Drozd M., Drozd A., Kharchenko V., Antoshchuk S. and Sulima J. (2011), “Checkability of the digital components in safety-critical systems: prob-

lems and solutions” // IEEE East-West Design & Test: Proceedings of the IEEE Symposium, Sevastopol, pp. 411–416 [Ukraine].

7. Drozd M. and Drozd A. (2014), “Safety-Related Instrumentation and Control Systems and a Problem of the Hidden Faults” // Digital Technologies: Proceedings of the 10th International Conference, Zhilina, pp. 137–140 [Slovak Republic].

8. Gillis D. (2007), The apocalypses that might have been // DAMN Interesting, vol. 298, available at: <http://www.popmech.ru/go.php?url=http%3A%2F%2Fwww.damninteresting.com%2F%3Fp%3D913>

9. Drozd A., Kuznietsov M., Antoshchuk S., Martynyuk A., Drozd M. and Sulima J. (2018), “Evolution of a Problem of the Hidden Faults in the Digital Components of Safety-Related Systems” // East-West Design & Test: Proceedings of the 16th IEEE Symposium, pp. 1–5, DOI: 10.1109/EWDTS.2018.8524806

10. Kharchenko V. S., Sklyar V. V. (edits) (2008), FPGA-based NPP I&C Systems: Development and Safety Assessment. RPC Radiy, National Aerospace University “KhAI”, SSTC on Nuclear and Radiation Safety, Kharkiv, 188 p. [Ukraine].

11. Kharchenko V. S., Siora A. A. and Bakhmach E. S. (2009), “Diversity-Scalable Decisions for FPGA-based Safety-Critical I&Cs: from Theory to Implementation” // Sixth ANS International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPI-HMIT 2009) April 5–9, Knoxville, Tennessee [USA].

12. Intel Quartus Prime Standard Edition User Guide: Getting Started, available at: <https://www.intel.com/content/www/us/en/programmable/documentation/yoq1529444104707.html>

13. Intel Quartus Prime Standard Edition User Guide: Power Analysis and Optimization, available at: <https://www.intel.com/content/www/us/en/programmable/documentation/xhv1529966780595.html>

14. MAX 10 FPGA Device Architecture, available at: <https://www.intel.com/content/www/us/en/programmable/documentation/sss1397439908414.html>

15. Intel FPGA Integer Arithmetic IP Cores User Guide, available at: <https://www.intel.com/content/www/us/en/programmable/documentation/sam1395330298052.html>

DOI: <https://doi.org/10.32836/2521-6643-2018-1-56-6>

UDC 004.386

V. O. Yakovenko, Doctor of Technical Sciences, Professor of the Department of Information Systems and Technologies, University of Customs and Finance
Yu. V. Ulianova, Ph.D. of Technical Sciences, Associated Professor of the Department of Information Systems and Technologies, University of Customs and Finance
O. O. Kaliaka, Student of the University of Customs and Finance

SOFTWARE IMPLEMENTATION OF NEURAL NETWORK TECHNOLOGIES FOR AUTOMATED TEXTUAL INFORMATION CLASSIFICATION

The results of the analysis of the state of highways suitable for the organization of high-speed traffic on the route Kyiv-Dnipro are presented, and the main directions of its implementation are identified. The calculations of 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 intensification of 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: *neural network; perceptron; text classification.*

Розглянуто завдання створення нейронної мережі для розпізнання та класифікації текстових документів. Проведено дослідження наявних моделей нейронних мереж і методів векторного подання тексту. Виявлено переваги та недоліки досліджуваних алгоритмів. Результатом дослідження є розроблений оригінальний алгоритм класифікації текстів із використанням технологій нейронних мереж на основі перцептрона, який можна навчати методом зворотного поширення помилки. На основі запропонованого авторами алгоритму розроблено програмний додаток та проведено апробацію розробленого алгоритму.

Ключові слова: *нейронна мережа; перцептрон; класифікація текстів.*

© V. O. Yakovenko, Yu. V. Ulianova, O. O. Kaliaka, 2018

Рассмотрено решение задачи создания нейронной сети для распознавания и классификации текстовых документов. Было проведено исследование существующих моделей нейронных сетей и методов векторного представления текста. Определены преимущества и недостатки исследуемых алгоритмов. Результатом работы является алгоритм классификации текстов с использованием технологий нейронных сетей на основе перцептрона, который можно обучать методом обратного распространения ошибки. На основе предложенного авторами алгоритма было разработано программное приложение и проведено апробацию предложенного алгоритма.

Ключевые слова: *нейронная сеть; перцептрон; классификация текстов.*

Problem formulation. The use and improvement of computer technologies opens up a range of new features to humankind, but along with this there are a number of other problems associated with the growth of processed arrays of text documents. During work with full-text databases a problem of documents searching and classification according to their content appears. Classification of documents can be regarded as one of the tasks of informational search, which consists of enrolling document in one of several categories based on its content.

There are following tasks of the classification: creation of thematic directories, spam filtering, electronic document management systems, tagging, automatic text translation [1]. Text document classification is a well known theme in the field of the information retrieval and text mining. Selection of most desired features in the text document plays a vital role in classification problem [2]. That is why the task of developing an algorithm of textual information classification in order to improve informational search in view of modern requirements for classification and characteristics of text data arrays is relevant.

Analysis of recent researches and publications. In order to solve this problem [3] there was considered the most popular classification methods such as: classification using the decision tree, the Bayesian classification method, support-vector machine method, k-nearest neighbours algorithm and the artificial neural network (NN). The support-vector machine method is a reference algorithm in terms of the quality of the classification. In traditional text classification, a document is represented as a bag of words where the words in other words terms are cut from their finer context i.e. their location in a sentence or in a document. Only the broader context of document is used with some type of term frequency information in the vector space. Consequently, semantics of words that can be inferred from the finer context of its location in a sentence and its relations with neighbouring words are usually ignored [4]. However, its main disadvantage is speed. Training requires a significant amount of memory and expenses of machine time.

The advantages of classifying using the decision tree are that the constructed tree is easy to analyze and the result of the algorithm can be interpreted visually. The disadvantages of the algorithm include the fact that constructing decision trees gives the same weight to “positive” and “negative” branching in the nodes. A large number of “negative” branches in the description of the rubric can lead to hard-to-interpret rules and re-learning of the classification algorithm. The main feature in the k-nearest neighbours method is the absence of a learning process. This method focuses on more similar to the analyzed text from the collection during classification. The main disadvantage of the algorithm is the low speed of classification.

The Bayes Classification method provides ease of implementation and low computing costs for training and classification [3; 5; 6]. However, this method has a significant disadvantage such as low quality of classification in the most real tasks [3]. In addition, performance depends on the accuracy of the estimated conditional probable conditions. Sometimes it's difficult to estimate accurately, especially when there is a lack of training data. That is why in paper [5] it is proposed to transform the probability estimation problem into an optimization problem and use three methodological approaches to solve it.

Over the past few years, neural networks have re-emerged as powerful machine-learning models, yielding state-of-the-art results in fields such as image recognition and speech processing. More recently, neural network models started to be applied also to textual natural language signals, again with very promising results [7]. An artificial neural network is an adaptive system that consists of a group of connected artificial neurons. Neural networks have high accuracy in processing both linear and nonlinear samples, but classification decision-making is difficult to formalize due to the nature of the neural networks organization and represent a non-trivial task, taking into account scalability with limited computing resources [2; 3].

As a result of analysis of classification methods, the neural network was selected. The neural network compared to other methods of classification has the greatest accuracy, but requires high computing power.

Purpose of the article is to develop automated analytical system for analysis of prepared arrays of text information documents using neural networks and their classification by categories.

Main material. An artificial (mathematical) neuron performs the transformation of the input signals vector, as follows [8]:

$$y = I(S); S = \sum w_i x_i, \quad (1)$$

where w_i – is the weight vector of the neuron (the weight of the synaptic bonds);
S – the result of the weighted summation;
I – neuron activation function.

Functionality of a neuron is simple, therefore, neurons are united in the network for solving specific problems. Training a neural network is reduced to the selection of the weight coefficients of each neuron provided that the network topology is chosen and activation function is selected.

There are the main types of classifying neural networks such as: singlelayer and multilayer perceptron, Gaussian neural classifier, Kohonen network, integrated distribution network, cascade network [9]. Perceptron is a neural network of direct distribution, the principle is transmission of the signal through N additional hidden layers to the output. Each node in the network is connected by M-number of scales from the previous layer. This creates the associations between the input and the output layers. In the classification tasks perceptron shows good accuracy but it depends on the number of layers in the network. Perceptron is a time-tested very flexible tool for solving many tasks.

Kohonen neural network differs from the perceptron in that there used unsupervised learning as learning method. Learning data is consist of only input variables and doesn't have relevant output values. It is using access threshold to solve classification problems with Kohonen networks, it plays the role of the maximum distance where the recognition takes place. If the activation level has "won" neuron that exceeds this threshold, then considered that the system did not make decisions [10].

Convolutional neural network was initially not purposed to work with text information and was used to "computer vision". This network, like perceptron, is network of direct distribution. The main feature of this network is the convolutional layers which may be many. The convolution operation is the multiplication of the input signal into a small matrix of weights and summation the results. The result is a map of signs. This method is very effective in classification tasks [11].

After selecting the type of neural network, the objective was to select an activation function. To the role of the activation function of the neural network were considered sigmoidal function and hyperbolic tangent [8; 9].

Sigmoid function is an S-shaped, continuously differentiated, monotone increasing function that can take values from 0 to 1. Sigmoid function (2) has the ability to amplify weak signals better than strong and prevents saturation from large signals.

$$f(x) = \frac{1}{1+e^{-x}}. \quad (2)$$

Another widely used activation function is the hyperbolic tangent. By form it is similar to the sigmoid function and is often used by biologists as a mathematical model of the nerve cell activation [12]. It can take values from -1 to 1.

As an activation function of the artificial neural network, it has the form given in the expression (3):

$$f(x) = \frac{e^{2x} - 1}{e^{2x} + 1}. \quad (3)$$

Solution. Finally the perceptron was chosen as a result of analysis of neural networks. All considered networks have good classification accuracy, but the perceptron is simpler and more flexible in setting up.

A sigmoid function was selected as an activation function in the neural network. Compared to a hyperbolic tangent, it can take less values, but for the task of classification this will be enough. Also, the derivative of the sigmoid function is easier to find and easier to program.

As a result of modeling was created the network, shown at fig. 1:

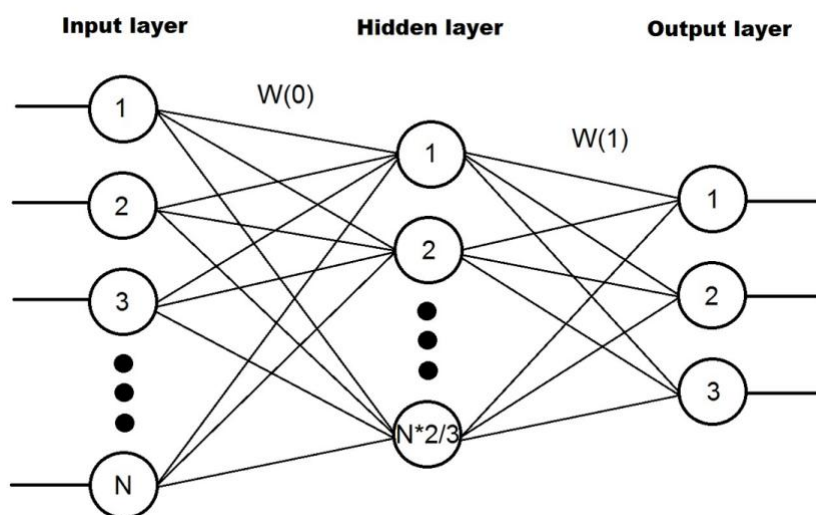


Fig. 1. Model of created neural network

In the developed model of neural network there are 3 layers of neurons: input, hidden and output.

The first two layers are dynamic, that means that they change the number of neurons depending on the size of input vector. The hidden layer is setting up depending on the input vector in the proportion of 2: 3. This gives to the neural network some flexibility and adaptability.

The output layer has a fixed number of neurons of 3, but may be changed depending on the needs of the user. Neuronal network with 3 output neurons can

takes up to 8 different results, but to facilitate learning in the developed model, each output neuron corresponds to separate classification category.

There are following steps to thoroughly make out the algorithm of recognizing the text as:

1. Create a dictionary.
2. Neural network training.
3. Documents recognition and information output.

Let's check described steps more detailed. Creating a dictionary is necessary for network training and text recognition and is one of the most important parts of both algorithm and subsequent program realization. Excel was chosen as the basis for the dictionary, there are several reasons for this:

- easy to edit;
- ability to use without installing special software;
- Ease of recovery.

The algorithm of creating a dictionary is down below:

- first you need to select and open the document that was chosen as the basis for the dictionary in the program;

- after loading the document is split into separate words, punctuation marks and duplicates are deleted and the obtained array of words are copied into an array of type `List <string>`.

- `<string>` array is copied to MS Excel document which is creating using the `Microsoft.Office.Interop.Excel` namespace.

If it is need, the created document can be edited and supplemented with new words.

To create the input signal vector it is necessary to convert it into a signal. N-gram was used as a conversion method, on the basis of which the dictionary was created. Statistical n-gram language models (LM) have been used successfully for speech recognition and many other applications/ they compute the probability of the nth word by conditioning on the previous n-1 history (h) words. They suffer from the shortage of long-range information, which limits performance. To capture the long-range information. One of the earliest attempts was a cache-based LM that took advantage that a word observed earlier in a document could occur again [13]. The dictionary is manually created previously, or it can automatically be create by program (you need to upload document with data). For productivity, it's necessary to use similar subjects documents with analyzed texts. The uploaded document is split into separate words, the repetitions and symbols removes. The next step is to copy data into a document that can be edited manually.

During the program execution, the documents that will be classified will be compared with this dictionary, and as a result, document vector will be created (fig. 2).

```

class Vector
{
    ССЫЛОК: 2
    public int[] VectorBuilder(string docName, List<string> dictionary)
    {
        int[] vector = new int[dictionary.Count];
        string fi = null;
        Word.Application app = new Word.Application();
        Object fileName = docName;
        var doc = app.Documents.Open(fileName);
        string rangeText = doc.Range().Text;
        fi = rangeText;
        app.ActiveDocument.Close();
        app.Quit();

        for (int j = 1; j < dictionary.Count; j++)
        {
            if (fi.Contains(dictionary[j]))
            {
                vector[j] = 1;
            }
            else
            {
                vector[j] = 0;
            }
        }
        return vector;
    }
}

```

Fig. 2. C# code with the method of creating a text vector

The project uses the backpropagation method. This method is the most popular for multilayer perceptron learning. In general, the backpropagation algorithm is sequence of following steps [14]:

1. Initiate weights with small random variables.
2. If the stop condition is not satisfied, follow steps 3–10.
3. For each training pair, complete steps 4–9.

Direct pass:

4. Each input neuron $x_i = 1 \dots n$ receives an input signal and distributes it to all hidden layer neurons.

5. Each hidden layer neuron $v_i = 1 \dots q$ summarizes its weighted input signals: $h_j = \sum_j^n w_{ij}x_i$, applies the activation function to the received sum, forming an output signal: $v_j = f(h_j)$, which is sent to all the neurons of the output layer.

6. Every output neuron $y_k, k = 1 \dots m$ sums up the weighted signals: $h_k = \sum_j^q w_{jk} v_j$, forming after the activation function the output signal of the network: $y = f'(h_k)$.

Backpropagation:

7. Each output neuron equates its value with the objective function and calculates it $\delta_k = (t_k - y_k) f'(h_k)$, after what determines the corrective member of the weights: $\Delta w_{jk} = \mu \delta_k v_j$ and the parameters δ_k sent to the hidden layer neurons.

8. Each hidden neuron v_j sums its δ -inputs from the output layer neurons: $h_k = \sum_k^m \delta_k w_{jk}$, the result is multiplied by the derivative of the activation function for expression $\delta_j : \delta_j = f'(h_j) \sum_k^m \delta_k w_{jk}$ and calculate the correction member: $\Delta w_{jk} = \mu \delta_k w_{jk}$.

Weights adjustment:

9. Weights between hidden and output layers are modified as: $w_{jk}(\text{new}) = w_{jk}(\text{old}) + \Delta w_{jk}$. Weights between input and hidden layers are adjusted in a similar way: $w_{jk}(\text{new}) = w_{jk}(\text{old}) + \Delta w_{jk}$.

10. Checking the stop condition to minimize the error between the ideal and the actual output of the network.

The algorithm of document classification with the proposed principles of classification consists of the following steps:

Step 1. To the program input comes one or more MS Word documents;

Step 2. The document is opens in the background and copies to the array;

Step 3. The array is handled by the Vector class;

Step 4. The text vector comes to the input of the neural network;

Step 5. We get the text classification in the output.

The documents are copied to the appropriate folders and the classification type is added to the title.

To test the algorithm, there was created a software application that is able to execute a number of experiments with designed neural network. The program setting are flexible and you can set the number of neurons at the NN levels, the number of training periods, the number of training data and the number of experiments.

During the software product development were set tasks the solution of which allowed to increase the comfort of user experience of the program, to automate some of the program processes and improve performance.

One of these tasks is the choice of dictionary data store. The essence of the task is to make the dictionary easy to transfer, edit by user without using of special software and create a new one if it necessary. Several modern DBMSs have been tested, including Oracle and MS SQL Server 2017. However, to complete

the task it was necessary to refuse from DB and choose MS Excel. This program has installed on most modern computers and most users to their needs without special skills can edit files.

The automated system allows:

- create and edit a dictionary;
- train the neural network for their needs;
- classify documents in batch;
- search the documents key words and quickly open them.

The class diagram of the projected system with a graphical representation of the structural interrelations of the logical model of the system is shown in fig. 3.

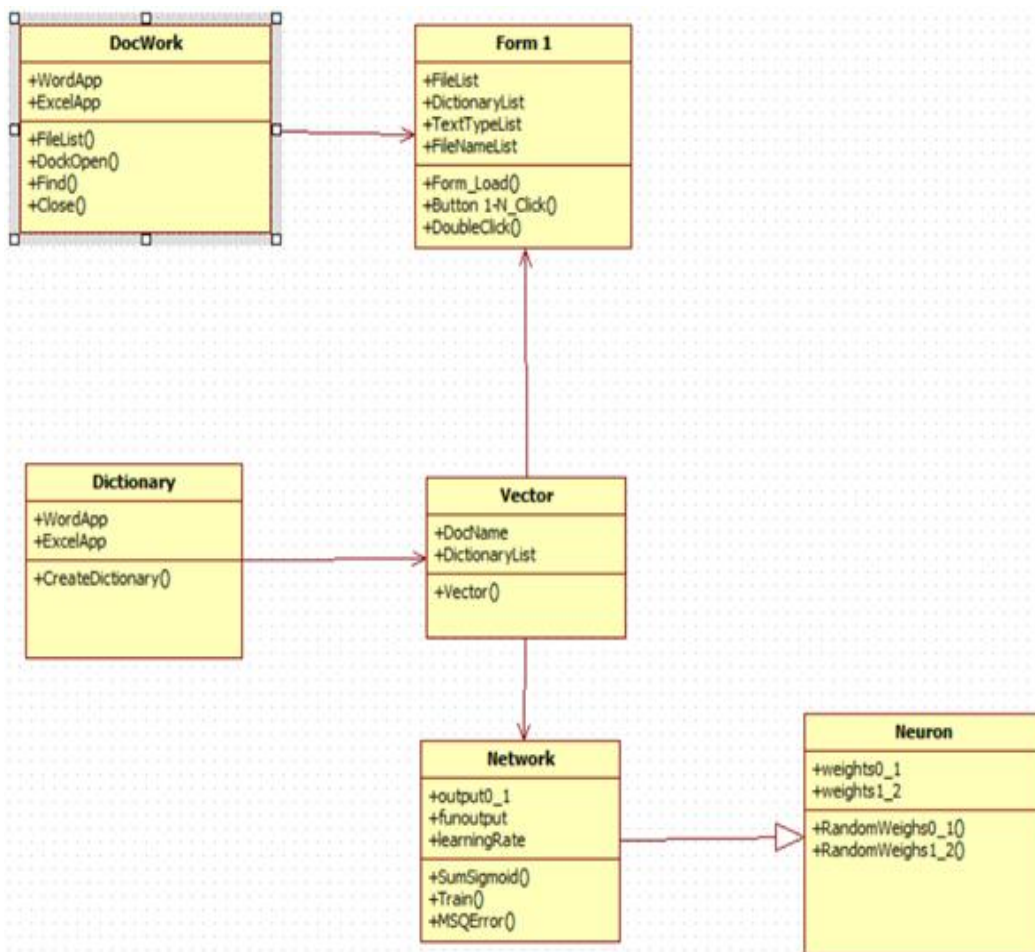


Fig. 3. Class diagram

To train the program you don't need text documents. Vectors are automatically generated and randomly assigned to a type. You can specify their number in the Trainset field. The Resultsets field determines quantity of vectors that will be generated to test the trained network (fig. 4).

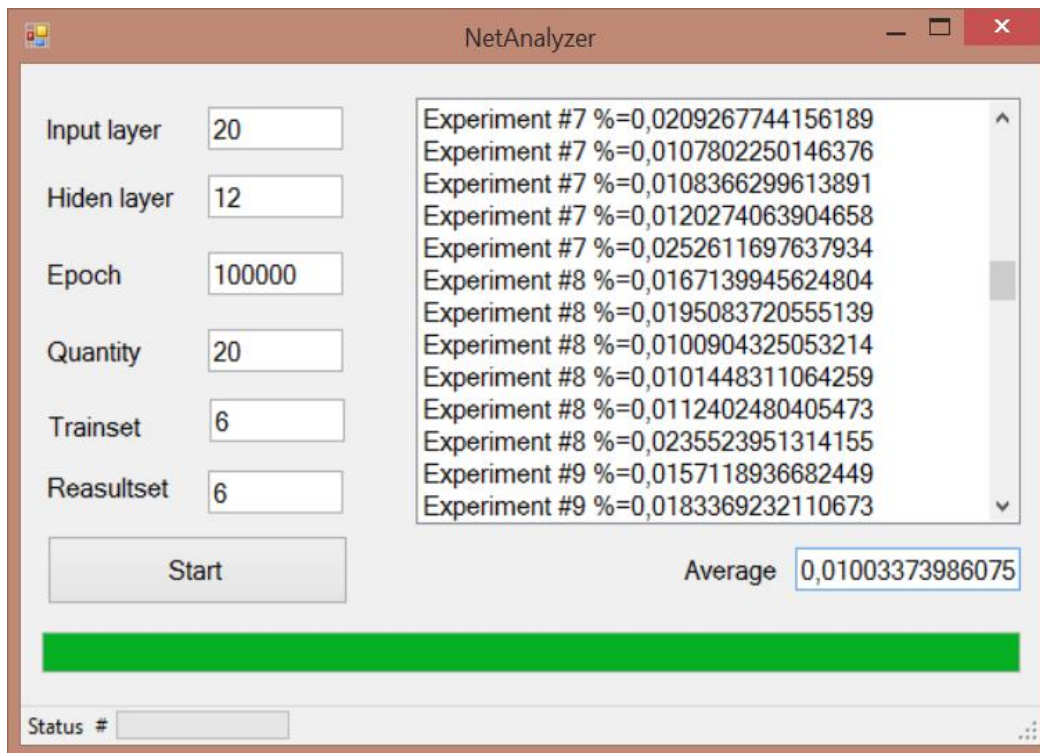


Fig. 4. Test

Thanks to the developed automated classification system there were performed several experiments with different data and the accuracy of the system was determined depending on the number of neurons in the layers of the neural network. Experiment was conducted several times for the best accuracy of the results. As a result, it was found that with increasing quantity of input neurons the accuracy of the result were reduced. With 20 Input Neurons and 12 Hidden, the error was 1 % and the training lasted for 10 seconds. With 40 Input Neurons and 26 Hidden Neurons, the error was already 6 % and training lasted for 5 minutes 20 seconds. At 100 and 66 neurons, the error was 20 % and the duration of training exceeded to 8 hours (table 1). According to the obtained data, we can conclude that the neural network will best recognize the small documents.

Table 1

Dependence of neurons quantity to the time of training and the accuracy of the neural network

Experiment number	Results		
	<i>Neuron Input/Hidden</i>	<i>Time</i>	<i>Accuracy</i>
1	20/12	10s	99 %
2	30/20	1m	96 %
3	40/26	5m20s	94 %
4	50/33	9m30s	92 %
5	60/40	45m	88 %
6	70/46	2h	86 %
7	100/66	8h	80 %

Thanks to the data obtained from the analysis of the test program results there was created a final software application that can categorize the real documents (fig. 5).

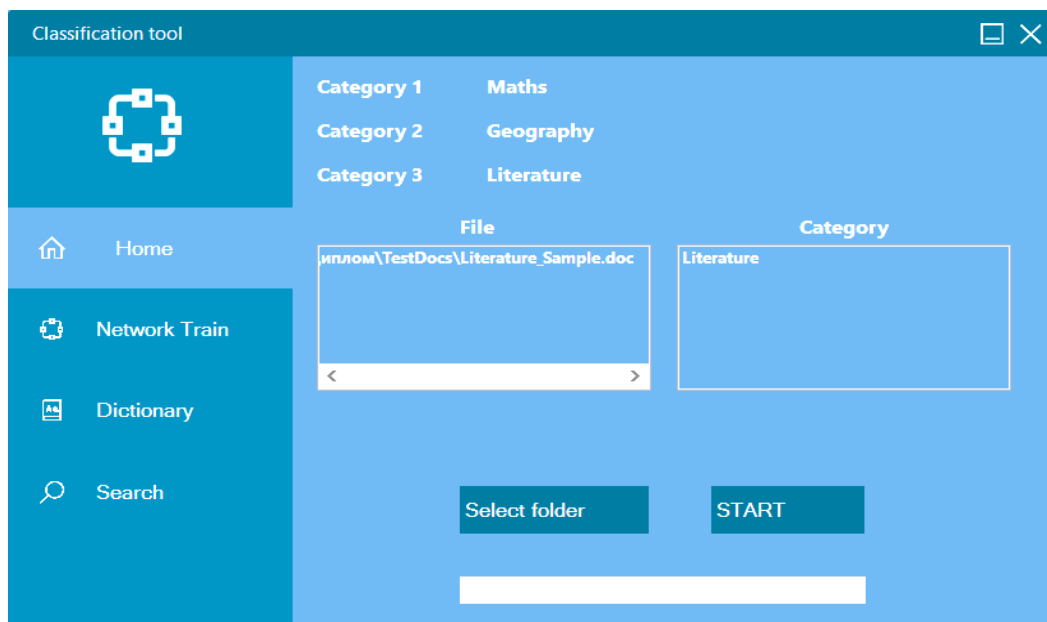


Fig. 5. Program interface

Conclusions and further researches directions. In this paper was proposed an algorithm for categorizing texts by category using a neural network with backpropagation as a learning method. Also was solved the task of profiteering input texts from repetitions and punctuation marks.

Algorithms for text preparation, the neural network and the dictionary creation were implemented programmatically using C# language. The algorithms were successfully tested and tuned. Optimal algorithm settings were set up as a result of the performed experiments to provide the best result of text categorization.

However, the algorithm for converting text into vector is not perfect. He gives an accurate result only if the required word is in the dictionary. This feature requires an increase in the size of the dictionary, which can lead to an increasing CPU usage of the computer.

The result of the work is the creation of a software product capable of classifying text documents by predefined categories. The system tests were performed, the accuracy checked and all the advantages and disadvantages of the perceptron, the method of training the network and the vectorization of information were revealed. It has been proved experimentally that the system is better able to classify small documents.

In the future, the algorithms can be further elaborated using other methods of text vector creating, such as Word2Vec.

List of sources used:

1. *Енчев А. С.* Автоматическая классификация текстовых документов // Математические структуры и моделирование. 2010. № 21. С. 65–81.

2. *Bharath Bhushan S. N., Danti A.* Classification of textdocumentsbased on score level fusion approach // Pattern Recognition Letters. 2017. Vol. 94. P. 118–126. URL: <https://doi.org/10.1016/j.patrec.2017.05.003>

3. *Волосюк Ю. В.* Методи класифікації текстових документів в задачах TextMining // Наукові записки Українського науково-дослідного інституту зв'язку. 2014. № 6 (34). С. 76–81.

4. *Altinel B., Ganiz M. C.* Semantic text classification: a survey of past and recent advances // Information Processing & Management. 2018. Vol. 54. Issue 6. P. 1129–1153. URL: <https://doi.org/10.1016/j.ipm.2018.08.001>

5. *Hadi W., Al-Radaideh Q. A., Alhawari S.* Integrating associative rule-based classification with Naive Bayes for text classification // Applied Soft Computing. 2018. Vol. 69. P. 344–356. URL: <https://doi.org/10.1016/j.asoc.2018.04.056>

6. *Diab D. M., El Hindi K.* Using differential evolution for fine tuning naive Bayesian classifiers and its application for text classification // Applied Soft Computing. 2017. Vol. 54. P. 183–199. URL: <https://doi.org/10.1016/j.asoc.2016.12.043>

7. Yang Y., Liu X. A re-examination of text categorization methods // Proc. of Int. ACM Conference on Research and Development in Information Retrieval (SIGIR-99). 2007. P. 42–49. URL: <https://doi.org/10.1145/312624.312647>

8. Корнеев В. В., Гареев А. Ф., Васютин С. В., Райх В. В. Базы данных. Интеллектуальная обработка информации. Москва: Нолидж. 2000. 352 с.

9. Новотарський М. А., Нестеренко Б. Б. Штучні нейронні мережі: обчислення // Праці Інституту математики НАН України. 2004. Т. 50. 408 с.

10. Сетлак Г. Использование искусственных нейронных сетей для решения задач классификации в менеджменте // Радіоелектроніка. Інформатика. Управління. Нейроінформатика та інтелектуальні системи. 2004. № 1. С. 127–135.

11. Воробьев Н. В., Пучков Е. В. Классификация текстов с помощью сверточных нейронных сетей. URL: <https://cyberleninka.ru/article/v/klassifikatsiya-tekstov-s-pomoschyu-svertochnyh-neyronnyh-setey>

12. Приходченко С. Д. Искусственный нейрон со сложной функцией активации // Науковий вісник національного гірничого університету. 2004. Вип. № 10. С. 92–95.

13. Akmal Haidar Md., O'Shaughnessy D. Novel topic n-gram count LM incorporating document-based topic distributions and n-gram counts // 22nd European Signal Processing Conference. 2014. P. 2310–2314.

14. Калініна І. О. Дослідження алгоритмів навчання нейронних мереж в задачах прогнозування // Наукові праці [Чорноморського державного університету імені Петра Могили]. Сер.: Комп'ютерні технології. 2009. Т. 117. Вип. 104. С. 160–171.

References:

1. Eprev A. S (2010), “Automatic classification of text documents” // Mathematical structures and modeling, vol. 21, pp. 65–81 [Russia].

2. Bharath Bhushan S. N. and Danti A. (2017), “Classification of text documents based on score level fusion approach” // Pattern Recognition Letters, vol. 94, pp. 118–126, available at: <https://doi.org/10.1016/j.patrec.2017.05.003>

3. Volosyuk Yu. V. (2014), “Metody klasyfikatsiyi tekstovykh dokumentiv v zadachakh TextMining” [“Methods of classification of text and documents in the tasks Text Mining”] // *Naukovi zapysky Ukrayins'koho naukovo-doslidnoho instytutu zv'yazku* [Scientific notes of the Ukrainian Research Institute of Communication], vol. 6(34), pp.76–81 [Ukraine].

4. Altinel B. and Ganiz M. C. (2018), “Semantic text classification: A survey of past and recent advances” // Information Processing & Management, vol. 54, issue 6, pp. 1129–1153, available at: <https://doi.org/10.1016/j.ipm.2018.08.001>

5. Hadi W., Al-Radaideh Q. A. and Alhawari S. (2018), “Integrating associative rule-based classification with Naive Bayes for text classification” // Applied

Soft Computing, vol. 69, pp. 344–356, available at: <https://doi.org/10.1016/j.asoc.2018.04.056>

6. Diab D. M. and El Hindi K. (2017), “Using differential evolution for fine tuning naive Bayesian classifiers and its application for text classification” // Applied Soft Computing, vol. 54, pp. 183–199, available at: <https://doi.org/10.1016/j.asoc.2016.12.043>

7. Yang Y. and Liu X. (2007), “A re-examination of text categorization methods” // Processing of Intelligent. ACM Conference on Research and Development in Information Retrieval (SIGIR-99), pp. 42–49, available at: <https://doi.org/10.1145/312624.312647>

8. Goldberg Y. (2016), “A primer on neural network models for natural language processing” // Journal of Artificial Intelligence Research, vol. 57, pp. 345–420.

9. Korneev V. V., Gareev A. F., Vasyutin S. V. and Reich V. V. (2000), Databases. Intellectual information processing, Press Knowledge, Moscow, 352 p. [Russia].

10. Novatorsky M. A. and Nesterenko B. B. (2004), “*Shtuchni neyronni mrezi: obchyslennya*” [“Artificial Neural Networks: Computing”] // *Pratsi Instytutu matematyky NAN Ukrainy* [Works of the Institute of Mathematics of the National Academy of Sciences of Ukraine], vol. 50, 408 p. [Ukraine].

11. Setlak G. (2004), “*Ispol'zovaniye iskusstvennykh neyronnykh setey dlya resheniya zadach klassifikatsii v menedzhmente*” [“The use of artificial neural networks for solving classification problems in management”] // *Radioelektronika. Informatyka. Upravlinnya. Neyroinformatyka ta intelektual'ni systemy* [Radioelectronics. Computer science. Control. Neuroinformatics and Intelligent Systems], vol. № 1, pp. 127–135 [Ukraine].

12. Vorobev N. V. and Puckov E. B. (2017), *Klassifikatsiya tekstov s pomoshch'yu svertochnykh neyronnykh setey* [The text classification using ultra-precise networks], available at: <https://cyberleninka.ru/article/v/klassifikatsiya-tekstov-s-pomoschyu-svertochnykh-neyronnykh-setey> [Russia].

13. Prihodcenko S. D. (2004), “*Iskusstvennyy neyron so slozhnoy funktsiyey aktivatsii*” [“Artificial neuron with a complex activation function”] // *Naukovyy visnyk national'noho hirnychoho universytetu* [Scientific Bulletin of National Mining University], vol. 10, pp. 92–95 [Ukraine].

14. Akmal Haidar Md. and O'Shaughnessy D. (2014), “Novel topic n-gram count LM incorporating document-based topic distributions and n-gram counts” // 22nd European Signal Processing Conference, pp. 2310–2314

15. Kalinina I. O. (2009), “*Doslidzhennya alhorytmiv navchannya neyronnykh mrezh v zadachakh prohozuvannya*” [“Further algorithms for neural neuralz in prediction problems”] // *Naukovi pratsi [Chornomors'koho derzhavnoho universytetu imeni Petra Mohyly]* [Scientific works. Series: of computer science], vol. 117, issue 104, pp. 160–171 [Ukraine].

DOI: <https://doi.org/10.32836/2521-6643-2018-1-56-7>

УДК 656.62

А. І. Кузьменко, кандидат технічних наук,
доцент кафедри транспортних
систем та технологій Університету митної
справи та фінансів

О. В. Трофімов, кандидат фізико-
математичних наук, доцент кафедри
транспортних систем та технологій
Університету митної справи та фінансів

УДОСКОНАЛЕННЯ ТРАНСПОРТНО-ЛОГІСТИЧНИХ ПРОЦЕСІВ ОБСЛУГОВУВАННЯ ВАНТАЖОПОТОКІВ НА ТЕРИТОРІЇ РІЧКОВОГО ПОРТУ

Проаналізовано потенціал річкового транспорту України. Розкрито основні проблеми сучасного стану річкових перевезень, розглянуто перспективи інтеграції річкових портів до європейської транспортної мережі. Визначено фактори стримування розвитку транспортно-логістичної діяльності порту та запропоновано можливі шляхи її вдосконалення. Складено схему можливих часових елементів логістичного ланцюжка обслуговування вантажопотоків під час їх обробки в річковому порту, формалізовано відповідні транспортні процеси з метою виявлення реальних резервів часу, за рахунок яких можна скоротити час перебування вантажів і транспортних засобів у порту під час перевалки вантажів із одного виду транспорту на інший та зменшити відповідні фінансові витрати.

Ключові слова: річкові порти; логістичні технології; транспортні вузли; перевантажувальні процеси; імітаційне моделювання.

Проанализирован потенциал речного транспорта Украины. Раскрыты основные проблемы современного состояния речных перевозок, рассмотрены перспективы интеграции речных портов в европейскую транспортную сеть. Определены сдерживающие факторы развития транспортно-логистической деятельности порта и предложены возможные пути ее усовершенствования. Составлена схема возможных временных элементов логистической цепочки обслуживания грузопотоков при их обработке в речном порту, формализованы соответствующие транспортные процессы с целью выявления реальных резервов времени, за счет которых возможно сократить время нахождения грузов и транспортных средств

© А. І. Кузьменко, О. В. Трофімов, 2018

в порту во время перевалки грузов с одного вида транспорта на другой и уменьшить соответствующие финансовые затраты.

Ключевые слова: речные порты; логистические технологии; транспортные узлы; перегрузочные процессы; имитационное моделирование.

The potential of Ukrainian river transport is analyzed. The main problems of the present state of river transport are revealed and the prospects of integration of river ports to the European transportation network are considered. An analysis of the current state of Ukrainian river transportation development has shown that the technical support and efficiency of using the resourceful navigable potential of Ukrainian rivers for a long period of time have a negative dynamics. But at the state level, the development of inland waterways is declared as a priority activity of the Ukrainian Ministry of Infrastructure.

The deterrent factors of transport-logistic activity development of the river ports are determined. These include: insufficient quantity and high percentage of deterioration of the river fleet; unattractive proposals of logistics and transportation services; insufficient values of transshipment operations time from concurrency point of view, which leads to an unacceptable increase in the cargo delivery time, etc.

Possible ways to improve the cargoes transshipment processes from ground types of transport to water and in the opposite direction due to introduction of logistic technologies are offered. Such an approach will provide an opportunity to correctly organize the interaction between different types of transport on the territory of the river port.

The scheme of possible logistic chain time elements for cargo flows treatment during the processing in the river port is made. It has been established that river ports is a significant element of cargo delivery logistics system during mixed transportation with the participation of water transport, which, in most cases, determine the time component of the whole logistic chain of goods delivery. The relevant transportation processes have been formalized in order to identify real time reserves by which it is possible to reduce the time during which cargo and vehicles are located at the port during the transfer process from one type of transport to another and to cut the corresponding financial costs.

Further research may be concerned to identifying the time reserves for other parts of the mixed cargo delivery logistics systems in order to accelerate the total transportation process and to reduce the total cost of transportation, which will increase the competitiveness of river transport and make it more attractive for organizations and enterprises that are customers of transportation services.

Key words: river ports; logistics technologies; transport nodes; transshipment processes; simulation modeling.

Постановка проблеми. Сучасна глобалізація світової економіки, збільшення товарообігу між віддаленими країнами та міжнародний розподіл праці ставлять на перший план транспортну складову будь-якої діяльності. У межах світової транспортної системи підвищилася конкуренція між окремими видами транспорту, збільшився внесок морського, авіаційного та автомобільного транспорту в загальносвітовий вантажообіг з одночасним зниженням питомої ваги залізниць і внутрішніх водних шляхів. За цих умов у багатьох країнах відбулася зміна транспортної політики. Основним стратегічним напрямом стало створення економічних передумов для повернення вантажопотоків на внутрішні водні шляхи та інтеграція внутрішніх водних шляхів у логістичні ланцюги постачань. Це дасть можливість гармонізувати та зробити більш збалансованою транспортну систему країни у цілому.

Розвиток внутрішніх водних шляхів декларується як пріоритетний напрям діяльності Міністерства інфраструктури України, а відновлення в повному обсязі судноплавства на Дніпрі, Дністрі та їх основних судноплавних притоках – одне з головних його завдань, що відображено в основних положеннях Національної транспортної стратегії України на період до 2030 року [1].

Перевезення вантажів внутрішнім водним транспортом – одне з найдешевших та екологічних видів перевезень. У багатьох країнах світу річковий транспорт відіграє значну роль у сфері економічної діяльності держави, оскільки забезпечує збереження навколишнього природного середовища та низьку собівартість вантажних перевезень у перерахунку на одну тону вантажу. За енергетичними витратами він у 5 разів ефективніший від залізничного та в 10 разів від автомобільного транспорту [2].

На жаль, показники, що характеризують стан і ефективність використання ресурсного судноплавного потенціалу річок України, тривалий період мають негативну динаміку. З часу набуття Україною незалежності довжина річкових водних артерій скоротилась майже удвічі (з 4 тис. км до 2,1 тис. км). Водночас скоротилася щільність річкових судноплавних шляхів у 1,75 раза; інтенсивність перевезень вантажів – у 4,3 раза, а інтенсивність перевезень пасажирів – у 7,5 раза [3].

Тому нині порушено проблему залучення вантажопотоків на внутрішні водні шляхи. Для цього необхідно виконати завдання розробки сучасних логістичних стратегій річкових портів України та пошуку можливостей їх реалізації. В силу того, що в більшості випадків річковий транспорт не забезпечує доставку вантажів за логістичною схемою “від дверей до дверей”, а є лише ланкою у ланцюгу змішаних перевезень, необхідно звернути увагу на функціонування річкових портів як пунктів взаємодії різних видів транспорту. Адже виконання завдання скорочення часу перебування транспортних засобів у системі обслуговування вантажопотоків на території річкового порту сприятиме підвищенню конкурентоздатності річкового транспорту.

Аналіз останніх досліджень і публікацій. Формування стратегії вдосконалення роботи річкового порту розглядається як необхідна умова розвитку ефективної ринкової економіки, тому її вивченню приділяли значну увагу багато вчених. Серед них можна назвати таких науковців, як: С. М. Боняр, Н. О. Валявська, М. Т. Дехтярук, С. С. Забара, Я. В. Літвінова, О. В. Мельник, А. О. Мурад'ян, Є. В. Нагорний, О. М. Тимощук, Н. Ю. Шраменко [4–12] та багато інших.

У праці [4] визначається роль річкових портів у логістичному ланцюзі постачань транспортної системи України. На основі розробленої логістичної стратегії передбачено створення річкових логістичних центрів (РЛЦ) у річкових портах з високим рівнем логістичної привабливості, які стануть організаторами доставки вантажів на певному етапі товароруху та сполучною логістичною ланкою на стику транспортних елементів системи постачань. З метою ефективної реалізації логістичної стратегії річкового порту запропоновано механізм реалізації логістичної стратегії річкового логістичного центру, який являє собою сукупність взаємопов'язаних систем логістичного забезпечення (систем управління процесом перевезення, інформаційного забезпечення, вибору оптимальних технологічних схем у порту та оптимальної взаємодії суміжних видів транспорту), методів управління (організаційних, економічних, техніко-технологічних, правових), логістичних принципів та технологій. Передбачено створення окремої комерційної структури – інформаційного логістичного центру (ІЛЦ), який би взяв на себе обов'язки щодо створення єдиного інформаційного простору. Це забезпечить інформаційний супровід логістичного руху вантажів, прийняття оптимальних управлінських рішень.

Автор дисертаційного дослідження [5] розглядає річковий порт як транспортний вузол, тобто елемент технологічних систем доставки вантажів, що є сукупністю технічних, технологічних, комерційних, правових рішень, які реалізуються із залученням багатьох посередників, найчастіше – декількох видів транспорту, спрямовані на організацію і здійснення процесу доставки вантажів від вантажовідправника до вантажоотримувача.

Оцінку річкового потенціалу внутрішніх водних шляхів України дано у статті [6], де розглянуто роль підприємств різних форм власності у його підвищенні. Зазначено, що річкові порти України відіграють велику роль у системі міжнародних транспортних транзитних коридорів, оскільки особлива роль більшості портів визначається тим, що вони можуть бути прямими учасниками міжнародних логістичних систем.

Метою дослідження [7] стало підвищення ефективності процесу перевалки вантажів шляхом розроблення методичних положень щодо встановлення

й дотримання погоджених норм часу на обслуговування вантажів і транспортних засобів. Це забезпечує у кінцевому рахунку скорочення витрат підприємств загальнотранспортного вузла на здійснення перевалки вантажів і транспортної клієнтури з доставки вантажів.

Раціональні технологічні параметри функціонування терміналу, що дозволяють оцінити його роботу, знайти резерви й упровадити заходи для ресурсозбереження та врахування ринкових вимог споживачів, визначено у праці [8]. Реалізація логістичного підходу під час розгляду складних систем передбачає врахування інтересів усіх учасників транспортного процесу. Традиційно в якості критерію ефективності функціонування системи розглядаються витрати на транспортне обслуговування вантажовласників. Однак окремі вантажовласники потребують прискореної переробки вантажів із готовністю нести за це додаткові витрати. Отже, виділяються дві категорії споживачів транспортних послуг. Перша – вантажовласники, для яких основним пріоритетом є швидкість доставки вантажів, а пріоритетом другої категорії – мінімальна вартість доставки. У цьому випадку основою функціонування будь-якої системи в транспортній галузі в ринкових умовах стає забезпечення високого рівня якості транспортного обслуговування зазначених категорій споживачів транспортних послуг.

Автор праці [8] зауважує, що в нинішніх умовах економічної кризи та зменшення обсягів перевезень внутрішнім водним транспортом необхідно впровадження інноваційних методів управління в пошуках шляхів відновлення річкових перевезень. Одним із основних напрямів розв'язання цієї проблеми є розробка логістичних стратегій для річкових портів України та схеми їх реалізації. Логістична стратегія має бути спрямована на вивчення можливості змін у діяльності річкових портів як складової транспортного вузла.

У дослідженні [5] подано методичний підхід реалізації стратегії розвитку річкових портів України. На основі [11] розглянуто роль портового провайдера в залученні контейнерних вантажопотоків до порту, запропоновано програмний продукт, який дає можливість автоматизувати розрахунки щодо вартості контейнерних вантажоперевезень різними видами транспорту. Розглянуто можливі сценарії оптимізації транспортно-логістичної системи роботи річкових портів з урахуванням контейнерних потоків. Представлено розроблений алгоритм прийняття рішень під час здійснення процесу управління контейнерними потоками в річкових портах.

Також у праці [6] запропоновано розробку автоматизованої системи управління роботою виробничо-перевантажувального комплексу порту, яку реалізовано у вигляді програмного комп'ютерного комплексу із застосуванням середовища візуального проектування Embarcadero C++Builder XE5.

Проте переважна більшість авторів у своїх дослідженнях не враховували наявність різноманітних форм власності та багатовекторної конкуренції, коли на ринку одночасно діють безліч організаційно й економічно самостійних суб'єктів – портів і складських комплексів. Таким чином, зазначені дослідження мають обмеження в застосуванні. У більшості названих праць не враховується характер надходження суден до причалів, отже, не розглядається його вплив на пропускну здатність причалу. Автори залишають поза увагою залежність між пропускну спроможністю фронтальної перевантажувальної техніки та іншими елементами причалу, що прийнятно тільки в роботі за прямим варіантом перевантаження. Однак на практиці значна кількість вантажу проходить через склад, що потребує додаткового внутрішньо-портового узгодження роботи елементів перевантажувального процесу. Розглянуті технологічні критерії також не враховують вартісні аспекти функціонування транспортних вузлів в умовах макрологістичної системи ринку. Більшість наявних економічних показників оминають інтереси всіх суб'єктів транспортного процесу, а якісні показники не враховують у комплексі ні технічні особливості, ні вартісні показники роботи портів комплексів, що не дає можливості використовувати їх для оцінки ефективності функціонування транспортних вузлів.

Мета статті – пошук шляхів удосконалення транспортно-логістичних процесів обслуговування вантажопотоків на території річкового порту за рахунок скорочення часу перевалки вантажів з одного виду транспорту на інший. Для цього пропонується знайти раціональний варіант технології обробки вантажів у річковому порту на підставі запропонованої схеми можливих часових елементів логістичного ланцюжка обслуговування вантажопотоків та визначено для кожного з часових елементів відповідних фінансових витрат.

Виклад основного матеріалу. Для більшості країн світу внутрішній водний транспорт найдешевший та найекологічніший, придатний для перевезення значних обсягів продукції, в основному, сировини. Але в Україні у 2014–2017 рр. обсяги перевезення внутрішнім водним транспортом становили лише 0,2–0,8 % від усіх транспортних перевезень (за даними презентації “Центру транспортних стратегій”), тоді як у Нідерландах частка перевезень внутрішніми водними шляхами (ВВШ) становить більше 30 %, а середній показник по країнах ЄС – 6–7 %. З 1990 р. протяжність водних шляхів, якими здійснюється судноплавство, в Україні скоротилась майже вдвічі (рис. 1) [13].

Перевезення вантажів річками у світі активно розвивається, оскільки це, як уже зазначалося, дешево та екологічно. Такі перевезення у 5 разів економічніші від залізничних і в 10 разів дешевші від автомобільних. Однак в Україні річками перевозиться менше 1 % вантажів (рис. 2).



Рис. 1. Порівняння протяжностей водних шляхів України та інших країн

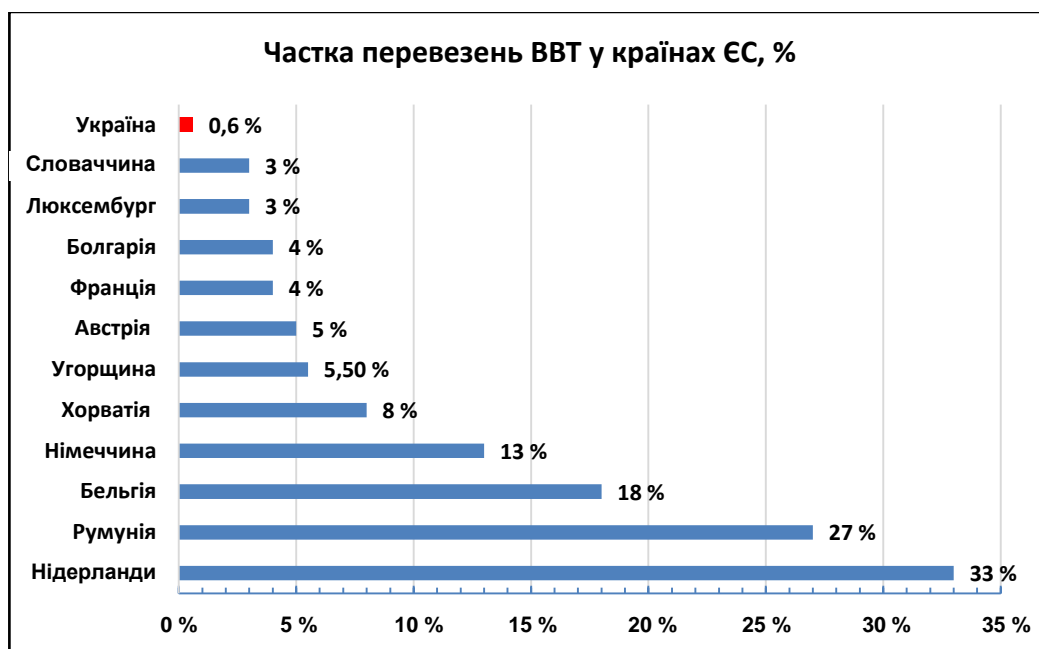


Рис. 2. Обсяги перевезень річковим транспортом в Україні та країнах ЄС

Порівняння ефективності використання водних ресурсів України з іншими країнами за довжиною судноплавних ділянок зображено на рис. 3.

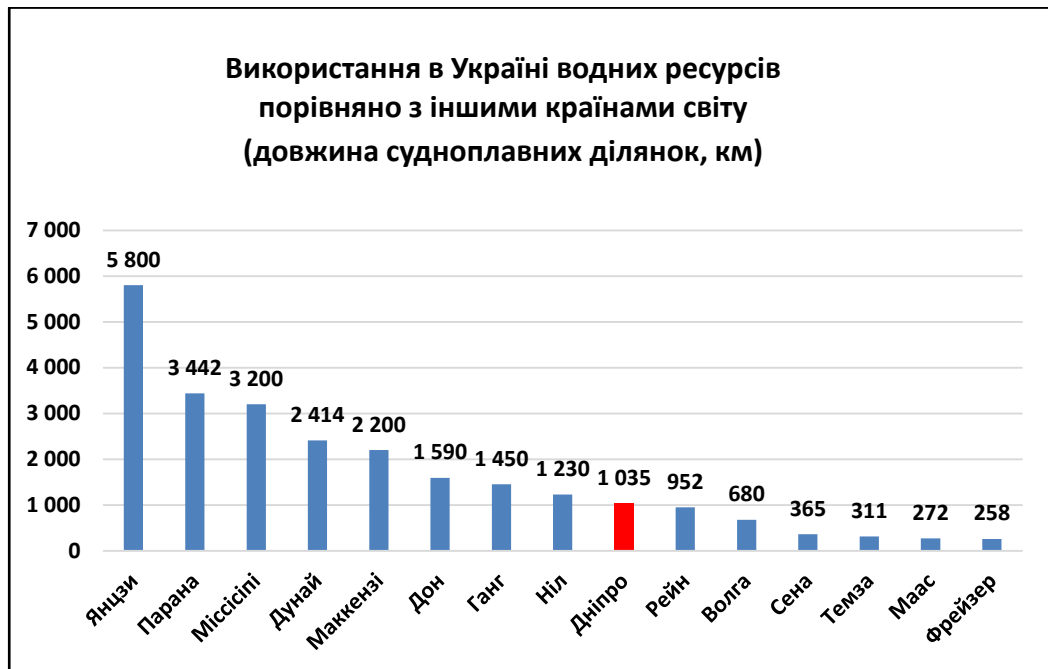


Рис. 3. Ефективність використання водних ресурсів України та інших країн світу за довжиною судноплавних ділянок

Загалом щорічно річковий комерційний флот України здатний перевозити 10–12 млн т вантажів, з яких: насипних – понад 9 млн т (будівельні матеріали, зерно, вугілля, руда), тарно-штучних – 1 млн т (метал, ліс, добрива), а також до 100 тис. TEU контейнерів. Отже, сукупно річковий комерційний флот має надлишок потужностей.

Близько 60 % перевезень на внутрішніх водних шляхах здійснюються між портами України (каботажні перевезення).

Ринок перевезень ВВШ оцінюється в 6,5 млн т на рік [14] та характеризується поступовим зростанням його обсягів. Це відбувається після тривалого падіння його обсягів перевезень, переважно за рахунок перевезень зерна та металу, починаючи з 2005 р. (рис. 4).

Обсяги перевезення небезпечних вантажів (за результатами моніторингу РІС) подано на рис. 5. На рис. 6–9 відображено результати статистичного аналізу щодо стану перевезень вантажів внутрішніми водними шляхами.



Рис. 4. Динаміка перевезення вантажів внутрішніми водними шляхами



Рис. 5. Перевезення небезпечних вантажів внутрішнім водним транспортом



Рис. 6. Динаміка вантажообігу

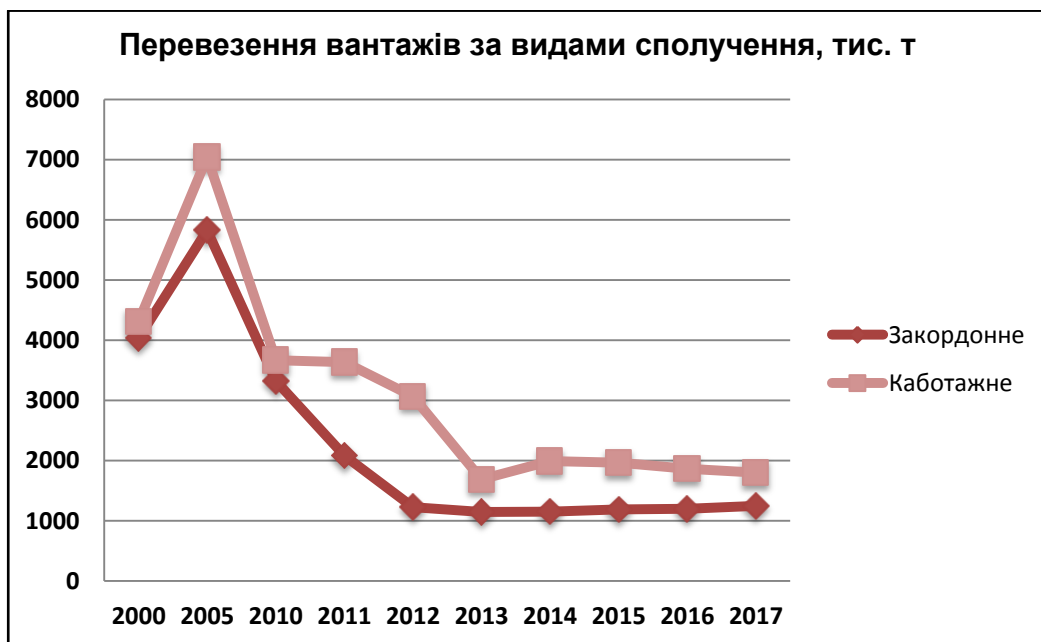


Рис. 7. Динаміка перевезень вантажів за видами сполучення



Рис. 8. Середня відстань перевезення однієї тонни вантажів



Рис. 9. Структура вантажів, що перевозяться річковим транспортом

Як зазначалося, річка Дніпро входить до переліку найважливіших внутрішніх водних шляхів Європи, має велике міжнародне значення, а її порти належать до категорії перспективних об'єктів для розвитку міжнародних комбінованих перевезень. Інфраструктура внутрішніх водних шляхів на р. Дніпро включає 6 шлюзів, 16 річкових портів і порто-пунктів. Відправлення та приймання зовнішньоторговельних вантажів здійснюється переважно через Запорізький, Дніпровський, Миколаївський, Херсонський річкові порти загального користування, а також річковий порт Полтавського гірничо-збагачувального комбінату у місті Горішні Плавні. В невеликих обсягах та епізодично здійснюється переробка зовнішньоторговельних вантажів у Київському, Черкаському, Кременчуцькому, Ново-Каховському річкових портах та на причалах, розташованих у місті Кам'янському. Загальна добова пропускна спроможність річкових портів становить близько 20 тис. т [15]. Обсяги переробки експортно-імпортних вантажів коливаються в межах 1,4–2,1 млн т щороку.

Необхідно зауважити, що значним недоліком внутрішнього водного транспорту є те, що він не здатний забезпечити доставку вантажів “від дверей до дверей”, тому може розглядатися лише як один із елементів логістичної системи (ЛС) доставки вантажів під час змішаних перевезень. На рис. 10 у спрощеному вигляді подано схему доставки вантажів за участю залізничного, автомобільного та річкового транспорту, де використано умовні позначення, а саме:

- C_v, C_o – вантажні склади відправника та одержувача відповідно;
- $T'_{\text{наз}}, T''_{\text{наз}}$ – транспортування вантажів наземними видами транспорту;
- $T_{\text{ВВШ}}$ – транспортування вантажів внутрішніми водними шляхами;
- $\Pi'_{\text{порт}}, \Pi''_{\text{порт}}$ – пункти перевалки вантажів з одного виду транспорту на інший (річкові порти).

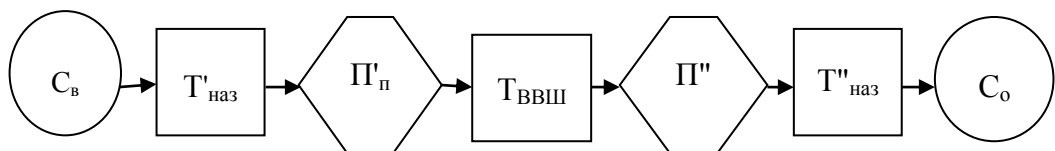


Рис. 10. Спрощена схема доставки вантажів за участю внутрішнього водного транспорту

Для даної логістичної системи загальний термін доставки T_d визначається так:

$$T_d = \sum_1^a t_{C_e} + \sum_1^d t_{T'_{наз}} + \sum_1^q t_{П'_{порт}} + \sum_1^l t_{T_{ВВШ}} + \sum_1^g t_{П''_{порт}} + \sum_1^h t_{T''_{наз}} + \sum_1^b t_{C_o}, \quad (1)$$

де $\sum_1^a t_{C_e}, \sum_1^b t_{C_o}$ – сумарний час перебування вантажів на складах відправника та одержувача відповідно;

$\sum_1^d t_{T'_{наз}}, \sum_1^h t_{T''_{наз}}$ – сумарний час транспортування вантажу наземними видами транспорту від складу відправника до порту відправлення та від порту призначення до складу одержувача відповідно;

$\sum_1^l t_{T_{ВВШ}}$ – сумарний час транспортування вантажу внутрішніми водними шляхами від порту відправлення до порту призначення;

$\sum_1^q t_{П'_{порт}}, \sum_1^g t_{П''_{порт}}$ – сумарний час перебування вантажів у річкових портах відправлення та призначення.

У рівнянні (1) літерами a, b, d, h, l, q та g позначено кількість окремих операцій, за якими розраховуються витрати часу для відповідних елементів логістичної технології доставки вантажів.

Оскільки термін доставки вантажів визначається як сума часових характеристик усіх ланок логістичного ланцюжка [16], було б доцільно проаналізувати кожен із певних елементів для з'ясування основних критеріїв, що впливають на цей час.

Важливою ланкою логістичної системи (ЛС) доставки вантажів під час змішаних перевезень за участю водного транспорту є річкові порти, особливостям функціонування яких і присвячено цю статтю. В системі змішаних перевезень річкові порти здебільшого визначають часову складову всього логістичного ланцюжка доставки вантажів.

Процеси перевалки вантажів із наземних видів транспорту на водний розглядаються у статті на прикладі Дніпровського порту, де здійснюється переробка вантажів, які перевозять прямим водним та змішаними автомобільно-водним і залізнично-водним сполученнями. У межах діяльності порту функціонують вантажні райони Амур-Гавань, Нові Кайдаки, Міський район і пристань Новомосковськ, а також причали незагального користування з

відвантаження щебеневої продукції та вивантаження піску. Територія порту включає в себе два вантажні райони (13 причалів).

Виробничі ресурси порту такі: довжина причалів загального користування становить 1924 м (загальна – 2250 м), на яких встановлено 24 портальних крани вантажністю від 5 до 20 т, (загальною вантажопідйомністю 265 т), 3 стрілочних крани вантажністю від 10 до 36 т, один монтажний кран вантажністю 75 т та один великоваговий кран вантажністю 100 т, а також 7 автовантажувачів вантажністю від 1,5 до 3 т. Площа критих складів становить 2,6 тис. м², відкритих складських майданчиків – 60 тис. м². Пропускна здатність порту – 5,7 млн т/рік. Можливе обслуговування суден з осадкою до 4 м.

На 1-му причалі району Амур-Гавань уведено в експлуатацію новий зерновий елеватор ємністю одноразового зберігання 30 тис. т (6 ємностей по 5 тис. т), обладнаний сучасним високотехнологічним устаткуванням. Зерновий елеватор надає послуги з приймання як із залізничного, так і з автомобільного транспорту, накопичення, зберігання, сушки, очищення, а також відвантаження зернових, олійних і технічних культур. Для накопичення зернових вантажів обладнано 6 несамохідних суден сумарною вантажомісткістю 7000 т.

Навантаження суден на естакадно-конвеєрному комплексі проводиться двома конвеєрними лініями із залізничних вагонів і автомобілів за прямим варіантом. При цьому продуктивність становить до 400 т за годину.

Основна номенклатура вантажів порту: пісок, вугілля, метали, щебінь, контейнери [15]. Дніпровський порт також спеціалізується на переробці зернових, металобрухту, металопрокату, польового шпату, пиломатеріалів, обладнання, тарно-штучних вантажів у біг-бегах і на палетах.

Річні обсяги переробки зовнішньоторговельних вантажів становлять від 200 до 400 тис. т. Потужність порту з переробки вантажів – 2,9 млн т/рік [17], тобто переробні потужності порту використовуються приблизно на 10 %. Незважаючи на досить високу технічну оснащеність, порт зазнає певних труднощів через недостатні глибини біля причалів, що потребує використання понтонів під час обробки багатонавантажувальних суден, а також у зв'язку з недостатньою кількістю складських площ. Основними чинниками, що визначають низьку конкурентоздатність річкового порту, також є:

- 1) недостатня кількість та великий відсоток зношування річкового флоту, що здатний реалізувати потенційний вантажопотік;
- 2) непривабливі вартісні показники логістично-транспортних послуг;
- 3) недостатні в конкурентному плані часові показники перевантажувальних операцій, що призводить до невиправданого збільшення часу доставки вантажів.

Отже, для вибору стратегії річкового порту необхідно дати оцінку його логістичної привабливості. Вона включає в себе багато різноманітних критеріїв. Серед них можна виокремити такі, як входження в міжнародні транспортні коридори, розташування поблизу промислових районів, наявність транспортного забезпечення (автошляхи, залізниці, аеропорти), складські потужності, можливість будівництва контейнерних терміналів, перспективні вантажопотоки, рівень використання пропускної здатності порту та можливість обслуговування суден типу “річка-море” [18].

Під час упровадження логістичних стратегій у процесі діяльності річкового порту необхідно застосовувати принципи моделювання та інформаційно-комп’ютерної підтримки використання різних моделей: математичних, економіко-математичних, графічних, імітаційних. Узгодження роботи різних видів транспорту та взаємодія всіх елементів річкового порту мають привести до зниження витрат на обслуговування вантажопотоків з урахуванням обмежень за часом виконання операцій.

З метою розв’язання задачі формування математичної моделі процесів декомпозиції вхідного потоку транспортних засобів на території річкового порту, яка б дозволяла визначати вартісні та часові параметри й давала можливість запроваджувати логістичні технології обслуговування вантажопотоків, що ґрунтуються на узгодженості використання наявних матеріальних і грошових ресурсів, було проаналізовано технології перевалки вантажів із наземних видів транспорту на водний у річковому порту.

Для подальшого дослідження прийняті такі способи обслуговування портових вантажопотоків: перевантаження вантажів із вагонів на судна за прямим варіантом, перевантаження вантажів із вагонів на судна через склад; перевантаження вантажів із автомобілів на судна за прямим варіантом та перевантаження вантажів із автомобілів на судна через склад. Кожен із цих способів має свої переваги й недоліки.

Безумовно, технологія перевантаження вантажів за прямим варіантом більш приваблива щодо часових параметрів і техніко-експлуатаційних показників роботи транспортних засобів та перевантажувальних механізмів. Але такий варіант обслуговування портових вантажопотоків потребує чіткого узгодження процесів у взаємодії різних видів транспорту, достатньої кількості навантажувально-розвантажувальної техніки, високого рівня розвитку портової інфраструктури й транспортних розв’язок на підходах до порту, відповідного організаційно-інформаційного забезпечення процесів перевалки вантажів тощо. Це не завжди можна забезпечити, зважаючи на сезонність роботи річкового транспорту та на сучасний стан його розвитку взагалі.

Варіант перевалки вантажів через склад не потребує чіткого дотримання графіка подавання транспортних засобів різних видів транспорту до

портових пристроїв і дає можливість накопичувати необхідний обсяг вантажу для завантаження великотоннажних суден. Утім, він має ряд недоліків, таких як збільшення простою транспортних засобів під вантажними операціями, необхідність наявності розвиненого комплексу сучасних складів, збільшення кількості навантажувально-розвантажувальних механізмів тощо.

Слід звернути увагу на той факт, що вантажопотоки, які надходять на територію річкового порту у вагонах та в автомобілях, обслуговуються переважно одними й тими ж механізмами, зберігаються на одних і тих же складах, що також потребує певної узгодженості у функціонуванні окремих підсистем логістичної системи змішаних перевезень. Іноді вантажі затримуються на певний час на складі або безпосередньо в транспортних засобах. Причини можуть бути різними (брак вільних перевантажувальних механізмів, порожніх вагонів, суден або автомобілів для перевантаження, комерційний брак, випадкові поламки, відсутність документів або неправильне їх оформлення, затримка зовнішньоторговельних вантажів за підсумками митних операцій тощо), але всі вони негативно впливають на логістичний ланцюжок у цілому, збільшуючи час перебування вантажу в річковому порту.

З метою скорочення часу перебування транспортних засобів у системі обслуговування вантажопотоків на території річкового порту пропонується визначити раціональний варіант технології обробки вантажів у річковому порту. Схему можливих часових елементів логістичного ланцюжка обслуговування вантажопотоків під час їх обробки в річковому порту зображено на рис. 11. Схеми розроблена для того випадку, коли вантажі прибувають у річковий порт у вагонах або автомобілях, а відправляються на судах внутрішнього водного транспорту.

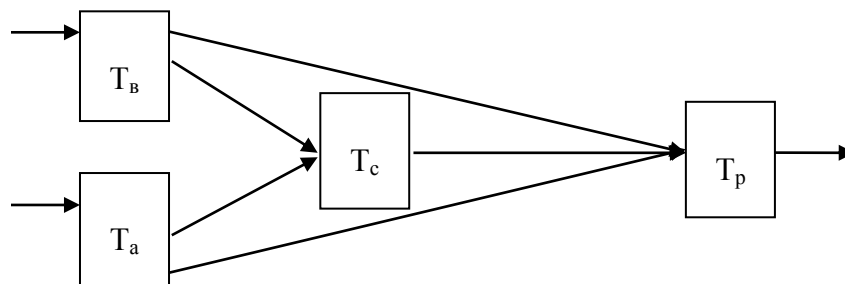


Рис. 11. Схеми можливих часових елементів логістичного ланцюжка обслуговування вантажопотоків під час їх обробки в річковому порту

На рис. 11 використано такі умовні позначення:
 T_B – час перебування вантажів у вагонах;
 T_a – час перебування вантажів у автомобілях;
 T_c – час виконання перевантажувальних операцій і перебування вантажів на складах;
 T_p – час перебування вантажів у річкових суднах.
 Згідно з даною схемою сумарний час перебування вантажів на території річкового порту складатиметься з таких елементів:

$$\sum t_{\Pi_{порт}} = \alpha \left(\gamma \sum_1^d t_a^n + \xi \sum_1^g t_a^c \right) + \beta \left(\varphi \sum_1^q t_e^n + \eta \sum_1^h t_e^c \right) + \sum_1^l t_p, \quad (2)$$

де $\sum_1^d t_a^n$ – сумарний час перебування вантажу в автомобілях, що мають бути перевантажені за прямим варіантом;

$\sum_1^g t_a^c$ – сумарний час перебування вантажу в автомобілях, що мають бути розвантажені на склад;

$\sum_1^q t_e^n$ – сумарний час перебування вантажу в вагонах, що мають бути перевантажені за прямим варіантом;

$\sum_1^h t_e^c$ – сумарний час перебування вантажу в вагонах, що мають бути розвантажені на склад;

$\sum_1^l t_p$ – сумарний час перебування вантажів у річкових суднах.

Вантажопотік після прибуття у річковий порт запропоновано розглядати як сукупність обсягів вантажу, що надходить в автомобілях (їхня частка дорівнює α), та обсягів вантажу, що надходить у залізничних вагонах (їхня частка становить β). Для цих часток справедливі такі припущення:

$$0 \leq \alpha \leq 1; 0 \leq \beta \leq 1;$$

$$\alpha + \beta = 1.$$

Так само вантажі, що потрапляють на територію річкового порту в автомобілях, поділяються на ті, які перевантажуються за прямим варіантом (з автомобіля на судно), та ті, що деякий час зберігаються на складі. Частки таких вантажів дорівнюватимуть відповідно γ та ξ . Для них справедливими є такі припущення:

$$0 \leq \gamma \leq 1; 0 \leq \xi \leq 1;$$

$$\gamma + \xi = 1.$$

Аналогічно встановлюються припущення для тих вантажів, що були доставлені в річковий порт у залізничних вагонах (частки вантажів, що надійшли у вагонах для прямого перевантаження та для розвантаження на склад, дорівнюватимуть відповідно η та φ :

$$0 \leq \eta \leq 1; 0 \leq \varphi \leq 1;$$

$$\eta + \varphi = 1.$$

У рівнянні (2) літерами d , g , q , h та l позначена кількість окремих операцій, за якими розраховуються витрати часу для певних елементів відповідних технологій обслуговування вантажопотоків у річковому порту.

Так, наприклад, елемент $\sum_1^l t_p$ складається з операцій, що передбачені

технологічним процесом роботи порту, й може включати операції підготовки маршруту приймання для вагонів, закріплення состава, відчеплення маневрового локомотива, обробки документів, митних операцій, операцій зі здійснення прикордонного, карантинного, ветеринарного, екологічного та інших видів державного контролю відповідно до прийнятої технології, безпосередньо перевантаження з вагона на судно, закріплення вантажів на судні, прибирання порожніх вагонів тощо.

У формулу (2) як окремі елементи можуть входити витрати часу на прямування автомобілів територією порту, їх маневрування та відстої, а також маневрові пересування вагонів між портовими пристроями. Останні залежать від типу маневрового локомотива, кількості вагонів у маневровому составі, довжини рейсів та напіврейсів, швидкості руху тощо та обумовлюються конкретними місцевими умовами. Кожен із елементів логістичного ланцюжка може також мати часові витрати на міжопераційні простої, які витікають із прийнятої технології роботи річкового порту.

Кожному часовому елементу відповідають фінансові витрати. Вони залежать від технічної оснащеності порту, прийнятої технології обслуговування вантажопотоків, пріоритетності операцій з перевалки вантажів та від багатьох інших чинників.

Модель функціонування Дніпровського порту як транспортного вузла докладно описано в праці [5]. У ній враховано стохастичну природу попиту на послуги річкового порту. Під час розв'язання задач пошуку ефективної організації взаємодії різних видів транспорту у річковому порту пропонується використовувати питомий показник ефективності K_e , що є відношенням прибутку від обслуговування клієнтури в річковому порту до вартості виробничих ресурсів, задіяних у процесі обробки вантажів:

$$K_e = \frac{T_{IT} \cdot Q_{\Sigma}^{обсл} - E_{\Sigma}}{C_R}, \quad (3)$$

де $Q_{\Sigma}^{обсл}$ – загальний обсяг вантажу, що був перевантажений у річковому порту протягом заданого періоду, т;

T_{IT} – тариф на переробку 1 т вантажу у річковому порту, грн/т;

E_{Σ} – сумарні витрати на обслуговування клієнтури в річковому порту протягом заданого періоду, грн;

C_R – сумарна вартість виробничих ресурсів, що використані у процесі переробки матеріального потоку, грн.

За прийнятим критерієм (3), ефективність функціонування річкового порту як транспортного вузла визначається співвідношенням прибутку від обслуговування вантажних одиниць різних видів транспорту до вартості виробничих ресурсів, задіяних у процесі обслуговування. Даний критерій ефективності є безрозмірним показником, який вказує на величину питомого прибутку на обслуговування, що припадає на грошову одиницю вартості виробничих ресурсів.

Але запропонований питомий показник ефективності не враховує залежності тарифу на переробку 1 т вантажу в річковому порту від виду транспорту, виду вантажу, сезонних впливів тощо. Тому пропонується доповнити формулу (3) відповідним коефіцієнтом $\sum_1^n k$, де n – кількість факторів, що впливають на формування відповідного тарифу.

Аналогічно пропонується коригувати також сумарні витрати на обслуговування клієнтури в річковому порту упродовж заданого періоду шляхом

уведення коефіцієнта $\sum_1^m z$, де m – кількість чинників, від яких залежать зазначені витрати. Наприклад, пріоритетність обслуговування вантажопотоків, статус клієнта тощо.

З урахуванням даних пропозицій залежність (3) набуває такого вигляду:

$$K_e = \frac{\sum_1^n k T_{IT} \cdot Q_{\Sigma}^{обсл} - \sum_1^m z E_{\Sigma}}{C_R} . \quad (4)$$

Для Дніпровського річкового порту на підставі параметрів попиту [5] також було отримано функціональні залежності критерію ефективності від кількості навантажувально-розвантажувальних механізмів (НРМ), що задіяні в процесі обслуговування матеріального потоку, для різних значень місткості складу (рис. 12).

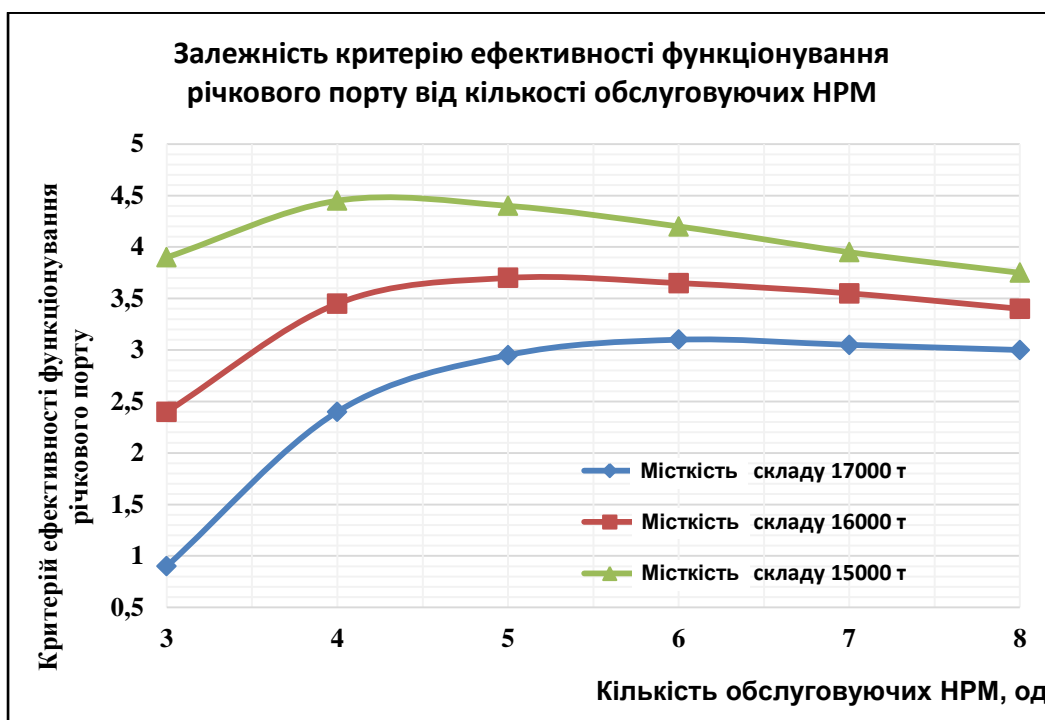


Рис. 12. Залежність критерію ефективності функціонування річкового порту від кількості обслуговуючих НРМ [5]

Зроблено висновок (рис. 12), що оптимальна кількість обслуговуючих механізмів пов'язана зі зміною ємності складу річкового порту: для ємності складу 15 тис. т оптимальна кількість НРМ становить 4 одиниці, для ємності складу 16 тис. т оптимальна кількість обслуговуючих механізмів становить 5 одиниць, а для ємності складу транспортного вузла 17 тис. т оптимальна кількість НРМ на фронті вантажних робіт становить 6 одиниць. Отримані залежності пропонується використовувати для обґрунтування управлінських рішень щодо організації процесу обробки вантажів під час перевалки з одного виду транспорту на інший на території Дніпровського річкового порту з метою збільшення привабливості річкових перевезень.

За умов обмеженості складських площ при наявному технічному розвитку Дніпровського порту пропонується переглянути даний критерій ефективності з урахуванням запропонованих коефіцієнтів, увести оновлений вартісний показник [19] та зосередити подальші дослідження на виявленні резервів часу на всіх технологічних елементах, задіяних у процесі перевалки вантажів з одного виду транспорту на інший на території річкового порту. Це дозволить зменшити загальний час доставки вантажів, отже, й знизити відповідні витрати.

Висновки з даного дослідження та перспективи подальших розвідок у даному напрямі. Аналіз сучасного стану розвитку річкового транспорту в Україні свідчить, що технічне забезпечення та ефективність використання ресурсного судноплавного потенціалу річок тривалий період має негативну динаміку, хоча на державному рівні розвиток внутрішніх водних шляхів декларується як пріоритетний напрям діяльності Міністерства інфраструктури України.

Важливою ланкою логістичної системи доставки вантажів під час змішаних перевезень за участю водного транспорту є річкові порти, які здебільшого визначають часову складову всього логістичного ланцюжка доставки вантажів.

Кожен із наявних способів перевалки вантажів із наземних видів транспорту на водний та у зворотному напрямі має свої недоліки й переваги, а остаточне рішення про застосування тієї чи іншої технології потребує формалізації транспортних процесів на території річкових портів для визначення часових і грошових параметрів логістичного ланцюга доставки вантажів.

Складена схема можливих часових елементів логістичного ланцюжка обслуговування вантажопотоків під час їх обробки в річковому порту уможливила проаналізувати роботу окремих її елементів для виявлення реальних резервів часу, за рахунок яких можна скоротити час розміщення вантажів і транспортних засобів у порту під час перевалки вантажів з одного виду транспорту на інший та зменшити відповідні фінансові витрати. Упровадження логістичних технологій у виробничі процеси сприятиме підвищенню ефектив-

ності обслуговування вантажопотоків. Такий підхід дасть можливість грамотно організувати взаємодію різних видів транспорту на території річкового порту.

Подальші дослідження можуть бути спрямовані на виявлення резервів часу на інших ланках логістичної системи змішаної доставки вантажів для прискорення загального часу та зменшення сумарної вартості перевезень, що підвищить конкурентоздатність річкового транспорту, зробить його більш привабливим для організацій і підприємств-замовників транспортних послуг.

Список використаних джерел:

1. Національна транспортна стратегія України на період до 2030 року : схвалено розпорядженням Кабінету Міністрів України від 30 травня 2018 р. № 430-р. URL : <http://zakon.rada.gov.ua/laws>

2. *Емельянова Е.* Ресурсный потенциал речного транспорта Украины: проблемы, задачи и меры по развитию и эффективному использованию. URL : <http://transport-journal.com/komentarii-obzori/resursnyij-potentsyal-rechnoho-transporta-ukraynu-problemyi-zadachy-u-meryi-po-razvytyyu-u-effektyvnomu-yspolzovanyuu/>

3. Розвиток річкового транспорту у контексті реалізації євроінтеграційних планів України : аналітична записка / Національний інститут стратегічних досліджень. URL : <http://www.niss.gov.ua/>

4. *Тимошук О. М., Мельник О. В.* Формування механізму реалізації логістичної стратегії річкових портів // Проблеми економіки. 2013. № 3. С. 149–155.

5. *Літвінова Я. В.* Удосконалення логістичного управління різними видами транспорту, складуванням та переробкою вантажів у транспортних вузлах : дис. ... к.т.н. (док. філософії): 05.22.01. Харків, Харк. нац. автом.-дорожній ун-т, 2017. 200 с.

6. *Боняр С. М., Валявська Н. О.* Зацікавленість підприємств у підвищенні конкурентоспроможності внутрішніх водних шляхів України // Водний транспорт. 2015. № 2. С. 97–103.

7. *Мурад'ян А. О.* Методичні основи узгодженого управління процесом перевалки вантажів у загальнотранспортних вузлах : дис. ... к.т.н.: 05.22.01. Одеса, Одеський нац. мор. ун-т, 2016. 166 с.

8. *Нагорний Є. В., Шраменко Н. Ю.* Визначення технологічних параметрів функціонування термінального комплексу в умовах ринку транспортних послуг // Вестник ХНАДУ. 2011. Вып. 53. С. 51–55.

9. *Мельник О. В.* Обґрунтування стратегії розвитку річкових портів // Інвестиції: практика та досвід. 2013. № 15. С. 99–101.

10. *Валявська Н. О.* Економічне обґрунтування впровадження стратегії диверсифікації в річкових портах України // Ефективна економіка. 2016. №1. URL : <http://www.economy.nayka.com.ua/?op=1&z=4875>

11. Про внутрішній водний транспорт : проект Закону України (дата реєстрації: 2475а від 04.08.2015). URL : http://www.mtu.gov.ua/uk/alias_50/51199.html

12. *Забара С. С., Дехтярук М. Т.* Розробка автоматизованої системи оптимізації роботи перевантажувального комплексу // *Восточно-Европейский журнал передовых технологий*. 2015. № 1/3 (73). С. 8–14.

13. Від Горішніх Плавнів і далі. Стан річкового транспорту в Україні : Інфографіка. Огляд галузі / Логістична компанія Zammler. URL: http://texty.org.ua/pg/article/txts/read/68935/Vid_Gorishnih_Plavniv_i_dali_Stan_richkovogo

14. *Гончарук О., Лавриненко І.* Зелена книга “Вантажні перевезення внутрішніми водними шляхами” / Офіс ефективного регулювання BRDO. 2017. Серпень. 80 с. URL : www.brdo.com.ua

15. Річкові порти України / у кн. : Транспортна екологія / О. І. Запорожець, С. В. Бойченко, О. Л. Матвеева та ін. Київ, Центр учбової літератури, 2017. URL: https://pidruchniki.com/92969/ekologiya/richkovi_porti_ukrayini

16. *Кузьменко А. І.* Удосконалення технології перевезення вантажів у міжнародному сполученні // *Вісник Академії митної служби України*. 2008. № 2 (38). С. 77–82.

17. Річкові термінали на Дніпрі. URL: <https://graintrade.com.ua/terminal/dnipropetrovskij-richkovij-port-ask-ukrrichflot-id1945>

18. *Кузьменко А. І., Шишка А. М.* Аналіз перспектив розвитку річкового транспорту в Україні // *Тенденції та перспект. розв. науки і освіти в умовах глобалізації : матеріали Міжнар. науков. інтернет-конфер. (Вип. 40). Переяслав-Хмельницький*. 2018. С. 676–680.

19. *Кузьменко А. І.* Удосконалення технології обробки вагонопотоків на станціях стикування колій різної ширини : дис. ... к.т.н.: 05.22.01. Дніпропетровськ. Дніпропетровський національний університет залізничного транспорту імені академіка В. Лазаряна, 2013. 204 с.

References:

1. CMU (2018), *Natsional'na transportna stratehiya Ukrayiny na period do 2030 roku* [National transport strategy of Ukraine for the period up to 2030] : order of the Cabinet of Ministers of Ukraine dated May 30, No. 430-p. : available at: <http://zakon.rada.gov.ua/lavs> [Ukraine].

2. Emel'yanova E. (2014), “*Resursnyj potencial rechnogo transporta Ukrainy: problemy, zadachi i mery po razvitiyu i ehffektivnomu ispol'zovaniyu*” [“Resource potential of river transport of Ukraine: problems, tasks and measures for development and effective use”] // *Journal Transport*. available at: <http://transport-journal.com/komentarii-obzori/resursnyij-potentsyal-rechnoho->

transporta-ukraynyi-problemyi-zadachy-y-meryi-po-razvytyyu-y-effektyvnomu-
yspolzovanyyu/ [Ukraine].

3. National Institute for Strategic Studies (2015), *Rozvytok richkovoho transportu u konteksti realizatsiyi yevrointehratsiynykh planiv Ukrayiny* [Development of river transport in the context of implementation of European integration plans of Ukraine] : analytical note. available at: <http://www.niss.gov.ua> [Ukraine].

4. Tymoshchuk O. M. and Mel'nyk O. V. (2013), "*Formuvannya mekhanizmu realizatsiyi lohistychnoyi stratehiyi richkovykh portiv*" ["Formation of the mechanism of realization of the logistic strategy of river ports"] // *Journal Problemy ekonomiky* [Problems of the economy], vol. 3, pp. 149–155 [Ukraine].

5. Litvinova Ya. V. (2017), *Udoskonalennya lohistychnoho upravlinnya riznyimi vydamy transportu, skladuvannyam ta pererobkoyu vantazhiv u transportnykh vuzlakh* [Improvement of logistic management of various types of transport, warehousing and processing of goods in transport nodes] : diss. ... Ph.D. (doc. philosophy), specialty: 05.22.01. KNADU, Kharkov, 200 c. [Ukraine].

6. Boniar S. M. and Valiavs'ka N. O. (2015), *Zatsikavlenist' pidpryyemstv u pidvyshchenni konkurentospromozhnosti vnutrishnikh vodnykh shlyakhiv Ukrayiny* ["The interest of enterprises in increasing the competitiveness of inland waterways of Ukraine"] // *Journal Vodnyy transport* [Water transport], vol. 2, pp. 97–103 [Ukraine].

7. Murad'ian A. O. (2016), *Metodychni osnovy uz-hodzhenoho upravlinnya protsesom perevalky vantazhiv u zahal'notransportnykh vuzlakh* [Methodical bases of the coordinated management of the process of transshipment of cargoes in transport nodes] : diss. ... Ph.D, specialty : 05.22.01, Press Odessa sea Univer., Odesa, 166 p. [Ukraine].

8. Nahornyj Ye. V. and Shramenko N. Yu. (2011), "*Vyznachennya tekhnolohichnykh parametriv funktsionuvannya terminal'noho kompleksu v umovakh rynku transportnykh posluh*" ["Definition of technological parameters of the functioning of the terminal complex in the market of transport services"] // *Vestnik KhNADU*, vol. 53, pp. 51–55 [Ukraine].

9. Mel'nyk O. V. (2013), "*Obgruntuvannya stratehiyi rozvytku richkovykh portiv*" ["Justification of the strategy of development of river ports"] // *Journal Investytsiyi: praktyka ta dosvid* [Investments: practice and experience], vol. 15, pp. 99–101 [Ukraine].

10. Valiavs'ka N. O. (2016), "*Ekonomichne obgruntuvannya vprovadzheniya stratehiyi dyversyfikatsiyi v richkovykh portakh Ukrayiny*" ["Economic justification for implementation of diversification strategy in river ports of Ukraine"] // *Journal Efektyvna ekonomika* [Effective economy], vol. 1, available at : <http://www.economy.nayka.com.ua/?op=1&z=4875> [Ukraine].

11. VRU (2015), *Pro vnutrishniy vodnyy transport* [On Inland Water Transport] : Draft Law of Ukraine (date of registration: 2475a dated 04.08.2015), available at: http://www.mtu.gov.ua/uk/alias_50/51199.html [Ukraine].

12. Zabara S. S. and Dekhtiaruk M. T. (2015), “*Rozrobka avtomatyzovanoj systemy optymizatsiyi roboty perevantazhuval’noho kompleksu*” [“Development of an automated system for optimizing the operation of a reloading complex”] // *Vostochno-Evropeyskyy zhurnal peredovykh tekhnolohyy* [East European Journal of Advanced Technology], vol. 1/3 (73), pp. 8–14 [Ukraine].

13. Logistics Company Zammler (2016), *Vid Horishnikh Plavniv i dali. Stan richkovoho transportu v Ukrayini* [From Gorišni Plavni and further. State of river transport in Ukraine] : Infographics. Industry Overview, available at: http://texty.org.ua/pg/article/txts/read/68935/Vid_Gorishnih_Plavniv_i_dali_Stan_richkovogo [Ukraine].

14. Goncharuk O., Lavrinenko I. (2017), *Zelena knyha “Vantazhni perevezennya vnutrishnimy vodnymy shlyakhamy”* [Green book "Freight traffic by inland waterways"] / Office of effective regulation of BRDO. August, 80 p., available at: www.brdo.com.ua [Ukraine].

15. Zaporozhets’ O. I., Boychenko S. V., Matvyeyeva O. L. et al (2017), *Richkovi porty Ukrainy* [River ports of Ukraine] / in the book. : Transport Ecology, Tutorial, Press *Tsentr uchbovoyi literatury* [Center for Educational Literature], Kyiv, 508 p. available at: https://pidruchniki.com/92969/ekologiya/richkovi_porti_ukrayini [Ukraine].

16. Kuz'menko A. I. (2008), “*Udoskonalennya tekhnolohiyi perevezennya vantazhiv u mizhnarodnomu spoluchenni*” [“Improving the technology of transportation of cargoes in international traffic”] // *Visnyk Akademiyi mytnoyi sluzhby Ukrainy* [Bulletin of the Academy of the Customs Service of Ukraine], vol. 2 (38), pp. 77–82 [Ukraine].

17. *Richkovi terminaly na Dnipri* [River terminals on the Dnipro River], available at: <https://graintrade.com.ua/terminal/dnipropetrovskij-richkovij-port-ask-ukrrichflot-id1945> [Ukraine].

18. Kuz'menko A. I. and Shyshka A. M. (2018), “*Analiz perspektyv rozvytku richkovoho transportu v Ukrayini*” [“Analysis of the Prospects for the Development of River Transport in Ukraine”] // *Tendentsiyi ta perspekt. rozv. nauky i osvity v umovakh hlobalizatsiyi* [Trends and Prospects. solving Science and Education in a Globalizing Environment] : materials International sciences internet confer (vol. 40). Pereyaslav-Khmelnitsky, pp. 676–680 [Ukraine].

19. Kuz'menko A. I. (2013), *Udoskonalennya tekhnolohiyi obrobky vahonopotokiv na stantsiyakh stykuvannya kolyi riznoyi shyryny* [Improvement of the technology of processing carriages at the stations of docking of tracks of different width]: dis. ... Ph.D, specialty: 05.22.01, Press DNU of Railway Transport named after Academician V. Lazaryan, Dnipropetrovsk, 204 p. [Ukraine].

Шановні автори!

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

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

2. Рукопис статті повинен мати такі елементи:

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

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

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

– **УДК**;

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

– **основний текст статті**;

– **список використаних джерел**.

3. Основний текст статті складається з таких структурних елементів:

Ключові слова (4–5 слів).

Постановка проблеми.

Аналіз останніх досліджень і публікацій.

Мета статті.

Виклад основного матеріалу.

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

Список використаних джерел оформлюється відповідно до ДСТУ 8302:2015.

Зазначені елементи виділяються в рукописі **напівжирним шрифтом**.

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

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

5. До редакції подаються:

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

– **електронний варіант статті**;

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

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

Передрук матеріалів дозволяється лише за письмової згоди редакції.

Матеріали, що публікуються, відображають позицію автора, яка може не збігатися з поглядом редакції. За достовірність фактів, статистичних даних та іншої інформації відповідальність несе автор.

Редакція залишає за собою право наукового та літературного редагування статей без додаткової консультації з автором. Листування з читачами ведеться лише на сторінках журналу.