

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ**

ВІСНИК

ЧЕРКАСЬКОГО ДЕРЖАВНОГО ТЕХНОЛОГІЧНОГО УНІВЕРСИТЕТУ

Серія : Технічні науки

Заснований у грудні 1996 р.

4/2017

Головний редактор д.т.н., професор **Лега Ю. Г.**

Редакційна колегія:

Заболотній С. В., д.т.н., доц.
(заступник головного редактора)
Астрелін І. М., д.т.н., проф.
Ващенко В. А., д.т.н., проф.
Волошин М. Д., д.т.н., проф.
Дідковський Р. М., д.т.н., проф.
Кажіс Р., д.т.н., проф. (Литва)
Канашевич Г. В., д.т.н., проф.
Котов В. М., д.т.н., проф. (Білорусь)
Кулик А. Я., д.т.н., проф.
Лужецький В. А., д.т.н., проф.
Лукашенко В. М., д.т.н., проф.
Мальований М. С., д.т.н., проф.
Мінаєв Б. П., д.х.н., проф.
Мусієнко М. П., д.т.н., проф.
Осипенко В. І., д.т.н., проф.
Палагін В. В., д.т.н., проф.
Паламарчук І. П., д.т.н., проф.
Первунінський С. М., д.т.н., проф.
Петрищев О. М., д.т.н., проф.
Положаєнко С. А., д.т.н., проф.
Рибін О. І., д.т.н., проф.
Рудницький В. М., д.т.н., проф.
Сетлак Г., д.ф.н. (Польща)
Слатінеану Л., д.т.н., проф. (Румунія)
Снитюк В. Є., д.т.н., проф.
Столяренко Г. С., д.т.н., проф.
Тесля Ю. М., д.т.н., проф.
Тимченко А. А., д.т.н., проф.
Хоменко О. М., к.х.н., доц.
*Мельник І. В. (відповідальний секретар
редакції)*

ЗАСНОВНИК І ВИДАВЕЦЬ –

Черкаський державний
технологічний університет

Свідоцтво про державну реєстрацію
друкованого засобу масової інформації
КВ № 6061 від 16.04.2002 р.

Виходить 4 рази на рік

АДРЕСА РЕДАКЦІЇ:

ЧДТУ, ІІ корпус, к. 246,
бульвар Шевченка, 460,
м. Черкаси, 18006,
тел. (0472) 73-02-29
chstu@chstu.cherkassy.ua

4 • 2017

ВІСНИК
Черкаського державного
технологічного університету

СЕРІЯ: ТЕХНІЧНІ НАУКИ

Затверджено до друку
рішенням Вченої ради
Черкаського державного
технологічного університету,
протокол № 7 від 18.12.2017 р.
за рекомендацією науково-
технічної ради ЧДТУ,
протокол № 4 від 27.11.2017 р.

Затверджено наказом
Міністерства освіти і науки України
№ 1328 від 21.12.2015
як фахове видання з технічних наук

Видання внесено до міжнародної бази індексування
та реферування наукових публікацій
Index Copernicus

Електронна версія: vtn.chdtu.edu.ua
<https://chdtu.edu.ua>

pISSN 2306-4412 / eISSN 2306-4455

Точка зору редколегії не завжди
збігається з позицією авторів.

При повному або частковому
передрукуванні матеріалів
посилання на “Вісник ЧДТУ”
є обов’язковим.

© “Вісник Черкаського
державного технологічного
університету”, № 4, 2017

© Автори випуску, 2017

ЗМІСТ

Новаковский А. Г., Антонюк В. С., Петренко С. Ф. Применения пьезоэлектрических актуаторов в микроманипуляторах	5
Гальченко В. Я. Оптимальный синтез структур электромагнитных измерительных преобразователей	11
Златкін А. А., Марусик О. С. Аналіз алгоритму мурашиних колоній та його модифікацій на прикладі вирішення задачі комівояжера	21
Мельник О. Г., Мельник Р. П. Оцінка оперативності прогнозування пожеж у житловому секторі	27
Лепський В. В. Методи інтегрованого управління загрозами забезпечення цінностей стейкхолдерів медичного проекту	32
Нахімі Мохаммад Ясін Мохаммад Хусайн. Роль використання структури декомпозиції робіт в управлінні змістом будівельних проектів	42
Петрищев О. Н., Базило К. В. Расчет электрического импеданса дискового пьезокерамического трансформатора с закороченным секторным электродом во вторичной электрической цепи	47
Петрищев О. Н., Базило К. В. Расчет коэффициента трансформации пьезокерамического трансформатора с секторными электродами	63
Базіло К. В., Зайка В. М., Бондаренко Ю. Ю., Петрушко Ю. А. Розробка ультразвукового пристрою для інтенсифікації біохімічних процесів у фармацевтиці	70
Тимченко А. А. Системний аналіз математичної задачі. Задачі побудови моделей	74
Рудницкий В. Н., Деткин В. Г., Хрулев Н. В., Кривоус Г. В. Функции и структура системы комплексного контроля вычислительных процессов	82
Харін О. О. Порівняльна оцінка факторіальних кодів	88
Куницька С. Ю. Технологія обробки інформації нормалізованих систем	94
Голуб М. В., Брик С. М., Гарасюта В. М., Савченко В. І., Сандига О. Ю. Технічні, технологічні умови та техніко економічні критерії електронно-променевої мікрообробки оптичних виробів малих розмірів	99
Прокопенко Т. О. Імітаційна модель прийняття рішень в управлінні організаційно-технологічними об'єктами	105
Панаско О. М., Хроленко М. В. Забезпечення захисту паролів користувачів в процедурах аутентифікації	111
Сисоєнко С. В., Мельник О. Г., Пустовіт М. О. Синтез операцій оберненого групового матричного криптографічного перетворення інформації	118
Миронець І. В., Кобрін В. О. Аналіз методів реалізації аутентифікації на основі маркерів доступу для корпоративної системи збереження та обміну даними	126
Миронець І. В., Маламуж А. В. Дослідження та оптимізація системи управління контентом для організації персонального сайту	134
Миронюк Т. В., Дуда Л. Т. Дослідження методів захисту онлайн спілкування	138
Лега Ю. Г., Гавриш О. С., Іващенко А. О., Бурдукова О. В., Багрій М. О. Аналіз потенційних характеристик квадратичного алгоритму вимірювання амплітуди гармонічного сигналу з флюктуючою частотою при когерентному прийомі	144

CONTENTS

<i>Novakovskii A. G., Antoniuk V. S., Petrenko S. F.</i> Applications of piezoelectric actuators in micromanipulators	5
<i>Galchenko V. Ya.</i> Optimum synthesis of structures of electromagnetic measuring transducers	11
<i>Zlatkin A. A., Marusik O. S.</i> Analysis of ant colonies algorithm and its modifications on the example of the solution of travelling salesman problem	21
<i>Melnyk O. G., Melnyk R. P.</i> Evaluation of the efficiency of fire forecasting in residential sector	27
<i>Lepskiy V. V.</i> The methods of integrated control by the threats of ensuring of the values of medical projects stakeholders	32
<i>Nakhimi Mokhammad Yasin Mokhammad Khusain.</i> The role of using the work breakdown structure in managing the content of construction projects	42
<i>Petrishchev O. N., Bazilo C. V.</i> Calculation of electrical impedance of disk piezoceramic transformer with a shorted sector electrode in secondary electrical circuit	47
<i>Petrishchev O. N., Bazilo C. V.</i> Calculation of transformation coefficient of piezoceramic transformer with sector electrodes	63
<i>Bazilo C. V., Zaika V. M., Bondarenko Yu. Yu., Petrushko Yu. A.</i> Development of ultrasonic device for intensification of biochemical processes in pharmaceutics	70
<i>Tymchenko A. A.</i> System analysis of mathematical task. Modeling tasks	74
<i>Rudnytskyi V. M., Detkin V. G., Khrulev N. V., Krivous G. V.</i> Functions and structure of the system of complex control of computational processes	82
<i>Kharin O. O.</i> Comparative evaluation of factorial codes	88
<i>Kunytska S. Yu.</i> Technology of information processing of normalized systems	94
<i>Holub M. V., Bryk S. M., Harasiuta V. M., Savchenko V. I., Sandyha O. Yu.</i> Technical, technological conditions and techno-economic criteria of electron-beam microprocessing of optical products of small sizes	99
<i>Prokopenko T. O.</i> Simulation model of decision-making in management by organizational and technological objects	105
<i>Panasko O. M., Khrolenko M. V.</i> Provision of user passwords protection in authentication procedures	111
<i>Sysoyenko S. V., Melnyk O. G., Pustovit M. O.</i> Synthesis of operations of reverse group matrix cryptographic transformation of information	118
<i>Myronets I. V., Kobrin V. O.</i> Analysis of methods for authentication implementation based on tokens of access for corporate system of data storage and sharing	126
<i>Myronets I. V., Malamuzh A. V.</i> Research and optimization of content management system for personal site organization	134
<i>Myronyuk T. V., Duda L. T.</i> Research of online communication protection methods	138
<i>Lega Yu. G., Havrysh O. S., Ivashchenko A. O., Burdukova O. V., Bagrii M. O.</i> Analysis of potential characteristics of the quadrated algorithm of measurement of harmonic signal amplitude with fluctuated frequency in coherent detection	144

А. Г. Новаковский,
В. С. Антонюк, д.т.н., профессор,
Национальный технический университет Украины
«Киевский политехнический институт имени Игоря Сикорского»
проспект Победы, 37, Киев, 13027, Украина
С. Ф. Петренко, д.т.н., профессор
НПК ООО «ЛИЛЕЯ», Киев, Украина

ПРИМЕНЕНИЯ ПЬЕЗОЭЛЕКТРИЧЕСКИХ АКТУАТОРОВ В МИКРОМАНИПУЛЯТОРАХ

В статье рассмотрены особенности использования пьезоэлектрических актуаторов в микроманипуляционных системах для осуществления перемещений на микронном уровне. Проведен анализ применения пьезоэлектрических актуаторов в микроманипуляционных системах разнообразных сфер деятельности человека. Показана эффективность использования пьезоэлектрических актуаторов в микрохирургии и биологии. Установлено, что перспективным является направление использования актуаторов в микроманипуляционных системах станков с ЧПУ для обеспечения перемещений во всех необходимых степенях свободы с минимальными погрешностями.

Ключевые слова: пьезоэлектрические актуаторы, микроманипуляторы, станки с ЧПУ, точность позиционирования, пьезоэлектрические преобразователи.

Актуальность. В настоящее время все более возрастающее значение приобретают прецизионные технологии, с которыми неразрывно связано создание новых устройств мехатроники и робототехники.

Создание таких устройств требует повышения точности приводов и, соответственно, точности перемещения их рабочих органов. Для осуществления микроперемещений на микронном уровне движения микроманипуляторов осуществляются за счет применения пьезоэлектрических актуаторов [1, 2].

Главным преимуществом таких устройств является беспрецедентная точность позиционирования, достигающая сотые и даже тысячные доли микрометра. Кроме того, они надежны, долговечны, обладают отличным быстродействием, развивают высокие ускорения и сочетают большое развиваемое усилие с компактностью. Очень важно и то, что пьезоактуаторы не имеют вращающихся и скользящих частей, не требуют смазывания и обслуживания, способны работать при низких температурах и в вакууме [3].

Так, например, в микрохирургии, благодаря замкнутой кинематической структуре, механизм платформы дельта-робота обладает большей жесткостью и выдерживает большую нагрузку в сравнении с механизмами, состав-

ленными в виде открытых кинематических цепей [4-6].

Применение роботизированных платформ позволяет осуществлять сверхточные манипуляции во время операции путем фильтрации тремора, а также масштабирования движения, чем значительно облегчает работу оператора и снижает вероятность ошибок, что весьма критично в данной области [7, 8].

Использование пьезоэлектрических актуаторов в микроманипуляционных системах также позволяет проведение операций на качественно новом уровне [9].

Вопросами проектирования робототехнических комплексов, их информационно-измерительных и управляющих систем, в том числе с применением пьезоэлектрических манипуляторов, занимались отечественные и зарубежные ученые В. П. Андреев, В. Л. Афонин, С. А. Воротников, Е. А. Девянин, М. Б. Игнатъев, П. Д. Крутько, Ю. В. Подураев, Л. Б. Рапопорт, А. М. Формальский, В. М. Шарапов, H. Asada, Y. Kuwata, M. Liu, A. Nüchter, S. Thrun, A. Waj-Fraj, A. West и др.

Исследования в области биологии при манипуляциях с клетками с применением пьезоэлектрических актуаторов значительно расширяют возможности экспериментальных исследований и позволяют снизить стоимость

проведения анализов ДНК и операции ЭКО [10-12].

Однако, несмотря на все выше заявленные преимущества, широкое распространение пьезоактуаторов ограничено рядом недостатков таких устройств, а именно: небольшой длиной хода, ограничивающей область их использования, и высокой ценой. Кроме того, при выборе между различными типами пьезоэлектрических актуаторов следует обращать внимание на исполняемое движение и требуемые характеристики устройств, что также снижает уровень их унификации.

Поэтому, в данной статье рассматриваются особенности применения пьезоэлектрических актуаторов в микроманипуляционных системах для осуществления перемещений на микронном уровне.

Целью данной статьи является анализ областей применения пьезоэлектрических актуаторов в микроманипуляторных системах с дальнейшими рекомендациями относительно применения этих систем для обеспечения перемещений с различными степенями свободы, гарантирующего минимум погрешности таких перемещений.

Анализ применения пьезоэлектрических актуаторов в микроманипуляторах. Широкая распространенность пьезоэлектрических актуаторов в микроманипуляционных системах, в первую очередь, связана с особенностями их функционирования.

В основе принципа их действия лежит обратный пьезоэлектрический эффект, то есть механическая деформация кристалла при воздействии на него электрического поля. При этом осуществляется преобразование электрического напряжения в небольшое, но крайне точно контролируемое линейное перемещение с высоким развиваемым усилием возвратно-поступательного движения.

Параллельную кинематическую структуру пьезоэлектрических актуаторов в микроманипуляторах используют системы наклона зеркал с одной подвижной платформой для всех направлений движения.

Данные системы показывают более высокую линейность характеристик, чем может быть достигнута путем последовательного переключения двух одноосных систем, при этом они остаются чрезвычайно компактными.

Системы наклона зеркал с пьезоэлектрическими актуаторами подходят как для высокودинамичной работы, такой как трек-

кинг, сканирование, стабилизация изображения, устранение дрейфа и вибрации, так и для статического позиционирования оптических систем и заготовок.

Известно также применение многослойного актуатора в контроллере потока припоя при производстве полупроводниковых систем, требующих сверхточного контроля (рис. 1) [13].

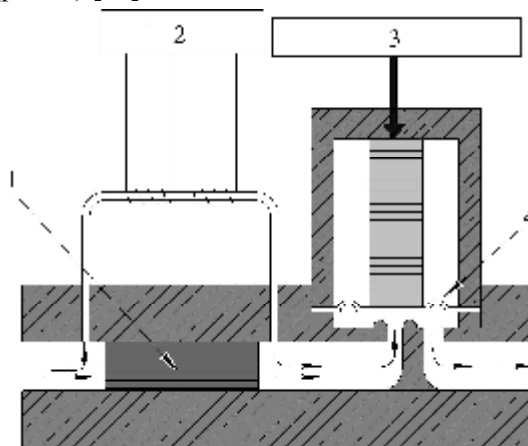


Рис. 1. Схема контроллера потока припоя в разрезе: 1 – проход; 2 – управление потоком; 3 – пьезоэлектрический актуатор; 4 – диафрагма

Использование пьезоэлектрического привода для управления мембраной позволяет контролировать поток точнее и быстрее, чем при использовании традиционного электромагнитного клапана.

Так, в работе [14] говорится про две разработанные системы управления для прецизионного позиционирования на основе усиливающего пьезоэлектрического актуатора, применяемые в многофункциональном тестовом оборудовании. В результате этого была разработана компьютерная модель упругой рамки усиливающего пьезоактуатора, проведено ее исследование, введены изгибные элементы в виде вырезов и оптимизированы их размеры для получения максимальной точности при максимальном диапазоне перемещения, что позволило обеспечить диапазон перемещения 104 мкм и увеличить точность позиционирования до 12 нм.

Следующий вариант использования пьезоактуаторов в промышленности – применение на этапе контроля точности положения системы экспонирования (рис. 2) [13].

Благодаря высокой гибкости и модульности конструкции, обеспечивающей минимальное время простоев, установки прецизионного совмещения и экспонирования широко

применяются в мире в области технологии микросистем, микроэлектромеханических систем (МЭМС) и биомикроэлектромеханических систем (БиоМЭМС), производства силовых компонентов, встроенной оптики и микрооптики, мультикристалльных модулей, в области нанотехнологий, тонкопленочных и гибридных технологий [15].

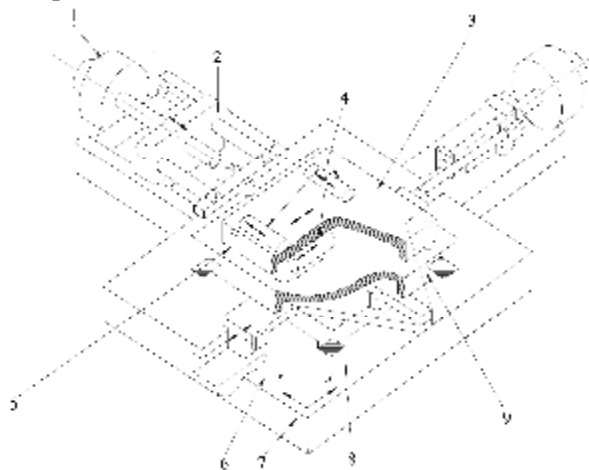


Рис. 2. Схема системы экспонирования в разрезе:
1 – двигатель постоянного тока; 2 – рамка привода оси Y; 3 – платформа прецизионного перемещения; 4 – пьезоэлектрический актуатор; 5 – поддерживающий гибкий вал; 6 – плоскость перемещения XY; 7 – основание; 8 – слайдер; 9 – стол для грубого перемещения

Грубое/быстрое перемещение в данной системе выполняется с помощью серводвигателя постоянного тока; прецизионное же перемещение осуществляется с помощью пьезоэлектрического привода [16]. Тот же метод применяется в других системах.

Так, например, известны оригинальные решения [17, 18], в которых пьезоэлектрические актуаторы применяются для сопоставления оптической оси оптоволоконного кабеля (рис. 3).

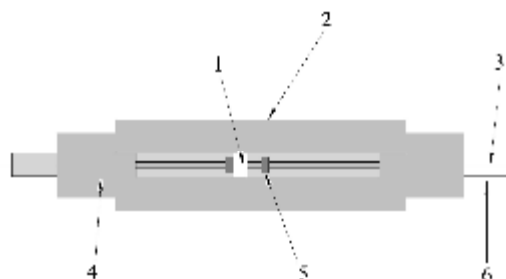


Рис. 3. Микроманипуляционная система сопоставления оптической оси оптоволоконного кабеля:
1 – воздушный зазор; 2 – пьезоэлектрический актуатор; 3 – оптоволоконный кабель; 4 – гнездо для оптоволоконного кабеля; 5 – зеркало; 6 – стеклянная гильза

Подобная система коррекции работает следующим образом: к пьезоэлектрическому приводу с отверстием в центре с двух сторон присоединяется оптоволоконный кабель.

Непосредственно привод центрирует оптическую ось двух кабелей на нанометровом уровне, что является одним из наиболее эффективных применений характеристик пьезоэлектрических актуаторов.

С 2000-х годов пьезоэлектрические актуаторы находят широкое применение в области потребительской электроники, например, в видеооборудовании. Одно из типичных применений – CCD привод.

Современные цветные видеокамеры для улучшения качества изображения используют метод «отклонения пикселей».

Суть метода – смещение CCD-матрицы на половину пикселя в горизонтальном направлении для увеличения количества «видимых пикселей».

Поскольку каждый CCD-пиксель обычно имеет размер от 5 до 7 мкм, расстояние отклонения составляет примерно половину от этого, или от 2,5 до 3,5 мкм.

Пьезоэлектрический актуатор также применяется для механической коррекции отклонений.

Универсальность, демонстрируемая применением данного устройства, привлекает внимание инженеров из-за его высокой точности позиционного управления и высокой скорости отклика при отслеживании съемки камеры.

Метод «отклонения пикселя» также используется для ЖК-проекторов с большой диагональю и видеокамер. Техника CCD привода также применяется для создания более компактного электронного оборудования, такого как цифровые камеры.

По мере увеличения количества пикселей число цифровых камер, в которых применяется метод стабилизации изображения, также увеличилось.

Бюджетные цифровые камеры часто корректируют размытие картинки, возникающее при дрожании рук, посредством электроники, дорогие же устройства, производящие изображения высокой четкости, корректируют «эффект дрожания рук» оптическими средствами.

Высокая скорость отклика пьезоэлектрического актуатора незаменима при выпол-

нении оптической коррекции изображения высокой чёткости.

Так, на рис. 4 схематично показана система коррекции изображения в цифровой камере.

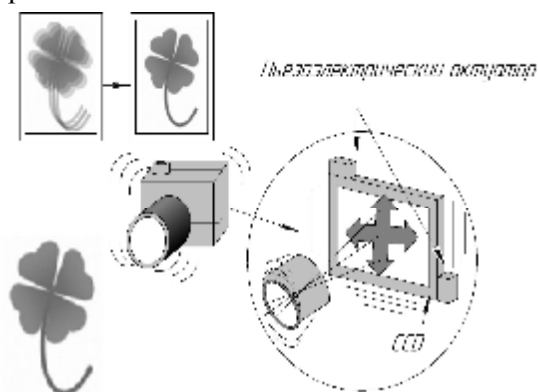


Рис. 4. Система коррекции изображения

Эта система корректирует эффект «дрожащих рук», перемещая CCD в плоскости XY и «нейтрализуя» эффект от движения рук, регистрируемых гиросенсором, соответственно пьезоэлектрический актуатор используется для управления матрицей CCD.

Выводы. Проведя анализ областей применения пьезоэлектрических актуаторов в микроманипуляторных системах, показана возможность применения этих устройств для обеспечения перемещений с различными степенями свободы, гарантирующего минимальные их погрешности.

Прогноз мирового рынка микроманипуляторных систем консалтинговой компанией "Yole Développement" (Франция) позволил установить, что на сегодняшний момент этот рынок почти достиг отметки 8 млрд. долл. США, а уже к 2021 году – составит около 12 млрд. долл. США [19].

Такое увеличение рынка микроманипуляторных систем связано с ростом спроса на них, резкое увеличение объемов производства, в свою очередь, ведет к значительному уменьшению себестоимости этих устройств. Так, например, типичный пьезоэлектрический актуатор в 2007 году стоил более одной тыс. долл. США, но уже в 2015 году аналогичное устройство при том же уровне функциональности имело стоимость около одного десятка долл. США.

Перспективным направлением является применение пьезоэлектрических актуаторов в микроманипуляционных системах станков с ЧПУ. С помощью таких систем можно обес-

печивать микроперемещения во всех необходимых степенях свободы в зависимости от поставленной задачи и с минимальными погрешностями (суммарная погрешность не должна превышать 5%).

Список литературы

1. Бобцов А. А., Бойков В. И., Быстров С. В., Григорьев В. В. Исполнительные устройства и системы для микроперемещений. Санкт-Петербург: СПбГУ ИТМО, 2011. 131 с.
2. Антонюк В. С., Белова А. В., Петренко С. Ф. Підвищення точності позиціонування лінійних направляючих мікроманіпуляційних систем з п'єзоелектричним двигуном. *Високі технології в машинобудуванні: зб. наук. праць*. Харків: НТУ «ХПІ», 2008. Вип. 2 (17). С. 12–20.
3. Пьезоэлектрические актуаторы пластинчатые изгибного типа. URL: <http://www.elpapiezo.ru/curve.shtml> (дата обращения: 15.10.2017).
4. Tan U. X., Latt W. T., Shee C. Y., Ang W. T. A low-cost flexure-based handheld mechanism for micromanipulation. *IEEE ASME Trans. Mechatronics*. 2011. Iss. 4. P. 773–778.
5. Choi D., Riviere C. Flexure-based manipulator for active handheld microsurgical instrument. *Proc. 27th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.* 2005. Iss. 5. P. 5085–5088.
6. Sungwook Y., Mac-Lachlan R. A., Riviere C. N. Manipulator design and operation for a six-degree-of-freedom handheld tremor-canceling microsurgical instrument *IEEE ASME Trans. Mechatronics*. 2015. V. 20 (2). P. 761–772.
7. Бардин В. А., Васильев В. А., Чернов П. С. Влияние внутренних дестабилизирующих факторов на пьезоактуаторы и системы нано- и микропозиционирования. *Университетское образование (МКУО-2014): XVIII Междунар. науч.-метод. конф.* (г. Пенза, 10-11 апреля 2014 г.). Пенза: Изд-во ПГУ, 2014. 584 с.
8. Fleming A. J. A review of nanometer resolution position sensors: Operation and performance. *Sensors and Actuators A*. 2013. № 190. P. 106–126.
9. Бардин В. А., Васильев В. А., Чернов П. С. Принципы построения и пер-

- спективы исследований пьезоактюаторов для нано- и микропозиционирования. *Нано- и микросистемная техника*. Москва: Новые технологии, 2015. № 1. С. 90–93.
10. Ramadan A., Inoue K., Arai T., Takubo T. New architecture of a hybrid two-fingered micro-nano manipulator hand: optimization and design. *Adv. Robot.* 2008. V. 2. Iss. 2–3. P. 235–260.
 11. Рябцов А. В. Специальные типы пьезоэлектрических актуаторов для оптических коммутационных устройств. *Вісник ДУИКТ*. 2013. № 1. С. 53–57.
 12. Antonjuk V. S., Pryhodko A. V. To study how micromanipulation system work at the nanoscale. *Вісник НТУУ «КПІ». Серія Приладобудування*. 2012. Вип. 44. С. 5–15.
 13. Ланин В., Турцевич А., Керенцев А. Дозирование припоя при автоматизированном монтаже кристаллов полупроводниковых приборов. *Компоненты и технологии*. 2008. № 11. С. 154–158.
 14. Амельченко А. Г., Бардин В. А., Васильев В. А. Системы управления и элементы усиливающего пьезоэлектрического актуатора для прецизионного позиционирования. *Известия высших учебных заведений. Поволжский регион. Технические науки*. 2015. № 3 (35). С. 111–124.
 15. Fleming M. B., Hutley M. C. Blazed diffractive optics. *Appl. Opt.* 1997. Iss. 36. P. 4635–4643.
 16. Bondarenko M., Bondarenko I. Power supply method of micro- and nanosystem engineering devices. *Energy Challenges & Mechanics: 6th International Symp. (Inverness, 14-18 August 2016)*. Inverness, Scotland, UK, 2016. P. 245–246.
 17. Канашевич Г. В., Бондаренко М. О. Сучасні варіанти з'єднань волоконно-оптичних ліній зв'язку. *Вісник Черкаського інженерно-технологічного інституту. Серія: Техн. науки: зб. наук. праць*. Черкаси: ЧІТІ, 1998. № 3. С. 56–62.
 18. Бардин В. А., Васильев В. А. Принципы построения пьезоактюаторов для нано- и микроперемещений. *Опто-, наноэлектроника, нанотехнологии и микросистемы: тр. XVI Междунар. конф.* Ульяновск: УлГУ, 2013. С. 316–317.
 19. Status of the MEMS industry 2016 Edition. Sample of the analysis – 2016. Lyon, France: Yole Development SARL.
- ### References
1. Bobtsov, A. A., Boikov, V. I., Bystrov, S. V., Grigorev, V. V. (2011) Implementing devices and systems for micromovements. SPb.: SPbGU ITMO, 131 p.
 2. Antoniuk, V. S., Belova, A. V., Petrenko, S. F. (2008) Improved positioning accuracy of linear guiding micromanipulation systems with piezoelectric motor. *Vysoki tehnolohiyi v mashynobuduvanni: collection of scientific works*. Kharkiv: NTU “KhPI”, v. 2 (17), pp. 12–20.
 3. Piezoelectric actuators lamellar bending type. URL: <http://www.elpapiezoz.ru/curve.shtml> (15.10.2017).
 4. Tan, U. X., Latt, W. T., Shee, C. Y., Ang, W.T. (2011) A low-cost flexure-based handheld mechanism for micromanipulation. *IEEE ASME Trans. Mechatronics*, iss. 4, pp. 773–778.
 5. Choi, D., Riviere, C. (2005) Flexure-based manipulator for active handheld microsurgical instrument. *Proc. 27th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc*, iss. 5, pp. 5085–5088.
 6. Sungwook, Y., MacLachlan, R. A., Riviere, C. N. (2015) Manipulator design and operation for a six-degree-of-freedom handheld tremor-canceling microsurgical instrument. *IEEE ASME Trans. Mechatron*, v. 20 (2), pp. 761–772.
 7. Bardin, V. A., Vasilev, V. A., Chernov, P. S. (2014) Influence of internal destabilizing factors on piezoactuators and nano- and micropositional systems. *Universitetskoye obrazovaniye (MKUO-2014): XVIII Internat. sci. method. conf.* (Penza, April 10-11, 2014). Penza: PSU, 584 p.
 8. Fleming, A. J. (2013) A review of nanometer resolution position sensors: operation and performance. *Sensors and Actuators A*, № 190, pp. 106–126.
 9. Bardin, V.A., Vasiliev, V. A., Chernov, P. S. (2015) Principles of construction and prospect of research of piezoelectric actuators for nano- and micropositioning. *Nano i mikrosistemnaya tehnika*. Moscow: Novyye tehnologiyi, iss. 1, pp. 90–93.
 10. Ramadan, A., Inoue, K., Arai, T., Takubo, T. (2008) New architecture of a hybrid two-fingered micro-nano manipulator hand: optimization and design. *Adv. Robot*, v. 2, iss. 2–3, pp. 235–260.

11. Ryabtsov, A. V. (2013) Special types of piezoelectric actuators for optical switching devices. *Visnyk DUIKT*, iss.1, pp. 53–57.
12. Antonjuk, V. S., Pryhodko, A. V. (2012) To study how micromanipulation system work at the nanoscale. *Visnyk NTUU "KPI"*, v. 44, pp. 5–15.
13. Lanin, V. Turtsevich, A., Kerentsev, A. (2008) Dosing of solder in the automated installation of crystals of semiconducting devices. *Komponenty i tehnologiyi*, iss. 11, pp. 154–158.
14. Amelchenko, A. G., Bardin, V. A. Vasiliev V. A. (2015) Control systems and elements of a reinforcing piezoelectric actuator for precision positioning. *Izvestiya vysshyyh uchebnyh zavedenuu. Povolzhskii region. Tehnicheskiye nauki*, iss. 3 (35), pp. 111–124.
15. Fleming, M. B., Hutley, M. C. (1997) Blazed diffractive optics. *Appl. Opt.*, iss. 36, pp. 4635–4643.
16. Bondarenko, M., Bondarenko, I. (2016) Power supply method of micro- and nano-system engineering devices. *Energy Challenges & Mechanics: 6th Internat. Symp. (Inverness, August 14-18, 2016)*. Inverness, Scotland, UK, pp. 245–246.
17. Kanashevich, G. V., Bondarenko, M. O. (1998) Modern variants of connections of fiber optic communication lines. *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu. Seria: Tehnichni nauky: collection of scientific works*. Cherkasy: ChITI, iss. 3, pp. 56–62.
18. Bardin, V. A., Vasil'ev, V. A. (2013) Principles of constructing piezoactuators for nano- and microspaces. *Opto-, nanoelektronika, nanotehnologiyi i mikrosistemy: proc. of XVI Internat. conf.* Ulyanovsk: USU, pp. 316–317.
19. Status of the MEMS industry 2016 Edition. Sample of the analysis – 2016, Lyon, France: Yole Development SARL.

A. G. Novakovskii,

V. S. Antoniuk, D.Sc., professor,

National Technical University of Ukraine “Igor Sikorsky Kiev Polytechnic Institute”

37, Peremohy ave., Kyiv, 03056, Ukraine,

S. F. Petrenko, D.Sc., professor

Research and production complex “Lileya”, Kyiv, Ukraine

APPLICATIONS OF PIEZOELECTRIC ACTUATORS IN MICROMANIPULATORS

In the article features of the use of piezoelectric actuators in micromanipulative systems for carrying out displacements at micron level are considered. The purpose of this article is to analyze the application areas of piezoelectric actuators in micromanipulative systems with further recommendations regarding the application of these systems to provide movement with varying degrees of freedom, which guarantees minimum errors in such displacements. The analysis of the application of piezoelectric actuators in micromanipulative systems of various areas of human activity has been carried out. The effectiveness of using piezoelectric actuators in microsurgery and biology is shown. It has been established that the direction of the use of actuators in micromanipulative systems of CNC machines is promising to ensure the movements in all necessary degrees of freedom with minimal errors.

Keywords: piezoelectric actuators, micromanipulators, CNC machines, positioning accuracy, piezoelectric transducers.

Статтю представляє В. С. Антонюк, д.т.н., професор.

В. Я. Гальченко, д.т.н., профессор

e-mail: halchvl@gmail.com

Черкасский государственный технологический университет
б-р Шевченко, 460, Черкасы, 18006, Украина

ОПТИМАЛЬНЫЙ СИНТЕЗ СТРУКТУР ЭЛЕКТРОМАГНИТНЫХ ИЗМЕРИТЕЛЬНЫХ ПРЕОБРАЗОВАТЕЛЕЙ

Электромагнитные измерительные преобразователи в обязательном порядке содержат в своем составе полезадающие элементы конструкции, к числу которых относятся катушки с постоянным или переменным током, постоянные магниты, ферромагнитные или токопроводящие немагнитные элементы, предназначенные для формирования электромагнитного потока. Проектирование новых преобразователей является наиболее эффективным в случае его реализации на основе решения обратной задачи, когда в качестве исходных данных задается их желаемая характеристика, а результатом служит реализующая эту характеристику конструкция. Рассматриваются методы как параметрического синтеза в линейной и нелинейной постановке, так и структурно-параметрического синтеза различных преобразователей. Приводятся примеры синтеза датчика линейных перемещений, вихретоковых преобразователей, коэрцитиметра, эталонов магнитных единиц, мер магнитной индукции, источников постоянного и переменного магнитного поля, применяемых в составе устройств намагничивания-размагничивания.

Ключевые слова: электромагнитные измерительные преобразователи, оптимальный синтез, обратная задача, параметрический синтез, структурный синтез, метаэвристики, однокритериальная оптимизация, многокритериальная оптимизация.

Вступление. Электромагнитные измерительные преобразователи (ЭИП) нашли широкое применение в промышленности. Непрерывно растущая потребность в новых ЭИП, характеризующихся улучшенными техническими и метрологическими характеристиками, предопределяет необходимость проектирования все новых их образцов. Для решения этой проблемы приходится проводить многовариантные проектные расчеты, результатом которых является выбор одного из вариантов, обеспечивающего приемлемые характеристики. Такой подход хоть и можно считать приемлемым, но вряд ли можно назвать эффективным. Условимся в дальнейшем считать каждый из рассматриваемых при проектировании конструктивных вариантов ЭИП, характеризующихся различным набором полезобразующих элементов, среди которых катушки с постоянным или переменным током, постоянные магниты, ферромагнитные или токопроводящие немагнитные элементы, предназначенные для формирования электромагнитного потока, структурой ЭИП. Процесс проектирования образцов ЭИП может быть более совершенным в результате его реализации на основе решения так называемой об-

ратной задачи. В этом случае формулировка задачи состоит в задании в качестве исходных данных желаемых характеристик ЭИП, а результатом служит реализующая эти характеристики структура. Обратные задачи характеризуются значительными трудностями при их решении, что обусловлено существенной неустойчивостью их решения, и относятся к классу некорректно поставленных задач. Эта особенность предполагает использование специальных математических методов их решения, в основе которых лежит идея регуляризации. Особенно сложно поддаются решению нелинейные обратные задачи. При моделировании ЭИП достаточно редко удается избежать нелинейной постановки задачи. Это оказывается возможным только лишь в редких случаях, когда в состав структуры ЭИП не входят ферромагнитные элементы конструкции или в случае незначительных по величине магнитных полей, что позволяет не учитывать нелинейный характер зависимости индукции поля от напряженности и делает возможным решение задачи в линейном приближении. Если же приходится решать нелинейную задачу, то вычислительные затраты многократно возрастают и к сложностям ре-

шения некорректных задач еще дополнительно добавляются проблемы решения нелинейных задач электродинамики, в общем случае, в трехмерном пространстве, что само по себе не является тривиальным. Чаще всего задачи электродинамики решаются численно с применением методов конечных элементов, граничных и пространственных интегральных уравнений, что обусловлено современными требованиями к точности решения таких задач.

Цель данной работы – обобщение опыта проектирования новых образцов ЭИП с усовершенствованными техническими и метрологическими характеристиками как задачи оптимального синтеза структур на основе решения обратных задач электродинамики и демонстрация на примерах преимуществ данного подхода.

Теоретическая часть

1. Оптимальный параметрический синтез датчиков линейных перемещений

Первоначально рассмотрим задачу в *линейной постановке*. При проектировании ряда измерительных приборов для получения первичной информации широкое применение находят магнитные датчики линейных перемещений (ДЛП). Основными преимуществами таких датчиков являются высокая чувствительность, возможность построения датчиков с широким диапазоном измеряемой величины, возможность синтеза заданной функции преобразования. Конструкция магнитного функционального ДЛП представлена на рис. 1. Магнитное поле генерируется обмотками соленоидного источника магнитного поля (СИМП) с постоянным током 2, которые располагаются на немагнитном каркасе 1. Продольная составляющая напряженности магнитного поля регистрируется ферро модуляционным чувствительным элементом 3, который закреплен на подвижном штоке 4. Обмотки располагаются в ферромагнитном экране 5. На основе ДЛП может строиться ряд других датчиков, таких как датчики давления, уровня, положения и т.д., что обуславливает повышенный интерес к их проектированию. При конструировании ДЛП в обязательном порядке решается задача синтеза СИМП, которые обеспечивают требуемое распределение магнитного поля на оси и располагаются в экране из ферромагнитного материала с диаметром D_e и длиной l_e (см. рис. 1), причем метрологические характеристики и чувствительность ДЛП зависят от точности синтеза и

конфигурации аксиальной составляющей напряженности магнитного поля в рабочей зоне, а габариты датчика – от эффективности использования длины СИМП в качестве рабочей зоны. Функция преобразования ДЛП может быть линейной или принимать иной вид, что зависит от распределения осевой составляющей поля вдоль оси датчика. Рабочая зона проектируемого СИМП задается в виде ограниченного числа контрольных точек на отрезке оси (с, d) с указанием в них требуемой напряженности поля H_c .

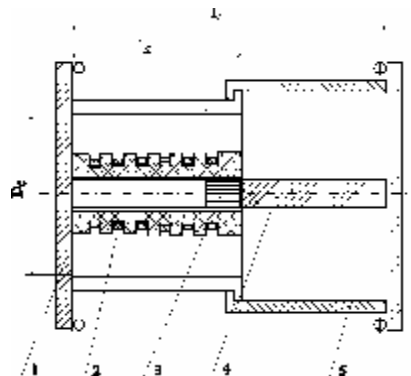


Рис. 1. Конструкция функционального магнитного ДЛП

Задача синтеза СИМП с заданным распределением напряженности поля на оси источника решается путем разбиения искомого источника на секции w_j на отрезке оси (a, b) и отыскания таких величин токов Iw_j в секциях, при которых среднеквадратичное отклонение действительного распределения поля в рабочей зоне от требуемого было бы минимальным. Дискретные источники поля могут включаться последовательно, встречно и/или согласно. Желательным представляется именно последовательное включение дискретных источников поля, так как в таком случае возможно питание СИМП от одного источника тока. Расстояние между секциями обмотки выбирается одинаковым, радиус секций обмоток также является постоянной величиной, что позволяет рассматривать линейную постановку задачи.

$$H_c(z) = \int_a^b K(z_j, z) w(z_j) dz_j,$$

$$a \leq z_j \leq b, \quad c \leq z \leq d$$

$$\int_c^d \left[\int_a^b K(z_j, z) w(z_j) dz_j - H_c(z) \right]^2 dz + \alpha \Omega,$$

где α – параметр регуляризации,

Ω – стабилизатор первого порядка.

Таким образом, задача сводится к решению интегрального уравнения Фредгольма 1-го рода.

На втором этапе рассмотрим подобную задачу, но уже в *нелинейной постановке*. Интерес представляет поиск оптимальной конфигурации информационной катушки ДЛП в пространстве геометрических параметров катушки. Решением задачи параметрического синтеза СИМП является такая совокупность геометрических размеров, координат, определяющих взаимное расположение секций, величин тока и количества витков в секциях, т.е. интенсивности дискретных источников магнитного поля и их расположения в пространстве, при которых обеспечивается требуемое распределение напряженности магнитного поля в заданной области, как показано на рис. 2.

Некоторые из возможных конфигураций распределения поля на оси ДЛП иллюстрируются рис. 3. Точность решения задачи синтеза СИМП характеризуется величиной максимального относительного отклонения действительной величины напряженности магнитного поля в рабочей зоне от требуемой. В частном случае нелинейная задача синтеза СИМП с непрерывной круговой обмоткой, которая решается относительно, например, радиусов, описывается нелинейным интегральным уравнением 1-го рода с оператором Урысона:

$$\int_{\Omega} K[x, s, y(s)] ds = f(x), \quad x \in Q,$$

где $K(x, s, y(s))$ – ядро ИУ;

$f(x)$ – правая часть уравнения с областью определения Q ;

$y(s)$ – искомая функция с областью определения Ω .

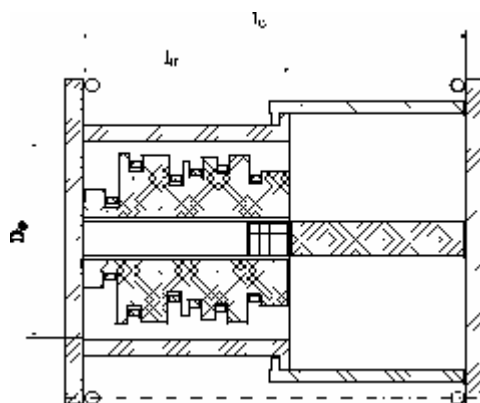


Рис. 2. Конструкция функционального ДЛП, для которого задача синтеза СИМП рассматривается в пространстве геометрических параметров катушки

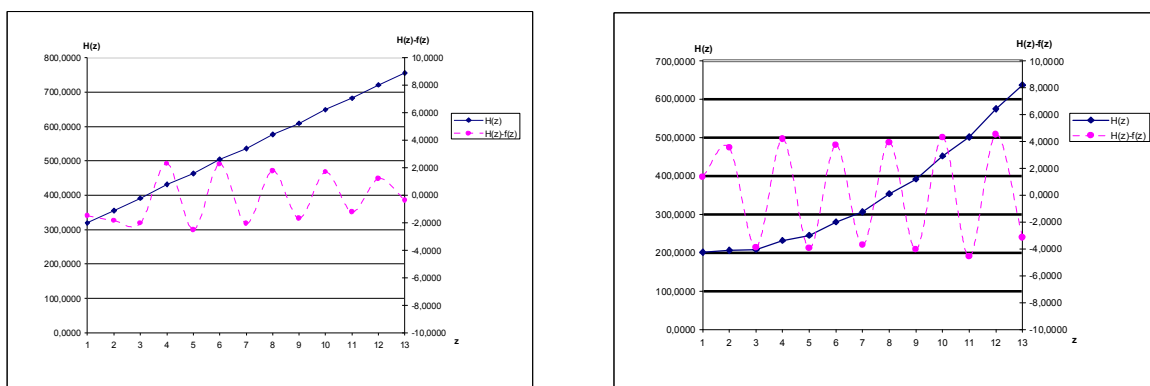


Рис. 3. Графики распределения информационного магнитного поля синтезированных катушек и абсолютного отклонения полученной напряженности поля от требуемой:

а) $H(z) = 20750 \cdot z + 300$, А/м

б) $H(z) = 10^6 \cdot (z - 10^{-3})^2 + 200$, А/м

Функция $K(x, s, y(s))$ представляет собой зависимость, по которой может быть рассчитана напряженность магнитного поля одной секции в заданной контрольной точке, $f(x)$ – требуемое значение напряженности магнитного поля в контрольной точке, $y(s)$ ассоциируется с искомыми параметрами СИМП, который обеспечивает заданную конфигурацию магнитного поля. Проблему синтеза СИМП предлагается рассматривать как задачу минимизации интегрального отклонения действительного распределения напряженности магнитного поля в контрольных точках от требуемого путем варьирования параметрами СИМП:

$$F = \sum_{i=1}^m |H(Q_i) - H(Q_i)_T|^\gamma \rightarrow \min,$$

где $H(Q_i)$ – действительное значение напряженности магнитного поля в i -й контрольной точке, $H(Q_i)_T$ – требуемое значение напряженности магнитного поля в i -й контрольной точке, m – число контрольных точек, в которых требуется обеспечение заданной напряженности поля, $\gamma = 8, 9, \dots$

2. Оптимальный параметрический синтез вихретоковых преобразователей

В вихретоковой дефектоскопии СИМП с рабочей зоной, расположенной в плоскости, перпендикулярной оси источника (рис. 4), находят применение в составе вихретоковых преобразователей (ВТП) с заданной конфигурацией зондирующего поля. Целью разработки и совершенствования методов синтеза та

ких ВТП является реализация в конструкциях ВТП новых технических возможностей, улучшение их эксплуатационных характеристик или повторение достигнутых в данном направлении результатов со значительными упрощениями конструкции. Использование указанных ВТП, в которых целенаправленное изменение конфигурации зондирующего поля в соответствии с заданными функциями распределения позволяет улучшить селективность и чувствительность преобразователей, повысить помехоустойчивость вследствие сужения зоны взаимодействия зондирующего поля с объектом, а также ограничения магнитных потоков рассеяния преобразователей, делает применение их достаточно перспективным. Конструктивные особенности структур ВТП представлены на рис. 4, где изображены ВТП с цилиндрической и радиальной генераторными катушками. Предлагается подход к синтезу СИМП, позволяющий решать задачу синтеза ВТП как в линейной постановке (варьированием параметрами I, ω), так и в нелинейной постановке (в пространстве переменных, определяющих геометрию генераторной катушки). Кроме того, предусмотрена возможность комбинирования указанных способов, т.е. выполнение поиска оптимального решения одновременным выбором геометрических параметров секций и их м.д.с. Выбор Z -координат секций может происходить как без ограничений, так и с условием, что некоторые секции сгруппированы и в обязательном порядке должны располагаться в одной плоскости.

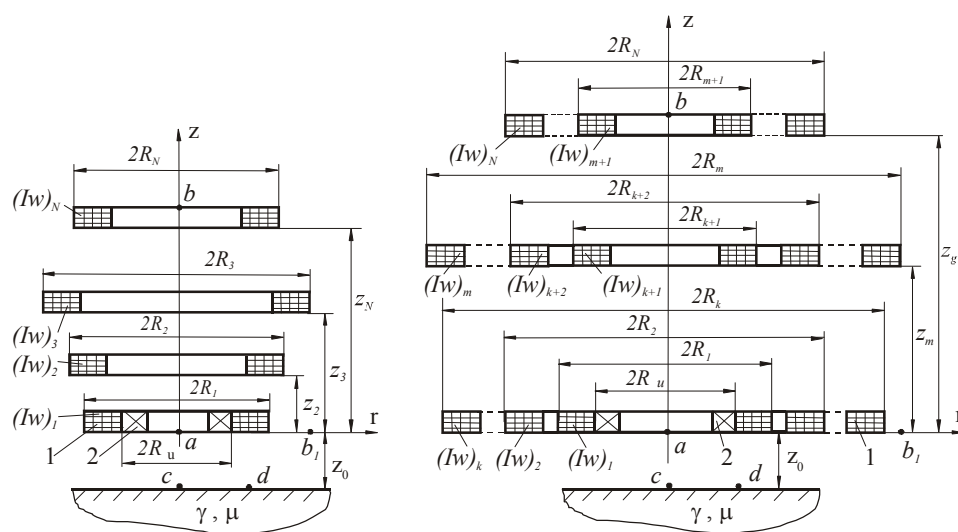


Рис. 4. Соленоидные источники магнитных полей накладных ВТП с рабочей зоной, расположенной в плоскости, перпендикулярной оси источника

Для решения задачи нелинейного параметрического синтеза СИМП с заданным распределением магнитного поля в области предложены специальные алгоритмы поиска оптимума в многомерной овражной ситуации. Основной идеей алгоритмов является организация покоординатного спуска вдоль ортогональных осей, соответствующих собственным векторам матрицы Гессе оптимизируемого функционала. Рассмотрена проблема учета ограничений на варьируемые параметры СИМП, вызванная необходимостью учета как простых ограничений для обеспечения требований к габаритам СИМП, так и специфических ограничений на взаимное расположение дискретных источников поля для выполнения условия их непересечения.

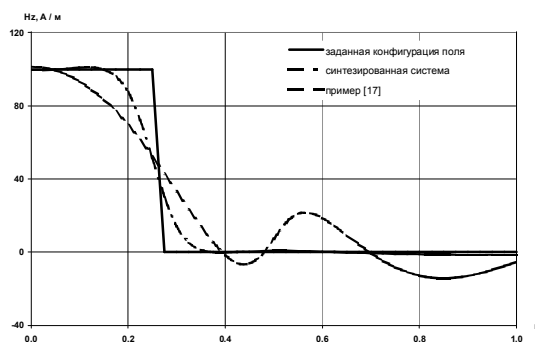


Рис. 5. Распределения зондирующих полей ВТП с П-образной формой в зоне контроля

Предложен модифицированный алгоритм покоординатного спуска с учетом ограничений на взаимное расположение секций СИМП с конечным поперечным сечением. Наибольший интерес вызывает магнитная система накладного ВТП с П-образной формой зондирующего поля в плоскости, параллельной рабочему торцу преобразователя (рис. 5).

3. Оптимальный структурно-параметрический синтез магнитных систем источников поля ЭИП

Исследуемые СИМП состоят из совокупности определенным образом расположенных в пространстве дискретных источников магнитных полей, которые в соответствии с принципом суперпозиции формируют некоторое распределение поля в рабочем объеме всей системы. Под дискретным источником магнитного поля понимается соленоидная секция — совокупность витков с током. В общем случае геометрическая форма секции

может быть произвольной. Магнитные системы могут быть как однородными по форме секций, так и смешанными (рис. 6). Интенсивность дискретного источника поля определяется числом витков и током, протекающим в нем. Подключенные последовательно секции магнитной системы питаются от единого источника тока. Дискретные переменные принято отождествлять со структурой магнитной системы, а непрерывные переменные — с параметрами рассматриваемой структуры. Следовательно, в качестве признаков структуры магнитной системы можно выделить число секций, их форму, направление намотки и число витков. Геометрические размеры и местоположение секций в пространстве являются параметрами структуры. Другими словами, магнитные системы, отличающиеся числом секций или их формой, а также характером подключения, имеют различную структуру, тогда как изменение расположения секций не является структурным преобразованием СИМП.

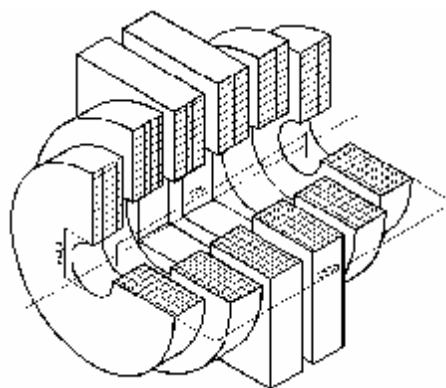


Рис. 6. Пример гетерогенной магнитной системы из шести секций

Концептуальная модель задачи оптимального структурного синтеза СИМП может быть сформулирована следующим образом. Необходимо найти оптимальную по сложности структуру магнитной системы, которая обеспечивала бы в пределах заранее обусловленной погрешности заданные пространственные свойства и физические параметры магнитного поля, создаваемого в рабочей области системы, а также соответствовала многочисленным конструктивным и иным требованиям: достижения особых размеров рабочей области; ограничений габаритных размеров системы; уменьшения потребляемой мощности и длины обмоточного провода и др. Опи-

санная задача оптимального структурного синтеза СИМП включает в себя несколько связанных между собой задач об определении: числа источников поля, их интенсивностей и геометрических форм, а также задачу нерегулярного размещения разнотипных источников. Таким образом, задача оптимального структурного синтеза является задачей глобальной векторной оптимизации, причем критерии отклонения поля и минимизации числа секций являются обязательными критериями, отражающими качество генерируемого в рабочей области СИМП поля и сложность системы. С математической точки зрения, рассматриваемая задача является многопараметрической многоэкстремальной задачей с ярко выраженной многосвязной невыпуклой областью поиска переменных размерности. Учитывая вышесказанное, становится очевидной целесообразность применения генетических алгоритмов для решения поставленной задачи. Генетические алгоритмы хорошо себя зарекомендовали как эффективные методы поиска для широкого класса задач оптимизации, не требующие дополнительной информации о характере исследуемой функции, которая может не иметь аналитического описания, ее свойствах (дифференцируемость, непрерывность и т.д.), не накладывающие ограничений на область поиска, которая может быть невыпуклой или многосвязной. Разработан метод и программное обеспечение оптимального структурного синтеза СИМП, базирующиеся на использовании генетического алгоритма, к отличительным особенностям которого относятся: модификации операторов генетического алгоритма, которые учитывают переменную длину представлений возможных решений в алгоритме; предложенная приближительная оценка подобия решений, введение которой обусловлено невозможностью вычисления расстояния Хемминга для их представлений; использование принципа Парето-доминирования для работы с вектором критериев оптимальности.

4. Оптимальный параметрический синтез аксиально-симметричных источников магнитного поля ЭИП с ферромагнитными элементами конструкции

Наряду с безарматурными источниками магнитного поля (ИМП) в составе ЭИП ши-

рокое применение нашли также источники, содержащие ферромагнитные элементы конструкции. Значительную долю таких устройств составляют устройства с аксиально-симметричными магнитными системами (АСМС). Наличие магнитной арматуры в составе ИМП существенно повышает сложность их синтеза. При проектировании источников поля, содержащих ферромагнитные элементы (ФЭ), необходимо определить значения их конструктивных параметров, которые бы обеспечили требуемое распределение магнитного поля с учетом их намагничивания. В силу сложного характера зависимости между значениями искомых параметров и топографией создаваемого поля задача поиска их оптимальных значений обычно формулируется и решается как задача параметрического синтеза. Также к проектируемому ИМП предъявляется ряд дополнительных требований, связанных с минимизацией объема их ФЭ, потребляемой мощности, ограничениями на допустимые геометрические размеры их конструктивных элементов и др., т.е. данная задача формулируется как многокритериальная. Проектирование ИМП с использованием метода оптимального параметрического синтеза предполагает построение параметризованных моделей источников. В процессе проведения синтеза, изменяя численные значения конструктивных параметров источников, удается подобрать их оптимальные значения, при которых получаемая топография магнитного поля в рабочем объеме Ω (рис. 7) в наилучшей степени соответствует необходимому физически реализуемому распределению поля. Отметим, что конфигурация магнитного поля в Ω контролируется в ряде контрольных точек, которые могут регулярно или нерегулярно располагаться в рабочем объеме.

Введем в рассмотрение модель АС ИМП, в которой в качестве варьируемых величин используются в общем случае геометрические размеры ФЭ конструкции и первичных источников поля (ПИП), численные значения протекающих токов I , а также координаты взаимного расположения конструктивных элементов в пространстве (см. рис. 7). В качестве ПИП в общем случае выступают катушки с током и постоянные магниты. ПИП и ФЭ могут использоваться при построении ИМП в произвольном количестве.

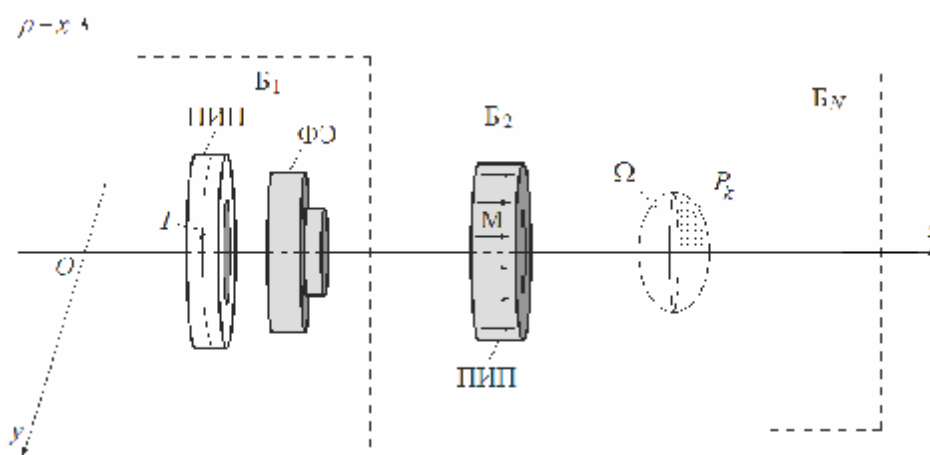


Рис. 7. Обобщенная схема аксиально-симметричных источников магнитного поля:
 $B_1, B_2, \dots, B_N$ – конструктивные блоки источника магнитного поля

Ферромагнитные элементы, входящие в состав ИМП, могут являться магнитопроводами, магнитными концентраторами, полюсными наконечниками, применение которых позволяет направленно изменять топографию поля, создаваемого ПИП. На практике на величины варьируемых параметров вводится ряд дополнительных ограничений, связанных с возможностью физической реализации ИМП. Эти ограничения могут быть связаны с требованиями к взаимной непересекаемости отдельных конструктивных элементов источников, допущениями о величине их минимальных и максимальных габаритов, предельным значением протекающих в катушках плотностей токов, не допускающим перегрев их обмоток. Для представления формы профиля МС предлагается ограничиться дискретизацией АС ИМП, при которой ФЭ представляются наборами цилиндрических или конических элементов. В рамках предложенной концепции решение задачи оптимального параметрического синтеза предполагает многократное повторение решения задачи расчета распределения поля в рабочем объеме при различных значениях конструктивных параметров магнитной системы. В оптимизационной постановке решение задачи оптимального параметрического синтеза ИМП предусматривает решение двух основных подзадач: эффективную реализацию метода расчета поля в рабочем объеме, а также разработку алгоритма многокритериальной оптимизации, позво-

ляющего находить оптимальные значения конструктивных параметров проектируемой магнитной системы с учетом ряда критериев. При этом высокой эффективности вычислительного процесса синтеза можно достичь при гармоничном сочетании алгоритмов расчета поля и оптимизации с учетом максимального числа специфических особенностей решаемой задачи. Для контроля получаемого распределения магнитного поля в рабочем объеме Ω вводится множество контрольных точек. В качестве погрешности синтеза магнитного поля заданной топографии принимается максимальное относительное отклонение напряженности поля в контрольных точках от требуемых значений. Требуемое значение напряженности магнитного поля может задаваться таблично или аналитически в виде некоторой функциональной зависимости. В основе метода синтеза применяется бионический алгоритм оптимизации, обеспечивающий возможность поиска глобального оптимума многоэкстремальных, многомерных овражных функций и функций, имеющих области типа «плато», являющихся характерными при решении задач данного типа, т.е. обратных задач в оптимизационной постановке. Значения целевых функций в рамках предложенного метода синтеза определяются алгоритмически, т.е. в результате численного расчета поля. В силу многоэкстремальности возникающих на практике оптимизируемых функций предложено в качестве основы такого алгоритма использо-

вать мультиагентные оптимизационные техники, обладающие глобальными поисковыми свойствами. Разработан гибридный бионический алгоритм оптимизации роем частиц с эволюционным формированием состава роя, позволяющий находить глобальное решение задачи параметрического синтеза. Гибридный алгоритм адаптирован для поиска Парето-оптимальных решений путем использования

рангов доминирования для каждого решения роя совместно с учетом приоритета каждого из частных критериев. Пример параметрического многокритериального синтеза коэрцитиметра с частично замкнутой магнитной системой и высокооднородным магнитным полем в рабочем объеме иллюстрируется рис. 8, 9.

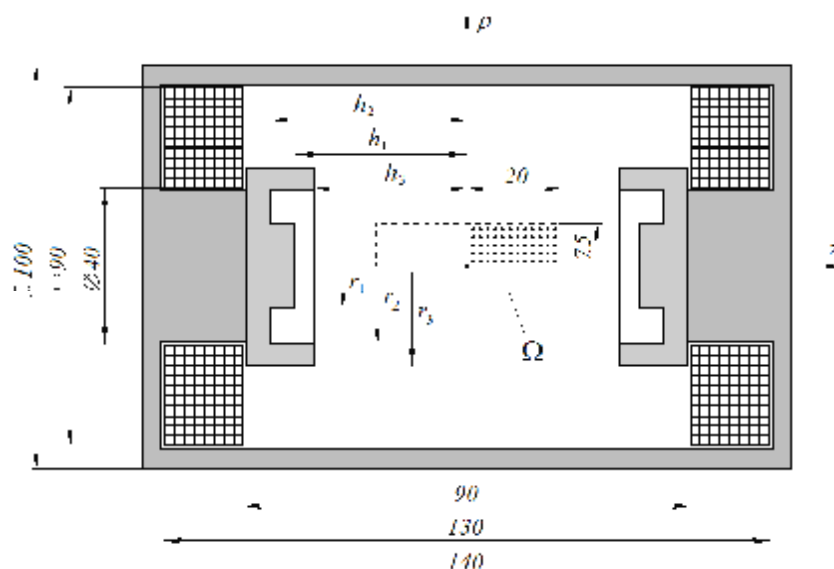


Рис. 8. Размеры и параметры синтезируемого коэрцитиметра с тремя полюсными элементами

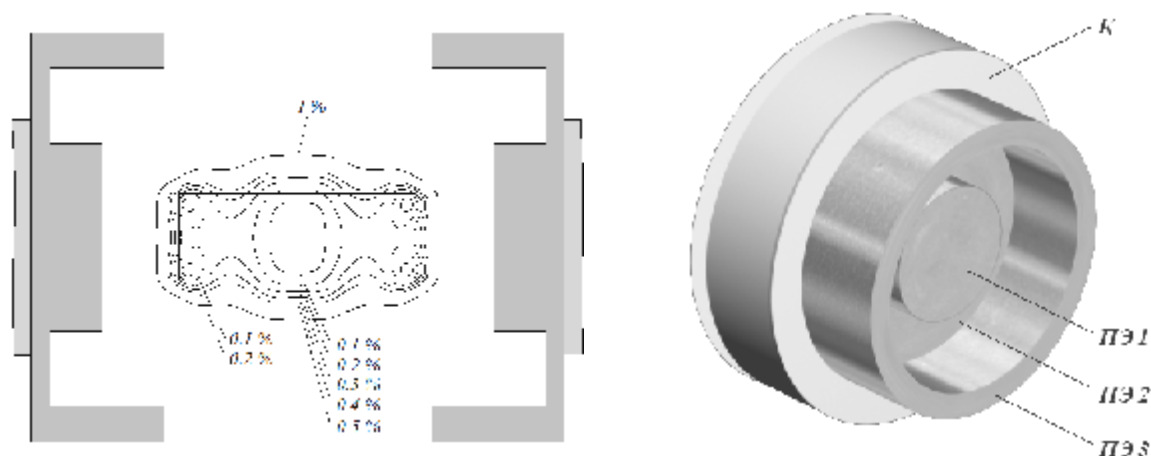


Рис. 9. Изолинии однородности поля в рабочем объеме коэрцитиметра и 3D-CAD модель полюсного наконечника магнитной системы коэрцитиметра:

K – катушка, ПЭ – полюсные элементы

Список литературы

References

- Galchenko V. Ya., Vorob'ev M. A. Structural synthesis of attachable eddy-current probes with a given distribution of the probing field in the test zone. *Russian Journal of Nondestructive Testing*. 2005. Vol. 41. No. 1. P. 29–33.
- Galchenko V. Ya., Yakimov A. N., Ostapushchenko D. L. Solution of the inverse problem of creating a uniform magnetic field in coercimeters with partially closed magnetic systems. *Russian Journal of Nondestructive Testing*. 2011. Vol. 47. No. 5. P. 295–307.
- Galchenko V. Ya., Yakimov A. N., Ostapushchenko D. L. Pareto optimal parametric synthesis of axisymmetric magnetic systems with allowance for nonlinear properties of the ferromagnet. *Technical Physics*. 2012. Vol. 57. No. 7. P. 893–899.
- Galchenko V. Ya., Yakimov A. N. A turmitobionic method for the solution of magnetic defectometry problems in structural-parametric optimization formulation. *Russian Journal of Nondestructive Testing*. 2014. Vol. 50. No. 2. P. 59–71.
- Galchenko V. Ya., Yakimov A. N. Creating uniform magnetization in short cylindrical ferromagnetic samples. *Russian Journal of Nondestructive Testing*. 2014. Vol. 50. No. 4. P. 198–204.
- Яковенко В. В., Гальченко В. Я., Донская Л. В. Синтез катушки в магнитной системе датчика линейных перемещений. *Электромеханика*. 1990. № 6. С. 75–78.
- Гальченко В. Я., Воробьев М. А. Использование генетических алгоритмов в структурном синтезе источников магнитных полей с заданными свойствами. *Информационные технологии*. 2003. № 7. С. 7–12.
- Гальченко В. Я., Якимов А. Н., Остапущенко Д. Л. Поиск глобального оптимума функций с использованием гибрида мультиагентной роевой оптимизации с эволюционным формированием состава популяции. *Информационные технологии*. 2010. № 10. С. 9–16.
- Гальченко В. Я., Якимов А. Н. Популяционные метаэвристические алгоритмы оптимизации роем частиц: учеб. пособие. Черкассы: ФЛП Третьяков А. Н., 2015. 160 с.
- Galchenko, V. Ya., Vorob'ev, M. A. (2005) Structural synthesis of attachable eddy-current probes with a given distribution of the probing field in the test zone. *Russian Journal of Nondestructive Testing*, vol. 41, No. 1, pp. 29–33.
- Galchenko V. Ya., Yakimov, A. N. Ostapushchenko, D. L. (2011) Solution of the inverse problem of creating a uniform magnetic field in coercimeters with partially closed magnetic systems. *Russian Journal of Nondestructive Testing*, vol. 47, No 5, pp. 295–307.
- Galchenko, V. Ya., Yakimov, A. N. Ostapushchenko, D. L. (2012) Pareto optimal parametric synthesis of axisymmetric magnetic systems with allowance for nonlinear properties of the ferromagnet. *Technical Physics*, vol. 57, No. 7, pp. 893–899.
- Galchenko, V. Ya., Yakimov, A. N. (2014) A turmitobionic method for the solution of magnetic defectometry problems in structural-parametric optimization formulation. *Russian Journal of Nondestructive Testing*, vol. 50, No. 2, pp. 59–71.
- Galchenko, V. Ya. Yakimov, A. N. (2014) Creating uniform magnetization in short cylindrical ferromagnetic samples. *Russian Journal of Nondestructive Testing*, vol. 50, No. 4, pp. 198–204.
- Yakovenko, V. V. Galchenko, V. Ya., Donaskaia, L. V. (1990) Synthesis of a coil in the magnetic system of a linear displacement transducer. *Elektromehnika*, No. 6, pp.75–78 [in Russian].
- Halchenko, V. Ya., Vorob'ev, M. A. (2003) The use of genetic algorithms in the structural synthesis of sources of magnetic fields with prescribed properties. *Informatsionnyye tehnologii*, No. 7, pp. 7–12 [in Russian].
- Galchenko, V. Ya., Yakimov, A. N., Ostapushchenko, D. L. (2010) Search for a global optimum of functions using a hybrid of multi-agent swarm optimization with evolutionary composition of the population composition. *Informatsionnyye tehnologii*, No. 10, pp. 9–16 [in Russian].
- Galchenko, V. Ya., Yakymov, A. N. (2015) Population meta-heuristic algorithms for optimization by a swarm of particles. *Cherkassy: FLP Tretyakov A. N.* 160 p. [in Russian].

V. Ya. Galchenko, *Dr.Tech.Sc., professor*
e-mail: halchvl@gmail.com
Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine

OPTIMUM SYNTHESIS OF STRUCTURES OF ELECTROMAGNETIC MEASURING TRANSDUCERS

Electromagnetic measuring transducers necessarily contain in their structure field-setting elements of the structure, including coils with direct or alternating current, permanent magnets, ferromagnetic or current-carrying non-magnetic elements intended for the formation of electromagnetic flow. The design of new transducers is the most effective in the case of its implementation based on the solution of the inverse problem, when the desired characteristic is given as the initial data, and the design realizing this characteristic is the result. Methods of both parametric synthesis in linear and nonlinear formulation and structurally-parametrical synthesis of various converters are considered. Examples of the synthesis of a linear displacement transducer, eddy current converters, coercimeters, standards of magnetic units, magnetic induction measures, sources of a constant and alternating magnetic field, used in magnetization-demagnetization devices, are given.

Keywords: *electromagnetic measuring transducers, optimal synthesis, inverse problem, parametric synthesis, structural synthesis, metaheuristics, one-criterion optimization, multi-criteria optimization.*

Статтю представляє В. Я. Гальченко, д.т.н., професор.

УДК 004. 724.4

А. А. Златкін, *д.т.н., професор*,
роб. тел. +380 (472) 730-271
e-mail: kafedra.itp@gmail.com

О. С. Марусик, *студентка магістратури кафедри інформаційних технологій проектування*
роб. тел.: +380 (093) 071-70-36
e-mail: oljamarusik@gmail.com
Черкаський державний технологічний університет
б-р Шевченка, 460, Черкаси, 18000, Україна

АНАЛІЗ АЛГОРИТМУ МУРАШИНИХ КОЛОНІЙ ТА ЙОГО МОДИФІКАЦІЙ НА ПРИКЛАДІ ВИРІШЕННЯ ЗАДАЧІ КОМІВОЯЖЕРА

У статті проведено детальний аналіз алгоритму мурашиних колоній – системи, заснованої на агентах, які імітують природну поведінку реальних мурашок. Охарактеризовано основні модифікації мурашиного алгоритму: алгоритм *Elitist Ant System*, алгоритм *Ant-Q*, алгоритм *Ant Colony System*, алгоритм *Max-min Ant System*, алгоритм *ASrank*. Описано пропонувані мурашиний алгоритм оптимізації для задачі комівояжера. Визначаючи алгоритм мурашиних колоній як один із найбільш перспективних напрямів «природних досліджень», наголошено, що використання детермінованої стратегії пошуку дозволило знайти оптимальний шлях значно швидше порівняно з ймовірнісною стратегією.

Ключові слова: мурашині колонії, феромон, задача комівояжера, алгоритм, модифікація.

Постановка проблеми. На сьогоднішній день процес обміну інформацією є одним із найголовніших аспектів діяльності як цілих організацій, так і кожної окремо взятої людини, а бездротові мережі є основним напрямком розвитку мережевої індустрії. Саме тому питання ефективної маршрутизації залишається важливим та актуальним, оскільки саме маршрутизація впливає на швидкість передачі інформації від одного користувача до іншого.

Основною перевагою створення спеціалізованих мереж є можливість встановлення зв'язу між терміналами звідусіль і в будь-який момент часу без допомоги фіксованої, централізованої мережевої інфраструктури. Проте питання ефективності вибору оптимальних маршрутів передачі даних все ще не втрачає своєї актуальності. Саме тому напрям так званих «природних обчислень» є перспективним рішенням основних задач динамічної маршрутизації, а саме швидкого пошуку надійних шляхів передачі даних між вузлами мережі.

Ідея мурашиного алгоритму полягає у моделюванні поведінки мурашок, пов'язаної з їх здатністю швидко знаходити найкоротшу дорогу від мурашника до джерела їжі і адаптуватися до умов, що змінюються, знаходячи нову найкоротшу дорогу. Алгоритм мурашиних колоній – це система, заснована на аген-

тах, які імітують природну поведінку реальних мурашок, такі як пошук їжі, перенесення її до гнізда тощо. При своєму русі мураха містить шлях феромоном, і ця інформація використовується іншими мурахами для вибору шляху. Це елементарне правило поведінки і визначає здатність мурах знаходити новий шлях, якщо старий виявляється недоступним. У такому алгоритмі кожний шлях, яким йде мураха, пов'язаний з вирішенням заданої проблеми, а кількість феромону, що нанесена на шлях, пропорційна тому, наскільки цей шлях відповідає поставленій задачі. Дійшовши до перепони, мурахи з однаковою ймовірністю будуть обходити її справа і зліва. Те саме буде відбуватися і на зворотному боці перешкоди. Коли мурахам потрібно зробити вибір між більш ніж двома шляхами, з більшою ймовірністю буде обраний шлях з більшою кількістю феромонів.

Така система була запропонована для вирішення комбінаторної задачі оптимізації та була визнана надійною, масштабованою й універсальною.

Аналіз останніх досліджень. Дослідження мурашиних алгоритмів почалося з середини 90-х років. Вагомі результати отримано у вирішенні таких непростих комбінаторних задач, як задача комівояжера, оптимізація маршрутів перевезень, квадратична задача

про призначення, завдання оптимізації мережових графіків і багато інших. Особливо ефективні мурашині алгоритми при динамічній оптимізації процесів у розподілених нестаціонарних системах, наприклад трафіків у телекомунікаційних мережах [1-2].

Алгоритм Ant System (AS) є своєрідною евристичною біонічною еволюційною системою, заснованою на інтелектуальному аналізі, і запропонованою італійським вченим М. Доріго спочатку для вирішення задачі комівояжера. Експериментальні результати доводять, що мурашиний алгоритм є дуже надійним і здатним знаходити оптимальне рішення, але, з другого боку, має дефект низької швидкості конвергенції та тенденцію до стагнації. Пізніше Л. М. Гамбарделла та М. Доріго висунули вдосконалений алгоритм – це алгоритм Ant-Q, який заміняє правило стохастичного пропорційного вибору правилом переходу псевдовипадкового пропорційного стану в Ant-Q. А на основі Ant-Q М. Доріго запропонував Ant Colony Systems (ACS). М. Доріго та інші вчені продовжують розробляти мурашині алгоритми в загальноживану методику оптимізації, що називається оптимізацією мурашиної колонії (ACO), і всі алгоритми, які відповідають схемі ACO, називаються мурашиними алгоритмами оптимізації [3]. На даний момент алгоритм оптимізації мурашиної колонії був використаний при вирішенні оптимальної комбінаторної задачі, проблеми оптимізації функцій, планування роботи, виявлення даних, маршрутизації мережі та досяг хороших результатів.

Результати перших експериментів із застосуванням мурашиного алгоритму для вирішення завдання комівояжера були багатообіцяючими, проте далеко не кращими порівняно з вже існуючими методами. Однак простота класичного мурашиного алгоритму (названого «мурашиною системою») залишала можливість для доробок – і саме алгоритмічні удосконалення стали предметом подальших досліджень Марко Доріго та інших фахівців у галузі комбінаторної оптимізації. В основному ці вдосконалення пов'язані з великим використанням історії пошуку та більш ретельно з дослідженням областей навколо вже знайдених вдалих рішень.

Метою цього дослідження є пошук шляхів для вдосконалення процесу роботи мурашиного алгоритму, що дасть можливість

покращити процес багатошляхової маршрутизації у мобільних мережах та в перспективі стане основою для розробки нових протоколів маршрутизації.

Виклад основного матеріалу. Алгоритм мурашиних колоній є одним із найперспективніших методів для вирішення задачі маршрутизації, проте він не є ідеальним, зокрема через те, що розподіл ймовірностей змінюється залежно від ітерацій, має велику залежність від параметрів налаштування, що можна підібрати лише на основі експериментів. Саме тому дослідження алгоритму призвело до створення ряду його модифікацій.

Алгоритм Elitist Ant System. Метод оптимізації роботи алгоритму мурашиної колонії, представлений Марком Доріго в 1992 р., є імовірнісним методом для вирішення обчислювальних задач, які можуть бути зведені до пошуку оптимальних шляхів через графи.

Раніше в усіх алгоритмах Ant System (AS) мурашки знаходять рішення, що базуються на двох основних компонентах: феромони та евристична інформація. Таким чином, AS перетворився на Elitist Ant System (EAS), де кожна мурашка, яка знаходить краще рішення, має можливість розмістити більше феромонів.

Практична реалізація алгоритму вказує як на переваги, так і на явні недоліки модифікації: збільшення кількості мурах в алгоритмі Elitist Ant System дозволяє значно зменшити кількість проведених алгоритмом ітерацій, проте у випадку, коли кількість мурах занадто велика, алгоритм швидко знаходить субоптимальне рішення і застряє в ньому.

Алгоритм Ant-Q. У 1995 р. Лука Гамбарделла і Марко Доріго опублікували роботу, в якій вони запропонували модифікацію алгоритму мурашиних колоній, запропонувавши інтерпретувати систему як ту, що може навчатись. Ant-Q отримав свою назву відповідно до методу машинного навчання Q-learning, та перейнявши багато ідей Q-навчання.

Кожному із ребер присвоюється величина, яка вказує на доцільність переходу по цьому шляху. Значення корисності переходу по ребру обчислюється, виходячи зі значень корисностей переходу за наступними ребрами в результаті попереднього визначення можливих наступних станів. Ці величини зберігаються у Q-таблиці, тобто дані модифікуються та змінюються у процесі роботи алгоритму [6-7].

Алгоритм Ant Colony System. У 1997 р. ті ж дослідники опублікували роботу, присвячену ще одному розробленому ними мурашиному алгоритму. Для підвищення ефективності порівняно з класичним алгоритмом ними були введені три основні зміни [6].

По-перше, рівень феромонів на ребрах оновлюється не тільки в кінці чергової ітерації, але й при кожному переході мурах з вузла у вузол. По-друге, в кінці ітерації рівень феромонів підвищується тільки на найкоротшому зі знайдених шляхів. По-третє, алгоритм використовує змінне правило переходу.

Max-min Ant System. У 1997 р. Томас Штютцле (Tomas Stützle) і Хольгер Хоос (Holger Hoos) запропонували мурашиний алгоритм, в якому підвищення концентрації феромонів відбувається тільки на кращих шляхах, пройдених мураками. Така велика увага до локальних оптимумів компенсується введенням обмежень на максимальну і мінімальну концентрацію феромонів на ребрах, які вкрай ефективно захищають алгоритм від передчасної збіжності до субоптимальних рішень.

На етапі ініціалізації концентрація феромонів на всіх ребрах встановлюється рівною максимальній. Після кожної ітерації алгоритму тільки один мураха залишає за собою слід – або найбільш успішний на цій ітерації, або, аналогічно алгоритму з елітизмом, елітний. Цим досягається, з одного боку, більш ретельне дослідження області пошуку, з другого – його прискорення.

Алгоритм ASrank. Бернд Бульнхаймер, Ріхард Хартл і Христина Штраусс розробили модифікацію класичного мурашиного алгоритму, в якому в кінці кожної ітерації мурахи ранжуються відповідно до довжини пройдених ними шляхів. Кількість феромонів, що залишена мурахою на ребрах, таким чином, призначається пропорційно його позиції. Крім того, для більш ретельного дослідження границь вже знайдених вдалих рішень, алгоритм використовує елітних мурах [6-7].

Аналіз алгоритму на прикладі задачі комівояжера. В процесі аналізу досліджувалися три варіанти алгоритму [4]:

1. При однаковій зміні феромону в усіх ребрах на 1.
2. При локальній зміні феромону на ребрах обернено пропорційно довжині ребра.
3. При глобальній зміні феромону в усіх ребрах (обернено пропорційно довжині шляху).

Також варіювалася кількість мурах, що розміщуються у вузлах мережі: 1–5, 10, 30, 50. Спочатку мурахи розміщувалися в усіх вузлах мережі. В ході експериментів генерувалися різні топології мережі, а також варіювалася кількість ітерацій і фіксувалася кількість ітерацій, при яких досягався оптимальний цикл. У наведених результатах таблиць цифра 0 означає, що не був знайдений жодний цикл, цифра 1 – знайдений неоптимальний шлях, 2 – знайдений оптимальний шлях (цикл) [8].

Результати експериментів з використанням детермінованої стратегії пошуку оптимального маршруту представлено у табл. 1–6.

Експерименти з використанням тактики пошуку оптимального шляху зі сталим приростом феромону (табл. 1–2).

Таблиця 1

Підхід до пошуку оптимального шляху з орієнтуванням на найбільшу концентрацію феромону

		Кількість мурах у вузлах перед запуском алгоритму							
		1	2	3	4	5	10	30	50
Номер ітерації	5	0	2	2	2	2	2	2	2
	50	0	2	2	2	2	2	2	2
	100	2	2	2	2	2	2	2	2
	250	2	2	2	2	2	2	2	2
	500	2	2	2	2	2	2	2	2
	1000	2	2	2	2	2	2	2	2
	1500	2	2	2	2	2	2	2	2

Таблиця 2

Підхід до пошуку оптимального шляху зі збереженням кращого знайденого шляху

		Кількість мурах у вузлах перед запуском алгоритму							
		1	2	3	4	5	10	30	50
Номер ітерації	5	2	2	2	2	2	2	2	2
	50	2	2	2	2	2	2	2	2
	100	2	2	2	2	2	2	2	2
	250	2	2	2	2	2	2	2	2
	500	2	2	2	2	2	2	2	2
	1000	2	2	2	2	2	2	2	2
	1500	2	2	2	2	2	2	2	2

Експерименти з використанням тактики пошуку оптимального шляху з приростом феромону на дугах, пропорційним довжині дуг (табл. 3–4).

Таблиця 3

**Підхід до пошуку оптимального шляху
з орієнтуванням на найбільшу
концентрацію феромону**

		Кількість мурах у вузлах перед запуском алгоритму							
		1	2	3	4	5	10	30	50
Номер ітерації	5	2	2	2	2	2	2	2	2
	50	2	2	2	2	2	2	2	2
	100	2	2	2	2	2	2	2	2
	250	2	2	2	2	2	2	2	2
	500	2	2	2	2	2	2	2	2
	1000	2	2	2	2	2	2	2	2
	1500	2	2	2	2	2	2	2	2

Таблиця 6

**Підхід до пошуку оптимального шляху зі
збереженням кращого знайденого шляху**

		Кількість мурах у вузлах перед запуском алгоритму							
		1	2	3	4	5	10	30	50
Номер ітерації	5	2	2	2	2	2	2	2	2
	50	2	2	2	2	2	2	2	2
	100	2	2	2	2	2	2	2	2
	250	2	2	2	2	2	2	2	2
	500	2	2	2	2	2	2	2	2
	1000	2	2	2	2	2	2	2	2
	1500	2	2	2	2	2	2	2	2

Таблиця 4

**Підхід до пошуку оптимального шляху зі
збереженням кращого знайденого шляху**

		Кількість мурах у вузлах перед запуском алгоритму							
		1	2	3	4	5	10	30	50
Номер ітерації	5	2	2	2	2	2	2	2	2
	50	2	2	2	2	2	2	2	2
	100	2	2	2	2	2	2	2	2
	250	2	2	2	2	2	2	2	2
	500	2	2	2	2	2	2	2	2
	1000	2	2	2	2	2	2	2	2
	1500	2	2	2	2	2	2	2	2

Експерименти з використанням тактики пошуку оптимального шляху з приростом феромону на дугах, пропорційним довжині знайденого замкнутого маршруту, що складається з цих дуг (табл. 5–6).

Таблиця 5

**Підхід до пошуку оптимального шляху
з орієнтуванням на найбільшу
концентрацію феромону**

		Кількість мурах у вузлах перед запуском алгоритму							
		1	2	3	4	5	10	30	50
Номер ітерації	5	0	0	0	0	2	2	2	2
	50	0	0	2	2	2	2	2	2
	100	0	2	2	2	2	2	2	2
	250	0	2	2	2	2	2	2	2
	500	0	2	2	2	2	2	2	2
	1000	0	2	2	2	2	2	2	2
	1500	0	2	2	2	2	2	2	2

Також було проведено аналогічні експерименти, але з використанням ймовірнісної стратегії пошуку оптимального маршруту. Результати представлено у табл. 7–10.

Експерименти з використанням тактики пошуку оптимального шляху з приростом феромону на дугах, пропорційним довжині дуг (табл. 7–8).

Таблиця 7

**Підхід до пошуку оптимального шляху
з орієнтуванням на найбільшу
концентрацію феромону**

		Кількість мурах у вузлах перед запуском алгоритму							
		1	2	3	4	5	10	30	50
Номер ітерації	5	0	2	0	0	2	0	1	0
	50	2	2	1	2	2	2	2	2
	100	1	2	1	2	2	2	2	2
	250	1	2	1	2	2	2	2	2
	500	1	2	1	2	2	2	2	2
	1000	1	2	1	2	2	2	2	2
	1500	1	2	1	2	2	2	2	2

Таблиця 8

**Підхід до пошуку оптимального шляху зі
збереженням кращого знайденого шляху**

		Кількість мурах у вузлах перед запуском алгоритму							
		1	2	3	4	5	10	30	50
Номер ітерації	5	0	2	1	2	2	1	2	2
	50	2	2	1	2	2	2	2	2
	100	2	2	1	2	2	2	2	2
	250	2	2	1	2	2	2	2	2
	500	2	2	1	2	2	2	2	2
	1000	2	2	1	2	2	2	2	2
	1500	2	2	1	2	2	2	2	2

Експерименти з використанням тактики пошуку оптимального шляху з приростом феромону на дугах, пропорційним довжині знайденого замкнутого маршруту, що складається з цих дуг (табл. 9–10).

Таблиця 9

Підхід до пошуку оптимального шляху з орієнтуванням на найбільшу концентрацію феромону

		Кількість мурах у вузлах перед запуском алгоритму							
		1	2	3	4	5	10	30	50
Номер ітерації	5	0	0	0	0	2	0	2	1
	50	0	0	2	2	2	1	2	2
	100	0	0	2	2	2	1	2	2
	250	0	0	2	2	2	1	2	2
	500	0	2	2	2	2	1	2	2
	1000	0	2	2	2	2	1	2	2
	1500	0	2	2	2	2	1	2	2

Таблиця 10

Підхід до пошуку оптимального шляху зі збереженням кращого знайденого шляху

		Кількість мурах у вузлах перед запуском алгоритму							
		1	2	3	4	5	10	30	50
Номер ітерації	5	0	2	2	2	2	2	2	2
	50	2	2	2	2	2	2	2	2
	100	2	2	2	2	2	2	2	2
	250	2	2	2	2	2	2	2	2
	500	2	2	2	2	2	2	2	2
	1000	2	2	2	2	2	2	2	2
	1500	2	2	2	2	2	2	2	2

Висновки. В роботі розглянуто мурашині алгоритми оптимізації і дано їх аналіз. Описано запропонований мурашиний алгоритм оптимізації для задачі комівояжера. Проведено його дослідження, в ході яких змінювалася стратегія відкладання феромону: були розглянуті і досліджені три стратегії: глобальна стратегія, локальна стратегія і постійна величина феромонів. Також змінювалася кількість мурах у вузлах мережі. Крім того, застосовувалися два типи стратегій вибору переходу: детермінована й імовірнісна. В результаті проведених досліджень були отримані наступні результати:

1. Збільшення кількості мурах у вузлах мережі від 1 до 2, 3–5 дає можливість поліпшити характеристики алгоритму і досягти мінімуму при меншій кількості ітерацій. При

подальшому збільшенні кількості мурах до 10, 30, 50 не дає ефекту.

2. Підхід, заснований на збереженні кращого шляху в ході роботи алгоритму, виявився більш ефективним.

3. Тактика приросту феромону, обернено пропорційна довжині дуг (локальна тактика), виявилася більш ефективною порівняно з глобальною тактикою і сталим приростом феромону.

4. Використання детермінованої стратегії пошуку дозволило знайти оптимальний шлях значно швидше порівняно з ймовірнісною стратегією.

Список літератури

1. Субботін С. О., Олійник А. О., Олійник О. О. Неітеративні, еволюційні та мультиагентні методи синтезу нечіткологічних і нейромережних моделей: монографія / під заг. ред. С. О. Субботіна. Запоріжжя: ЗНТУ, 2013. 375 с.
2. Ant colony optimization. URL: <http://iridia.ulb.ac.be/~mdorigo/ACO/ACO.html>
3. Goss S., Aron S., Deneubourg J.-L., Pasteels J.-M. Self-organized shortcuts in the Argentine ant, *Naturwissenschaften*. 2016. Vol. 76. P. 579–581.
4. Кажаров А. А., Курейчик В. М. Муравьиные алгоритмы для решения транспортных задач. *Известия Российской академии наук. Теория и системы управления*. 2014. № 1. С. 32–45.
5. Штовба С. Д. Муравьиные алгоритмы, Exponenta Pro. *Математика в приложениях*. 2014. № 4.
6. Dorigo M. Ant colony optimization. Scholarpedia. 2013.
7. Bonabeau E., Dorigo M., Theraulaz G. *Swarm intelligence: from natural to artificial systems*. Oxford University Press. 2012.
8. Ватулин Э. И., Титов В. С. Анализ результатов применения алгоритма муравьиной колонии в задаче поиска пути в графе при наличии ограничений. *Известия Южного федерального университета. Технические науки*. 2014. № 12 (161). С. 111–120.

References

1. Subbotin, S. O., Oliynyk, A. O., Oliynyk, O. O. (2013) Non-iterative, evolutionary and multi-agent methods of the synthesis of

- fuzzy logical and neuronet models: monograph. In: S. O. Subbotin (ed.). Zaporizhzhia: ZNTU, 375 p. [in Ukrainian].
2. Ant colony optimization. URL: <http://iridia.ulb.ac.be/~mdorigo/ACO/ACO.html>
 3. Goss, S., Aron, S. Deneubourg, J.-L., Pasteels, J.-M. (2016) Self-organized short-cuts in the Argentine ant, *Naturwissenschaften*, vol. 76, pp. 579–581.
 4. Kazharov, A. A., Kureychik, V. M. (2014) Ant algorithms for transport tasks solving. *Izvestiya Rossiyskoy akademii nauk. Teoriya i sistemy upravleniya*, № 1, pp. 32–45 [in Russian].
 5. Shtovba, S. D. (2014) Ant algorithms, Exponenta Pro. *Matematika v prilozeniyakh*, № 4 [in Russian].
 6. Dorigo, M. (2013) ant colony optimization. Scholarpedia.
 7. Bonabeau, E. Dorigo, M., Theraulaz, G. (2012) Swarm intelligence: from natural to artificial systems, Oxford University Press.
 8. Vatutin, E. I., Titov, V. S. (2014) The analysis of the results of ant colony algorithm application in the task of the search of the way in the graph under constraints. *Izvestiya Yuzhnogo federal'nogo universiteta. Tekhnicheskiye nauki*, № 12 (161), pp. 111–120 [in Russian].

A. A. Zlatkin, D.Sc., professor,
office tel. +380 (472) 730-271
e-mail: kafedra.itp@gmail.com

O. S. Marusik, student of the magistracy department of design information technologies
office tel. +380 (093) 071-70-36
e-mail: oljamarusik@gmail.com

Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine

ANALYSIS OF ANT COLONIES ALGORITHM AND ITS MODIFICATIONS ON THE EXAMPLE OF THE SOLUTION OF TRAVELLING SALESMAN PROBLEM

In the article a detailed analysis of ant colonies algorithm – a system based on agents that imitate natural behavior of real ants – is carried out. The main modifications of ant algorithm, such as: Elitist Ant System algorithm, Ant-Q algorithm, Ant Colony System algorithm, Max-min Ant System algorithm, ASrank algorithm, are characterized. The proposed ant optimization algorithm for travelling salesman problem is described. Determining ant colonies algorithm as one of the most promising areas of "natural research", it is emphasized that the use of deterministic search strategy has allowed to find the optimal path much faster than by means of probabilistic strategy.

Keywords: ant colonies, pheromone, travelling salesman problem, algorithm, modification.

Статтю представляє А. А. Златкін, д.т.н., професор.

О. Г. Мельник, к.т.н., ст. наук. співробітник,
e-mail: melnyk.olja.2014@gmail.com,

Р. П. Мельник, к.т.н.

Черкаський інститут пожежної безпеки імені Героїв Чорнобиля
Національного університету цивільного захисту України
вул. Онопрієнка, 8, Черкаси, 18034, Україна

ОЦІНКА ОПЕРАТИВНОСТІ ПРОГНОЗУВАННЯ ПОЖЕЖ У ЖИТЛОВОМУ СЕКТОРІ

У статті проведено оцінювання оперативності прогнозування пожеж у житловому секторі. Для цього було визначено швидкість реалізації моделей прогнозування пожеж, кількість об'єктів моніторингу з урахуванням технічних засобів збору та прийому інформації, кількість моделей з урахуванням часу, потрібного для моніторингу.

Було встановлено, що основним обмежувальним фактором часу обробки моделей є час доступу до даних на зовнішніх запам'ятовувальних пристроях.

Оцінювання швидкодії проводилося на основі отриманих залежностей з урахуванням сучасних характеристик персональних комп'ютерів та каналів зв'язку (Інтернет).

В результаті визначення часу прийому даних для однієї моделі доведено, що розроблені методи та засоби прогнозування пожеж у житловому секторі можуть забезпечити прогнозування в реальному часі передумов до виникнення пожеж у місті з населенням до 7 млн. залежно від характеристик технічних засобів.

Ключові слова: прогнозування пожеж, метод групового урахування аргументів, система залишкових класів, система числення, час прогнозування, оперативність прогнозування.

Постановка проблеми. Запобігання виникненню пожеж є вкрай важливим питанням сьогодення. Аналіз масиву карток обліку пожеж в Україні [1] свідчить про збільшення кількості пожеж на 17,6 % за дев'ять місяців 2017 року порівняно з аналогічним періодом минулого року. Особливе занепокоєння викликає збільшення на 21,8 % пожеж у житловому секторі, що становить 73,5 % від загальної кількості пожеж. Пожежі в житловому секторі викликають суспільний резонанс, несуть безпосередню загрозу життю та здоров'ю громадян, завдають значних матеріальних збитків. Тому актуальним питанням сьогодення є підвищення рівня пожежної безпеки саме житлового сектору.

Державна політика у сфері цивільного захисту, захисту населення і територій від надзвичайних ситуацій та запобігання їх виникненню повинна бути спрямована на удосконалення існуючих та розробку нових методів і засобів моніторингу, прогнозування та профілактику пожеж на основі сучасних інформаційних технологій.

Аналіз останніх досліджень. Серед останніх досліджень і публікацій варто виділити роботи, в яких проведено ряд досліджень щодо ризику виникнення пожеж у житловому

секторі [2–3]; розроблено метод прогнозування передумов виникнення пожеж у житловому секторі та побудовано інформаційну систему моніторингу пожежної безпеки [4–5]; доведено можливість застосування методу групового урахування аргументів до прогнозування пожеж у житловому секторі [6].

Проте в цих дослідженнях не проводилося оцінювання оперативності прогнозування пожеж у житловому секторі.

Метою роботи є визначення часу прогнозування пожеж у житловому секторі та оцінювання оперативності прогнозування, а також визначення кількості об'єктів моніторингу з урахуванням технічних засобів збору та прийому інформації.

Виклад основного матеріалу. В цілому прогнозуванням пожеж на сьогодні займаються здебільшого на основі статистичної інформації за допомогою стандартного пакета прикладних програм MS Excel, що дозволяє спрогнозувати явище за допомогою лінійної регресії діапазону відомих даних. Але використання цього способу прогнозування в житловому секторі не є ефективним і точним, тому що не враховує характеристик кожної окремої квартири.

На нашу думку, точним є прогнозування пожежі за станом електроспоживання кожної квартири за допомогою методу групового урахування аргументів (МГУА) [6–8], який фактично є методом пошуку закономірностей з автоматичним вибором вигляду функціональної структури й параметрів моделі на основі інформації, яка міститься в короткій вибірці статистичних даних. Під час прогнозування пожеж у житлових будинках МГУА враховує стан проводки та стан споживання електроенергії, відстежує відхилення від прогнозованого споживання електроенергії. І якщо ці відхилення такі, що можуть призвести до пожежного стану електромережі, то надходить сигнал, який вимагає звернути особливу увагу на стан квартири.

Перевагами адаптації МГУА до методу прогнозування пожеж у житловому секторі є:

- знаходження оптимальної складності структури моделі, адекватної рівню завад у вибірці даних;

- гарантія знаходження найбільш точної чи незміщеної моделі – метод не пропускає найкращого рішення під час перебору всіх варіантів;

- будь-які нелінійні функції чи ознаки, що можуть мати вплив на вихідну змінну, використовуються як вхідні аргументи.

Адаптація МГУА до предметної області дозволяє вирішити проблему забезпечення моніторингу та прогнозування пожеж у житловому секторі в реальному часі.

В роботі [9] доведено можливість застосування системи залишкових класів для забезпечення швидкості розрахунку моделей квартир з метою прогнозування пожеж, обґрунтовано правильність вибору системи числення, яка найбільш ефективно виконує операції додавання, віднімання та множення, оскільки було зазначено, що поліном МГУА будується на основі зазначених операцій.

Подальші дослідження було спрямовано на пошук системи числення, яка найбільш ефективно реалізує систему залишкових класів з урахуванням сучасного розвитку обчислювальної техніки. Було побудовано та досліджено оптимально-надлишкові системи числення, що дають змогу при найменшій складності апаратних засобів вирішити цю задачу. Але їх недоліком є те, що вони не дозволяють гарантовано виявити помилку. А помилки прогнозування передумов до виникнення пожеж у житловому секторі призведуть до нера-

ціонального використання сил та засобів контролюючих органів, підрозділів ДСНС України та значної втрати коштів.

Для забезпечення швидкості й достовірності реалізації системи залишкових класів запропоновано реалізувати її на основі позиційної двійково-четвіркової системи числення з постійною кількістю одиниць [10]. Перевагами цієї системи числення є те, що вона легко перетворюється, гарантовано знаходить помилки непарної кратності, при цьому гарантовано виявляє однократні помилки (ймовірність виявлення помилок при 8-розрядній обробці – 94 %, при 16-розрядній і більше обробці – 99 %), має велику несиметрію нулів та одиниць, що дає можливість адаптуватися до реальних каналів зв'язку та обчислювальної техніки.

Для оцінювання оперативності прогнозування пожеж у житловому секторі необхідно визначити швидкість реалізації моделей прогнозування пожеж. Для цього розглянемо послідовність операцій, пов'язаних з прогнозуванням пожеж на основі моделі [4]. Для технологічної реалізації цієї моделі необхідно виконати такі дії:

- 1) прочитати повідомлення та попередньо обробити дані;

- 2) виділити адресу, виділити дані та попередньо обробити дані;

- 3) виконати пошук моделі;

- 4) завантажити моделі;

- 5) обробити вхідні дані на основі моделі;

- 6) прочитати результат та прийняти рішення.

Виходячи з послідовності дій, час прогнозування можна оцінити як:

$$T_{\text{прогноз.}} = t_1 + t_2 + t_3 + t_4 + t_5 + t_6,$$

де t_1 – час обробки повідомлення;

t_2 – час виділення адреси моделі;

t_3 – час пошуку моделі;

t_4 – час завантаження моделі;

t_5 – час обробки вхідних даних на основі моделі;

t_6 – час прийняття рішення.

Час прогнозування складається з часу роботи двох систем:

- 1) час роботи системи передачі попередньої обробки даних, який напряму пов'язаний з характеристиками каналу зв'язку;

- 2) час прогнозування, який пов'язаний з характеристиками засобів обробки інформації персональним комп'ютером.

Для оцінювання часу роботи каналу зв'язку нам необхідно визначити обсяг даних, що надходять до системи:

1. Визначимо обсяг даних, що надходять до системи:

$$V_o = K_o \cdot (R + R_c),$$

де K_o – кількість об'єктів моніторингу, яка визначається кількістю квартир (приміщень), що входять до системи прогнозування пожеж, і визначає кількість моделей прогнозування;

R – результат вимірювання спожитої електроенергії, який визначається характеристиками лічильника;

R_c – службова інформація для забезпечення достовірності передачі інформації, перешкодозахищеності й т.ін.

2. Визначимо пропускну здатність прийому даних у системі прогнозування передумов до виникнення пожежі:

Пропускна здатність системи буде меншою із пропускну здатностей каналу зв'язку чи периферійного обладнання мережевої підтримки комп'ютера. Розглянемо пропускну здатність каналу зв'язку:

$$Q_I^n = \frac{V_I}{t} \quad Q_K^n = \frac{V_K}{t}$$

$$t_I^n = \frac{V_o}{Q_I^n} = \frac{V_o}{V_I} \cdot t = \frac{K_o(R + R_c)}{V_I} \cdot t \quad (1)$$

$$t_I^n \leq t_M,$$

де Q_I^n – пропускна здатність каналом зв'язку;

Q_K^n – пропускна здатність прийняття інформації комп'ютером (швидкодія мережевої карти);

t_M – час циклу моніторингу електроспоживання;

t_I^n – час прийому даних з каналу зв'язку;

V_I – обсяг даних, визначений каналом зв'язку.

Розглянемо пропускну здатність периферійного обладнання мережевої підтримки. Визначимо час прийому даних з каналу зв'язку для однієї моделі:

$$t_K^n = \frac{V_o}{Q_K^n} = \frac{V_o}{V_K} \cdot t = \frac{K_o(R + R_c)}{V_K} \cdot t \quad (2)$$

$$t_K^n \leq t_M$$

$$t_{II} = \begin{cases} t_I^n, & \text{якщо } t_I^n < t_K^n \\ t_K^n, & \text{якщо } t_I^n > t_K^n \end{cases}$$

$$t_{II} \leq t_M$$

Визначення часу прийому даних для однієї моделі дає можливість визначити кількість об'єктів моніторингу з урахуванням технічних засобів збору та прийому інформації.

3. Визначимо кількість об'єктів моніторингу з урахуванням технічних засобів збору та прийому інформації.

На основі (1) отримаємо:

$$K_o^1 = \frac{t_I^n \cdot V_I}{(R + R_c) \cdot t}$$

На основі (2) отримаємо:

$$K_o^2 = \frac{t_K^n \cdot V_K}{(R + R_c) \cdot t}$$

$$K_o = \begin{cases} K_o^1 & K_o^1 < K_o^2 \\ K_o^2 & K_o^1 > K_o^2 \end{cases}. \quad (3)$$

4. Визначимо кількість моделей з урахуванням часу, потрібного для моніторингу:

$$t_M^R = K_o \cdot (t_2 + t_3 + t_4 + t_5 + t_6)$$

$$K_o = \frac{t_M^R}{t_2 + t_3 + t_4 + t_5 + t_6} \text{ при } t_M^R \leq t_M.$$

Для оцінювання оперативності прогнозування пожеж у житловому секторі необхідно розрахувати час обробки повідомлення, час виділення адреси моделі, час пошуку моделі та час завантаження моделі з урахуванням технічних характеристик засобів зв'язку та обчислювальної техніки.

Для проведення розрахунку часу обробки моделі необхідно визначити обсяг моделей у табличній формі. При деструктизації таблиці з точністю в 0,1 Вт обсяг інформаційної моделі буде становити 50 кілобайт. Основним обмежуючим фактором часу обробки моделей буде час доступу до даних на зовнішніх запам'ятовувальних пристроях.

Висновок. Таким чином, розроблені методи та засоби прогнозування пожеж у житловому секторі забезпечать прогнозування в реальному часі передумов до виникнення пожеж у місті з населенням до 7 млн. залежно від характеристик технічних засобів.

Список літератури

1. Аналіз масиву карток обліку пожеж (POG_STAT) за 9 місяців 2017 року. URL: <http://undicz.dsns.gov.ua/ua/Analiz-masivu-kartok-obliku-pozhezh.html> (дата звернення 03.11.2017).
2. Мовчан І. О. Методологія визначення соціального пожежного ризику. *Системи обробки інформації*. 2015. Вип. 5 (130). С. 181–184.
3. Гуліда Е. М., Башинський О. І., Мовчан І. О. Прогнозування виникнення пожеж в житловому секторі на підставі аналізу техногенного ризику. *Пожежна безпека: зб. наук. праць ЛДУ БЖД*. 2012. № 20. С. 150–154.
4. Мельник О. Г. Розробка методу прогнозування передумов виникнення пожеж у житловому секторі. *Пожежна безпека: теорія і практика: матеріали II міжнар. наук.-практ. конф. (12 жовтня 2012 р.)*. Черкаси: АПБ ім. Героїв Чорнобиля, 2012. С. 344–346.
5. Дендаренко В. Ю., Мельник О. Г., Чепурний Г. П. Побудова інформаційної системи моніторингу пожежної безпеки. *Збірник наукових праць Харківського університету Повітряних Сил*. 2014. Вип. 3 (40). С. 167–170.
6. Мельник О. Г., Мельник Р. П. Застосування методу групового урахування аргументів до прогнозування пожеж у житловому секторі. *Надзвичайні ситуації: безпека та захист: матеріали VII всеукр. наук.-практ. конф. з міжнар. участю (20–21 жовтня 2017 р.)*. Черкаси, 2017. С. 7–8.
7. Голуб С. В. Багаторівневе моделювання в технологіях моніторингу оточуючого середовища: монографія. Черкаси: Вид-во ЧНУ ім. Богдана Хмельницького, 2007. 220 с.
8. Голуб С. В., Рудницький В. М., Мельник О. Г., Дендаренко В. Ю. Технологія багаторівневого моніторингу пожежної безпеки. Методи та засоби реалізації: монографія. Харків: Вид-во ТОВ «Щедра садиба плюс», 2014. 140 с.
9. Мельник О. Г. Формування вимог до векторної основи системи залишкових класів з урахуванням рішення задачі прогнозування пожеж у житловому секторі. *Системи озброєння і військова техніка*. 2015. № 1 (41). С. 165–167.
10. Мельник О. Г. Схемотехнічні основи реалізації системи залишкових класів в двійково-четвірковій системі числення. *Системи обробки інформації*. 2011. № 8 (98). С. 93–95.

References

1. Analysis of the array of fire counting cards (POG_STAT) for 9 months of 2017. URL: <http://undicz.dsns.gov.ua/ua/Analiz-masivu-kartok-obliku-pozhezh.html> (date of access 03.11.2017) [in Ukrainian].
2. Movchan, I. O. (2015) Methodology of determining the social fire risk. *Systemy obrobky informatsii*, No. 5 (130), pp. 181–184 [in Ukrainian].
3. Hulida, E. M., Bashynskyi, O. I., Movchan, I. O. (2012) Forecasting of fires in residential sector on the basis of the analysis of technogenic risk. *Pozhezhna bezpeka: zb. nauk. prats LDU BZhD*, No. 20, pp. 150–154 [in Ukrainian].
4. Melnyk, O. H. (2012) The development of the method of forecasting the preconditions for the emergence of fires in residential sector. *Pozhezhna bezpeka: teoriia i praktyka: the 2nd Internat. sci. and pract. conf. (Oct., 12)*. Cherkasy: APB im. Heroyiv Chornobylya, pp. 344–346 [in Ukrainian].
5. Dendarenko, V. Yu., Melnyk, O. H., Chepurnyi, H. P. (2014) Construction of an information system for fire safety monitoring. *Zbirnyk naukovykh prats Kharkivskoho universytetu Povitrianykh Syl*, No. 3 (40), pp. 167–170 [in Ukrainian].
6. Melnyk, O. H., Melnyk, R. P. (2017) Application of the method of group consideration of arguments for the prediction of fires in residential sector. *Nadzvychaini sytuatsii: bezpeka ta zakhyst: the VI All-Ukr. sci.-pract. conf. with internat. participation (October, 20–21)*. Cherkasy, pp. 7–8 [in Ukrainian].
7. Holub, S. V. (2007) Multilevel modeling in environmental monitoring technologies: monograph. Cherkasy: Vyd-vo ChNU im. Bohdana Khmelnytskoho, 220 p. [in Ukrainian].
8. Holub, S. V., Rudnytskyi, V. M., Melnyk, O. H., Dendarenko, V. Yu. (2014) Technology of multi-level monitoring of fire safety. Methods and means of realization:

- monograph. Kharkiv: Vyd-vo TOV «Shchedra sadyba plus», 140 p. [in Ukrainian].
9. Melnyk, O. H. (2015) Formation of requirements to vector basis of the system of residual classes taking into account the decision of the task of forecasting fires in residential sector. *Systemy ozbroiennia i viiskova tekhnika*, No. 1 (41), pp. 165–167 [in Ukrainian].
10. Melnyk, O. H. (2011) Circuit bases for realization of the system of residual classes in binary-quadded system of calculation. *Systemy obrobky informatsii*, No. 8 (98), pp. 93–95 [in Ukrainian].

O. G. Melnyk, *Ph.D., senior researcher*,
e-mail: melnyk.olja.2014@gmail.com,

R. P. Melnyk, *Ph.D.*

Cherkasy Institute of Fire Safety named after Chernobyl Heroes
of National University of Civil Protection of Ukraine
Onoprienko str., 8, Cherkasy, 18034, Ukraine

EVALUATION OF THE EFFICIENCY OF FIRE FORECASTING IN RESIDENTIAL SECTOR

The evaluation of the efficiency of fires forecasting in residential sector is conducted in the article. For this purpose, the speed of the realization of fire forecasting models, the number of the objects, that are monitored, taking into account technical means of collecting and receiving information, and the number of models subject to the time required for monitoring, are determined.

It has been found that the time of data access on external storage devices is the main limiting factor for the time of models processing.

The evaluation of the speed of operation has been carried out on the basis of the received dependencies, taking into account modern characteristics of personal computers and communication channels (Internet).

As a result of determining the time, taken for importation of data for one model, it has been proved that the developed methods and means of fire forecasting in residential sector can provide real-time forecasting of preconditions for the fire breaking-out in a city with a population up to 7 millions, depending on the characteristics of technical means.

Keywords: *fire forecasting, method of group accounting of arguments, system of residual classes, system of calculation, forecasting time, efficiency of forecasting.*

*Рецензенти: Рудницький В. М., д.т.н., професор,
Кириченко О. В., д.т.н., с.н.с.*

В. В. Лепський, к.мед.н., доцент,
докторант кафедри спеціалізованих комп'ютерних систем
Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна
e-mail: cherkassymsek@ukr.net

МЕТОДИ ІНТЕГРОВАНОГО УПРАВЛІННЯ ЗАГРОЗАМИ ЗАБЕЗПЕЧЕННЯ ЦІННОСТЕЙ СТЕЙКХОЛДЕРІВ МЕДИЧНОГО ПРОЕКТУ

Процеси євроінтеграції, загальної глобалізації відповідно до міжнародних вимог, норм і стандартів вимагають від України значних змін в усіх галузях господарювання, у тому числі в Системі охорони здоров'я (СОЗ). Реформування і подальше ефективне функціонування СОЗ потребує реалізації великої кількості проектів і програм як на рівні держави, так і на рівнях регіонів та окремих медичних закладів.

Стратегічне управління проектно-орієнтованим медичним закладом (ПОМЗ) покликане забезпечити конкурентоспроможне ефективне функціонування ПОМЗ у тривалій перспективі на основі забезпечення цінностей усіх стейкхолдерів ПОМЗ.

У статті пропонуються методи інтегрованого управління загрозами забезпечення цінностей стейкхолдерів ПОМЗ, що дозволять підвищити ефективність, гнучкість та адаптованість стратегічного управління ПОМЗ і управління його проектами до нестабільних умов українського сьогодення, конкуренції та високих ризиків.

Ключові слова: медичний заклад, інтегроване управління проектно-орієнтованим медичним закладом, загрози, цінності стейкхолдерів.

Постановка проблеми. Специфікою вибору та реалізації проектів, портфелів і програм у проектно-орієнтованому медичному закладі (ПОМЗ) є необхідність досягнення сталого розвитку закладу на базі забезпечення цінностей головних стейкхолдерів та об'єктів ПОМЗ, якими є: акціонери (власники); споживачі медичних послуг (пацієнти та суспільство як інтегрований споживач медичних послуг); бізнес-процеси; медичний та допоміжний персонал ПОМЗ.

Впровадження ціннісно-орієнтованого підходу до управління проектами в умовах непростого українського сьогодення вимагає глибокого аналізу загроз, ризиків та перешкод для реалізації проектів і забезпечення цінностей усіх стейкхолдерів ПОМЗ, розробки і застосування якісно нового методологічного інструментарію управління такими загрозами в проектах, програмах і портфелях проектів саме для медичних закладів України.

Аналіз останніх досліджень. Управлінню медичними закладами присвячено чимало праць українських вчених, зокрема Радиша Я. Ф., Білинської М. М., Лехана В. М., Слабкого Г. О., Солоненко І. М., Долота В. Д.; Масауд Алі Алгхдафі, Султан А., Романенко М. В., Ровинська Н. Ю., Данченко О. Б.

розглядають процес управління та стратегічного планування медичними закладами в розрізі проектного підходу.

Сутність сучасних медичних закладів суттєво обмежує застосування відомих ефективних засобів управління саме специфікою подібних проектно-орієнтованих організацій. На відміну від більшості проектно-орієнтованих організацій (ПОО), наприклад будівельної або ІТ-ПОО, в медичних закладах мають місце розриви у вертикалі управління сталим розвитком організації [1].

Стійкість організації на значному часовому інтервалі має розглядатися в різних площинах управління і діяльності. При цьому кількість таких площин визначається сферою діяльності організації. У будь-якому випадку розробка стратегії є складною управлінською задачею. Такі суттєві та значущі показники, як задоволення споживачів продукту проекту, їх безпека, соціальна та екологічна відповідальність, визначають підґрунтя сталого розвитку проектно-орієнтованого медичного закладу, в першу чергу, саме із середини організації, і вже потім, у другу чергу, ззовні – взаємодією зі стейкхолдерами, як показано в [1].

Зазвичай як інструмент реалізації стратегії використовують портфельне управління

[2], але особливості ПОО медичного закладу (ПОМЗ) виокремлюють певні проблеми.

У результаті дослідження [3] виділено проблему протиріччя інтересів основних стейкхолдерів проектів ПОМЗ, до яких відносяться інвестори або власники бізнесу та споживачі медичних послуг.

Здійснено аналіз та ідентифікацію цінностей стейкхолдерів проектів проектно-орієнтованого медичного закладу [4].

Задача полягає в усуненні протиріччя та формуванні таких механізмів управління, що задовольнятимуть усіх стейкхолдерів медичного закладу і забезпечуватимуть його ефективну діяльність та розвиток як проектно-орієнтованої організації.

Однак будь-яка система має враховувати стохастичність навколишнього (у цьому випадку – проектного) середовища, яка реалізується у неможливості абсолютно точного прогнозування поведінки середовища, особливо пов'язаного з високим ступенем невизначеності. Сучасні умови реалізації медичних проектів саме цим і характеризуються, вони відбуваються в так званому «турбулентному середовищі» [5, 6, 7]. З точки зору управлінських дисциплін, «турбуленція здійснює вплив ... на систему, джерело якого найчастіше неформалізоване або має непряму дію» [6, с. 73].

Метою роботи є розробка методів гнучкого інтегрованого управління загрозами забезпечення цінностей стейкхолдерів медичного проекту ПОМЗ.

Виклад основного матеріалу. Загрози забезпечення цінностей стейкхолдерів медичного проекту ПОМЗ вимагають ефективного реагування з метою забезпечення стійкості системи управління проектом і вчасного, в рамках заданих обмежень, досягнення результату. Загрозою забезпечення цінностей одного стейкхолдера може бути зміна відношення до медичного проекту ПОМЗ іншого стейкхолдера. В межах цієї парадигми буде здійснено подальший аналіз.

Система реагування на такі загрози має бути спрямована, перш за все, на недопущення їх реалізації або, в крайньому випадку, на мінімізацію наслідків тих загроз, що відбудуться і втіляться у проблеми проектів.

Тому систему управління мінімізацією загроз забезпечення цінностей стейкхолдерів медичних проектів ПОМЗ слід розглядати як таку, що має складатися з двох частин (що

вирішують дві різні задачі). Перша з частин повинна стосуватися активності проекту щодо прогнозування можливих загроз і розроблення методів протидії цим загрозам. Однак це звужує коло загроз до спектра таких, що можуть бути виведені аналітично. Не враховується турбулентність як ознака сучасного проектного оточення і пов'язана з нею слабка передбачуваність.

Звідси виникає необхідність у другій частині зазначеної системи управління, що має бути спрямована не стільки на прогнозування загроз, скільки на підвищення гнучкості і оперативності системи з метою вчасної (в найкоротші терміни) та ефективної генерації адекватних протидій на загрози, що не були спрогнозовані системою управління медичним проектом.

Розробимо відповідні управлінські методи. Метод, що реалізує першу задачу, назовемо методом проактивного планування реакцій на загрози медичному проекту ПОМЗ, другу – методом ситуативного управління загрозами медичному проекту ПОМЗ. Розглянемо обидва методи докладніше.

Метод проактивного планування реакцій на загрози медичному проекту ПОМЗ

Метод спрямовано на планування реакцій на загрози проекту ПОМЗ заздалегідь, з урахуванням прогнозування майбутніх загроз і механізмів їх виникнення.

Сформулюємо метод як такий, що складається з наступних 11 кроків, які реалізуються послідовно. Однак деякі кроки методу передбачають за певних умов повернення до попередніх. Схему методу із відповідними розгалуженнями зображено на рис. 1.

1. Визначення системи проактивних індикаторів оцінювання зацікавлених сторін медичних проектів ПОМЗ.

З метою оцінювання відношення зацікавлених сторін до медичного проекту ПОМЗ, яке потрібне для своєчасного виявлення загроз, що починають надходити від них, необхідно сформулювати базу відповідних індикаторів.

Наведемо перелік таких індикаторів, що пропонуються в межах цієї дисертаційної роботи, які мають бути розроблені для кожного стейкхолдера медичного проекту ПОМЗ:

– індикатор стану зацікавленої сторони (перелік параметрів, за якими можна оцінити відношення стейкхолдера до медичного проекту ПОМЗ);

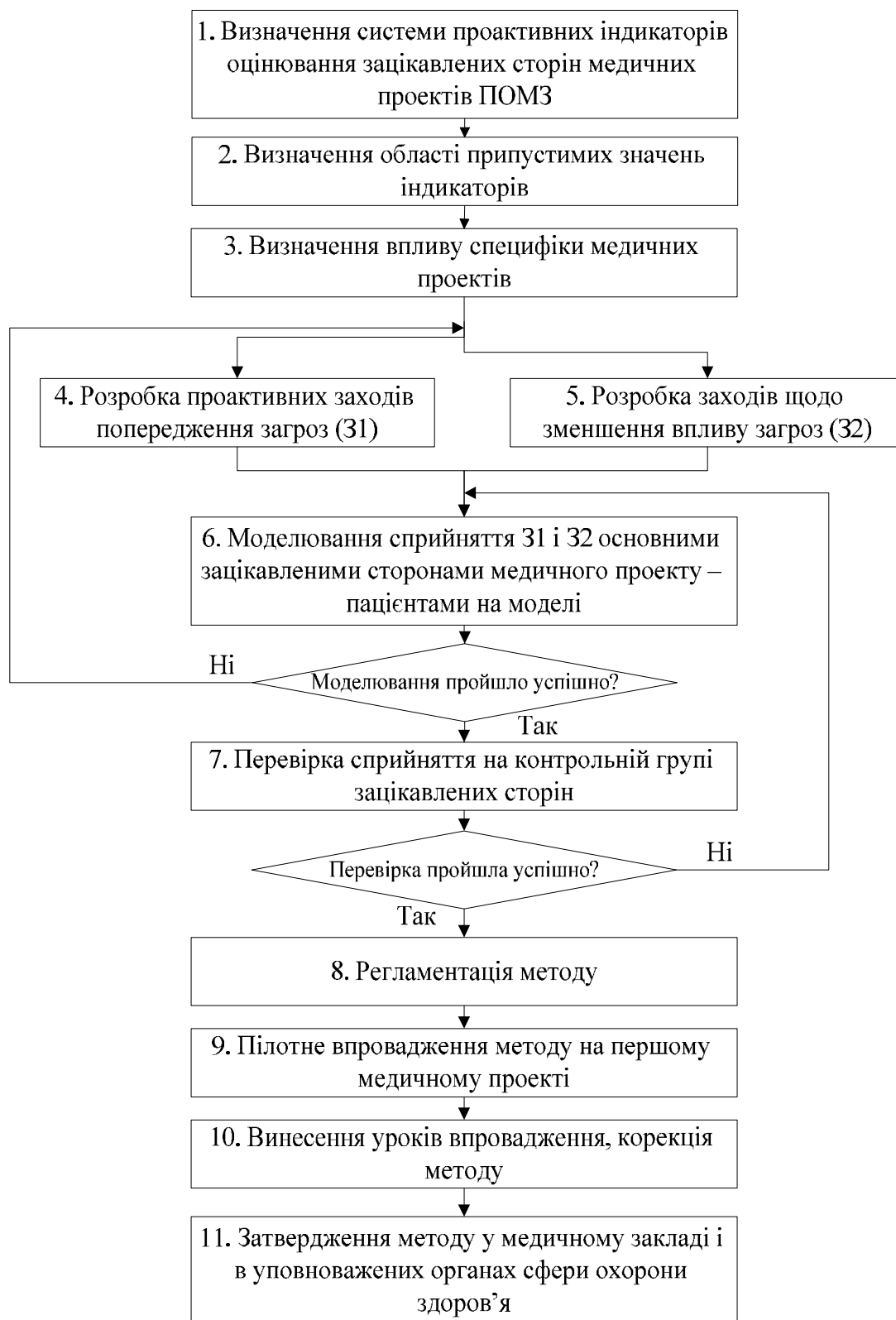


Рис. 1. Схема реалізації методу проактивного планування реакцій на загрози медичному проекту POM3

– індикатор можливості загрози з боку зацікавленої сторони (перелік змін параметрів оцінки відношення стейкхолдера до медичного проекту ПОМЗ, які вказують на виникнення можливого негативного відношення стейкхолдера до проекту);

– індикатор зростання ймовірності здійснення загрози з боку зацікавленої сторони до порогового значення (перелік таких змін параметрів відношення стейкхолдерів до медичного проекту ПОМЗ, які вказують на наближення загрози для проекту з боку зацікавленої сторони);

– індикатор появи загрози з боку зацікавленої сторони (перелік таких значень параметрів, що свідчать про наявну загрозу проекту ПОМЗ з боку зацікавленої сторони).

2. Визначення області припустимих значень індикаторів.

Усі індикатори мають нижню і верхню межу значень, які необхідно визначити. Області припустимих значень визначаються для кожного індикатора відносно кожної зацікавленої сторони медичних проектів ПОМЗ.

3. Визначення впливу специфіки медичних проектів.

Специфічні тільки для медичних проектів стейкхолдери (пацієнти, родичі пацієнтів, медичний персонал ПОМЗ, фармацевтичні компанії) можуть генерувати тільки унікальні загрози для проекту внаслідок їх специфічності, тоді як інші зацікавлені сторони (інвестори або власники, адміністрація, постачальники та обслуговуючі організації, місцеві органи влади тощо) можуть генерувати як загальні загрози, притаманні їх впливам на будь-який проект інваріантно до предметної галузі, так і специфічні – для конкретного типу проекту. Необхідно визначити вплив специфіки медичних проектів на формування відношення зацікавлених сторін, на можливі зміни відношення внаслідок зазначеної специфіки, що має відображатися у переліку та значеннях відповідних індикаторів.

4. Розробка проактивних заходів попередження загроз (31).

З урахуванням ідентифікованих загроз для медичних проектів ПОМЗ розробляються адекватні заходам заходи попередження, які спрямовані на зменшення ймовірності загроз з проактивною, прогнозуючою дією. Проводиться зіставлення вартості втрат від загроз і

вартості заходів попередження. У випадку перевищення вартості заходів попередження над вартістю втрат від загрози заходи попередження необхідно переглянути або, у випадку неможливості останнього, прийняти загрозу як таку, що може відбутися без застосування до неї заходів попередження.

5. Розробка заходів щодо зменшення впливу загроз (32).

Існує ймовірність, що, які б не були заходи попередження, загроза переросте у проблему для медичного проекту ПОМЗ. Тому в межах реалізації принципу проактивності необхідно розробити заходи реагування на проблему, за умови, що загрози не вдалося уникнути. Такі заходи розробляються для усіх ідентифікованих загроз, включаючи ті з них, до яких не було розроблено проактивних заходів попередження.

6. Моделювання сприйняття 31 і 32 основними зацікавленими сторонами медичного проекту – пацієнтами на моделі.

Створюється імітаційна модель медичного проекту ПОМЗ і оточення – зацікавлених сторін. В модель включаються проактивні індикатори оцінювання зацікавлених сторін, а також параметри проекту і його системи управління. Проводиться імітаційне моделювання впливу загроз оточення на проект ПОМЗ, включаючи стрес-тестування, яке передбачає різку зміну декількох вхідних параметрів (у цьому випадку зміна може мати значення нижньої або верхньої межі області припустимих значень). У випадку негативних результатів тестування розробка 31 і 32 проводиться наново з урахуванням результатів моделювання, тобто повторюється реалізація пунктів 4 і 5 цього методу.

7. Перевірка сприйняття 31 і 32 на контрольній групі зацікавлених сторін.

Застосування заходів 31 і 32 проводиться для контрольної групи стейкхолдерів, визначається зміна відношення стейкхолдерів і перевіряється ефективність заходів 31 і 32. У випадку невдачі необхідно повернутися до кроку моделювання (крок 6) для повторної перевірки.

8. Регламентация методу.

Після успішної апробації методу і на моделі (крок 6), і на контрольній групі зацікавлених сторін (крок 7) відбувається формалізація методу для умов ПОМЗ у вигляді регламенту.

Регламент має передбачати послідовність здійснення методу у вигляді схеми, множини показників та індикаторів моделі співвідношень медичного проекту і стейкхолдерів, організаційну прив'язку методу до оргструктури ПОМЗ, правила зміни регламенту у випадку отримання нової інформації.

9. Пілотне впровадження методу на першому медичному проекті.

Після регламентації методу обирається найбільш типовий проект ПОМЗ, на якому відбувається пілотне впровадження методу. Період пілотного впровадження має охоплювати протидію загрозам від усіх зацікавлених сторін проекту, під час чого мають оцінюватися як самі заходи 31 і 32, так і метод у цілому.

10. Винесення уроків впровадження, корекція методу.

Під час пілотного впровадження та під час його фіналізації мають фіксуватися уроки застосування методу. Для цього має бути розроблена відповідна формалізована база знань. За результатами аналізу уроків пілотного впровадження метод має коректуватися у частинах кроків методу для конкретного ПОМЗ, проактивних індикаторів оцінювання зацікавлених сторін, параметрів моделі проекту і медичного закладу та інших аспектів методу.

11. Затвердження методу у медичному закладі і в уповноважених органах сфери охорони здоров'я.

Після остаточної формалізації методу проактивного планування реакцій на загрози медичному проекту ПОМЗ має відбуватися його формальне затвердження. Для цього готуються аналітичні матеріали щодо моделювання методу, результатів його апробації на контрольній групі зацікавлених сторін, а також у межах пілотного проекту та інші супутні матеріали, що стосуються розробки і верифікації методу. Метод затверджується в декілька етапів, першим із яких є затвердження у медичному закладі, останнім – затвердження в уповноважених органах сфери охорони здоров'я.

Розглянемо наступний метод.

Метод ситуативного управління загрозами медичному проекту ПОМЗ

Метод спрямовано на налаштування системи управління з метою збільшення її гнучкості і забезпечення швидкого її реагування на загрози з боку зацікавлених сторін ПОМЗ.

У методі використовується модель сценарної оцінки, висвітлена у джерелах [8–13].

Сформулюємо метод як такий, що складається з наступних 10 кроків. Схему методу зображено на рис. 2.

1. Створення сценарної моделі алгоритму адаптації системи управління ПОМЗ до нових непередбачуваних загроз, що з'являються.

Полягає у представленні досліджуваного об'єкта (системи управління ПОМЗ) як моделі, виявленні ключових факторів впливу, результируючих критеріїв, визначенні шкали оцінювання. Модель повинна мати властивості високого рівня адаптивності до змін навколишнього середовища проекту ПОМЗ, що, перш за все, визначається його зацікавленими сторонами.

2. Стрес-тестування отриманої моделі.

Проводиться експеримент щодо стійкості системи управління ПОМЗ на сценарній моделі. Експеримент передбачає різку зміну кількох параметрів зовнішнього середовища. При цьому така комбінація зовнішніх впливів має визнаватися експертами як вірогідна. Модель може витримати тестування, залишившись стійкою, або не витримати, вказавши на руйнівні впливи для системи управління деяких зі стресів, що їх спричинять зацікавлені сторони медичного проекту ПОМЗ.

3. Аналіз альтернативного ряду поведінкових характеристик моделі.

Модель досліджується з точки зору її реакції не тільки на стресові впливи, але й на малі та середні у різних комбінаціях. Робиться низка висновків щодо стійкості системи управління, її гнучкості, мобільності, ефективності тощо.

4. Тестування сценарної моделі на історичних даних (back-тестування).

Проведення back-тестування має на меті апробацію методологічних розробок на історичних і гіпотетичних даних. Оцінюється адекватність моделі системи управління, а також ефективність її реакції на зміну інтересів або виникнення загроз з боку зацікавленої сторони медичного проекту ПОМЗ.

За результатами тестування (кроки 2–4 цього методу) модель системи управління ПОМЗ або витримує експеримент, і тоді здій-

снюється наступний крок методу, або необхідно повернутися знову до розробки моделі (крок 1 цього методу).

5. Розробка механізму формування резервного фонду на покриття непередбачуваних загроз.

Одним із підходів щодо зміцнення стійкості системи управління є формування фонду покриття непередбачуваних витрат (так званого резервного фонду). Прийнятною вважається величина резервного фонду у розмірі від 5 до 10 % бюджету проекту.

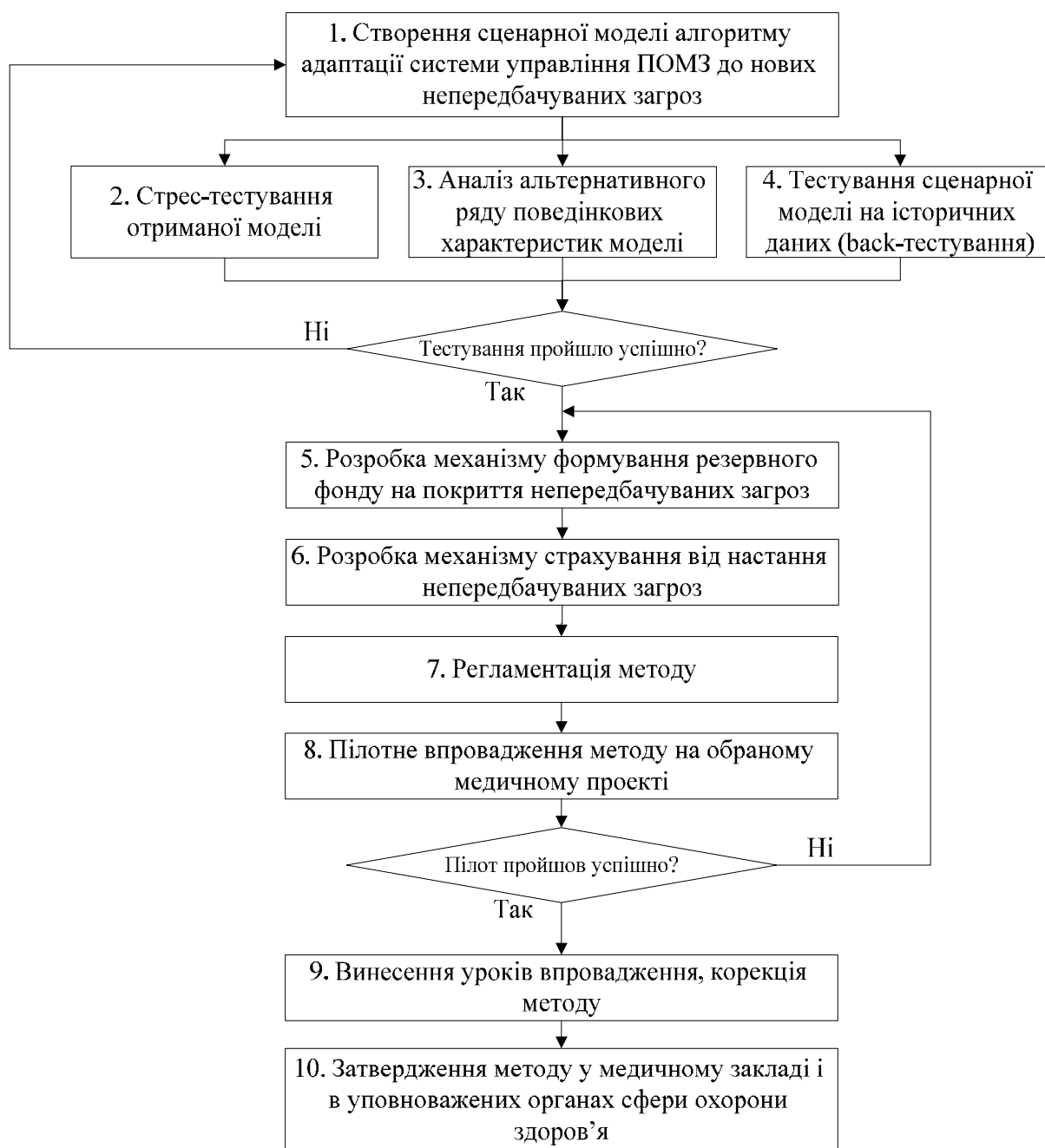


Рис. 2. Схема реалізації методу ситуативного управління загрозами медичному проекту ПОМЗ

Обов'язково необхідно визначити джерела наповнення резервного фонду, а також правила користування цим фондом.

6. Розробка механізму страхування від настання непередбачуваних загроз.

Іншим підходом щодо мінімізації впливу ситуативних непередбачуваних загроз є страхування. Необхідно розробити дієвий механізм захисту від основних суттєвих загроз, що можуть походити від зацікавлених сторін медичних проектів ПОМЗ, і закріпити його у відповідному договорі страхування.

7. Регламентация методу.

Після успішної апробації методу і розробки механізму формування резервного фонду, а також механізму страхування відбувається формалізація методу для умов ПОМЗ у вигляді регламенту. Регламент має передбачати послідовність здійснення методу у вигляді схеми, імітаційну модель системи управління ПОМЗ, алгоритми тестування моделі (стрес-тестування, back-тестування, модель аналізу альтернативного ряду поведінкових характеристик системи управління), організаційну прив'язку методу до оргструктури ПОМЗ, правила зміни регламенту у випадку отримання нової інформації.

8. Пілотне впровадження методу на обраному медичному проекті.

Після регламентації методу необхідно обрати медичний проект ПОМЗ для пілотного впровадження методу. Тривалість пілотного проекту має бути достатньою для перевірки гнучкості системи до непередбачуваних загроз, коли, як мінімум, до одної з таких, що виникла, буде застосований механізм використання резервного фонду, і, як мінімум, до одної – буде задіяний механізм страхування.

9. Винесення уроків впровадження, корекція методу.

Під час пілотного впровадження та під час його фіналізації мають фіксуватися уроки застосування методу. Для цього має бути розроблена відповідна формалізована база знань. За результатами аналізу уроків пілотного впровадження метод має коректуватися у частинах кроків методу для конкретного ПОМЗ, параметрів моделі системи управління ПОМЗ, параметрів моделей аналізу альтернативного ряду поведінкових характеристик, back-тестування, стрес-тестування та інших аспектів методу.

10. Затвердження методу у медичному закладі і в уповноважених органах сфери охорони здоров'я.

Після остаточної формалізації методу ситуативного управління загрозами медичному проекту ПОМЗ має відбуватися його формальне затвердження. Для цього готуються аналітичні матеріали щодо моделювання методу, результатів його тестування і апробації в межах пілотного проекту та інші супутні матеріали, що стосуються розробки і верифікації методу. Метод затверджується в декілька етапів, першим з яких є затвердження у медичному закладі, останнім – затвердження в уповноважених органах сфери охорони здоров'я.

Загалом, обидва методи (метод проактивного планування реакцій на загрози медичному проекту ПОМЗ та метод ситуативного управління загрозами медичному проекту ПОМЗ) мають бути апробовані для кожного типу медичного проекту (лікувального, організаційного, наукового), і за результатами апробації мають бути відкориговані елементи методів і їх моделі для створення різновидів методів для типів медичних проектів. Це дозволить збільшити точність методів, їх спеціалізованість, адекватність та ефективність.

Висновки. Стратегічне управління сталим розвитком ПОМЗ повинне мати ефективний методологічний інструментарій щодо реалізації проектів, орієнтований на забезпечення цінностей стейкхолдерів ПОМЗ та його ефективне функціонування в тривалій перспективі. У нестабільних умовах нашої держави та ринкової економіки як такої проекти медичних закладів зазнають впливів та загроз з боку як зовнішнього, так і внутрішнього середовища проектів.

Для забезпечення успішної реалізації проектів ПОМЗ, з акцентом на забезпечення цінностей усіх його стейкхолдерів, запропоновано методи проактивного планування реакцій на загрози та ситуативного управління загрозами медичному проекту ПОМЗ, що мають слугувати гнучкому, оперативному інтегрованому управлінню проектами ПОМЗ.

Список літератури

1. Ким Е. А. Реализация масштабных инновационных проектов на основе стратегического партнерства в проектно-ориентированных компаниях: автореф. дис. ... канд. экон. наук. URL: http://guu.ru/files/referate/2015/kim_e_otz_nau.pdf
2. Илларионов А. В., Клименко Э. Ю. Портфель проектов: инструмент стратегического управления предприятием. Москва: Альпина Паблишер, 2013. 312 с.
3. Лепский В. В. Концепция стратегического управления проектами, программами и портфелями медицинского учреждения. *Управління проектами, програмами, портфелями*: тези доп. 1-ї Міжнар. наук.-практ. конф.: [у 2 т.] / відп. за вип. Тесленко П. О. Т. 2. Одеса: Бондаренко М. О., 2016. С. 75–77.
4. Лепський В. В. Ідентифікація цінностей стейкхолдерів проектів проектно-орієнтованого медичного закладу. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*. Черкаси: ЧДТУ, 2017. № 3.
5. Бушуев С. Д., Бушуева Н. С. Управление проектами в условиях турбулентности окружения. *Управління проектами у розвитку суспільства*: тези доп. IX Міжнар. конф. Тема: “Управління програмами та проектами в умовах глобальної фінансової кризи” / відп. за вип. С. Д. Бушуев. Київ: КНУБА, 2012. С. 31–33.
6. Ярошенко Р. Ф., Ярошенко Т. А. Турбулентність в управлінні програмами розвитку фінансових установ. *Управління розвитком складних систем*. 2011. № 7. С. 73–75.
7. Домбровський М. З. Обґрунтування параметрів структурованої моделі проектних дій енергокомпаній в турбулентному середовищі. *Вісник Національного технічного університету «ХПІ»*. Серія: Стратегічне управління, управління портфелями, програмами та проектами. 2015. № 1. С. 195–200.
8. Gausemeier J., Fink A., Schlake O. (1996) SzenarioManagement – Planen und Führen mit Szenarien [Scenario management – Planning and leading with scenarios]. Munchen, Germany: Carl Hanser Verlag, 390 s.
9. Яременко О. Сценарне планування як інтелектуальна модель. *Економічні стратегії*. 2005. № 1. С. 17–20.
10. Батьковский А. М., Булава И. В., Кравчук П. В. и др. Методология и инструментарий управления инновационной деятельностью экономических систем в условиях транснационализации экономики и ее неустойчивого посткризисного развития / под ред. А. М. Батьковского. Москва: МЭСИ, 2010. 360 с.
11. Рогов М. А. Новая парадигма риск-менеджмента. *Моделирование и анализ безопасности и риска в сложных системах: труды Междунар. науч. школы МА БР*. 2003. (20–23 августа 2003 г.). Санкт-Петербург: Изд-во СПбГУАП, 2003. С. 90–96.
12. Попов С. А. Сценарное планирование в системе стратегического менеджмента. *Консультант директора*. 2001. № 25. С. 16.
13. Постанова Кабінету Міністрів України від 16 лютого 2011 р. № 232 «Про затвердження Методики виявлення ризиків здійснення державно-приватного партнерства, їх оцінки та визначення форми управління ними». URL: <http://zakon2.rada.gov.ua/laws/show/232-2011-%D0%BF>.

References

1. Kim, E. A. (2015) Implementation of large-scale innovative projects based on strategic partnership in project-oriented companies: thesis abstract for Ph.D. in technical science. URL: http://guu.ru/files/referate/2015/kim_e_otz_nau.pdf
2. Illarionov, A. V., Klimenko, E. Yu. (2013) Project portfolio: strategic management tool]. Moscow: Alpina Publisher, 312 p. [in Russian].
3. Lepskiy, V. V. (2016) Concept of strategic management projects, programs and portfolios of medical institutions. *Upravlinnia proektamy, prohramamy, portfeliamy*: pro-

- ceedings of the First Internat. sci.-pract. conf. (in 2 vol.). Odesa, Ukraine: Bondarenko M.O., pp. 75–77 [in Russian].
4. Lepsky, V. V. (2017) Identification of stakeholders' values of project-oriented medical institution projects. *Visnyk Cherkaskogo derzhavnogo tehnolohichnogo universitetu. Seria: Tehnichni nauky*. Cherkasy, Ukraine: ChDTU, No. 3 [in Ukrainian].
 5. Bushuev, S. D., Bushueva, N. S. (2012) Project management in the conditions of environment turbulence. *Upravlinnia proektamy u rozvytku suspilstva. Tema: "Upravlinnia prohramamy ta proektamy v umovakh hlobalnoi finansovoi kryzy"*: proceedings of the IX Internat. conf. Kyiv: KNUBA, pp. 31–33 [in Russian].
 6. Yaroshenko, R. F., Yaroshenko, T. A. (2011) Turbulence in the management of financial institutions development programs. *Upravlinnya rozvytkom skladnyh system*. Kyiv No. 7, pp. 73–75 [in Ukrainian].
 7. Dombrovsky, M. Z. (2015) Justification of parameters of a structured model of project actions of power companies in a turbulent environment. *Visnyk Natsionalnoho tekhnichnogo universytetu «KhPI». Seria: Stratehichne upravlinnia, upravlinnia portfeliamy, prohramamy ta proektamy*. Kharkiv, No. 1, pp. 195–200 [in Ukrainian].
 8. Gausemeier, J., Fink, A., Schlake O. (1996) SzenarioManagement – Planen und Führen mit Szenarien [Scenario management – Planning and leading with scenarios]. Munchen, Germany: Carl Hanser Verlag, 390 p.
 9. Yaremenko, O. (2005) Script planning as an intelligent model. *Economichni strategiyi*, No. 1, pp. 17–20 [in Ukrainian].
 10. Batkovskiy, A. M., Bulava, Y. V., Kravchuk, P. V. et al. (2010) Methodology and tools for managing the innovation activity of economic systems in the conditions of transnationalization of the economy and its unstable post-crisis development. In: A. M. Batkovskiy (ed.). Moscow: MESI, 360 p. [in Russian].
 11. Rogov, M. A. (2003) A new paradigm of risk management. *Modelirovanie i analiz bezopasnosti i riska v slozhnyh sistemah*: proceedings of MA BR Internat. sci. school. (August, 20–23). St. Petersburg: Izd-vo SPbGUAP, pp. 90–96 [in Russian].
 12. Popov, S. A. (2001) Scenarial planning in the system of strategic management. *Konsul'tant direktora*, No. 25, p. 16 [in Russian].
 13. On approval of the methods for identifying the risks of public-private partnership implementation, assessment and definition of their management form: resolution of the Cabinet of Ministers of Ukraine dated February, 16, 2011, No. 232. URL: <http://zakon2.rada.gov.ua/laws/show/232-2011-%D0%BF> (accessed October 03, 2017)

V. V. Lepskiy, PhD in Medical Sciences, doctoral candidat
of the Department of special computer systems
Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine
e-mail: cherkassymsek@ukr.net

THE METHODS OF INTEGRATED CONTROL BY THE THREATS OF ENSURING OF THE VALUES OF MEDICAL PROJECTS STAKEHOLDERS

The processes of European integration, universal globalization, in accordance with international requirements, norms and standards, require from Ukraine significant changes in all branches of economy, including the Healthcare System. Reforming and further effective functioning of Healthcare System requires the implementation of a large number of projects and programs both at the state level and at the level of regions and individual medical institutions.

Strategic management by project-oriented medical institution (POMI) is intended to ensure the competitive effective functioning of POMI and its sustainable development in the long term, based on the securing of the values of all stakeholders of the POMI, which are: shareholders (owners); consumers of medical services (patients and society as an integrated consumer of medical services), business processes; medical and auxiliary staff of POMI.

The article proposes the methods of integrated management by the threats of providing the values of POMI stakeholders, namely: methods for proactive planning of reactions for the threats and situational threat's management of POMI's medical project.

Further testing and correction of methods for different types of medical projects will increase their efficiency, flexibility and adaptability of POMI's strategic management and the management of its projects to the volatile current Ukrainian conditions, competition and high risks.

Keywords: *medical institution, integrated management by project-oriented medical institution, threats, values of stakeholders.*

Рецензенти Данченко О. Б., д.т.н.,
 Коломицева О.В., д.е.н., професор.

Нахімі Мохаммад Ясін Мохаммад Хусайн, аспірант
Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна
e-mail: mohammadyasin095@gmail.com

РОЛЬ ВИКОРИСТАННЯ СТРУКТУРИ ДЕКОМПОЗИЦІЇ РОБІТ В УПРАВЛІННІ ЗМІСТОМ БУДІВЕЛЬНИХ ПРОЕКТІВ

У статті розглянуто та запропоновано принципи побудови структури декомпозиції робіт (WBS) в управлінні змістом будівельних проектів. Було розкрито переваги використання WBS та представлено IT-інструменти для побудови WBS: Matchware MindView, RationalPlan. Охарактеризовано переваги використання цих IT-інструментів і на основі будівельних проектів описано три кроки для побудови WBS. Розглянуто практику створення WBS з командою проекту.

Ключові слова: *управління змістом проекту, управління проектами, управління будівельними проектами, WBS проекту, будівельні проекти.*

Постановка проблеми. Реалізація будь-яких проектів передбачає застосування знань і процесів управління проектами у різних галузях знань. Однією з таких галузей є управління змістом проекту. Зв'язок між нею та іншими галузями знань проявляється у неможливості управляти проектом без його змісту.

Практичне управління проектами для будівництва охоплює 14 областей знань з управління проектами, які є необхідними для успішних проектів у будівельній галузі. Для кожної області знань пояснюються процеси для управління обсягом, часом, ризиком, вартістю та управління ресурсами [1].

Управління змістом проекту передбачає виконання послідовності процесів (ініціалізація, планування змісту, розробка змісту, визначення змісту, перевірка змісту, контроль за змінами змісту), що взаємодіють не тільки між собою, але й з процесами інших складових управління будівельними проектами.

Визначення змісту робіт проекту може здійснюватися за двома методами:

- використання шаблонів ієрархічної структури робіт;
- декомпозиція робіт проекту.

Найкраще визначення WBS – це таке, яке надає стандарт проектного менеджменту РМВОК: «Орієнтований на результат ієрархічний розклад робіт, який повинна виконати команда проекту», точніше, ієрархічна структура, де кожний спадний рівень представляє все більш детальне визначення робіт проекту [2].

У певних сферах, і особливо в будівництві, обов'язково є чітко визначений та детальний план проекту. Але, щоб отримати це, потрібно починати з обсягу проекту та створити WBS, яка є центральним елементом, який повинен бути представлений зацікавленим сторонам або спонсорам. Їм потрібно побачити, що буде виконано.

Управління проектами будівництва є надзвичайно складним процесом. Для того щоб зробити цей процес успішним, керівник проекту повинен мати чудові навички спілкування та планування, а також мати можливість обговорити із зацікавленими сторонами плани та стратегії проекту. Існує багато завдань, етапів та процедур, які можуть змінюватися під час проекту.

Успішний проект повинен починатися з чіткого обґрунтування та визначення проекту, щоб потім діяти згідно з докладним стратегічним планом і демонструвати очевидні результати. Деякі елементи процесу стратегічного планування початку проекту, такі як: розмір, область і місце розташування продукту, можуть відрізнятися від елементів закінчення проекту. Але, як правило, управління проектом для будівництва має багато спільного з іншими типами проектів.

Існують певні цілі в управлінні будівельними проектами, які повинні бути чітко визначені під час процесу стратегічного планування. Вони можуть змінюватися протягом усього проекту залежно від будь-яких ресурсних обмежень або інших потенційних впливів.

Протягом процесу планування проект може бути організований різними способами:

1. Послідовність задач, в якій проект повністю розділений на етапи відповідно до технології виконання.

2. Паралельне виконання, в якому проект містить незалежні частини, які відбуваються одночасно.

3. Відокремлене виконання, в якому різні завдання можуть перекривати одне одного.

Аналіз останніх джерел досліджень і публікацій. У будівельних проектах на початковому етапі управління проектами використовують професійні інструменти. Одним із таких інструментів є WBS проекту. Зарубіжний і вітчизняний досвід у сфері управління проектами показує, що WBS є невід'ємною частиною планування проекту. Цьому питанню присвячено велику кількість робіт і розробок. Серед них роботи вітчизняних вчених (С. Бушуєв, Н. Бушуєва, Т. Гречко, О. Пономаренко та ін.) та зарубіжних вчених (Alison Dykstra, Paul Netscher, P. Andreas, F. Lawrence Bennett, Dennis P. Miller, Hans Ottosson та ін.). Основу детальної розробки WBS описано в Міжнародному стандарті з управління проектами «Guide to the Project Management Body of Knowledge» (PMBOK). С. Бушуєв вказує, що структура декомпозиції робіт є засобом для створення системи управління проектом, тому що дозволяє вирішувати проблеми організації робіт, розподілу відповідальності, оцінювання вартості, створення системи звітності тощо [3].

Dennis P. Miller ретельно пояснює ключі до ефективної розробки WBS через восьмиетапний процес. Процес «восьми кроків» починається із зосередження зусиль на визначенні проекту через його результати. Наступні кроки йдуть через процес визначення задач проекту, їх послідовності й призначення ресурсів. Останній крок включає в себе оцінювання тривалості й перевірку на шкалі часу проекту [4].

Мета роботи. Метою дослідження є: представити структуру декомпозиції робіт у сфері управління будівельними проектами та обґрунтувати основні положення її побудови; проаналізувати WBS проекту в управлінні змістом будівельних проектів, дати чітке пояснення переваг цього методу в будівництві; описати методи побудови WBS з використанням допоміжних ІТ-інструментів для отримання результатів у будівельних проектах.

Виклад основного матеріалу. Проект будівництва має кінцевий термін та процес, орієнтований на результат, для завершення його з конкретними цілями. Ключовою частиною плану будівництва є WBS.

Після правильної WBS можна спланувати графік проекту. З кожного пакета робіт у WBS менеджер проекту з членами своєї команди може перелічити необхідні дії для побудови кожного компонента. Час, ресурси та вартість потім розподіляються на кожну задачу компонента, після чого створюється графік проекту, а потім встановлюється базовий план графіка [5].

WBS будівельних проектів визначають робочі завдання для кожного члена команди, субпідрядника, архітектора та зовнішнього інженера-консультанта, що працює над проектом. Вона також визначає результати, які отримає клієнт.

Першим кроком розробки WBS є визначення сфери та основних результатів будівельного проекту. Потім потрібно розбити кожен із цих результатів на менші результати, доки не буде можливості досягти рівня індивідуального призначення члена команди або субпідрядника. Коли менеджер проекту працює в рамках цього процесу розбиття, він вказує кінцевий результат, який він хоче отримати від кожного завдання.

По-друге, WBS проекту також базується на методології будівництва, яка буде використовуватися для проекту. Як приклад WBS проекту будівництва водоспаду буде дуже відрізнятися від проекту, який використовує методологію спіралі. У проекті методології водоспаду все планування буде завершено до початку будівництва. У проекті методології спіралі будівельні роботи починаються, перш ніж закінчується все планування. І гнучкий метод планування буде дуже відрізнятися від перших двох типів. Тут ви завершуєте компоненти ітераційно з великою кількістю взаємодій з клієнтом і представленням результатів на кожному кроці.

По-третє, WBS проекту будівництва повинна визначити процедури тестування і контролю якості та критерії прийняття результатів, які будуть використовуватися в різних контрольних точках проекту. Деякі з цих контрольних точок можуть бути випробуванням матеріалів, інші контрольні точки можуть бути порівнянням того, що було затверджено планом [6].

Як бачимо, WBS дуже важлива для всього процесу планування і відстеження проекту. Рекомендації щодо розробки WBS включають наступні етапи [7]:

1. Після того як замовник проекту визначає масштаб, спільну мету проекту, керівник проекту починає створення WBS шляхом розкладання проекту на 4–7 основних результатів.

2. Потрібно визначити кожен з основних результатів у вимірних параметрах.

3. Щоб завершити WBS, керівник проекту бере кожен із основних результатів і далі розкладає їх на менші результати, поки не досягне завдання правильного розміру для окремого виконавця проекту.

1. Навіщо використовувати WBS?

Ця структура має ряд переваг на додаток до визначення і організації робіт по проекту. Бюджет проекту може бути виділений на верхні рівні WBS, а бюджети підрозділів можуть бути швидко розраховані на основі WBS кожного проекту. Виділяючи часові та вартісні оцінки для конкретних розділів WBS, можна швидко розробити графік і бюджет проекту. В процесі виконання проекту окремі розділи WBS можна відстежувати для визначення ефективності витрат за проектом та виявлення проблем і проблемних областей в організації проекту.

WBS в проектах також можуть використовуватися для визначення потенційних ризиків у будівельних проектах. Якщо WBS має гілку, яка не визначена чітко, вона являє собою ризик визначення області дії. Ці ризики слід відстежувати в журналі проекту і переглядати в ході виконання будівельного проекту. Інтегруючи WBS з організаційною структурою проекту, керівник проекту також може визначити точки зв'язку і сформулювати план комунікації для всієї команди проекту [5, 6, 8].

Коли проект відстає, посилення на WBS швидко визначить основні результати, на які впливає невиконаний робочий пакет. WBS також може бути закодована та зафарбована різними кольорами, щоб представляти статус виконання. Наприклад: червоний колір – для зірваних задач, жовтий – для ризикованих задач, зелений – для цілей і синій – для завершених результатів. Це ефективний спосіб створення карти прогресу проекту і залучення уваги керівництва до ключових областей WBS.

При створенні WBS слід враховувати наступні рекомендації:

- верхній рівень являє собою кінцевий результат або проект;

- в підзадачах містяться робочі пакети, які призначаються відділу, підрозділу організації або окремому виконавцю;

- всі елементи структури не повинні бути визначені на одному рівні;

- робочий пакет визначає обсяги, тривалість і витрати для задач, необхідних для виконання його підзадач;

- робочі пакети не повинні перевищувати 10 днів тривалості;

- робочі пакети повинні бути незалежними від інших робочих пакетів WBS;

- робочі пакети є унікальними та не повинні дублюватися на WBS.

2. Інструменти для створення WBS

Створення WBS – це командна робота. Одним із ефективних методів є організація мозкового штурму з різними відділами, які будуть задіяні в проекті.

Існує кілька доступних IT-інструментів, які підтримують мозковий штурм і WBS. MatchWare MindView – це простий у використанні програмний пакет для відображення мозкового штурму, який підтримує WBS проектів, межі проектів, діаграми Ганта і легко експортує їх у Microsoft Project для подальшого визначення розкладу [9].

Ключовою перевагою MatchWare MindView є простота використання структур розбиття робіт у графіках проектів високого рівня. Природним продовженням WBS є графік проекту. Шляхом мозкового штурму менеджер проекту може легко призначити оцінки бюджету та тривалості. Ці оцінки бюджету і тривалості можуть бути легко експортовані в Microsoft Excel або Microsoft Project для додаткового планування та аналізу. Керівники проектів потребують інструментів, які допомагають прискорити їх роботу і зменшити адміністративне навантаження, яке супроводжує процеси управління проектами.

RationalPlan дотримується керівних принципів PMBOK, а також пропонує користувачам вбудований довідник про задачі проекту. Після першого етапу, коли менеджер проекту вказує обсяги проекту, його відводять на етап побудови WBS. Тут він може створити WBS проекту лише з назвами результатів і з

можливістю додавати деякі нотатки для кожного результату [10].

На наступному кроці RationalPlan автоматично генерує графік проекту, і менеджер проекту може продовжувати деталізувати кожну роботу, додавши список дій, встановити тривалості та створити залежності.

3. Переваги використання WBS у будівельному проекті

WBS надає менеджеру проекту і команді необхідну інфраструктуру завдань, яка буде використовуватись надалі для створення докладного кошторису витрат, а також для забезпечення планування задач проекту на максимально детальному і точному рівні.

Чотири основні переваги розробки WBS [11]:

1. WBS змушує команду створювати докладні кроки.

WBS змушує менеджера проекту, членів команди та клієнтів визначати заходи, необхідні для створення і доставки продукту або послуги.

2. WBS закладає основу для графіка і бюджету проекту.

Чітко визначена WBS дозволяє виділяти ресурси для конкретних завдань, допомагає в створенні календарного графіка і полегшує розрахунок надійного бюджету.

3. WBS створює систему підзвітності в проекті.

Рівень деталізації на WBS полегшує залучення людей до відповідальності за виконання своїх завдань. Чітко визначену задачу можна доручити конкретній людині, яка потім відповідає за її завершення.

4. Створення WBS породжує залученість команди.

Хоча керівник проекту часто розробляє WBS самотійно, він буде прагнути до участі в цій роботі членів команди для встановлення деталей WBS. Це стимулюватиме участь команди в плануванні проекту.

Звичайно, розробка WBS – непросте завдання. Це може бути кропіткий процес, який займає досить багато часу. Велика WBS (одна, яка ідентифікує кілька тисяч задач) може зайняти кілька днів. Чим більший обсяг проекту, тим більшою буде WBS. Більше людей повинні надати інформацію, а потім затвердити частину, за яку вони несуть відповідальність. Після затвердження WBS вимагає постійної обробки та контролю [11].

Висновок. В основі розробки WBS проекту є можливість розвитку хорошої практики планування способом досягнення консенсусу між ключовими стейкхолдерами проекту щодо підходу до кожного з результатів. Особливістю досягнення узгодженості керівника проекту з командою є можливість запропонувати різні способи досягнення кінцевого результату в будівельному проекті. Що стосується великих складних будівельних проектів, потрібно мати можливість залучити фахівців з певних видів результатів у будівельному проекті, а також використовувати IT-інструменти побудови WBS.

Список літератури

1. Ottosson Hans. Practical project management for building and construction. July 23, 2012.
2. Project Management Institute. A guide to the project management body of knowledge (PMBOK® Guide). Fifth Edition. 2013.
3. Бушуев С. Д., Бушуева Н. С. Современные подходы к развитию методологии управления проектами. *Управління проектами та розвиток виробництва*. 2005. № 1. С. 5–19.
4. Miller Dennis P. Building a project work breakdown structure: visualizing objectives, deliverables, activities, and schedules. August 1, 2008.
5. Dykstra A. Construction project management: a complete introduction. January 1, 2011.
6. Netscher Paul. Successful construction project management: practical guide. April 14, 2014.
7. Billows R. Create WBS: best practices. URL: <http://4pm.com/2015/10/01/work-breakdown-structure-is-it-just-a-to-do-list/> (дата звернення: 13.09.2018).
8. Andreas P. The construction project management success guide. April 4, 2014.
9. MatchWare. The world's best WBS software. URL: <https://www.matchware.com/wbs-software> (дата звернення: 04. 02. 2020).
10. RationalPlan Project management software. URL: <https://www.rationalplan.com> (дата звернення: 09. 02. 2018).
11. Project management tips. Benefits of the work breakdown structure URL: <http://pmtips.net/blog-new/benefits-work-breakdown-structure> (дата звернення: 28. 10. 2018).

References

- Ottosson, Hans (2012) Practical project management for building and construction, July 23.
- Project Management Institute (2013) A guide to the project management body of knowledge (PMBOK® Guide), fifth ed.
- Bushuev, S. D. Bushueva, N. S. (2005) Modern approaches to the development of the methodology of project management. *Upravlinnya proektamy ta rozvytok vyrobnytstva*, № 1, pp. 5–19 [in Russian].
- Miller, Dennis P. (2008) Building a project work breakdown structure: visualizing objectives, deliverables, activities, and schedules, August 1.
- Dykstra, Alison (2011) Construction project management: a complete introduction, January 1.
- Netscher, Paul (2014) Successful construction project management: practical guide, April 14.
- Billows, R. (2018) Create WBS: best practices. URL: <http://4pm.com/2015/10/01/work-breakdown-structure-is-it-just-a-to-do-list/>
- Andreas, P. (2014) The construction project management success guide, April 4.
- MatchWare. The world's best WBS software (2020). URL: <https://www.matchware.com/wbs-software>
- RationalPlan (2018) Project management software. URL: <https://www.rationalplan.com>
- Project management tips (2018) Benefits of the work breakdown structure. URL: <http://pmtips.net/blog-new/benefits-work-breakdown-structure>

Nakhimi Mokhammad Yasin Mokhammad Khusain, Ph.D. student

Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine
e-mail: mohammadyasin095@gmail.com

THE ROLE OF USING THE WORK BREAKDOWN STRUCTURE IN MANAGING THE CONTENT OF CONSTRUCTION PROJECTS

In this paper, the principles of constructing work breakdown structure (WBS) in managing the content of construction projects are considered and proposed. The advantages of using WBS are revealed and IT tools for building WBS, such as: Matchware MindView, RationalPlan are presented. The advantages of using these IT tools are characterized and three steps for building WBS on the basis of construction projects are described. The practice of creating a WBS with a project team is considered.

Keywords: project content management, project management, construction project management, project WBS, construction projects.

Рецензенти Данченко О. Б., д.т.н.,
 Коломицева О.В., д.е.н., професор.

УДК 621.373.826.032:534.232.082.73

О. Н. Петрищев¹, д.т.н., профессор,
К. В. Базило², к.т.н., доцент

¹Национальный технический университет Украины
«Киевский политехнический институт имени Игоря Сикорского»
просп. Победы, 37, Киев, 03056, Украина

²Черкасский государственный технологический университет
б-р Шевченко, 460, Черкасы, 18006, Украина

РАСЧЕТ ЭЛЕКТРИЧЕСКОГО ИМПЕДАНСА ДИСКОВОГО ПЬЕЗОКЕРАМИЧЕСКОГО ТРАНСФОРМАТОРА С ЗАКОРОЧЕННЫМ СЕКТОРНЫМ ЭЛЕКТРОДОМ ВО ВТОРИЧНОЙ ЭЛЕКТРИЧЕСКОЙ ЦЕПИ

Пьезоэлектрические диски с секторным электродированием поверхности являются практически основным элементом многих микроэлектромеханических систем. Однако в настоящее время отсутствуют надежные и достоверные методики построения математических моделей пьезоэлектрических устройств, которые могли бы использоваться в качестве теоретических основ расчета характеристик и параметров этого класса функциональных элементов современной пьезоэлектроники. В результате исследования математической модели реального устройства можно определить тот набор геометрических, физико-механических и электрических параметров реального объекта, который обеспечивает реализацию технических показателей функционального элемента пьезоэлектроники, оговоренных в техническом задании. Это существенно сокращает время и стоимость разработки новых функциональных элементов пьезоэлектроники.

Основной результат настоящей статьи заключается в том, что впервые построена теория неосесимметричных планарных колебаний тонкого пьезокерамического диска, которая опирается на адекватное описание физического состояния колеблющегося пьезоэлектрика.

Ключевые слова: пьезоэлектрический трансформатор, физические процессы, математическая модель, секторные электроды.

Введение. В работе [1] дана постановка задачи о расчете параметров напряженно-деформированного состояния тонкого пьезокерамического диска с разрезными электродами (рис. 1). Как показано в статье [1], определение разности потенциалов U_2 на электрической нагрузке Z_2 во вторичной цепи пьезоэлектрического трансформатора является, вообще говоря, далеко не тривиальной задачей. Для того, чтобы осознать особенности выполнения некоторых вычислительных процедур, которые описаны в постановочной статье [1], рассмотрим более простую как в смысле выполнения расчетов, так и в смысле планирования и постановки эксперимента ситуацию, когда секторный электрод во вторичной электрической цепи пьезоэлектрического трансформатора накоротко замкнут на общую шину, т. е. когда электрическая нагрузка $Z_2 = 0$. В этом случае электрический потенциал $U(\varphi)$ на поверхности $z = \alpha$ (символом α обозначена толщина пьезокера-

мического диска) определяется очевидным образом:

$$U(\varphi) = \begin{cases} U_0 \forall \varphi \in [-\vartheta_0, \vartheta_0], \\ 0 \forall \varphi \notin [-\vartheta_0, \vartheta_0], \end{cases} \quad (1)$$

что эквивалентно следующему разложению

$$U(\varphi) = \sum_{m=0}^{\infty} \Phi^{(m)} \cos m\varphi, \quad (2)$$

где $\Phi^{(0)} = U_0 \vartheta_0 / \pi$;

$\Phi^{(m)} = 2U_0 \sin m\vartheta_0 / (m\pi) \forall m \geq 1$; U_0 — амплитудное значение электрического потенциала на секторном электроде 1 (рис. 1).

Зная разность потенциалов U_1 и U_0 , можно легко определить электрический импеданс $Z_{\text{эп}}^{(1)}$ вырожденного пьезоэлектрического трансформатора по известному электрическому импедансу Z_1 :

$$Z_{\text{эп}}^{(1)} = \frac{U_0 Z_1}{U_1 - U_0}. \quad (3)$$

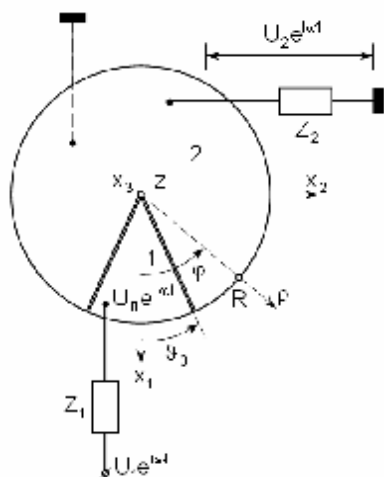


Рис. 1. Расчетная схема объекта

Разность потенциалов U_0 можно определить двумя путями – теоретически и экспе-

риментально. И в том, и в другом случае знание разности потенциалов U_0 позволяет определить входной электрический импеданс $Z_{эл}^{(1)}$ пьезоэлектрического трансформатора.

Таким образом, основной **целью** настоящей статьи является определение разности электрических потенциалов U_0 по схеме вычислительных процедур, которая изложена в работе [1].

1. Определение параметров напряженно-деформированного состояния пьезо-керамического диска

Отправной точкой в схеме построения математической модели дискового пьезоэлектрического трансформатора с секторными электродами является корректное решение дифференциальных уравнений установившихся гармонических колебаний:

$$\frac{\partial \sigma_{\rho\rho}(\rho, \varphi)}{\partial \rho} + \frac{1}{\rho} \frac{\partial \sigma_{\rho\varphi}(\rho, \varphi)}{\partial \varphi} + \frac{1}{\rho} [\sigma_{\rho\rho}(\rho, \varphi) - \sigma_{\varphi\varphi}(\rho, \varphi)] + \rho_0 \omega^2 u_\rho(\rho, \varphi) = 0, \quad (4)$$

$$\frac{\partial \sigma_{\varphi\rho}(\rho, \varphi)}{\partial \rho} + \frac{1}{\rho} \frac{\partial \sigma_{\varphi\varphi}(\rho, \varphi)}{\partial \varphi} + \frac{2}{\rho} \sigma_{\rho\varphi}(\rho, \varphi) + \rho_0 \omega^2 u_\varphi(\rho, \varphi) = 0, \quad (5)$$

где механические напряжения $\sigma_{\rho\rho}(\rho, \varphi)$, $\sigma_{\rho\varphi}(\rho, \varphi) = \sigma_{\varphi\rho}(\rho, \varphi)$ и $\sigma_{\varphi\varphi}(\rho, \varphi)$ определены в работе [1] выражениями (37), (14) и (38) соответственно; ρ_0 – плотность пьезоэлектрической керамики; ω – круговая частота. Решения системы уравнений (4), (5), т. е. ампли-

тудные значения компонентов вектора смещения материальных частиц $u_\rho(\rho, \varphi)$ и $u_\varphi(\rho, \varphi)$ должны обеспечить выполнение третьего закона Ньютона на боковой поверхности $\rho = R$, т. е. граничных условий следующего содержания:

$$\sigma_{\rho\rho}(\rho, \varphi)|_{\rho=R} = [c_{11}^* \varepsilon_{\rho\rho}(\rho, \varphi) + c_{12}^* \varepsilon_{\varphi\varphi}(\rho, \varphi) + e_{31}^* U(\varphi)/\alpha]|_{\rho=R} = 0, \quad (6)$$

$$\sigma_{\rho\varphi}(\rho, \varphi)|_{\rho=R} = 2c_{66}^* \varepsilon_{\rho\varphi}(\rho, \varphi)|_{\rho=R} = 0, \quad (7)$$

где $c_{11}^* = c_{11}^E - (c_{12}^E)^2 / c_{33}^E$; $c_{12}^* = c_{12}^E (1 - c_{12}^E / c_{33}^E)$; $c_{66}^* = (c_{11}^E - c_{12}^E) / 2 = (c_{11}^* - c_{12}^*) / 2$ – модули упругости для режима планарных колебаний тонкого диска; $c_{\beta\lambda}^E$ – справочные значения модулей упругости поляризованной по толщине пьезокерамической пластинки; $e_{31}^* = e_{31} - e_{33} c_{12}^E / c_{33}^E$ – пьезоэлектрический модуль для режима планарных колебаний

тонкого пьезокерамического диска; e_{31} и e_{33} – справочные значения пьезоэлектрических модулей. Компоненты тензора деформаций определяются через компоненты вектора смещения следующим образом [2]: $\varepsilon_{\rho\rho} = \partial u_\rho / \partial \rho$; $\varepsilon_{\varphi\varphi} = \partial u_\varphi / (\rho \partial \varphi) + u_\rho / \rho$; $\varepsilon_{\rho\varphi} = [\partial u_\rho / (\rho \partial \varphi) + \partial u_\varphi / \partial \rho - u_\varphi / \rho] / 2$. В работе [1] показано, что нормальное напряжение $\sigma_{\varphi\varphi}(\rho, \varphi)$ определяется следующим образом:

$$\sigma_{\varphi\varphi}(\rho, \varphi) = c_{12}^* \varepsilon_{\rho\rho}(\rho, \varphi) + c_{11}^* \varepsilon_{\varphi\varphi}(\rho, \varphi) + e_{13}^* U(\varphi) / \alpha. \quad (8)$$

Компоненты вектора смещения материальных частиц диска $u_\rho(\rho, \varphi)$ и $u_\varphi(\rho, \varphi)$ будем искать в следующем виде:

$$u_p(\rho, \varphi) = \sum_{m=0}^{\infty} U_p^{(m)}(\rho) \cos m\varphi, \quad (9)$$

$$u_k(\rho, \varphi) = - \sum_{m=0}^{\infty} U_\varphi^{(m)}(\rho) \sin m\varphi, \quad (10)$$

где $U_\varphi^{(0)}(\rho) \equiv 0$.

Подставляя определения (9) и (10) в формулы для расчета деформаций $\varepsilon_{pp}(\rho, \varphi)$, $\varepsilon_{p\varphi}(\rho, \varphi)$ и $\varepsilon_{\varphi\varphi}(\rho, \varphi)$, а полученные результаты

в соотношения (6) – (8), приходим к следующим расчетным формулам:

$$\sigma_{pp}(\rho, \varphi) = \sum_{m=0}^{\infty} \left\{ c_{11}^* \frac{\partial U_p^{(m)}(\rho)}{\partial \rho} + c_{12}^* \left[\frac{U_p^{(m)}(\rho)}{\rho} - \frac{m U_\varphi^{(m)}(\rho)}{\rho} \right] + \frac{e_{31}^*}{\alpha} \Phi^{(m)} \right\} \cos m\varphi, \quad (11)$$

$$\sigma_{\varphi\varphi}(\rho, \varphi) = \sum_{m=0}^{\infty} \left\{ c_{12}^* \frac{\partial U_p^{(m)}(\rho)}{\partial \rho} + c_{11}^* \left[\frac{U_p^{(m)}(\rho)}{\rho} - \frac{m U_\varphi^{(m)}(\rho)}{\rho} \right] + \frac{e_{31}^*}{\alpha} \Phi^{(m)} \right\} \cos m\varphi, \quad (12)$$

$$\sigma_{p\varphi}(\rho, \varphi) = c_{66}^E \sum_{m=0}^{\infty} \left[-\frac{m U_p^{(m)}(\rho)}{\rho} - \frac{\partial U_\varphi^{(m)}(\rho)}{\partial \rho} + \frac{U_\varphi^{(m)}(\rho)}{\rho} \right] \sin m\varphi. \quad (13)$$

При вычислении производных поперечным ρ и φ от нормальных напряжений $\sigma_{pp}(\rho, \varphi)$ и $\sigma_{\varphi\varphi}(\rho, \varphi)$ необходимо помнить, что разложение (2) обеспечивает выполнение равенства (1). По этой причине $\partial U(\varphi)/\partial \rho = 0$ и $\partial U(\rho)/\partial \varphi = 0$. Подставляя соотношения (11) – (13) в уравнения (4) и (5), получаем формулы

для расчета сумм рядов со знакопеременными членами $\cos m\varphi$ и $\sin m\varphi$. Суммы таких рядов равны нулю только лишь в том случае, когда коэффициенты при знакопеременных функциях $\cos m\varphi$ и $\sin m\varphi$ равны нулю. Последнее приводит к обыкновенным дифференциальным уравнениям следующего вида:

$$\rho^2 \frac{\partial^2 U_p^{(m)}(\rho)}{\partial \rho^2} + \rho \frac{\partial U_p^{(m)}(\rho)}{\partial \rho} + [\gamma \rho^2 - \nu_m^2] U_p^{(m)}(\rho) = -Q_\varphi^{(m)}(\rho), \quad (14)$$

$$\rho^2 \frac{\partial^2 U_\varphi^{(m)}(\rho)}{\partial \rho^2} + \rho \frac{\partial U_\varphi^{(m)}(\rho)}{\partial \rho} + [\lambda \rho^2 - \mu_m^2] U_\varphi^{(m)}(\rho) = -Q_p^{(m)}(\rho), \quad (15)$$

где $\gamma = \omega \sqrt{\rho_0 / c_{11}^*}$ и $\lambda = \omega \sqrt{\rho_0 / c_{66}^E}$ – волновые числа радиальных и окружных колебаний материальных частиц пьезоэлектрического диска; $\nu_m^2 = 1 + (1 - k)m^2/2$; $k = c_{12}^* / c_{11}^*$ – параметр пьезоэлектрика, причем, в отличие от коэффициента Пуассона, параметр $k < 1$ и

ограничения $k \leq 0,5$ не существует; $\mu_m^2 = 1 + c_{11}^* m^2 / c_{66}^E = 1 + 2m^2 / (1 - k)$, поскольку $c_{66}^E = (c_{11}^E - c_{12}^E) / 2 = (c_{11}^* - c_{12}^*) / 2$. Правые части уравнений (14) и (15) определяются следующими выражениями:

$$Q_\varphi^{(m)}(\rho) = \frac{(3k - 1)m}{2} \left[U_\varphi^{(m)}(\rho) - \frac{k + 1}{3k - 1} \rho \frac{\partial U_\varphi^{(m)}(\rho)}{\partial \rho} \right],$$

$$Q_p^{(m)}(\rho) = \frac{(3 - k)m}{1 - k} \left[U_p^{(m)}(\rho) + \frac{k + 1}{3 - k} \rho \frac{\partial U_p^{(m)}(\rho)}{\partial \rho} \right]. \quad (16)$$

Отчетливо видно, что при $m = 0$ уравнение (14) принимает вид хорошо известного [3] уравнения установившихся осесимметричных радиальных колебаний тонкого пьезоэлектрического диска.

Получить точное решение системы уравнений (14), (15) при произвольном значении $m \geq 1$ не представляется возможным.

Вместе с тем, применяя метод последовательных приближений, можно сколь угодно близко подойти к точному решению этой системы уравнений.

Представим точные решения системы уравнений (14), (15), т. е. функции $U_p^{(m)}(\rho)$ и $U_\phi^{(m)}(\rho)$, в виде следующих разложений:

$$U_p^{(m)}(\rho) = U_p^{(m,0)}(\rho) + \sum_{n=1}^{\infty} \Delta U_p^{(m,n)}(\rho), \quad U_\phi^{(m)}(\rho) = U_\phi^{(m,0)}(\rho) + \sum_{n=1}^{\infty} \Delta U_\phi^{(m,n)}(\rho), \quad m \geq 1, \quad (17)$$

где $U_p^{(m,0)}(\rho)$ и $U_\phi^{(m,0)}(\rho)$ – нулевые, т. е. самые грубые, приближения к точным решениям $U_p^{(m)}(\rho)$ и $U_\phi^{(m)}(\rho)$; $\Delta U_p^{(m,n)}(\rho)$ и $\Delta U_\phi^{(m,n)}(\rho)$ – по-

правки n -го порядка к $n-1$ приближению к точному решению $U_p^{(m)}(\rho)$ и $U_\phi^{(m)}(\rho)$, т. е. $U_p^{(m,1)}(\rho) = U_p^{(m,0)}(\rho) + \Delta U_p^{(m,1)}(\rho)$;

$$U_p^{(m,2)}(\rho) = U_p^{(m,1)}(\rho) + \Delta U_p^{(m,2)}(\rho) = U_p^{(m,0)}(\rho) + \Delta U_p^{(m,1)}(\rho) + \Delta U_p^{(m,2)}(\rho)$$

и т. д. Полагая, что имеет место неравенство $|Q_\phi^{(m)}(\rho)| < |Q_p^{(m)}(\rho)|$, нулевые приближения к точному решению системы уравнений (14),

(15) будем искать как решения следующей системы уравнений:

$$\rho^2 \frac{\partial^2 U_p^{(m,0)}(\rho)}{\partial \rho^2} + \rho \frac{\partial U_p^{(m,0)}(\rho)}{\partial \rho} + [(\gamma\rho)^2 - \nu_m^2] U_p^{(m,0)}(\rho) = 0, \quad (18)$$

$$\rho^2 \frac{\partial^2 U_\phi^{(m,0)}(\rho)}{\partial \rho^2} + \rho \frac{\partial U_\phi^{(m,0)}(\rho)}{\partial \rho} + [(\lambda\rho)^2 - \mu_m^2] U_\phi^{(m,0)}(\rho) = -Q_p^{(m,0)}(\rho), \quad (19)$$

где

$$Q_p^{(m,0)}(\rho) = \frac{(3-k)m}{1-k} \left[U_p^{(m,0)}(\rho) + \frac{k+1}{3-k} \rho \frac{\partial U_p^{(m,0)}(\rho)}{\partial \rho} \right]. \quad (20)$$

Решение уравнения (18) очевидно:

$$U_p^{(m,0)}(\rho) = A_0^{(m)} J_{\nu_m}(\gamma\rho), \quad (21)$$

где $A_0^{(m)}$ – подлежащая определению константа; $\nu_m = \sqrt{1 + (1-k)m^2/2}$ – дробный порядок

функции Бесселя. Подставляя решение (21) в определение (20), можем записать, что

$$Q_p^{(m,0)}(\rho) = A_0^{(m)} F_{\nu_m}^{(0)}(\gamma\rho), \quad (22)$$

где

$$F_{\nu_m}^{(0)}(\gamma\rho) = \frac{(3-k)m}{1-k} \left\{ J_{\nu_m}(\gamma\rho) + \left(\frac{k+1}{3-k} \right) \gamma\rho \left[J_{\nu_m-1}(\gamma\rho) - \frac{\nu_m}{\gamma\rho} J_{\nu_m}(\gamma\rho) \right] \right\}.$$

Решение уравнения (19), следуя общеизвестной технологии решения неоднородных

обыкновенных дифференциальных уравнений [4], будем искать в виде

$$U_\phi^{(m,0)}(\rho) = [C_0^{(m)} + C_0^{(m)}(\rho)] J_{\mu_m}(\lambda\rho) + D_0^{(m)}(\rho) N_{\mu_m}(\lambda\rho), \quad (23)$$

где $C_0^{(m)}$ – подлежащая определению константа; $C_0^{(m)}(\rho)$ и $D_0^{(m)}(\rho)$ – варьируемые константы;

$\mu_m = \sqrt{1 + 2m^2/(1-k)}$ – дробный порядок функции Бесселя $J_{\mu_m}(\lambda\rho)$ и функции Неймана $N_{\mu_m}(\lambda\rho)$.

Потребуем, чтобы варьируемые константы $C_0^{(m)}(\rho)$ и $D_0^{(m)}(\rho)$ обеспечивали минимальное количество вычислений, т. е. удовлетворяли условию

$$\frac{\partial C_0^{(m)}(\rho)}{\partial \rho} J_{\mu_m}(\lambda \rho) + \frac{\partial D_0^{(m)}(\rho)}{\partial \rho} N_{\mu_m}(\lambda \rho) = 0. \quad (24)$$

$$\rho^2 \lambda \frac{\partial C_0^{(m)}(\rho)}{\partial \rho} \left[J_{\mu_m-1}(\lambda \rho) - \frac{\mu_m}{\lambda \rho} J_{\mu_m}(\lambda \rho) \right] + \rho^2 \lambda \frac{\partial D_0^{(m)}(\rho)}{\partial \rho} \left[N_{\mu_m-1}(\lambda \rho) - \frac{\mu_m}{\lambda \rho} N_{\mu_m}(\lambda \rho) \right] = -Q_p^{(m,0)}(\rho). \quad (25)$$

Решение системы уравнений (24), (25) позволяет определить первые производные варьируемых констант $C_0^{(m)}(\rho)$ и $D_0^{(m)}(\rho)$ в следующем виде:

$$\begin{aligned} \frac{\partial C_0^{(m)}(\rho)}{\partial \rho} &= \frac{\pi}{2\rho} Q_p^{(m,0)}(\rho) N_{\mu_m}(\lambda \rho), \\ \frac{\partial D_0^{(m)}(\rho)}{\partial \rho} &= -\frac{\pi}{2\rho} Q_p^{(m,0)}(\rho) J_{\mu_m}(\lambda \rho). \end{aligned} \quad (26)$$

Выполнив интегрирование в левых и правых частях соотношений (26), получаем

$$C_0^{(m)}(\rho) = \frac{\pi}{2} \int_0^\rho \frac{1}{x} Q_p^{(m,0)}(x) N_{\mu_m}(\lambda x) dx, \quad (27)$$

$$D_0^{(m)}(\rho) = -\frac{\pi}{2} \int_0^\rho \frac{1}{x} Q_p^{(m,0)}(x) J_{\mu_m}(\lambda x) dx. \quad (28)$$

$$\begin{aligned} C_0^{(m)}(\rho) &= \frac{\pi}{2} \lim_{\varepsilon \rightarrow 0} \left\{ \int_\varepsilon^\rho \frac{1}{x} Q_p^{(m,0)}(x) N_{\mu_m}(\lambda x) dx - \int_\varepsilon^R \frac{1}{x} Q_p^{(m,0)}(x) N_{\mu_m}(\lambda x) dx \right\} = \\ &= -\frac{\pi}{2} \int_\rho^R \frac{1}{x} Q_p^{(m,0)}(x) N_{\mu_m}(\lambda x) dx. \end{aligned} \quad (29)$$

Принимая во внимание соотношения (28) и (29), общее решение (23) можно записать в следующем виде:

$$U_\varphi^{(m,0)}(\rho) = C_0^{(m)} J_{\mu_m}(\lambda \rho) - \frac{\pi}{2} A_0^{(m)} \left[J_{\mu_m}(\lambda \rho) \int_\rho^R \frac{1}{x} F_{v_m}^{(0)}(\gamma x) N_{\mu_m}(\lambda x) dx + N_{\mu_m}(\lambda \rho) \int_0^\rho \frac{1}{x} F_{v_m}^{(0)}(\gamma x) J_{\mu_m}(\lambda x) dx \right]. \quad (30)$$

На боковой поверхности $\rho = R$ пьезоэлектрического диска, который совершает неосесимметричные планарные колебания и

Вычислив (с учетом условия (24)) первую и вторую производную от предполагаемого решения (23) и подставив результаты вычислений вместе с выражением (23) в уравнение (19), получаем следующее равенство:

Поскольку функция Неймана неограниченно возрастает при $x \rightarrow 0$ [5], постольку выражение (27) имеет особенность типа $1/0$. Для того, чтобы избавиться от этой бесконечности, дополним варьируемую константу $C_0^{(m)}(\rho)$ постоянной $\Pi_0^{(m)}$, которую определим следующим образом:

$$\Pi_0^{(m)} = \frac{\pi}{2} \lim_{\varepsilon \rightarrow 0} \int_\varepsilon^R \frac{1}{x} Q_p^{(m,0)}(x) N_{\mu_m}(\lambda x) dx.$$

При этом, очевидно,

$$\frac{\partial}{\partial \rho} [C_0^{(m)}(\rho) + \Pi_0^{(m)}] = \frac{\pi}{2\rho} Q_p^{(m,0)}(\rho) N_{\mu_m}(\lambda \rho),$$

откуда

находится в пустоте, должны выполняться, как того требует третий закон Ньютона, следующие граничные условия:

$$\sigma_{\rho\varphi}^{(m,0)}(\rho) \Big|_{\rho=R} = 0, \quad (31)$$

$$\sigma_{\rho\rho}^{(m,0)}(\rho) \Big|_{\rho=R} = 0, \quad (32)$$

где

$$\sigma_{\rho\varphi}^{(m,0)}(\rho) = c_{66}^E \left[-\frac{m}{\rho} U_\rho^{(m,0)}(\rho) - \frac{\partial U_\varphi^{(m,0)}(\rho)}{\partial \rho} + \frac{U_\varphi^{(m,0)}(\rho)}{\rho} \right],$$

$$\sigma_{\rho\rho}^{(m,0)}(\rho) = c_{11}^* \left\{ \frac{\partial U_\rho^{(m,0)}(\rho)}{\partial \rho} + \frac{k}{\rho} [U_\rho^{(m,0)}(\rho) - m U_\varphi^{(m,0)}(\rho)] + \frac{e_{31}^*}{\alpha c_{11}^*} \Phi^{(m)} \right\}.$$

Подставляя нулевые приближения в граничное условие (31), приходим к выводу, что $U_{\rho}^{(m,0)}(\rho)$ и $U_{\varphi}^{(m,0)}(\rho)$, определенные выражениями (21) и (30) соответственно, в формулу для расчета составляющей касательного напряжения $\sigma_{\rho\varphi}^{(m,0)}(\rho)$, а полученный результат –

$$F_A^{(m,0)}(\gamma, \lambda, R) = mJ_{\nu_m}(\gamma R) + \frac{\pi}{2} [\lambda R N_{\mu_m-1}(\lambda R) - (\mu_m - 1) N_{\mu_m}(\lambda R)] \int_0^R \frac{1}{x} F_{\nu_m}^{(0)}(\gamma x) J_{\mu_m}(\lambda x) dx ;$$

$$F_C^{(m,0)}(\lambda, R) = \lambda R J_{\mu_m-1}(\lambda R) - (\mu_m + 1) J_{\mu_m}(\lambda R).$$

Из равенства (33) следует, что

$$C_0^{(m)} = -A_0^{(m)} \frac{F_A^{(m,0)}(\gamma, \lambda, R)}{F_C^{(m,0)}(\lambda, R)},$$

после чего выражение (30) принимает следующий вид:

$$U_{\varphi}^{(m,0)}(\rho) = -A_0^{(m)} \left\{ J_{\mu_m}(\lambda \rho) \left[\frac{F_A^{(m,0)}(\gamma, \lambda, R)}{F_C^{(m,0)}(\lambda, R)} + \frac{\pi}{2} \int_{\rho}^R \frac{1}{x} F_{\nu_m}^{(0)}(\gamma x) N_{\mu_m}(\lambda x) dx \right] + \right. \\ \left. + \frac{\pi}{2} N_{\mu_m}(\lambda \rho) \int_0^{\rho} \frac{1}{x} F_{\nu_m}^{(0)}(\gamma x) J_{\mu_m}(\lambda x) dx \right\}. \quad (34)$$

Подставляя выражения (21) и (34) в формулу для расчета числовых значений составляющей нормального напряжения $\sigma_{\rho\rho}^{(m,0)}(\rho)$, получаем

$$\sigma_{\rho\rho}^{(m,0)}(\rho) \Big|_{\rho=R} = \frac{c_{11}^*}{R} \left[A_0^{(m)} \frac{\Psi_0^{(m)}(\gamma, \lambda, R)}{F_C^{(m,0)}(\lambda, R)} + \frac{2e_{31}^* R \sin m \vartheta_0}{\alpha c_{11}^* m \pi} U_0 \right] = 0, \quad (35)$$

где

$$\Psi_0^{(m)}(\gamma, \lambda, R) = F_C^{(m,0)}(\lambda, R) [\gamma R J_{\nu_m-1}(\gamma R) - (\nu_m - k) J_{\nu_m}(\gamma R)] + km \left[F_A^{(m,0)}(\gamma, \lambda, R) J_{\mu_m}(\lambda R) + \right. \\ \left. + \frac{\pi}{2} N_{\mu_m}(\lambda R) F_C^{(m,0)}(\lambda, R) \int_0^R \frac{1}{x} F_{\nu_m}^{(0)}(\gamma x) J_{\mu_m}(\lambda x) dx \right]. \quad (36)$$

Из условия (35) находим константу $A_0^{(m)}$:

$$A_0^{(m)} = - \frac{U_0 \beta_m}{\Psi_0^{(m)}(\gamma, \lambda, R)} F_C^{(m,0)}(\lambda, R), \quad (37)$$

где $\beta_m = 2e_{31}^* R \sin m \vartheta_0 / (\alpha c_{11}^* m \pi)$ – размерный (метр/вольт) весовой множитель.

где

$$F_{\mu_m}^{(0)}(\lambda \rho) = J_{\mu_m}(\lambda \rho) \left[F_A^{(m,0)}(\gamma, \lambda, R) + \frac{\pi}{2} F_C^{(m,0)}(\lambda, R) \int_{\rho}^R \frac{1}{x} F_{\nu_m}^{(0)}(\gamma x) N_{\mu_m}(\lambda x) dx \right] + \\ + \frac{\pi}{2} N_{\mu_m}(\lambda \rho) F_C^{(m,0)}(\lambda, R) \int_0^{\rho} \frac{1}{x} F_{\nu_m}^{(0)}(\gamma x) J_{\mu_m}(\lambda x) dx.$$

Таким образом, нулевое приближение к точным решениям уравнений (14) и (15) записывается в следующем виде:

$$U_{\rho}^{(m,0)}(\rho) = - \frac{U_0 \beta_m F_C^{(m,0)}(\lambda, R)}{\Psi_0^{(m)}(\gamma, \lambda, R)} J_{\nu_m}(\gamma \rho), \quad (38)$$

$$U_{\varphi}^{(m,0)}(\rho) = \frac{U_0 \beta_m}{\Psi_0^{(m)}(\gamma, \lambda, R)} F_{\mu_m}^{(0)}(\lambda \rho), \quad (39)$$

Первое приближение к точному решению $U_p^{(m)}(\rho)$, т. е. функция $U_p^{(m,1)}(\rho)$, определяется как решение следующего уравнения:

$$\rho^2 \frac{\partial^2 U_p^{(m,1)}(\rho)}{\partial \rho^2} + \rho \frac{\partial U_p^{(m,1)}(\rho)}{\partial \rho} + [(\gamma\rho)^2 - v_m^2] U_p^{(m,1)}(\rho) = -Q_\phi^{(m,1)}(\rho), \quad (40)$$

где

$$Q_\phi^{(m,1)}(\rho) = \frac{U_0 \beta_m}{\Psi_0^{(m)}(\gamma, \lambda, R)} \Phi_{\mu_m}^{(0)}(\lambda\rho);$$

$$\Phi_{\mu_m}^{(0)}(\lambda\rho) = \frac{(3k-1)m}{2} \left[F_{\mu_m}^{(0)}(\lambda\rho) - \frac{k+1}{3k-1} \rho \frac{\partial F_{\mu_m}^{(0)}(\lambda\rho)}{\partial \rho} \right].$$

После подстановки в уравнение (40) выражения $U_p^{(m,1)}(\rho) = U_p^{(m,0)}(\rho) + \Delta U_p^{(m,1)}(\rho)$, получаем следующее уравнение:

$$\rho^2 \frac{\partial^2 \Delta U_p^{(m,1)}(\rho)}{\partial \rho^2} + \rho \frac{\partial \Delta U_p^{(m,1)}(\rho)}{\partial \rho} + [(\gamma\rho)^2 - v_m^2] \Delta U_p^{(m,1)}(\rho) = -\frac{U_0 \beta_m}{\Psi_0^{(m)}(\gamma, \lambda, R)} \Phi_{\mu_m}^{(0)}(\lambda\rho). \quad (41)$$

Несложно показать, что решение уравнения (41) имеет следующий вид:

$$\Delta U_p^{(m,1)}(\rho) = A_1^{(m)} J_{v_m}(\gamma\rho) - \frac{U_0 \beta_m}{\Psi_0^{(m)}(\gamma, \lambda, R)} W_p^{(m,1)}(\gamma\rho), \quad (42)$$

где

$$W_p^{(m,1)}(\gamma\rho) = \frac{\pi}{2} \left[J_{v_m}(\gamma\rho) \int_{\rho}^R \frac{1}{x} \Phi_{\mu_m}^{(0)}(\lambda x) N_{v_m}(\gamma x) dx + N_{v_m}(\gamma\rho) \int_0^{\rho} \frac{1}{x} \Phi_{\mu_m}^{(0)}(\lambda x) J_{v_m}(\gamma x) dx \right].$$

Поправка $\Delta U_\phi^{(m,1)}(\rho)$ к нулевому приближению $U_\phi^{(m,1)}(\rho)$ определяется из уравнения

$$\rho^2 \frac{\partial^2 \Delta U_\phi^{(m,1)}(\rho)}{\partial \rho^2} + \rho \frac{\partial \Delta U_\phi^{(m,1)}(\rho)}{\partial \rho} + [(\lambda\rho)^2 - \mu_m^2] \Delta U_\phi^{(m,1)}(\rho) = -\Delta Q_\phi^{(m,1)}(\rho), \quad (43)$$

где

$$\Delta Q_\phi^{(m,1)}(\rho) = A_1^{(m)} F_{v_m}^{(0)}(\gamma\rho) - \frac{U_0 \beta_m}{\Psi_0^{(m)}(\gamma, \lambda, R)} \Xi_p^{(m,1)}(\gamma\rho);$$

$$\Xi_p^{(m,1)}(\gamma\rho) = \frac{(3-k)m}{1-k} \left[W_p^{(m,1)}(\gamma\rho) + \frac{k+1}{3-k} \rho \frac{\partial W_p^{(m,1)}(\gamma\rho)}{\partial \rho} \right].$$

Решение уравнения (43) записывается в следующем виде:

$$\Delta U_\phi^{(m,1)}(\rho) = C_1^{(m)} J_{\mu_m}(\lambda\rho) - \frac{\pi}{2} A_1^{(m)} \left[J_{\mu_m}(\lambda\rho) \int_{\rho}^R \frac{1}{x} F_{v_m}^{(0)}(\gamma x) N_{\mu_m}(\lambda x) dx + \right. \\ \left. + N_{\mu_m}(\lambda\rho) \int_0^{\rho} \frac{1}{x} F_{v_m}^{(0)}(\gamma x) J_{\mu_m}(\lambda x) dx \right] + \frac{\pi U_0 \beta_m}{2 \Psi_0^{(m)}(\gamma, \lambda, R)} \left[J_{\mu_m}(\gamma\rho) \int_{\rho}^R \frac{1}{x} \Xi_p^{(m,1)}(\gamma x) N_{\mu_m}(\lambda x) dx + \right. \\ \left. + N_{\mu_m}(\gamma\rho) \int_0^{\rho} \frac{1}{x} \Xi_p^{(m,1)}(\gamma x) J_{\mu_m}(\lambda x) dx \right]. \quad (44)$$

Граничное условие (31) принимает вид

$$\Delta\sigma_{\rho\phi}^{(m,1)}(\rho)\Big|_{\rho=R} = 0, \quad (45)$$

где

$$\Delta\sigma_{\rho\phi}^{(m,1)}(\rho) = c_{66}^E \left[-\frac{m}{\rho} \Delta U_{\rho}^{(m,1)}(\rho) - \frac{\partial \Delta U_{\phi}^{(m,1)}(\rho)}{\partial \rho} + \frac{\Delta U_{\phi}^{(m,1)}(\rho)}{\rho} \right].$$

Подставляя в определение поправки $\Delta\sigma_{\rho\phi}^{(m,1)}(\rho)$ выражения (42) и (44), а полученный результат – в условие (45), получаем следующее уравнение:

$$-A_1^{(m)} F_A^{(m,0)}(\gamma, \lambda, R) - C_1^{(m)} F_C^{(m,0)}(\lambda, R) + \frac{U_0 \beta_m}{\Psi_0^{(m)}(\gamma, \lambda, R)} W_{\rho\phi}^{(m,1)}(\gamma, \lambda, R) = 0, \quad (46)$$

где

$$W_{\rho\phi}^{(m,1)}(\gamma, \lambda, R) = \frac{\pi}{2} \left\{ m N_{\nu_m}(\gamma R) \int_0^R \frac{1}{x} \Phi_{\mu_m}(\lambda x) J_{\nu_m}(\gamma x) dx - \right. \\ \left. - [\lambda R N_{\mu_m-1}(\gamma R) - (\mu_m - 1) N_{\mu_m}(\gamma R)] \int_0^R \frac{1}{x} \Xi_{\rho}^{(m,1)}(\gamma x) J_{\mu_m}(\lambda x) dx \right\}.$$

Из уравнения (46) следует, что

$$C_1^{(m)} = -A_1^{(m)} \frac{F_A^{(m,0)}(\gamma, \lambda, R)}{F_C^{(m,0)}(\lambda, R)} + \frac{U_0 \beta_m}{\Psi_0^{(m)}(\gamma, \lambda, R)} \frac{W_{\rho\phi}^{(m,1)}(\gamma, \lambda, R)}{F_C^{(m,0)}(\lambda, R)}. \quad (47)$$

Граничное условие (32) после подстановки в него определений первых приближений $U_{\rho}^{(m,1)}(\rho) = U_{\rho}^{(m,0)}(\rho) + \Delta U_{\rho}^{(m,1)}(\rho)$ и $U_{\phi}^{(m,1)}(\rho) = U_{\phi}^{(m,0)}(\rho) + \Delta U_{\phi}^{(m,1)}(\rho)$ к точным реше-

ниям уравнений (14) и (15) принимает следующий вид:

$$\Delta\sigma_{\rho\rho}^{(m,1)}(\rho)\Big|_{\rho=R} = 0, \quad (48)$$

где

$$\Delta\sigma_{\rho\rho}^{(m,1)}(\rho) = c_{11}^* \left\{ \frac{\partial \Delta U_{\rho}^{(m,1)}(\rho)}{\partial \rho} + \frac{1}{\rho} [\Delta U_{\rho}^{(m,1)}(\rho) - m \Delta U_{\phi}^{(m,1)}(\rho)] \right\}; \quad (49)$$

слагаемое $e_{31}^* \Phi^{(m)} / (\alpha c_{11}^*)$ в формуле (49) отсутствует, потому что оно сформировало амплитудный множитель $A_0^{(m)}$ в нулевом приближении.

Подставляя выражения (42) и (44) в определение (49), а полученный результат – в граничное условие (48), получаем, с учетом соотношения (47), следующий результат:

$$A_1^{(m)} \frac{\Psi_0^{(m)}(\gamma, \lambda, R)}{F_C^{(m,0)}(\lambda, R)} - \frac{U_0 \beta_m F_A^{(m,1)}(\gamma, \lambda, R)}{\Psi_0^{(m)}(\gamma, \lambda, R) F_C^{(m,0)}(\lambda, R)} = 0, \quad (50)$$

где

$$F_A^{(m,1)}(\gamma, \lambda, R) = km J_{\mu_m}(\lambda R) W_{\rho\phi}^{(m,1)}(\gamma, \lambda, R) + F_C^{(m,0)}(\lambda, R) \times \\ \times \left\{ R \left[\frac{\partial W_{\rho}^{(m,1)}(\gamma R)}{\partial \rho} - \frac{k}{\rho} W_{\rho}^{(m,1)}(\gamma R) \right] \Big|_{\rho=R} + \frac{\pi}{2} km N_{\mu_m}(\lambda R) \int_0^R \frac{1}{x} \Xi_{\rho}^{(m,1)}(\gamma x) J_{\mu_m}(\lambda x) dx \right\}.$$

Из уравнения (50) определяется константа $A_1^{(m)}$:

$$A_1^{(m)} = \frac{U_0 \beta_m}{[\Psi_0^{(m)}(\gamma, \lambda, R)]^2} F_A^{(m,1)}(\gamma, \lambda, R). \quad (51)$$

Выражение (51) завершает процедуру построения первых приближений $U_p^{(m,1)}(\rho)$ и $U_\phi^{(m,1)}(\rho)$ к точным решениям уравнений (14) и (15). Все последующие приближения строятся по схеме, которая была реализована при по-

строении первого приближения. Принимая это во внимание, можно записать общие выражения для амплитудных множителей $A_n^{(m)}$ и $C_n^{(m)}$ n -го приближения в следующем виде:

$$A_n^{(m)} = \frac{U_0 \beta_m}{[\Psi_0^{(m)}(\gamma, \lambda, R)]^{n+1}} F_A^{(m,n)}(\gamma, \lambda, R),$$

$$C_n^{(m)} = -A_n^{(m)} \frac{F_A^{(m,0)}(\gamma, \lambda, R)}{F_C^{(m,0)}(\lambda, R)} + \frac{U_0 \beta_m}{[\Psi_0^{(m)}(\gamma, \lambda, R)]^n} \frac{W_{\rho\phi}^{(m,n)}(\gamma, \lambda, R)}{F_C^{(m,0)}(\lambda, R)}.$$

Как следует из соотношений (47) и (51), первые приближения доопределяют амплитуды радиальных и окружных смещений. Частотные свойства планарных колебаний, т. е. набор резонансных частот, определяются сразу, на первом шаге, при вычислении нулевого приближения, и остаются неизменными при любом последующем приближении к точным значениям компонентов вектора смещения материальных частиц тонкого пьезокерамического диска.

Совершенно очевидно, что корни уравнения

$$\Psi_0^{(m)}(\gamma, \lambda, R) = 0 \quad (52)$$

доставляют числовые значения резонансных частот $\Omega_p^{(m)}$ ($p = 1, 2, 3, \dots$; $m = 1, 2, 3, \dots$; $\Omega = \gamma R$ – безразмерная частота) планарных неосесимметричных колебаний тонкого пьезокерамического диска. При $m = 0$ выражение (36) для расчета числовых значений функции $\Psi_0^{(m)}(\gamma, \lambda, R)$ принимает следующий вид:

$$\Psi_0^{(0)}(\gamma, \lambda, R) = F_C^{(0,0)}(\lambda, R) F_A^{(0,0)}(\gamma, R),$$

где $F_C^{(0,0)}(\lambda, R) = \lambda R J_0(\lambda R) - 2J_1(\lambda R)$;
 $F_A^{(0,0)}(\gamma, R) = \gamma R J_0(\gamma R) - (1 - k)J_1(\gamma R)$.

Уравнение $\Psi_0^{(0)}(\gamma, \lambda, R) = 0$ допускает две реализации, а именно $F_C^{(0,0)}(\lambda, R) = 0$ (при этом $F_A^{(0,0)}(\lambda, R) \neq 0$) или $F_A^{(0,0)}(\lambda, R) = 0$ (при этом $F_C^{(0,0)}(\lambda, R) \neq 0$). Первая ситуация соответствует осесимметричным крутильным колебаниям тонкого пьезокерамического диска. Вторая ситуация соответствует хорошо изученным [6] осесимметричным радиальным колебаниям. Одновременное выполнение условий $F_C^{(0,0)}(\lambda, R) = 0$ и $F_A^{(0,0)}(\lambda, R) = 0$ невозможно по физическим соображениям.

Рассмотрим ситуацию, когда выполняется условие $F_A^{(0,0)}(\lambda, R) = 0$. При этом $F_C^{(0,0)}(\lambda, R) \neq 0$ и окружной компонент $U_\phi^{(0)}(\rho) = 0$, т. е. в тонком пьезокерамическом диске существуют осесимметричные радиальные колебания материальных частиц. Числовые значения первых шести резонансных частот, т. е. первых шести корней уравнения $F_A^{(0,0)}(\lambda, R) = 0$, представлены в табл. 1.

Таблица 1

Числовые значения резонансных частот осесимметричных радиальных колебаний тонкого пьезокерамического диска ($m = 0$)

k	x_1	x_2	x_3	x_4	x_5	x_6
0,30	2,048850	5,389364	8,571859	11,731787	14,883847	18,032222
0,35	2,079508	5,398928	8,577761	11,736076	14,887220	18,035003
0,40	2,109198	5,408461	8,583657	11,740362	14,890591	18,037782
0,45	2,137971	5,417963	8,589546	11,744646	14,893961	18,040561
0,50	2,165871	5,427433	8,595426	11,748926	14,897330	18,043339
0,55	2,192942	5,436869	8,601299	11,753203	14,900696	18,046116
0,60	2,219221	5,446270	8,607163	11,757477	14,904062	18,048892

Примечание: $x_n = \gamma_n R = 2\pi f_n R / \sqrt{c_{11}^* / \rho_0}$; $n = 1, 2, \dots, 6$.

Следует особо подчеркнуть, что числовые значения корней уравнения $F_A^{(0,0)}(\lambda, R) = 0$

определялись в предположении, что потери на вязкое трение в объеме пьезокерамики равны

нулю. Вместе с тем, из результатов экспериментальных исследований [6] следует, что потери энергии упругих колебаний в пьезокерамиках типа ЦТС достаточно велики. Усредненное в диапазоне частот $0 \leq \Omega \leq 20$ значение добротности пьезокерамики $Q_n \leq 80$. При конечном значении добротности Q_n волновые числа γ и λ становятся комплекснозначными величинами, причем $\gamma = \gamma_0(1 - i/(2Q_n))$ и $\lambda = \lambda_0(1 - i/(2Q_n))$, где $\gamma_0 = \omega/\sqrt{c_{11}^*/\rho_0}$ и $\lambda_0 = \omega/\sqrt{c_{66}^E/\rho_0}$ – определенные без учета потерь энергии в материале пьезокерамики волновые числа радиальных и окружных колебаний материальных частиц тонкого диска.

На рис. 2 приведены графики модуля функции $F_A^{(0,0)}(\gamma, R)$, рассчитанные без учета потерь энергии, т. е. при $Q_n \rightarrow \infty$ (пунктирная кривая), и для добротностей $Q_n = 40; 80$. Из показанных на рис. 2 построений следует, что в реальном эксперименте возможно надежно зарегистрировать первые две резонансные частоты. Третий резонанс определяется с трудом, но все-таки определяется. Четвертый и последующие за ним резонансы в реальном эксперименте на больших пьезокерамических дисках практически не видны. Таким образом, последующее определение корней уравнения (52) будем осуществлять в диапазоне безразмерных частот $0 \leq \Omega \leq 10$. Для диска из пьезокерамики типа ЦТС с модулем упругости $c_{11}^* = 76,1$ ГПа и плотностью $\rho_0 = 7430$ кг/м³ значение безразмерной частоты $\Omega = 10$ при

радиусе $R = 33 \cdot 10^{-3}$ м соответствует циклической частоте $f = 154$ кГц.

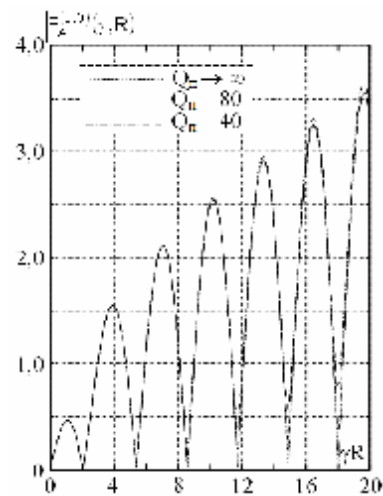


Рис. 2. Частотно зависимое изменение модуля функции $F_A^{(0,0)}(\gamma, R)$ при различных значениях потерь энергии в объеме пьезокерамики

На рис. 3а показано частотно зависимое изменение интегрального слагаемого

$$W_{v_m}^{(\mu_m)}(\gamma, \lambda, R) = \int_0^R \frac{1}{x} F_{v_m}^{(0)}(\gamma x) J_{\mu_m}(\lambda x) dx$$

в формуле (36) для расчета числовых значений функции $\Psi_0^{(m)}(\gamma, \lambda, R)$. На рис. 3б показаны графики произведения интеграла на функцию Неймана $N_{\mu_m}(\lambda R)$, которая, как известно, обращается в бесконечность при стремлении своего аргумента к нулю. Значения интеграла $W_{v_m}^{(\mu_m)}(\gamma, \lambda, R)$ определялись, естественно, численно.

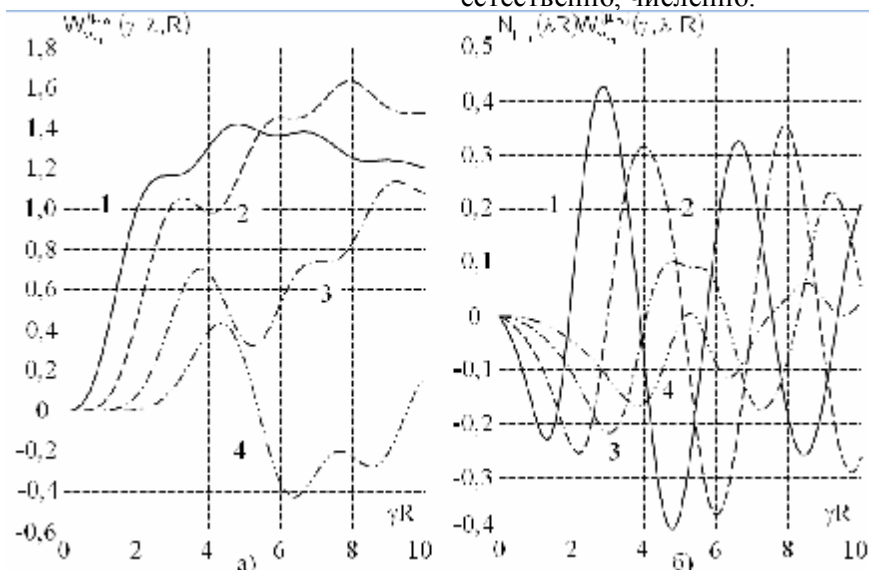


Рис. 3. Частотно зависимое изменение интегрального слагаемого в формуле для расчета числовых значений функции $\Psi_0^{(m)}(\gamma, \lambda, R)$

Цифрами в поле рисунков обозначены значения параметра m . Параметр $k = 0,35$. При построении графиков, показанных на рис. 3, потери энергии в объеме пьезокерамики не учитывались. При вычислениях, которые были выполнены для реального материала с добротностью $Q_p = 80$, было установлено, что мнимая часть интеграла меньше действительной более чем на два порядка. Это позволяет утверждать, что результаты расчетов, при выполнении которых учитываются потери в пьезокерамике, отличаются от результатов, которые получены без учета потерь, на доли процента. Основная цель расчетов, результаты которых графически представлены на рис. 3, заключается в том, чтобы показать, что функция $\Psi_0^{(m)}(\gamma, \lambda, R)$ сохраняет конечные значения, т. е. не теряет аналитич-

ности, во всех точках частотного диапазона $0 \leq \Omega \leq 10$.

В табл. 2 представлены результаты вычисления корней уравнения (52) для пьезокерамики с бесконечной добротностью для параметра $m = 1$. Прочерки в седьмой и восьмой колонках означают, что $(x_7, x_8) > 10$. Прочерки в первой и второй колонках означают, что действительные значения корней уравнения $\Psi_0^{(1)}(\gamma, \lambda, R) = 0$ отсутствуют. Числовые значения корней уравнения $\Psi_0^{(1)}(\gamma, \lambda, R) = 0$ размещены по колонкам табл. 2 в соответствии с принципом: монотонному изменению числовых значений параметра k соответствует монотонное изменение действительных значений корней уравнения.

Таблица 2

Корни уравнения $\Psi_0^{(1)}(\gamma, \lambda, R) = 0$

k	x_1	x_2	x_3	x_4
0,30	-	-	3,911623	5,539152
0,35	-	-	3,829236	5,437504
0,40	-	-	3,744709	5,306088
0,45	-	-	3,657736	5,151679
0,50	2,227320	2,641923	3,567747	4,979361
0,55	2,119035	2,710795	3,473761	4,791539
0,60	2,038388	2,717757	3,374220	4,588571

k	x_5	x_6	x_7	x_8
0,30	5,948812	7,676985	8,756947	9,563390
0,35	5,850308	7,438342	8,768293	9,224752
0,40	5,759540	7,189047	-	-
0,45	5,669546	6,926937	-	-
0,50	5,576048	6,648404	8,469996	8,777221
0,55	5,479674	6,346246	8,039970	8,856692
0,60	5,392088	6,000142	7,645511	9,127612

В табл. 3 приведены действительные значения корней уравнения $\Psi_0^{(m)}(\gamma, \lambda, R) = 0$ для фиксированных значений параметра $m = 2; 3; 4$. Можно отметить, что с ростом значений параметра m возрастают начальные числовые значения первого действительного корня частотного уравнения $\Psi_0^{(m)}(\gamma, \lambda, R) = 0$. Помимо этого, уменьшается количество действительных корней в частотном диапазоне $0 \leq \Omega \leq 10$. Если для $m = 1$ при $k < 0,40$ в диапазоне безразмерных частот $0 \leq \Omega \leq 10$

существует шесть действительных корней, то при $m = 2$ их уже пять, при $m = 3$ - два, и для $m = 4$ остается всего один действительный корень. Говоря иными словами, спектр собственных чисел граничной задачи (14), (15), (31), (32) монотонно перемещается в область более высоких безразмерных частот $\Omega = \gamma R$ при увеличении номера m окружной гармоники планарных колебаний тонкого пьезокерамического диска.

Таблица 3

Числовые значения корней уравнения $\Psi_0^{(m)}(\gamma, \lambda, R) = 0$

m = 2						
k	x ₁	x ₂	x ₃	x ₄	x ₅	x ₆
0,30	5,224122	6,316289	7,181977	8,888322	9,426647	-
0,35	5,147395	6,283961	7,042483	8,669918	9,308233	-
0,40	5,063123	6,224496	6,899122	8,436622	9,188273	-
0,45	4,971017	6,137198	6,750816	8,189068	9,078037	9,872740
0,50	4,870746	6,023171	6,595927	7,926521	9,032471	9,425329
0,55	4,761809	5,884059	6,432273	7,647168	-	-
0,60	4,643407	5,721184	6,257216	7,348024	-	-

m = 3						
k	x ₁	x ₂	x ₃	x ₄	x ₅	x ₆
0,30	-	-	8,437364	-	-	-
0,35	-	-	8,278501	9,842421	-	-
0,40	-	-	8,110490	9,658245	-	-
0,45	6,358329	6,612469	7,932131	9,449698	9,932386	-
0,50	6,155154	6,619131	7,741788	9,219171	9,751691	-
0,55	5,960942	6,571897	7,537102	8,968205	9,588124	-
0,60	5,752409	6,489583	7,314335	8,697224	9,481170	-

m = 4						
k	x ₁	x ₂	x ₃	x ₄	x ₅	x ₆
0,30	-	-	-	-	9,638074	-
0,35	-	-	-	-	9,450503	-
0,40	-	-	7,155191	7,426474	9,248442	-
0,45	-	-	6,969645	7,410500	9,031968	-
0,50	-	-	6,809497	7,354129	8,799033	-
0,55	-	-	6,659742	7,269690	8,554081	-
0,60	4,559561	5,131281	6,514170	7,160959	8,299302	-

В завершение обсуждения результатов решения уравнения (52) необходимо подчеркнуть, что данные табл. 2 и 3 справедливы для весьма специфической ситуации, когда на одном из двух секторных электродов постоянно поддерживается нулевой электрический потенциал.

Определим электрический импеданс $Z_{эл}^{(1)}$.

2. Расчет электрического импеданса пьезокерамического диска под секторным электродом

Поскольку нулевое приближение к точным значениям компонентов вектора смещения материальных частиц диска сразу обеспечивает точное определение резонансных частот, расчет электрического импеданса $Z_{эл}^{(1)}$ будем выполнять в предположении, что напряженно-деформированное состояние диска определяется нулевым приближением, т. е.

$$u_p(\rho, \varphi) = -U_0 \frac{e_{31}^*}{\alpha c_{11}^*} \sum_{m=0}^{\infty} \frac{\sin m \vartheta_0}{m\pi} \frac{F_C^{(m,0)}(\lambda, R)}{\Psi_0^{(m)}(\gamma, \lambda, R)} J_{\nu_m}(\gamma \rho) \cos m\varphi,$$

$$u_\varphi(\rho, \varphi) = -U_0 \frac{e_{31}^*}{\alpha c_{11}^*} \sum_{m=0}^{\infty} \frac{\sin m \vartheta_0}{m\pi} \frac{F_{\mu_m}^{(0)}(\lambda \rho)}{\Psi_0^{(m)}(\gamma, \lambda, R)} \sin m\varphi. \quad (53)$$

Следуя методике, которая изложена в работе [1], определяем аксиальный компонент $D_z^{(1)}(\rho, \varphi)$ вектора электрической индукции под секторным электродом № 1

$$\begin{aligned}
D_z^{(1)}(\rho, \varphi) &= e_{31}^* [\varepsilon_{\rho\rho}(\rho, \varphi) + \varepsilon_{\varphi\varphi}(\rho, \varphi)] - \frac{\chi_{33}^*}{\alpha} U_0 = \\
&= e_{31}^* \left\{ \frac{\partial u_\rho(\rho, \varphi)}{\partial \rho} + \frac{1}{\rho} \left[\frac{\partial u_\varphi(\rho, \varphi)}{\partial \varphi} + u_\rho(\rho, \varphi) \right] \right\} - \frac{\chi_{33}^*}{\alpha} U_0 = \\
&= -\frac{\chi_{33}^*}{\alpha} U_0 \left[2K_{31}^2 \gamma R \sum_{m=0}^{\infty} \frac{\sin m \vartheta_0}{m\pi} W_z^{(m,0)}(\gamma, \lambda, \rho) \cos m\varphi + 1 \right], \quad (54)
\end{aligned}$$

где $\chi_{33}^* = \chi_{33}^E + e_{33}^2/c_{33}^E$ – диэлектрическая проницаемость пьезокерамики в режиме планарных колебаний тонкого диска; χ_{33}^E – справочное значение диэлектрической проницаемости, которое определяется для режима постоянства (равенства нулю) упругих деформаций; $K_{31}^2 = (e_{31}^*)^2 / (\chi_{33}^* c_{11}^*)$ – квадрат коэффициента электромеханической связи для режи-

ма планарных колебаний диска из поляризованной по толщине пьезокерамики; $W_z^{(m,0)}(\gamma, \lambda, \rho)$ – нулевое приближение к точному значению линейного инварианта тензора деформаций (объемная деформация) в режиме планарных колебаний. Числовые значения функции $W_z^{(m,0)}(\gamma, \lambda, \rho)$ рассчитываются по формуле

$$W_z^{(m,0)}(\gamma, \lambda, \rho) = F_C^{(m,0)}(\lambda, R) \left[J_{\nu_m-1}(\gamma\rho) - \frac{\nu_m-1}{\gamma\rho} J_{\nu_m}(\gamma\rho) \right] + \frac{m}{\gamma\rho} F_{\mu_m}^{(0)}(\lambda\rho). \quad (55)$$

Амплитудное значение полного электрического заряда $Q^{(1)}$ на секторном электроде № 1 определяется следующим образом:

$$\begin{aligned}
Q^{(1)} &= \int_{2\pi-\vartheta_0}^{\vartheta_0} \int_0^R \rho D_z^{(1)}(\rho, \varphi) d\rho d\varphi = \\
&= -C_1^* U_0 \left[\frac{4K_{31}^2}{\pi} \sum_{m=0}^{\infty} \frac{\sin^2 m \vartheta_0}{m^2 \vartheta_0} \frac{\Psi_z^{(m,0)}(\gamma, \lambda, R)}{\Psi_0^{(m)}(\gamma, \lambda, R)} + 1 \right], \quad (56)
\end{aligned}$$

где $C_1^* = \chi_{33}^* R^2 \vartheta_0 / \alpha$ – динамическая электрическая емкость секторного электрода № 1; символом $\Psi_z^{(m,0)}(\gamma, \lambda, R)$ обозначена следующая безразмерная аналитическая конструкция:

$$\Psi_z^{(m,0)}(\gamma, \lambda, R) = \frac{1}{\gamma R} \int_0^{\gamma R} \gamma \rho W_z^{(m,0)}(\gamma, \lambda, \rho) d(\gamma\rho). \quad (57)$$

Амплитуда электрического тока $I^{(1)}$, который протекает в проводнике, соединяющем

источник электрических сигналов и секторный электрод № 1 (рис. 1), определена в работе [1] следующим образом: $I^{(1)} = -i\omega Q^{(1)}$. Поскольку $Z_{\text{эл}}^{(1)} = U_0 / I^{(1)}$, постольку, после очевидных действий, получаем выражение для расчета входного электрического импеданса

$$Z_{\text{эл}}^{(1)} = \frac{1}{i\omega C_1^* \Psi^{(0)}(\gamma, \lambda, R)}, \quad (58)$$

где

$$\Psi^{(0)}(\gamma, \lambda, R) = \frac{4K_{31}^2}{\pi} \sum_{m=0}^{\infty} \frac{\sin^2 m \vartheta_0}{m^2 \vartheta_0} \frac{\Psi_z^{(m,0)}(\gamma, \lambda, R)}{\Psi_0^{(m)}(\gamma, \lambda, R)} + 1.$$

Функция $\Psi^{(0)}(\gamma, \lambda, R)$ является нулевым приближением к точному значению функции $\Psi(\gamma, \lambda, R)$, которая определяет частотно зависимое изменение входного электрического импеданса $Z_{\text{эл}}^{(1)}$ вырожденного пьезоэлектрического трансформатора. Когда $\Psi^{(0)}(\gamma, \lambda, R) \rightarrow \infty$, а это наблюдается тогда, когда $\Psi_0^{(m)}(\gamma, \lambda, R) = 0$, электрический импе-

данс $Z_{\text{эл}}^{(1)} \rightarrow 0$, что соответствует физическому состоянию электромеханической системы, которое называется электромеханическим резонансом. В ближайшей окрестности частоты электромеханического резонанса функция $\Psi^{(0)}(\gamma, \lambda, R) = 0$ и $Z_{\text{эл}}^{(1)} \rightarrow \infty$, что соответствует электромеханическому антирезонансу.

На рис. 4а-г показаны результаты расчетов по формуле (58) модуля электрического

импеданса $Z_{эл}^{(1)}$ для различных значений углового размера ϑ_0 секторного электрода. Числовые значения ϑ_0 в дуговых градусах указаны в поле рисунков. Расчеты были выполнены для пьезокерамики типа ЦТС со следующими значениями физико-механических параметров: $c_{33}^E = 108,6$ ГПа; $c_{11}^E = 94,8$ ГПа; $c_{12}^E = 44$ ГПа; $\chi_{33}^E = 7,0227 \cdot 10^{-9}$ Ф/м; $e_{33} = 13,17$ Кл/м²; $e_{31} = -5,89$ Кл/м²; $\rho_0 = 7428$ кг/м³. Размеры пьезокерамического диска: радиус $R = 33 \cdot 10^{-3}$ м, толщина $a = 3 \cdot 10^{-3}$ м. Расчет выполнялся для двух значений добротности Q_p пьезокерамики – 80 единиц (сплошные кривые) и 160 единиц (штриховые кривые). Параметр пьезокерамики $k = c_{12}^*/c_{11}^* = 0,34$. По осям ординат от-

кладываются значения модуля $Z_{эл}^{(1)}$ в килоомах, по осям абсцисс – значения циклической частоты f в килогерцах. Счет электрического импеданса начинался с частоты $f = 5$ кГц. При выполнении вычислений суммировались первые три окружных гармоники, т. е. выражения со значениями индекса $m = 0, 1$ и 2 . Отчетливо видно, что с увеличением углового размера ϑ_0 секторного электрода в диапазоне частот $(5 \div 100)$ кГц проявляются электромеханические резонансы, которые обусловлены нулевой окружной гармоникой (резонансы 1 и 4 на рис. 4в), первой окружной гармоникой (резонансы 2 и 5) и второй гармоникой (резонансы 3 и 6). Это позволяет выполнить экспериментальную проверку теоретических результатов, которые были изложены выше.

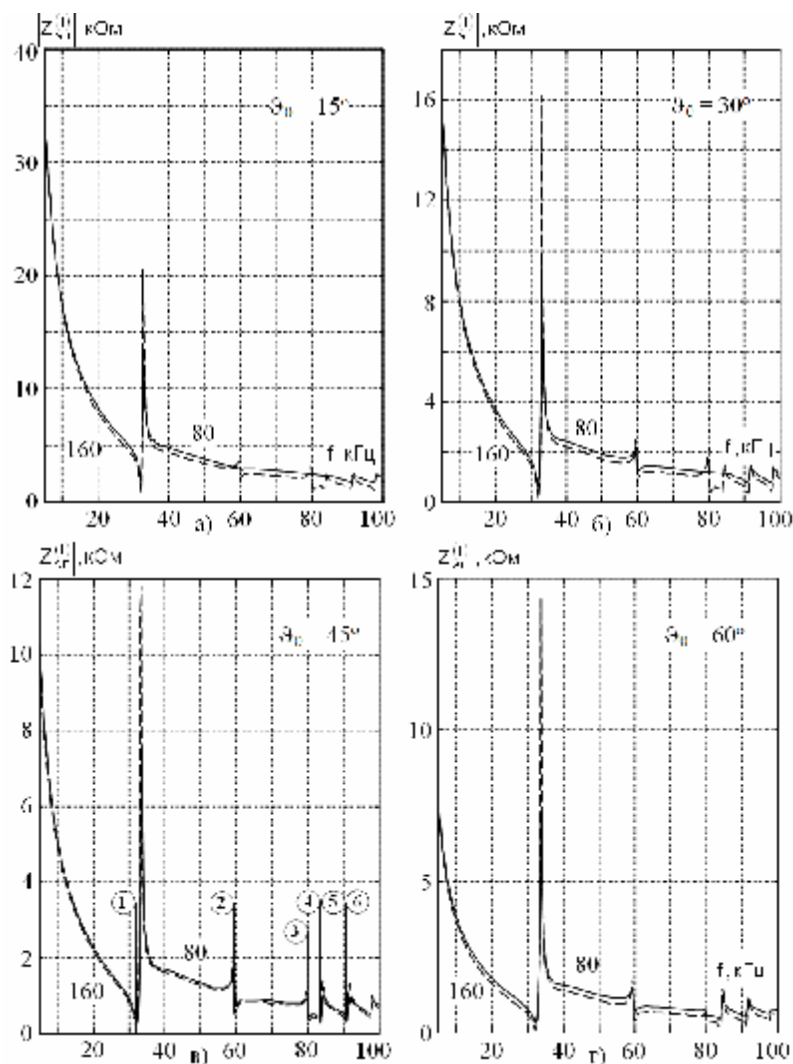


Рис. 4. Модуль электрического импеданса $Z_{эл}^{(1)}$ части пьезокерамического диска под секторным электродом 1

Выводы. Основной результат настоящей статьи заключается в том, что впервые построена теория неосесимметричных планарных колебаний тонкого пьезокерамического диска, которая опирается на адекватное описание физического состояния колеблющегося пьезоэлектрика.

Список литературы

1. Петрищев О. Н., Базило К. В. Принципы и методы построения математических моделей дисковых пьезоэлектрических трансформаторов с секторными электродами. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*. 2017. № 2. С. 33–44.
2. Петрищев О. Н. Гармонические колебания пьезокерамических элементов. Часть 1. Гармонические колебания пьезокерамических элементов в вакууме и метод резонанса – антирезонанса. Киев: Аверс, 2012. 300 с.
3. Петрищев О. Н., Базило К. В. Принципы и методы расчета передаточных характеристик дисковых пьезоэлектрических трансформаторов. Часть 2. Методика расчета параметров и характеристик простейшего дискового пьезоэлектрического трансформатора. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*. 2015. № 4. С. 10–23.
4. Смирнов В. И. Курс высшей математики. Т. 2. Санкт-Петербург: БХВ-Петербург, 2008. 848 с.
5. Справочник по специальным функциям с формулами, графиками и математическими таблицами / под ред. М. Абрамовица и И. Стиган. Москва: Наука, 1979. 832 с.
6. Петрищев О. Н., Базило К. В. Определение электрического импеданса пьезокерамического диска и его расчет в области средних

и высоких частот. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*. 2016. № 3. С. 36–49.

References

1. Petrishchev, O. N. and Bazilo, C. V. (2017) Principles and methods of constructing mathematical models of disk piezoelectric transformers with sector electrodes. *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu. Seria: Tehnichni nauky*, No. 2, pp. 33–44 [in Russian].
2. Petrishchev, O. N. (2012). Harmonic oscillations of piezoceramic elements. Part 1. Harmonic oscillations of piezoceramic elements in vacuum and resonance-antiresonance method. Kyiv: Avers, 300 p. [in Russian].
3. Petrishchev, O. N. and Bazilo, C. V. (2015) Calculation principles and methods of the transfer characteristics of disk piezoelectric transformers. Part 2. Method of parameters and characteristics calculation of the simplest disk piezoelectric transformer. *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu. Seria: Tehnichni nauky*, No. 4, pp. 10–23 [in Russian].
4. Smirnov V. I. (2008) Course of higher mathematics. Vol. 2. St. Petersburg: BXV-Peterburg, 848 p. [in Russian]
5. Handbook on special functions with formulas, diagrams and mathematical tables (1979). In: M. Abramowitz and I. Stigun (eds). Moscow: Nauka, 832 p. [in Russian].
6. Petrishchev, O. N. and Bazilo, C. V. (2016) Calculation of electrical impedance of piezoceramic disk and its calculation in the range of medium and high frequencies. *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu. Seria: Tehnichni nauky*, No. 3, pp. 36–49 [in Russian].

O. N. Petrishchev¹, *Dr.Tech.Sc., professor,*
C. V. Bazilo², *Ph.D. (Eng.), associated professor*
¹National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"
Peremogy ave., 37, Kyiv, 03056, Ukraine
²Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine

CALCULATION OF ELECTRICAL IMPEDANCE OF DISK PIEZOCERAMIC TRANSFORMER WITH A SHORTED SECTOR ELECTRODE IN SECONDARY ELECTRICAL CIRCUIT

Piezoelectric disks with partial covering by electrodes of one or two surfaces are often used to create various functional piezoelectronic devices. Disks with sector covering by electrodes are almost the main element of many microelectromechanical systems. Currently, there are no reliable and valid methods of constructing of mathematical models of piezoelectric transformers, which could be used as a theoretical basis for characteristics and parameters calculating of this class of functional elements of modern piezoelectronics. As a result of research of mathematical model of a real device, a set of geometrical, physical, mechanical and electrical parameters of a real object that provides implementation of technical indicators of functional element of piezoelectronics specified in technical task can be determined. This significantly reduces time and cost of the development of new functional elements of piezoelectronics. The cost of the saved resources is the commercial price of mathematical model.

The purpose of this article is to determine the difference of electrical potentials according to the scheme of computational procedures of disk piezoceramic transformers with cut electrodes.

The main result of this article is that for the first time a theory of non-axisymmetric planar oscillations of a thin piezoceramic disk, which is based on adequate description of physical state of oscillating piezoelectric materials, is constructed.

Keywords: *piezoelectric transformer, physical processes, mathematical model, sector electrodes.*

Статтю представляє О. М. Петріщев, д.т.н., професор.

УДК 621.373.826.032:534.232.082.73

О. Н. Петришев¹, д.т.н., профессор,
К. В. Базило², к.т.н., доцент

¹Национальный технический университет Украины
«Киевский политехнический институт имени Игоря Сикорского»
просп. Победы, 37, Киев, 03056, Украина

²Черкасский государственный технологический университет
б-р Шевченко, 460, Черкассы, 18006, Украина

РАСЧЕТ КОЭФФИЦИЕНТА ТРАНСФОРМАЦИИ ПЬЕЗОКЕРАМИЧЕСКОГО ТРАНСФОРМАТОРА С СЕКТОРНЫМИ ЭЛЕКТРОДАМИ

Основной результат настоящей статьи заключается в том, что предложена рациональная методика построения математической модели пьезокерамического трансформатора с секторным электродированием рабочей поверхности диска, которая не предполагает решения бесконечной системы алгебраических уравнений.

Пьезоэлектрические диски с секторным электродированием поверхности являются практически основным элементом многих микроэлектромеханических систем. Однако в настоящее время отсутствуют надежные и достоверные методики построения математических моделей пьезоэлектрических устройств, которые могли бы использоваться в качестве теоретических основ расчета характеристик и параметров этого класса функциональных элементов современной пьезоэлектроники. В результате исследования математической модели реального устройства можно определить тот набор геометрических, физико-механических и электрических параметров реального объекта, который обеспечивает реализацию технических показателей функционального элемента пьезоэлектроники, оговоренных в техническом задании. Это существенно сокращает время и стоимость разработки новых функциональных элементов пьезоэлектроники.

Ключевые слова: пьезоэлектрический трансформатор, физические процессы, математическая модель, секторные электроды.

Введение. В работе [1] дана постановка задачи о расчете параметров напряженно-деформированного состояния тонкого пьезокерамического диска с разрезными электродами (рис. 1) и предложена универсальная методика определения разности электрических потенциалов U_2 на электрической нагрузке Z_2 во вторичной электрической цепи пьезоэлектрического трансформатора. В работе [2] методом последовательных приближений выполнено решение системы дифференциальных уравнений установившихся планарных неосесимметричных колебаний тонкого пьезокерамического диска с разрезными электродами. Определены расчетные формулы для компонентов вектора смещения материальных частиц колеблющегося диска и выполнена оценка электрического импеданса первичной электрической цепи пьезоэлектрического трансформатора для режима короткого замыкания во вторичной электрической цепи. Основным результатом статьи [2] является по-

строение альтернативной предлагаемой в монографии [3] теории неосесимметричных планарных колебаний тонких пьезокерамических дисков.

В настоящей статье, которая является логическим продолжением и завершением публикаций [1, 2], предлагается усовершенствованная (по сравнению с предлагаемой в работе [1]) методика построения математической модели пьезокерамического трансформатора, расчетная схема которого показана на рис. 1, что и является **целью** данной работы.

1. Методика построения математической модели пьезокерамического трансформатора с секторными электродами

Как и ранее [1], математической моделью пьезоэлектрического трансформатора будем называть аналитическое выражение $K(\omega, \Pi)$ (ω – круговая частота; символ Π обозначает набор геометрических, физико-механических и электрических параметров трансформатора (рис. 1)), которое определя-

64

ния пьезомодулей и модулей упругости для поляризованной по толщине диска пьезокерамики; α и R - толщина и радиус диска, причем $\alpha/R \ll 1$; ϑ_0 - половинный угол раскрытия секторного электрода в первичной электрической цепи пьезокерамического трансформатора; $\gamma = \omega/\sqrt{c_{11}^*/\rho_0}$ - волновое число радиальных колебаний тонкого диска; ρ_0 - плотность пьезокерамики. Символами $J_q(\gamma\rho)$ ($q = 0, 1, v_m$) обозначены функции Бесселя соответствующих порядков; дробный порядок $v_m = \sqrt{1 + (1-k)m^2/2}$, где $k = c_{12}^*/c_{11}^*$; $c_{12}^* = c_{12}^E(1 - c_{12}^E/c_{33}^E)$. Частотно зависящая функция $F_B^{(0,m)}(\lambda) = (1 + \mu_m)J_{\mu_m}(\lambda R) - \lambda R J_{\mu_m-1}(\lambda R)$, где

$\lambda = \omega/\sqrt{(c_{11}^* - c_{12}^*)/(2\rho_0)}$ - волновое число окружных планарных колебаний материальных частиц тонкого пьезокерамического диска; $\mu_m = \sqrt{1 + 2m^2/(1-k)}$ - дробный порядок функций Бесселя $J_{\mu_m}(\lambda R)$ и Неймана $N_{\mu_m}(\lambda R)$, которые присутствуют в математическом описании окружной составляющей планарных колебаний тонкого диска. Символом $\Psi_0^{(m)}(\gamma, \lambda, R)$ обозначено нулевое приближение к точному значению частотного уравнения неосесимметричной, номера m , моды планарных колебаний тонкого пьезокерамического диска. Числовые значения функции $\Psi_0^{(m)}(\gamma, \lambda, R)$ задаются следующим выражением:

$$\Psi_0^{(m)}(\gamma, \lambda, R) = F_B^{(0,m)}(\lambda) [\gamma R J_{v_m-1}(\gamma R) - (v_m - k) J_{v_m}(\gamma R)] - km \left[F_A^{(0,m)}(\gamma, \lambda) J_{\mu_m}(\lambda R) - \frac{\pi}{2} F_B^{(0,m)}(\lambda) N_{\mu_m}(\lambda R) \int_0^R \frac{1}{x} F_{v_m}^{(0)}(\gamma x) J_{\mu_m}(\lambda x) dx \right], \quad (5)$$

где функции $F_A^{(0,m)}(\gamma, \lambda)$ и $F_{v_m}^{(0)}(\gamma x)$ определяются следующим образом:

$$F_A^{(0,m)}(\gamma, \lambda) = m J_{v_m}(\gamma R) + \frac{\pi}{2} [(1 + \mu_m) N_{\mu_m}(\lambda R) - \lambda R N_{\mu_m-1}(\lambda R)] \int_0^R \frac{1}{x} F_{v_m}^{(0)}(\gamma x) J_{\mu_m}(\lambda x) dx;$$

$$F_{v_m}^{(0)}(\gamma x) = \frac{(3-k)m}{1-k} \left\{ J_{v_m}(\gamma x) + \frac{k+1}{3-k} [\gamma x J_{v_m-1}(\gamma x) - v_m J_{v_m}(\gamma x)] \right\}.$$

Функция $\Psi_\phi^{(0,m)}(\rho)$ рассчитывается по формуле

$$\Psi_\phi^{(0,m)}(\rho) = \frac{1}{\Psi_0^{(m)}(\gamma, \lambda, R)} \left\{ \left[F_A^{(0,m)}(\gamma, \lambda) - \frac{\pi}{2} F_B^{(0,m)}(\lambda) \int_\rho^R \frac{1}{x} F_{v_m}^{(0)}(\gamma x) N_{\mu_m}(\lambda x) dx \right] J_{\mu_m}(\lambda \rho) - \frac{\pi}{2} F_B^{(0,m)}(\lambda) N_{\mu_m}(\lambda \rho) \int_0^\rho \frac{1}{x} F_{v_m}^{(0)}(\gamma x) J_{\mu_m}(\lambda x) dx \right\}.$$

Числовые значения корней $\chi_n^{(m)} = \gamma_n^{(m)} R$ ($n = 1, 2, 3, \dots$) уравнения $\Psi_0^{(m)}(\gamma_n, \lambda_n, R) = 0$ для окружных гармоник с номерами $m \geq 1$ в диапазоне значений безразмерных волновых чисел (частот) $\gamma R \leq 10$ для параметра упругих свойств пьезокерамики $k = c_{12}^*/c_{11}^* = 0,34$ показаны в табл. 1.

Следует обратить внимание на то, что первый корень $\chi_1^{(1)}$ или, что то же самое, частота первого электромеханического ре-

зонанса для первой ($m = 1$) окружной моды, имеет меньшее значение по сравнению с частотой первого электромеханического резонанса осесимметричных радиальных колебаний. С ростом номера m окружной моды числовые значения безразмерной частоты $\gamma_1^{(m)} R$ монотонно возрастают, и поэтому общее число корней уравнения $\Psi_0^{(m)}(\gamma_n, \lambda_n, R) = 0$ в любом фиксированном диапазоне числовых значений безразмерных волновых чисел (частот) имеет фиксированное (ограниченное) значение.

Таблица 1

Числовые значения корней уравнения $\Psi_0^{(m)}(\gamma_n, \lambda_n, R) = 0$

$m \setminus \chi_n^{(m)}$	$\chi_1^{(m)}$	$\chi_2^{(m)}$	$\chi_3^{(m)}$	$\chi_4^{(m)}$	$\chi_5^{(m)}$	$\chi_6^{(m)}$
1	1,085045	2,464587	3,674256	7,571771	8,735141	9,413737
2	2,057536	3,134450	4,846928	6,378587	6,729860	-
3	2,966933	3,690970	6,101373	6,889025	8,130622	-
4	3,819653	4,700591	9,486512	-	-	-
5	4,618638	5,552675	-	-	-	-
6	5,374142	6,435415	-	-	-	-
7	6,098880	7,336232	-	-	-	-
8	6,802725	8,245702	-	-	-	-
9	7,492040	9,157764	-	-	-	-
10	8,170770	-	-	-	-	-
11	8,841415	-	-	-	-	-
12	9,505634	-	-	-	-	-

Примечание: прочерк в ячейке означает, что числовое значение корня больше 10.

Рассматривая конструкцию выражений (3) и (4), можно сделать вывод, что потенциалы U_0 и U_2 линейно связаны между собой. Для того, чтобы определить эту связь, выполним расчет амплитудного значения U_2 электрического потенциала на секторном электроде 2 во вторичной электрической цепи трансформатора.

Очевидно, что

$$U_2 = I_2 Z_2, \quad (6)$$

где I_2 – амплитудное значение электрического тока в проводнике, который соединяет электрическую нагрузку Z_2 с секторным электродом 2. В монографии [4] показано, что амплитуда электрического тока $I_2 = -i\omega Q_2$, где Q_2 – амплитудное значение изменяющегося во времени по закону $e^{i\omega t}$ электрического заряда на секторном электроде 2. Электрический заряд

$$Q_2 = \int_{\vartheta_0}^{2\pi - \vartheta_0} \int_0^R \rho D_z^{(2)}(\rho, \varphi) d\rho d\varphi, \quad (7)$$

где $D_z^{(2)}(\rho, \varphi)$ – аксиальный компонент вектора электрической индукции под секторным электродом 2. Числовое значение $D_z^{(2)}(\rho, \varphi)$ в тонком, совершающем планарные колебания, пьезоэлектрическом диске определяется следующим образом:

$$D_z^{(2)}(\rho, \varphi) = e_{31}^* [\varepsilon_{\rho\rho}(\rho, \varphi) + \varepsilon_{\varphi\varphi}(\rho, \varphi)] + \chi_{33}^* E_z^{(2)}, \quad (8)$$

где $\varepsilon_{\rho\rho}(\rho, \varphi) = \partial u_\rho(\rho, \varphi) / \partial \rho$,

$\varepsilon_{\varphi\varphi}(\rho, \varphi) = \partial u_\varphi(\rho, \varphi) / (\rho \partial \varphi) + u_\rho(\rho, \varphi) / \rho$ – дефор-

мации сжатия-растяжения вдоль радиальной и окружной криволинейной оси соответственно; алгебраическая сумма $\varepsilon_{\rho\rho}(\rho, \varphi) + \varepsilon_{\varphi\varphi}(\rho, \varphi)$ является линейным инвариантом тензора деформации в цилиндрической системе координат и имеет смысл объемной деформации тонкого пьезокерамического диска; $\chi_{33}^* = \chi_{33}^E + e_{33}^2 / c_{33}^E$ – диэлектрическая проницаемость для режима постоянства (равенства нулю) нормального напряжения σ_{zz} ; $E_z^{(2)} = -U_2 / \alpha$ – аксиальный компонент вектора напряженности электрического поля под секторным электродом 2.

Подставляя в определения компонентов тензора деформации выражения (3) и (4), а полученные результаты – последовательно в соотношения (8) и (7), после выполнения тривиальной операции интегрирования можем записать следующее выражение:

$$Q_2 = -K_{31}^2 U_0 C_2^* \Xi_0(\gamma, \lambda) - U_2 C_2^* \Xi_2(\gamma, \lambda), \quad (9)$$

где $K_{31}^2 = (e_{31}^*)^2 / (\chi_{33}^* c_{11}^*)$ – квадрат коэффициента электромеханической связи в режиме планарных колебаний тонкого пьезокерамического диска. Числовое значение K_{31}^2 характеризует эффективность двойного преобразования энергии в пьезокерамике и является энергетической характеристикой материала. Символом C_2^* обозначена динамическая электрическая емкость секторного электрода 2, причем $C_2^* = (\pi - \vartheta_0) R^2 \chi_{33}^* / \alpha$. Символами $\Xi_0(\gamma, \lambda)$ и $\Xi_2(\gamma, \lambda)$ обозначены следующие аналитические конструкции:

$$\begin{aligned}\Xi_0(\gamma, \lambda) &= \frac{2\vartheta_0 J_1(\gamma R)}{\pi[\gamma R J_0(\gamma R) - (1-k)J_1(\gamma R)]} - \frac{4}{\pi - \vartheta_0} \sum_{m=1}^{\infty} \frac{\sin^2 m\vartheta_0}{m^2 \pi} \times \\ &\times \left\{ \frac{F_B^{(0,m)}(\lambda)}{\Psi_0^{(m)}(\gamma, \lambda, R)} J_{\nu_m}(\gamma R) - \frac{m}{R} \int_0^R \Psi_\varphi^{(0,m)}(\rho) d\rho \right\}; \\ \Xi_2(\gamma, \lambda) &= 1 + \frac{2K_{31}^2(\pi - \vartheta_0)J_1(\gamma R)}{\pi[\gamma R J_0(\gamma R) - (1-k)J_1(\gamma R)]} - \frac{4K_{31}^2}{\pi - \vartheta_0} \sum_{m=1}^{\infty} \frac{\sin^2 m\vartheta_0}{m^2 \pi} \times \\ &\times \left\{ \frac{F_B^{(0,m)}(\lambda)}{\Psi_0^{(m)}(\gamma, \lambda, R)} J_{\nu_m}(\gamma R) - \frac{m}{R} \int_0^R \Psi_\varphi^{(0,m)}(\rho) d\rho \right\}.\end{aligned}$$

Так как $U_2 = -i\omega Q_2 Z_2$, то после подстановки выражения (9) в это определение, которое с очевидностью следует из соотношения (6), получаем следующее уравнение:

$$U_2 [1 + i\omega C_2^* Z_2 \Xi_2(\gamma, \lambda)] = i\omega C_2^* Z_2 \Xi_0(\gamma, \lambda) K_{31}^2 U_0,$$

откуда следует, что

$$U_2 = \Psi_2(\gamma, \lambda) U_0, \quad (10)$$

где частотно зависимый коэффициент пропорциональности

$$\Psi_2(\gamma, \lambda) = \frac{i\omega C_2^* Z_2 K_{31}^2 \Xi_0(\gamma, \lambda)}{1 + i\omega C_2^* Z_2 \Xi_2(\gamma, \lambda)}.$$

Теперь определим потенциал U_0 через потенциал U_1 источника электрической энергии в первичной электрической цепи пьезоэлектрического трансформатора.

Из показанной на рис. 1 расчетной схемы следует, что

$$U_0 = \frac{U_1 Z_{\text{эл}}^{(1)}}{Z_1 + Z_{\text{эл}}^{(1)}}, \quad (11)$$

где $Z_{\text{эл}}^{(1)}$ – электрический импеданс части пьезоэлектрического диска, которая покрыта секторным электродом 1. Следуя закону Ома для участка электрической цепи, определим $Z_{\text{эл}}^{(1)}$ следующим соотношением:

$$Z_{\text{эл}}^{(1)} = \frac{U_0}{I_1}, \quad (12)$$

где $I_1 = -i\omega Q_1$ – амплитудное значение электрического тока в проводнике, который соединяет источник электрической энергии и секторный электрод 1 первичной электрической цепи пьезоэлектрического трансформатора. Электрический заряд Q_1 на секторном электроде 1 определяется стандартным образом:

$$Q_1 = 2 \int_0^{\vartheta_0} \int_0^R \rho D_z^{(1)}(\rho, \varphi) d\rho d\varphi, \quad (13)$$

где

$D_z^{(1)}(\rho, \varphi) = e_{31}^* [\varepsilon_{\rho\rho}(\rho, \varphi) + \varepsilon_{\varphi\varphi}(\rho, \varphi)] - \chi_{33}^* U_0 / \alpha$ – аксиальный компонент вектора электрической индукции в деформируемом пьезоэлектрическом диске под секторным электродом 1.

Подставляя в определение компонентов тензора деформации выражения (3) и (4), в которых потенциал U_2 заменяется правой частью выражения (10), после вычисления интеграла (13) получаем следующий результат:

$$Q_1 = -C_1^* U_0 \Xi_1(\gamma, \lambda), \quad (14)$$

где $C_1^* = \vartheta_0 R^2 \chi_{33}^* / \alpha$ – динамическая электрическая емкость части пьезоэлектрического диска под секторным электродом 1. Частотно зависящая функция $\Xi_1(\gamma, \lambda)$ определяется следующим выражением:

$$\begin{aligned}\Xi_1(\gamma, \lambda) &= 1 + 4K_{31}^2 \frac{[\vartheta_0 + \Psi_2(\gamma, \lambda)(\pi - \vartheta_0)]J_1(\gamma R)}{\pi[\gamma R J_0(\gamma R) - (1-k)J_1(\gamma R)]} - 4K_{31}^2 \frac{\vartheta_0}{\pi} [1 - \Psi_2(\gamma, \lambda)] \times \\ &\times \sum_{m=1}^{\infty} \left(\frac{\sin m\vartheta_0}{m\vartheta_0} \right)^2 \left\{ \frac{F_B^{(0,m)}(\lambda)}{\Psi_0^{(m)}(\gamma, \lambda, R)} J_{\nu_m}(\gamma R) - \frac{m}{R} \int_0^R \Psi_\varphi^{(0,m)}(\rho) d\rho \right\}.\end{aligned}$$

После расчета электрического заряда Q_1 по формуле (14) определяется электрический ток $I_1 = i\omega C_1^* U_0 \Xi_1(\gamma, \lambda)$ и электрический импеданс

$$Z_{\text{эп}}^{(1)} = \frac{1}{i\omega C_1^* \Xi_1(\gamma, \lambda)}. \quad (15)$$

Подставляя соотношение (15) в определение потенциала U_0 , получаем следующую расчетную формулу:

$$U_0 = \frac{U_1}{1 + i\omega C_1^* Z_1 \Xi_1(\gamma, \lambda)}.$$

После подстановки последнего соотношения в определение (10) потенциала U_2 , получаем возможность для записи выражения для расчета коэффициента трансформации $K(\omega, \Pi)$:

$$K(\omega, \Pi) = \frac{U_2}{U_1} = \frac{\Psi_2(\gamma, \lambda)}{1 + i\omega C_1^* Z_1 \Xi_1(\gamma, \lambda)}. \quad (16)$$

Соотношение (16) имеет смысл математической модели пьезоэлектрического трансформатора с секторным электродированием рабочей поверхности диска. Предлагаемая методика построения функции $K(\omega, \Pi)$ не предполагает решения бесконечной системы алгебраических уравнений, что, без сомнения, выгодно отличает её от схемы вычислительных процедур, которая изложена в работе [1].

Выводы. В статье предложена рациональная методика построения математической модели пьезокерамического трансформатора с секторным электродированием рабочей поверхности диска, которая не предполагает решения бесконечной системы алгебраических уравнений.

Список литературы

1. Петрищев О. Н., Базило К. В. Принципы и методы построения математических моделей дисковых пьезоэлектрических трансформаторов с секторными электродами. *Вісник Черкаського державного техно-*

логічного університету. Серія: Технічні науки. 2017. № 2. С. 33–44.

2. Петрищев О. Н., Базило К. В. Расчет электрического импеданса дискового пьезокерамического трансформатора с закороченным секторным электродом во вторичной электрической цепи. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки.* 2017. № 4. С. 47–62.
3. Шульга М. О., Карлаш В. Л. Резонансні електромеханічні коливання п'єзоелектричних пластин. Київ: Наукова думка, 2008. 270 с.
4. Петрищев О. Н. Гармонические колебания пьезокерамических элементов. Часть 1. Гармонические колебания пьезокерамических элементов в вакууме и метод резонанса – антирезонанса. Киев: Аверс, 2012. 300 с.

References

1. Petrishchev, O. N. and Bazilo, C. V. (2017) Principles and methods of mathematical models constructing of disk piezoelectric transformers with sector electrodes. *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu. Seria: Tehnichni nauky*, No. 2, pp. 33–44 [in Russian].
2. Petrishchev, O. N. and Bazilo, C. V. (2017) Calculation of electrical impedance of disk piezoceramic transformer with a shorted sector electrode in the secondary electrical circuit. *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu. Seria: Tehnichni nauky*, No. 4, pp. 47–62 [in Russian].
3. Shulha, O. M. and Karlash, V. L. (2008). Resonant electromechanical oscillations of piezoelectric plates. Kyiv: Naukova dumka, 270 p. [in Ukrainian].
4. Petrishchev, O. N. (2012). Harmonic oscillations of piezoceramic elements. Part 1. Harmonic oscillations of piezoceramic elements in vacuum and resonance-antiresonance method. Kyiv: Avers, 300 p. [in Russian].

O. N. Petrishchev¹, *Dr.Tech.Sc., professor,*
C. V. Bazilo², *Ph.D. (Eng.), associated professor*
¹National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"
Peremogy ave., 37, Kyiv, 03056, Ukraine
²Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine

CALCULATION OF TRANSFORMATION COEFFICIENT OF PIEZOCERAMIC TRANSFORMER WITH SECTOR ELECTRODES

The purpose of this article is to develop an improved technology of mathematical model constructing of disk piezoceramic transformers with cut electrodes.

The main result of this article is that a rational method for mathematical model constructing of piezoceramic transformer with sector electrodes is proposed. This does not involve solving an infinite system of algebraic equations.

Piezoelectric disks with partial covering by electrodes of one or two surfaces are often used to create various functional piezoelectronic devices. Disks with sector covering by electrodes are almost the main element of many microelectromechanical systems. Currently, there are no reliable and valid methods of constructing of mathematical models of piezoelectric transformers, which could be used as a theoretical basis for characteristics and parameters calculating of this class of functional elements of modern piezoelectronics. As a result of research of mathematical model of a real device, a set of geometrical, physical, mechanical and electrical parameters of a real object that provides implementation of technical indicators of functional element of piezoelectronics specified in technical task can be determined. This significantly reduces time and cost of the development of new functional elements of piezoelectronics. The cost of the saved resources is the commercial price of mathematical model.

Keywords: *piezoelectric transformer, physical processes, mathematical model, sector electrodes.*

Статтю представляє О. М. Петріщев, д.т.н., професор.

К. В. Базіло, к.т.н., доцент,
В. М. Зайка, к.т.н.,
Ю. Ю. Бондаренко, к.т.н., доцент,
Ю. А. Петрушко

Черкаський державний технологічний університет
б-р Шевченка, 460, Черкаси, 18006, Україна

РОЗРОБКА УЛЬТРАЗВУКОВОГО ПРИСТРОЮ ДЛЯ ІНТЕНСИФІКАЦІЇ БІОХІМІЧНИХ ПРОЦЕСІВ У ФАРМАЦЕВТИЦІ

Одним із перспективних фізичних методів впливу на речовини з метою інтенсифікації технологічних процесів є метод, що базується на використанні механічних коливань ультразвукового діапазону. Деякі процеси в біотехнології, такі як екстрагування, суспендування, фільтрування і навіть приготування сумішей, нерідко вимагають багато часу для отримання якісного продукту і можуть бути інтенсифіковані ультразвуком. Дослідження механізмів біологічної дії ультразвуку, розробка нових ультразвукових методів і обладнання принесуть відчутну користь практичній медицині, ветеринарії, біотехнології і пов'язаним з ними галузям народного господарства, переробної промисловості, а також теоретичної та експериментальної медицини.

Метою роботи є дослідження можливостей використання ультразвуку у фармацевтиці та розробка мобільного пристрою для інтенсифікації біотехнологічних процесів.

Ключові слова: ультразвук, біотехнології, інтенсифікація хімічних процесів, фармацевтика.

Вступ. Одним із перспективних фізичних методів впливу на речовини з метою інтенсифікації технологічних процесів є метод, що базується на використанні механічних коливань ультразвукового діапазону.

Найбільш успішно ультразвукові коливання використовуються в процесах, пов'язаних з рідкими станами реагентів, оскільки тільки в них виникає специфічний процес – ультразвукова кавітація, що забезпечує максимальний енергетичний вплив на різні речовини [1].

В основі всіх ультразвукових технологій лежать ефекти взаємодії ультразвуку з середовищем. Потужний ультразвук викликає в рідких середовищах ряд специфічних ефектів – кавітацію, інтенсивні мікро- і макропотоки, що приводять до швидкого і якісного перемішування компонентів середовища, утворення стійких емульсій, екстрагування розчинних компонентів з частинок, які знаходяться в рідині, набухання і руйнування цих частинок [2].

Метою роботи є дослідження можливостей використання ультразвуку у фармацевтиці та розробка мобільного пристрою для інтенсифікації біотехнологічних процесів.

Матеріали та методи. Деякі процеси в біотехнології – екстрагування, суспендування,

фільтрування і навіть приготування сумішей – нерідко вимагають багато часу для отримання якісного продукту і можуть бути інтенсифіковані ультразвуком [2].

Вплив ультразвукових коливань на різні технологічні процеси дозволяє:

- не менше ніж в 10-1000 разів прискорити процеси, що проходять між двома або кількома неоднорідними середовищами (розчинення, очищення, знежирення, знегажування, фарбування, подрібнення, просочення, емульгування, екстрагування, кристалізація, полімеризація, запобігання утворенню накипу, гомогенізація, ерозія, хімічні та електрохімічні реакції тощо);

- збільшити вихід корисних продуктів (наприклад екстрактів) і надати їм додаткових властивостей (наприклад біологічної активності та стерильності);

- отримати нові речовини (наприклад тонкодисперсні емульсії та суспензії) і реалізувати технологічні процеси, які не реалізовані традиційними методами [1].

Енергетична криза, збільшення попиту на продукцію з поліпшеними і екологічно безпечними якостями викликали необхідність розвитку нових технологій вилучення екстрактних речовин з рослинних (зокрема олійних) матеріалів, які знаходять своє застосування в

харчовій промисловості (олійно-жирова галузь, харчові добавки), косметології (екстракти масла і різні комплексні препарати), хімічної промисловості (природні барвники тощо). Особливий інтерес становлять екстрактивні речовини (масла), які є безпечними для навколишньо-

го середовища і не роблять шкідливого впливу на здоров'я людини, про що свідчать численні роботи, описані в [3].

Перспективні напрями застосування ультразвуку для інтенсифікації біотехнологічних процесів зображено на рис. 1.

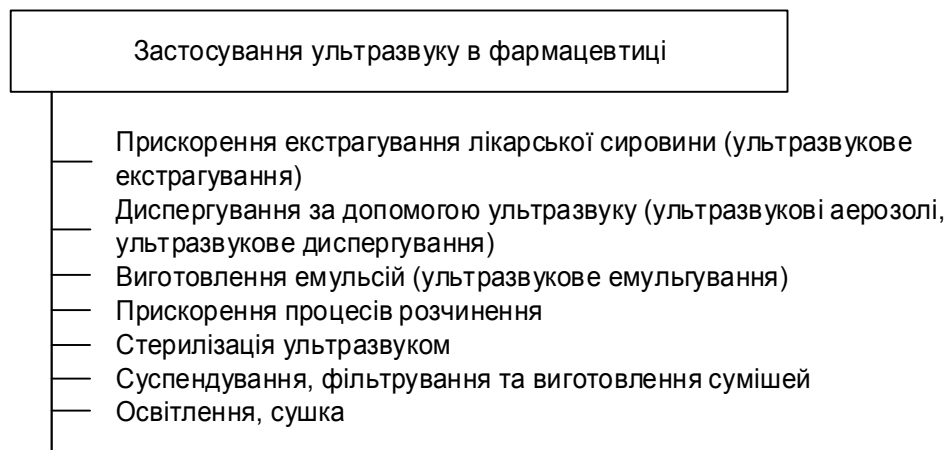


Рис. 1. Методи інтенсифікації біотехнологічних процесів за допомогою ультразвуку у фармацевтичній та хімічній промисловості

Як відомо, найбільше поширення в ультразвуковій медичній техніці отримали п'єзоелектричні перетворювачі. Дозволяючи отримувати акустичні коливання в діапазоні частот від кількох кГц до десятків і сотень МГц, вони використовуються в апаратах для ультразвукової терапії, в діагностичних приладах, що застосовуються у медицині та ветеринарії, в пристроях для ультразвукової стимуляції біотехнологічних процесів [2].

Ультразвукові пристрої – це також потужні блендери та гомогенізатори, застосування яких не обмежується лише лабораторією та промисловістю. Ультразвукові гомогенізатори – пристрої, що забезпечують подрібнення та змішування (як правило, рідких) фаз за рахунок кавітації. Ультразвукові гомогенізатори використовуються для гомогенізації сумішей рідин, а також застосовуються в ультразвукових системах зволоження повітря, генераторах диму. Ультразвукові пристрої також знайшли своє місце на кухнях для гурманів.

Молекулярна кухня радикально пориває зі старими уявленнями про кулінарію. Її метою стає досягнення ідеального смаку – чистого і вдосконаленого. Над отриманням нових комбінацій смаків і консистенцій працюють кухарі-фізики, хіміки та біохіміки. Аромати

одних страв витягають і передають іншим із застосуванням ультразвуку [4].

Подальші дослідження авторів будуть спрямовані на створення мобільних малогабаритних ультразвукових систем для інтенсифікації хімічних процесів у фармацевтиці та харчовій промисловості на основі п'єзоелектричних випромінювачів.

Експерименти та результати. На рис. 2 зображено схему генератора імпульсів, який може бути використаний при створенні ультразвукових коливань для інтенсифікації хімічних процесів у фармацевтиці, а також у такій галузі медицини, як ультразвукова хірургія [5]. При зануренні в розчин дезінфектанту ультразвукові коливання викликають інтенсивні мікропотоки рідини поблизу інструменту, очищаючи його поверхню. Крім того, збільшуючи проникність мембран клітин хвороботворних бактерій відносно дезінфікуючої речовини, ультразвук підвищує ефективність його дії, що дозволяє на порядок знизити концентрацію цієї речовини в розчині [6].

Зовнішній вигляд портативного генератора імпульсів з підвищуючим перетворювачем напруги DC-DC Step-up ($U_{\text{жив}} = 4,2 \text{ В}$, $U_{\text{DC-DC}} = 40 \text{ В}$) зображено на рис. 3. Генератор має можливість живитись і від напруги 220 В.

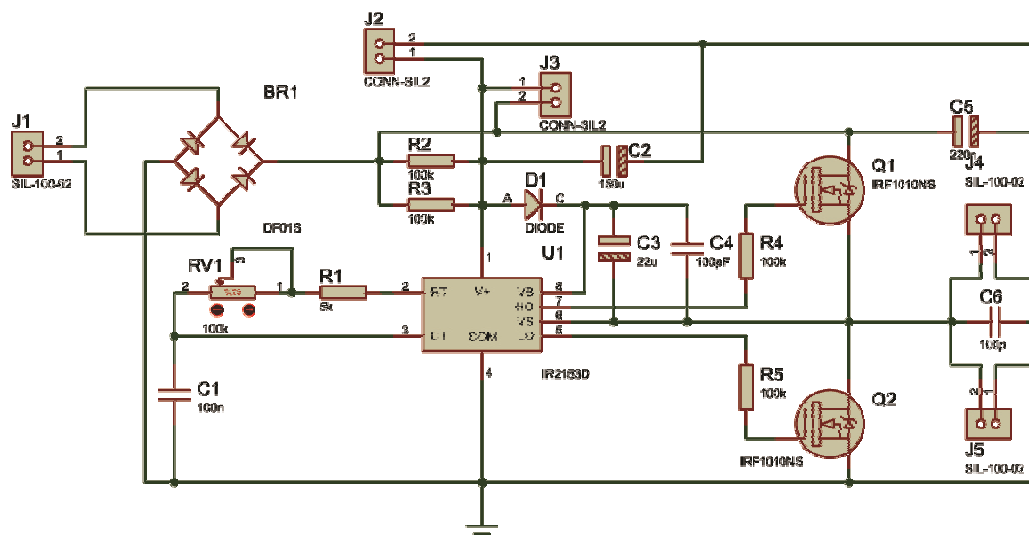


Рис. 2. Схема електрична принципова генератора імпульсів



Рис. 3. Генератор імпульсів

Розроблену конструкцію пристрою для інтенсифікації біохімічних процесів зображено на рис. 4. Запропонований пристрій матиме такі переваги, що дадуть змогу використовувати його й у різних галузях промисловості та медицини:

– мобільність та автономність, що забезпечується шляхом використання змінних Li-ion акумуляторів, які мають значний запас потужності;

– надійність та значний строк служби активних елементів, що забезпечується використанням активних елементів з високоякісної п'єзокераміки;

– зручність в експлуатації та простота в керуванні.

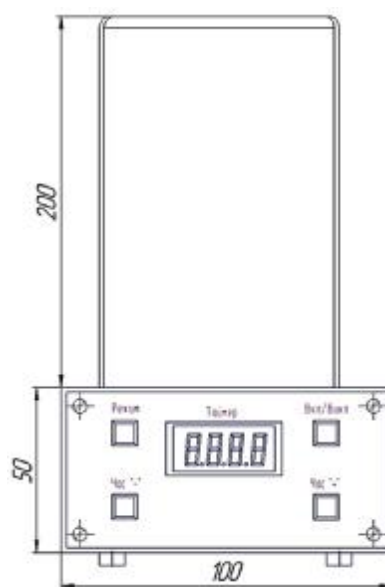


Рис. 4. Зовнішній вигляд пристрою для інтенсифікації біохімічних процесів

Висновки. Подальші дослідження механізмів біологічної дії ультразвуку, розробка нових ультразвукових методів і обладнання можуть принести відчутну користь практичній медицині, ветеринарії, біотехнології і пов'язаним з ними сферам народного господарства, переробної промисловості, а також теоретичної та експериментальної медицини.

Список літератури

1. Исследование возможности применения ультразвука в фармации. Центр ультразвуковых технологий. URL: <http://u-sonic.ru/upload/ultrasound%20in%20pharmacy.pdf>

2. Акопян Б. В., Ершов Ю. А. Основы взаимодействия ультразвука с биологическими объектами: Ультразвук в медицине, ветеринарии и экспериментальной биологии. Москва: Изд-во МГТУ им. Н.Э. Баумана, 2005. 224 с.
3. Шорсткий И. А. Совершенствование процесса экстрагирования масляных материалов на основе применения электрофизического воздействия: дис. ... канд. техн. наук: 05.18.12. Краснодар, 2016. 158 с.
4. Знакомьтесь, молекулярная кухня! URL: <http://volshebnaya-eda.ru/kulinarnyj-klass/enciklopedii/molekulyarnaya-kuxnya/>
5. Патент України на корисну модель № 116996. Спосіб створення ультразвукових коливань в хірургічному інструменті / К. В. Базіло, Ю. Ю. Бондаренко, В. М. Заїка, Ю. А. Петрушко, Л. О. Федорук; № 201613588 від 29.12.2016, опубл. 12.06.2017, Бюл. № 11.
6. Базіло К. В., Бондаренко Ю. Ю., Заїка В. М., Петрушко Ю. А., Федорук Л. О. Застосування п'єзоелектричних елементів в ультразвуковій хірургії. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*. 2016. № 4. С. 53–56.

References

1. Investigation of the possibility of ultrasound's using in pharmacy. Centre of ultrasound technologies. URL: <http://u-sonic.ru/upload/ultrasound%20in%20pharmacy.pdf>
2. Akopyan, B. V., Ershov, Yu. A. (2005). Fundamentals of ultrasound interaction with biological objects: Ultrasound in medicine, veterinary medicine and experimental biology. Moscow: Izd-vo MGTU im. N.E. Bauman, 224 p. [in Russian].
3. Shorstkij, I. A. (2016). Improvement of the process of oil materials extraction based on the application of electro-physical effect: thesis of Ph.D. Krasnodar, 158 p. [in Russian].
4. Meet molecular cuisine! URL: <http://volshebnaya-eda.ru/kulinarnyj-klass/enciklopedii/molekulyarnaya-kuxnya/>
5. Bazilo, C. V., Bondarenko, Yu. Yu., Zaika, V. M., Petrushko, Yu. A., Fedoruk, L. O. (2017). Method of formation of ultrasonic oscillations in a surgical instrument. Patent of Ukraine No. 116996 [in Ukrainian].
6. Bazilo, C. V., Bondarenko, Yu. Yu., Zaika, V. M., Petrushko, Yu. A., Fedoruk, L. O. (2016). Application of piezoelectric elements in ultrasonic surgery. *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu. Seria: Tehnichni nauky*, No. 4, pp. 53–56 [in Ukrainian].

C. V. Bazilo, Ph.D. (Eng.), associate professor,

V. M. Zaika, Ph.D. (Eng.),

Yu. Yu. Bondarenko, Ph.D. (Eng.), associate professor,

Yu. A. Petrushko

Cherkasy State Technological University

Shevchenko blvd, 460, Cherkasy, 18006, Ukraine

DEVELOPMENT OF ULTRASONIC DEVICE FOR INTENSIFICATION OF BIOCHEMICAL PROCESSES IN PHARMACEUTICS

A method based on the use of mechanical vibrations of ultrasonic range is one of promising physical methods of influence on the substances to intensify technological processes. The purpose of this paper is to investigate the possibilities of ultrasound's using to intensify biotechnological processes. Some processes in biotechnology, such as extraction, suspension, filtration and even preparation of mixtures often take a long time to produce a qualitative product and can be intensified by ultrasound. Investigation of mechanisms of ultrasound's biological effect, development of new ultrasonic methods and equipment will bring tangible benefits to practical medicine, veterinary medicine, biotechnology and related fields of national economy, processing industry, as well as theoretical and experimental medicine.

The purpose of this work is to study the possibilities of ultrasound's use in pharmaceuticals and to develop a mobile device for intensification of biotechnological processes.

Key words: ultrasound, biotechnology, intensification of chemical processes, pharmaceuticals.

Рецензенти: Палагін В. В., д.т.н., професор,

Гордієнко В. І., д.т.н., с.н.с.

УДК 681.32

А. А. Тимченко, д.т.н., професор*

Черкаський державний технологічний університет
6-р Шевченка, 460, м. Черкаси, 18006, Україна**СИСТЕМНИЙ АНАЛІЗ МАТЕМАТИЧНОЇ ЗАДАЧІ.
ЗАДАЧІ ПОБУДОВИ МОДЕЛЕЙ***«В будь-якій науці стільки істини,
скільки в ній математики»*

Еммануїл Кант

Викладено результати системного аналізу категорій: <система> → <модель>, <задача> → <розв'язок>, а також <мета> → <засіб>. Об'єктом дослідження виступають моделі лінійних статичних та динамічних систем. Розглядаються різні види постановок задач, котрі впливають із практичних застосувань. Проведений системний аналіз задач дає можливість відповідно систематизувати програмно-методичні та програмно-технічні засоби їх розв'язування на ЕОМ.

Ключові слова: елементи, зв'язки, структура, система «вхід – вихід», модель взаємодій, граф потоків сигналів, системний аналіз та підхід, задача, пряма та обернена задачі.

Вступ. Методика системного аналізу.
Розглянемо метод системного аналізу як послідовність етапів дослідження:

<ціль (вимоги)> → <задачі> → <методи (алгоритми)> → <інформаційно-методичні та програмно-технічні засоби> → <результати (оцінки)>.

Послідовність будемо розглядати як кортеж:

$$S = \langle E_{ij}, Z, T_z, A_z, 3 \rangle, \quad (1)$$

де E_{ij} – композиція цілей;

$T_z ((M_z, C_z), K_z(R_z))$ – метод розв'язання: M_z – модель задачі Z ; C_z – обмеження, R_z – результат розв'язку задачі Z ; K_z – оцінка результату; $A_z = (Q, Y, B, E_{ij}(H))$ – алгоритм розв'язання: Q – динамічна операція алгоритму, Y – його структура, B – простір даних, H – цільова множина; $3 = (M, O, I, \Pi, T)$ – відповідно види забезпечення: M – методичне, O – організаційне, I – інформаційне, Π – програмне, T – технічне [1–3].

Мета дослідження. Вимоги та оцінки.
Як мету дослідження будемо розглядати процес побудови математичних моделей при роботі широкого класу мереж (матеріальних, енергетичних та інформаційних). При подальшому дослідженні вважаємо, що вузол кожної з мереж можливо розглядати як систему:

<вхід (входи)> → <перетворення> → <вихід (виходи)>.

В задачах проектування систем мереж використовується технологічна послідовність етапів дослідження, яка будується на базі класичної технологічної послідовності [3]:

<синтез> → <аналіз> →
<прийняття рішень>.

На кожному з етапів задаються відповідно вимоги до вибору варіантів на базі критеріальних функцій (від жорстких до більш помірних), а також відбувається верифікація (контроль та оцінка) з метою досягнення виконання відповідної вимоги типу предикат:

$$\chi_c = [X_m - X_c = 0], \\ \chi_g = [X_m(t) - X_c(t) = e(t)].$$

Розглядаючи вузол мережі як статичну χ_c (або динамічну χ_g) систему, яка може бути описана відповідним співвідношенням [4]:

$$A X - B Y = 0. \quad (\dot{X} = A X + B Y). \quad (2)$$

Тоді можливими є такі постановки задач: традиційно-пряма задача, обернена задача а також задача ідентифікації параметрів.

Системний аналіз задач дослідження.
В основу викладення результатів системного аналізу задач покладено технологічне (еволюційне) визначення складної системи [4]:

$$\Sigma = (E(\omega_\alpha)_{\alpha \in \Lambda}, (Z_\tau(s))_{\substack{\tau \in \Gamma \\ s \in S}}, (f_{e\alpha\tau})_{\substack{e \in E, \alpha \in \Lambda \\ \tau \in \Gamma}}, (\chi_{\alpha\tau})_{\substack{\alpha \in \Lambda \\ \tau \in \Gamma}}, \chi, J), \quad (3)$$

де $E(\cdot)$ – множина елементів; (ω_a) – сімейство структур; $(Z_t(\cdot))$ – сімейство просторів сигналів S ; (f_{cat}) – сімейство операторів елементів системи Σ ; χ_{at}, χ – простір цілей; $J_{at}, J(\chi_{at}, \chi)$ – цільові функції.

Це є деякою мірою технологічна послідовність перетворень моделей системи залежно від *етапу обслуговування* (користуючись поняттям «теорія обслуговування»). Такого типу моделі мають інтегративні властивості відповідно до етапів системного аналізу:

<структуризація> → <алгоритмізація> →
<цілеорієнтація>,

де система (модель) відповідно *структурується, алгоритмізується і технологічно виконується* відповідно до послідовності

<структура> → <функція> →
→ <технологія>.

Прямі задачі побудови моделі формуються наступним чином (*структурний етап*).

Надано результати експериментальних вимірів (типу значень входів – виходів), отриманих як пасивними методами, так і плануванням експериментів, які проводяться при дослідженні основних законів природи (механічні, теплові, електротехнічні та інші). На перших етапах використання законів природи система розглядається як частина середовища (матеріального, енергетичного або інформаційного), яка в подальшому розглядається як можливість створення сукупності пов'язаних відповідним чином елементів. Це може бути або макет, або математична чи імітаційна моделі.

Системні дослідження моделей як на *структурному*, так і на *функціональному* рівнях представлені в роботах [5–6].

Зворотні задачі (при побудові моделей як статички, так і динаміки) розв'язуються різними групами фахівців як інженерно-прикладними, так і теоретико-математичними методами системного аналізу, який, будучи системно-технологічною (дослідницькою) дисципліною, дає змогу виявити як сукупність елементів, так і зв'язки між ними.

Ясно, що перед тим, як приймати рішення, його потрібно відповідним чином підготувати, щоб задовольнити *системні вимоги* (від повного задоволення через оптимальність до «попадання в допустиму область»). Ця технологія цілком укладається в поняття концепції «чорного ящика» (стохастичний ме-

тод), яка в подальшому наповнюється відповідно в «сірий ящик» (статистичний підхід), а також «білий ящик» (детермінована постановка), де використовується технологічне (еволюційне) визначення системи у вигляді (3).

Системна постановка задачі побудови математичної моделі статичної системи.

1а. Знайти невідоме X (вихід), знаючи Y (вхід) і матриці A та B (традиційно *пряма задача*). Формально можна записати $X = A^{-1} B Y$.

1б. Задаючи значення X як відомого, а також матриць A та B , знайти невідомий вхід Y .

Формально це запишеться (традиційна *обернена задача*): $Y = B^{-1} A X$.

2. Знайти невідомі матриці A та B при заданих входах (Y) і виходах (X) (*задача ідентифікації параметрів моделі*). Розглянемо використання системного підходу до задач створення моделей лінійних статичних систем.

Статичний елемент як система

Розглянемо статичну систему як елемент. В цьому випадку математичні елементи – це окремі рівняння системи алгебраїчних рівнянь.

У математичному вигляді це система двох алгебраїчних рівнянь поелементного (x) та системного (z) виходів: $ax = by$, $z = cx$.

В подальшому для *візуалізації* математичної залежності використовуються *графи потоків сигналів*. Математична модель елемента впливає із закону про вузол мережі, де $ax - by = 0$, тобто алгебраїчна сума вузла дорівнює нулю.

Структурний етап

Задача 1а. Будемо вважати, що задана досліджувана система має один вхід y й один вихід x і складається з одного елемента з параметрами a і b , а $c = 1$.

Потрібно знайти вихід x системи, використовуючи цю залежність, тобто розв'язуючи при цьому алгебраїчне рівняння: $x = a^{-1}by$, причому на графі необхідно перенести сумарний вузол з входу елементів на його виходи, тобто перенести вершину суми з початку графу до його кінця.

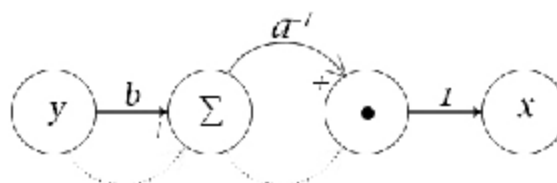


Рис. 1. Граф Мейсона статичного елемента

Задача 1б. Інколи виникає потреба пошуку невідомого входу y при заданому виході x , тоді $y = b^{-1}ax$.

Продовжуючи структурні дослідження, можемо стверджувати, що формальні залежності є параметризованою моделлю деякої фізичної системи, причому, змінюючи значення коефіцієнтів параметра, можемо отримати додаткові структурні варіанти: наприклад, як використання з'єднання не тільки прямих зв'язків (паралельне з'єднання), а й зворотних (рис. 2).

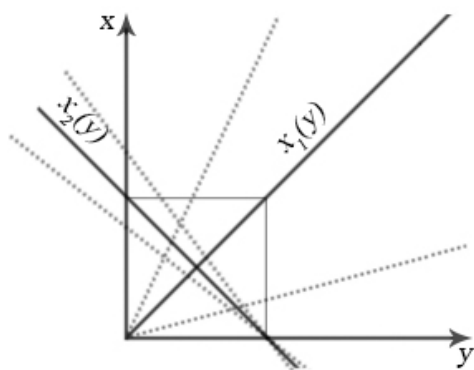


Рис. 2. Статичні характеристики

В свою чергу, можна було б вважати, що коефіцієнт перетворення a є комплексним значенням циклу (a, l) на попередньому етапі дослідження системи: $a = a(1 \mp l a)^{-1}$. (4)

Параметричний етап

Відомі три підходи до дослідження: детермінований, статистичний і ймовірнісний (стохастичний). Можлива також послідовність від повної невизначеності до повної визначеності, і навпаки.

Задача 2. Потрібно знайти невідомі значення параметрів a і b залежності (2) для подальшого уточнення моделі, одержуючи при цьому конкретну залежність, що відповідає статичній характеристиці реальної фізичної системи (рис. 2.) Маючи два невідомі параметри a та b , як мінімум, потрібно скласти систему двох алгебраїчних рівнянь відносно цих параметрів:

$$x_1 a = y_1 b, \quad x_2 a = y_2 b. \quad (5)$$

Ясно, що при цьому необхідні дані про закони зміни змінних x та y , які дослідник отримує в результаті фізичних експериментів (пасивних або активних). Ці дослідження практично не відрізняються від традиційного дослідження функцій однієї змінної. Тому,

зазвичай отримується змінна $x = f^{-1}(y)$ та її обернена $y = f^{-}(x)$. Використовуючи значення цих спостережень, вимірних даних, визначаємо при цьому невідомі параметри a та b [7–8].

Постановка задачі ідентифікації

Розглядається об'єкт, що має одну вихідну змінну x_i та декілька вхідних змінних y_j , представлених вектором $y = (y_1, y_2, \dots, y_m)$. Відомі дані спостережень про значення вихідної та вхідних змінних подано в табл. 1.

Таблиця 1

Дані спостережень

Змінні	Спостереження		
	1		n
Вхідна змінна y_1	y_{11}	...	y_{n1}
Вхідна змінна y_2	y_{12}	...	y_{n2}
Вихідна змінна x_1	x_1	...	x_n
Вихідна змінна x_2	Використання режиму 2		

Задача ідентифікації (апроксимації) полягає у знаходженні функціональної залежності заданого виду, що найліпше відповідає даним спостережень з точки зору критерію методу найменших квадратів [5].

Нехай x_i – спостережувані значення вихідної змінної, $x_i^f = f(y_i)$ – розраховані за даною функціональною залежністю $f(y_i)$, знаючи значення вихідної змінної. Ідея критерію методу найменших квадратів полягає в тому, що розбіжність між спостережуваними і розрахованими значеннями вихідної змінної повинна бути мінімальною. Якщо розбіжність вимірювати сумою різниць $e = (x_i - x_i^f)$, то може статися так, що навіть при великих значеннях загальна розбіжність є досить незначною. Тоді розбіжність вимірюють сумою квадратів різниць $\varepsilon = \sum_i (x_i - x)^2$ [7–8].

Статична система як матричний елемент

Розглянемо модель фізичної системи, яка має два входи і два виходи та два елементи і зв'язки – прямі й зворотно-перехресні, що існують між елементами, на прикладі двох рівнянь (рис. 3):

$$\begin{aligned} x_1 &= a_{11}^{-1} ((b_{11} + b_{12}y_2) - a_{12}x_2), \\ x_2 &= a_{22}^{-1} ((b_{21}y_1 + b_{22}y_2) - a_{21}x_1). \end{aligned} \quad (6)$$

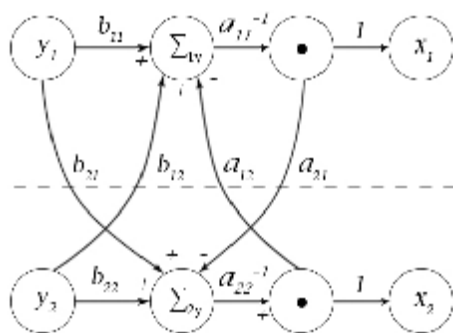


Рис. 3. Граф Мейсона моделі двоканальної системи

Розглянемо розв'язок двох рівнянь, де між елементами існують тільки прямі зв'язки:

$$\begin{aligned} x_1 &= A_{11}^{-1} (a_{22} b_{11} y_1 - a_{12} b_{11} y_2), \\ x_2 &= A_{22}^{-1} (a_{22} b_{11} y_1 - a_{12} b_{11} y_2), \\ A_{11} &= A_{22} = (a_{11} a_{22} - a_{12} a_{21}). \end{aligned} \quad (7)$$

Розв'язана система двох рівнянь (автономна) зображена на рис. 4.

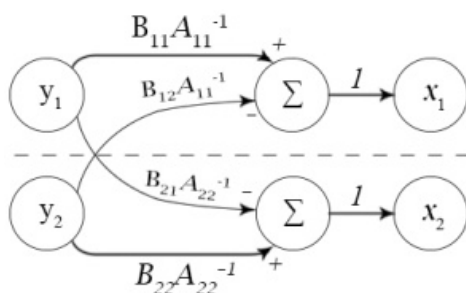


Рис. 4. Граф-схема двох незалежних рівнянь

Системна постановка задачі побудови математичної моделі динамічної системи

Математичні динамічні елементи на першому етапі – елементарні, (наприклад лінійні диференціальні залежності), а в загальному випадку – функціональні залежності типу коефіцієнтів впливу одного елемента на інший. Ясно, що перед тим, як приймати рішення, його потрібно відповідним чином підготувати, щоб задовольнити системні вимоги: від повної відповідності через оптимальність до «попадання в допустиму область».

Системні дослідження лінійної динамічної системи як на структурному, так і на функціональному рівнях представлені в роботах [9–10], де розглядається матричне рівняння

$$\dot{X}(t) = AX(t) + BY(t), \quad (8)$$

яке є подальшим розвитком рівняння (2) і в операторному записі має вигляд

$$(p - A) X = B Y, \quad P = \frac{d}{dt} \quad (9)$$

за рахунок використання похідної вектора виходу $X(t)$. При цьому можливі наступні постановки задач.

Структурний етап (задача структурної ідентифікації):

Задача 1а. Знайти невідоме $X(t)$ (вихід), знаючи вхід $Y(t)$, матриці A , B та $\dot{X}(t)$.

Формально можна записати $X(t) = A^{-1} B Y(t)$.

Задача 1б. Задаючи значення $X(t)$ як відомого, а також матриці A , B та $\dot{X}(t)$, знайти невідомий вхід $Y(t)$.

Формально це запишеться $Y(t) = B^{-1} A X(t)$ (традиційна обернена задача).

Параметричний етап. (задача параметричної ідентифікації)

2. Знайти невідомі матриці A та B при заданих входах $X(t)$, $\dot{X}(t)$ та виходах $Y(t)$.

Системний підхід до аналізу задач та створення динамічних систем

Розглянемо динамічну систему як динамічний елемент.

В математичному вигляді це система двох рівнянь: елементного ($\dot{x}(t)$) та системного ($z(t)$) виходів:

$$px(t) = a x(t) + b y(t), \quad z = cx(t). \quad (10)$$

В подальшому для візуалізації математичної залежності використовуються графи потоків сигналів. Вираз (10) впливає із закону про вузол: $px(t) - a x(t) - b y(t) = 0$, $p = \frac{d}{dt}$.

Задача 1а. (структурний етап). Будемо вважати, що задана досліджувана фізична система має один вхід $y(t)$ і один вихід $x(t)$, і складається з одного динамічного елемента з параметрами a і b , причому $c = 1$.

Потрібно знайти вихід системи, використовуючи цю залежність (10), тобто розв'язуючи при цьому це алгебраїчне рівняння. Граф Мейсона моделі зображено на рис. 5.

$$x(t) = p^{-1}(by(t) - ax(t)), \quad p^{-1} = \int_0^1 dt.$$

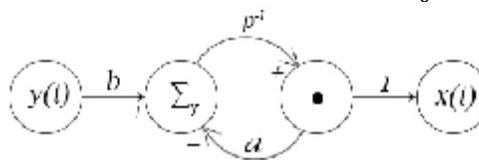


Рис. 5. Граф Мейсона моделі динамічного елемента

Задача 1б. Інколи виникає потреба пошуку невідомого входу y при заданому виході x , його похідній $\dot{x}$. Тоді $y(t) = b^{-1}(p - a)x$.

Продовжуючи структурні дослідження, можемо стверджувати, що наведені вище формальні залежності є параметризованою мо-

деллю фізичної системи, причому, змінюючи значення коефіцієнтів параметрів, можемо отримати додаткові структурні варіанти: наприклад, як з'єднання не тільки прямих зв'язків (паралельне з'єднання, послідовне з'єднання, а також зворотно-паралельне).

Задача 2 (параметричний етап). Для подальшого дослідження потрібно знайти невідомі значення параметрів матриць A і B залежності (9), одержуючи при цьому конкретний розв'язок, що відповідає динамічним характеристикам реальної фізичної системи. Ясно, що при цьому необхідні дані про закони зміни змінних $x(t)$ та $y(t)$, які дослідник отримує в результаті *фізичних* експериментів (пасивних або активних) (табл. 2).

Таблиця 2

Дані спостережень

Змінні	Спостереження		
	t_1	...	t_n
Вхідна змінна $y_1(t)$	y_{11}	...	y_{n1}
Вхідна змінна $y_2(t)$	y_{12}	...	y_{n2}
Вихідна змінна $x_1(t)$	x_{11}	...	x_{1n}
Вихідна змінна $x_2(t)$	x_{21}	...	x_{2n}
Похідна змінна $\dot{x}_1(t)$	$\dot{x}_{11}$	...	$\dot{x}_{1n}$
Похідна змінна $\dot{x}_2(t)$	$\dot{x}_{21}$	...	$\dot{x}_{2n}$

Використовуючи параметризовану модель, отримаємо розв'язок диференційного рівняння першого порядку (рис. 6).

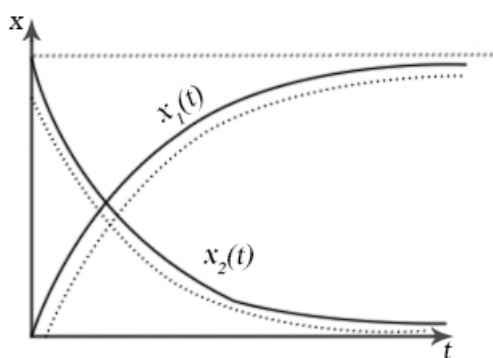


Рис. 6. Графіки переходних процесів

Динамічна система як матричний елемент. Розглянемо приклад двох рівнянь – фізична система має два входи і два виходи та два елементи і зв'язки між елементами, включаючи не тільки прямі, а й зворотно-перехресні (рис. 6, 7).

Ці дослідження практично не відрізняються від традиційного дослідження функцій однієї змінної. Використовуючи вимірні значення та підставляючи їх у рівняння даних, ми вважаємо, що $x(t) \equiv x_i(t)$, а $y(t) \equiv y_i(t)$.

Задачі 1а та 1б формулюються таким чином: шукається структура моделі динамічної системи у вигляді матричного рівняння, де матриці A та B відповідно задані.

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}, \quad (11)$$

де $x(t) = (x_1(t), x_2(t))$ – вектор виходів, $y(t) = (y_1(t), y_2(t))$ – вектор входів, $\dot{x}(t) = (\dot{x}_1(t), \dot{x}_2(t))$ – вектор похідних.

Система операторних рівнянь має вигляд графа Мейсона та зображена на рис. 7.

$$x_1(t) = p^{-1}(b_{11}y_1 + b_{12}y_2 - a_{11}x_1 - a_{12}x_2)$$

$$x_2(t) = p^{-1}(b_{21}y_1 + b_{22}y_2 - a_{21}x_1 - a_{22}x_2)$$

$$p = \frac{d}{dt}, \quad p^{-1} = \int_0^1 dt.$$

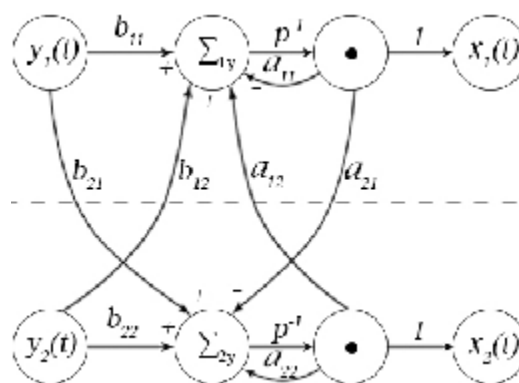


Рис. 7. Граф-схема системи двох диференціальних рівнянь

Розглянемо задачу *автономності* каналів відповідно до системи наведених вище операторних рівнянь, розв'язуючи їх відносно виходів $x_1(t)$ та $x_2(t)$. Тоді в матричному вигляді можливо записати

$$A(p) X = B(p) Y, \quad (12)$$

$$A(p) = \begin{pmatrix} (a_{11} + p) & a_{12} \\ a_{21} & (a_{22} + p) \end{pmatrix},$$

$$B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}, X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}.$$

Табличні значення похідних $\dot{x}_1(t)$, $\dot{x}_2(t)$ можливо знайти із апроксимованих таблиць $\dot{x}_1(t)$, $\dot{x}_2(t)$, використовуючи програму IDENT [7], як у попередньому прикладі. Підготувавши необхідні дані для програми IDINS

в режимі $x(t)/y(t)$, вводячи значення вхідних та вихідних змінних відповідно до таблиць даних в момент часу t_i , знаходимо матриці A та B . Результати дослідження фізичної системи задані табл. 2. Для перевірки використовується програмне середовище [8].

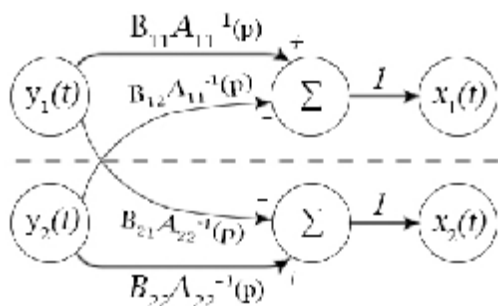


Рис. 8. Граф-схема системи двох елементів та входів і виходів

$$\begin{aligned} x_1(t) &= A_{11}^{-1}(p)(B_{11}y_1 + B_{12}y_2), \\ x_2(t) &= A_{22}^{-1}(p)(B_{21}y_1 + B_{22}y_2), \\ A_{11}(p) &= A_{22}(p). \end{aligned} \quad (13)$$

Підводячи підсумок плану системного дослідження, можна зробити висновок, що використаний системний підхід до аналізу моделей у вигляді такої послідовності етапів:

<цілі>→<задачі>→<алгоритми>→
<програми>→<програмно-методичний комплекс ФАКТОР>→<та програмно-технічний комплекс у вигляді ЕОМ>

При цьому використана категорія:
<об'єкт дослідження>→<процес дослідження>.

Системний аналіз ефективності процесів та якості результатів

Будемо вважати системним дослідженням процес отримання моделі цілеспрямованої системи у базисі системних властивостей системних ресурсів та структурах життєвих циклів, реалізацію якого можна описати відображенням [9–10]

$$F_d: \langle S_v, S_r, S_c \rangle \rightarrow R_z, \quad (14)$$

де S_v – системні властивості, S_r – системні ресурси, S_c – структура життєвого циклу системи, R_z – результуючий варіант.

З позиції системного підходу F_d визначають як багаторівневі та багатовимірні перетворення вихідних даних, результуючими категоріями є аспекти будови (архітектурні та структурні характеристики), оптимальні параметри процесів та відповідні оцінки в категоріях ефективності та якості. Будемо вважа-

ти, що основна мета цього дослідження, пов'язаного з побудовою адекватних моделей як статичних, так і динамічних систем, досягнута з використанням методу системного аналізу та підходу (табл. 3).

Таблиця 3

Логічна схема дослідження

Рівні	Етапи		
	Структуризація	Алгоритмізація	Цілеорієнтація
Будова	$AX=BY$	$\dot{X}(t)=AX(t)+BY(t)$	$\chi_b = [X_m - X_c = 0]$
Функція	A, B	$A(p), B(p)$	$\chi_f = [X_m(t) - X_c(t) = 0]$
Оцінка	$E = (X_m - X_c)$ $E \rightarrow \text{ont}$ ($E=0$)	$E(t) = (X_m(t) - X_c(t))$ $E(t)=0$	$J=J(\chi_b, \chi_f)$ $J \rightarrow \text{ont}$

Основні висновки. Таким чином, можливо підвести підсумок проведеному аналізу двох класів лінійних систем: *статичних та динамічних*. На базі закону про вузол на графі потоків-сигналів формуються закони про статичну або про динамічну *рівновагу*. Це відповідає двом першим законам Ньютона. На базі цих законів формуються постановки відповідно таких типів задач: знайти невідомі виходи або входи (структурний етап), а також вирази для перетворення елементів (параметричний етап).

При цьому використовується деяка *сукупність математичних підзадач*, які пов'язані з розв'язанням алгебраїчних або диференціальних рівнянь. На прикладах моделей систем з двома входами та виходами розглядається система двох алгебраїчних або диференціальних рівнянь.

Викладення матеріалу супроводжується представленням у вигляді графів потоків-сигналів Мейсона, що дає можливість візуалізувати всі процеси побудови математичних моделей як структурної, так і параметричної ідентифікації. В подальшому бажано розглянути питання використання математичних моделей при проектуванні складних систем.

Список літератури

References

1. Тимченко А. А. Системний аналіз процесів і моделей взаємозв'язків та взаємодій. Лінійні статичні системи. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*. 2017. № 1. С. 111–117.
2. Тимченко А. А. Системний аналіз процесів і моделей взаємозв'язків та взаємодій. Лінійні динамічні системи. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*. 2017. № 3. С. 127–128.
3. Тимченко А. А. Системні дослідження в науці та техніці. Частина V. Математичне моделювання. Системний підхід. Системний аналіз моделей та методів їх побудови. Черкаси: ЧДТУ, 2012. 55 с. (Бібліотечка Вісника Черкаського державного технологічного університету.)
4. Тимченко А. А. Эволюционное определение сложной системы. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*. 2010. № 1. С. 105–110.
5. Гетманцев В. Д. Лінійна алгебра і лінійне програмування: навч. посіб. Київ: Либідь, 2011. 256 с.
6. Гантеев А. В., Якимова А. С., Босов А. В. Обыкновенные дифференциальные уравнения в примерах и задачах: учеб. пособие. Москва: Изд-во МАИ, 2010. 380 с.
7. Комплекс программ факторизации, идентификации и прогнозирования характеристик сложных систем «ФАКТОР». Киев: ИК им. В. М. Глушкова АН УССР, 2015. 2 с.
8. Дьяконов В. Г. Mathematica 5.1; 5.2; 6.0. Программирование и математические вычисления. ДМК Пресс, 2010. 576 с.
9. Тимченко А. А. Системні дослідження в науці та техніці. Частина II. Технологія наукових досліджень. Черкаси: ЧДТУ, 2016. 68 с.
10. Тимченко А. А. Системний підхід до наукового дослідження (етапи розвитку науково-технічної задачі). Частина III. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*. 2015. № 4. С. 145–151.
1. Tymchenko, A. A. (2017) System analysis of processes and models of interconnections and interactions. Linear static systems. *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu. Seria: Tehnichni nauky*, № 1, pp. 111–117 [in Ukrainian].
2. Tymchenko, A. A. (2017) System analysis of processes and models of interconnections and interactions. Linear dynamic systems. *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu. Seria: Tehnichni nauky*, № 3, pp. 127–128 [in Ukrainian].
3. Tymchenko, A. A. (2012) System research in science and technology. Part V. Mathematical modeling. System approach. System analysis of models and methods of their construction. Cherkasy: ChDTU, 55 p (*Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu. Seria: Tehnichni nauky*) [in Ukrainian].
4. Tymchenko, A. A. (2010) Evolutionary definition of a complex system. *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu. Seria: Tehnichni nauky*, № 1, pp. 105–110 [in Russian].
5. Hetmantsev, V. D. (2011) Linear algebra and linear programming. Kyiv: Lybid, 256 p. [in Ukrainian].
6. Ganteev, A. V, Yakymova, A. S, Bosov, A.V. (2010) Ordinary differential equations in examples and tasks. Moscow: Publishing house MAI, 380 p. [in Russian].
7. A complex of programs of factorization, identification and forecasting of characteristics of complex systems "FACTOR" (2015). Kyiv: IK im. V. M. Glushkova AN USSR, 2 p. [in Russian].
8. Dyakonov, V. G. (2010) Mathematica 5.1; 5.2; 6.0. Programming and mathematical calculations. DMK Press, 576 p. [in Russian].
9. Tymchenko, A. A. (2016) System research in science and technology. Part II. Technology of scientific research. Cherkasy: ChDTU, 68 p. [in Ukrainian].
10. Tymchenko, A. A. (2015) System approach to scientific research (stages of development of scientific and technical task). Part III. *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu. Seria: Tehnichni nauky*, № 4, pp. 145–151 [in Ukrainian].

A. A. Tymchenko, Dr.Tech.Sc., professor*
Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine

SYSTEM ANALYSIS OF MATHEMATICAL TASK. MODELING TASKS

The results of system analysis of the categories: $\langle \text{system} \rangle \rightarrow \langle \text{model} \rangle$, $\langle \text{task} \rangle \rightarrow \langle \text{solution} \rangle$, and also $\langle \text{aim} \rangle \rightarrow \langle \text{means} \rangle$ are stated. The models of linear static and dynamic systems act as an object of research. Various kinds of problem definitions which arise out of practical applications are considered. Conducted system analysis of tasks allows to systematize program-methodological and program-technical means of their solution on computer at wider application.

The technology and research system as networks of connected elements, where network communication is determined as a structure, are considered.

Key words: *elements, relations, structure, “input – output” system, interaction model, graph of signal flows, system analysis and approach, task, direct and indirect tasks.*

**У підготовці статті до друку взяли участь к.т.н., доцент Андрієнко В. О., магістри: Чабан Ю. В., Теслюк Д. В.*

Статтю представляє А. А. Тимченко, д.т.н., професор.

В. Н. Рудницький, д.т.н., профессор,
e-mail: rvn_2008@ukr.net

В. Г. Деткин, к.т.н., доцент,
e-mail: ded@nensi.net

Н. В. Хрулев, к.т.н., доцент,
e-mail: hrulev@ukr.net

Г. В. Кривоус, заведующий лабораториями
e-mail: krivous_gv@gmail.com

Черкасский государственный технологический университет,
б-р Шевченко, 460, Черкасы, 18006, Украина

ФУНКЦИИ И СТРУКТУРА СИСТЕМЫ КОМПЛЕКСНОГО КОНТРОЛЯ ВЫЧИСЛИТЕЛЬНЫХ ПРОЦЕССОВ

Рассмотрены вопросы синтеза структуры системы комплексного контроля вычислительных процессов. Определены условия исправного состояния вычислительного процесса. Для интеллектуализации контроля вычислительного процесса предлагается использовать нейронную сеть с ансамблевой организацией, что позволит не только обнаружить сбой правильного выполнения вычислительного процесса, но и определить причины и место сбоя, выполнить анализ причин, вызвавших сбой, спрогнозировать поведение вычислительного процесса во времени. Синтез структуры системы предлагается выполнить на основе функционально-структурного подхода, предложенного в работах Е. П. Балашова. В результате декомпозиции целевой функции формируется дерево функций, которое определяет основные показатели системы комплексного контроля вычислительных процессов, такие как производительность, надежность, функциональность, и оказывает первоочередное влияние на структуру. Приведены результаты синтеза структуры системы комплексного контроля вычислительных процессов на основе предложенного дерева функций.

Ключевые слова: вычислительный процесс, контроль, дерево функций, функционально-структурный подход, структура, нейронная сеть.

Постановка проблемы. С расширением сферы применения компьютеров возрастает цена сбоев в их работе, особенно в областях, связанных с потенциальной угрозой техногенных катастроф, промышленном производстве, банковской сфере.

Известны методы и средства диагностирования и отладки цифровых и микропроцессорных систем [1–5], позволяющие обнаруживать неисправности как аппаратного, так и программного обеспечения.

С другой стороны, на структурные, схемотехнические и программные решения систем комплексного контроля выполнения вычислительного процесса существенное влияние оказывают уровень развития микроэлектроники, информационных технологий, нейросетевые технологии [6–10].

Применение нейросетевых технологий в системах комплексного контроля вычислительных процессов позволит интеллектуализировать контроль и диагностику вычисли-

тельных процессов, получить новые, ранее не доступные свойства системы [7–10].

Таким образом, проблема создания систем комплексного контроля вычислительных процессов, соответствующих современным требованиям, актуальна и представляет определенный научный и практический интерес.

Анализ последних исследований и публикаций. Проблемы, направления и перспективы развития микроэлектроники рассмотрены в [6]. Принципы построения автоматизированных систем технического обслуживания сложных объектов радиоэлектронной техники исследованы в [1]. Конструкционные и функциональные аспекты некоторых систем диагностирования электронных модулей описаны в [2, 3]. Методы и средства диагностирования и отладки цифровых и микропроцессорных систем приведены в [4, 5]. Нейронные сети с ансамблевой организацией рассмотрены в [7, 8]. Функции и структура нейросетевого модуля для использования в

системах ЧПУ описаны в [10]. Теоретические вопросы отладки, контроля и диагностирования, а также технические средства отладки, контроля и диагностирования рассмотрены в [11–13]. Методология синтеза систем на основе функционально-структурного подхода рассмотрена в [14].

Цель статьи. Целью данной статьи является синтез, на основе функционально-структурного подхода [14], структуры системы комплексного контроля вычислительных процессов, что позволит выполнить разработку схемотехнических и программных решений разрабатываемой системы.

Изложение основного материала. Ход выполнения вычислительного процесса отображается на системной шине. Представим его в следующем виде:

$$P = \langle A, D, C, T \rangle,$$

где P – вычислительный процесс;

A – множество состояний шины адреса;

D – множество состояний шины данных;

C – множество состояний шины управления;

T – множество значений времени выполнения операций вычислительного процесса.

Совокупность значений A , D , C и T представляет собой некоторое событие $EV = f(A, D, C, T)$. Вычислительный процесс отображается на системной шине в виде последовательности таких событий – трассы вычислительного процесса.

Наблюдая за трассой, можно обнаружить нарушение исправного выполнения вычислительного процесса.

Для контроля исправного выполнения вычислительного процесса определим допустимые значения события $EV = f(A, D, C, T)$. Тогда, в случае выхода одного или нескольких параметров за пределы допустимых значений, можно сделать вывод о нарушении исправного выполнения вычислительного процесса.

Событие $EV = f(A, D, C, T)$ можно рассматривать как состоящее из элементарных событий:

$$EV = EV_A + EV_D + EV_C;$$

где $EV_A = f(A, T)$ – событие шины адреса;

$EV_D = f(D, T)$ – событие шины данных;

$EV_C = f(C, T)$ – событие шины управления.

Исправное состояние вычислительного процесса характеризуется допустимыми значениями элементарных событий $EV_A = f(A)$,

$EV_D = f(D)$, $EV_C = f(C)$ и, соответственно, обобщающего события $EV = f(A, D, C, T)$.

Из вышесказанного следует, что правильный вычислительный процесс характеризуется некоторым множеством допустимых состояний шины адреса $A_{доп}$, которое определяется расположением кода исполняемой программы и данных в памяти компьютера, некоторым множеством допустимых состояний шины данных $D_{доп}$, некоторым множеством допустимых состояний шины управления $C_{доп}$.

Для определения соответствия $EV = f(A, D, C, T)$ допустимым $A_{доп}$, $D_{доп}$ и $C_{доп}$ в определенные моменты времени T можно применить известные решения [3, 5, 11–13], которые обеспечат быстрое действие, необходимое для наблюдения процессов на системной шине.

Для интеллектуализации контроля исправного выполнения вычислительного процесса предлагается использовать нейронную сеть с ансамблевой организацией [7, 8].

Использование нейронной сети позволит не только обнаружить сбой вычислительного процесса, но и определить причины и место сбоя, выполнить анализ причин, вызвавших сбой, спрогнозировать поведение вычислительного процесса во времени.

В соответствии с функционально-структурным подходом [9] структурная организация системы комплексного контроля вычислительных процессов должна соответствовать ее функциональному назначению и условиям эксплуатации.

Представим систему комплексного контроля вычислительных процессов в виде математического описания:

$$S_{ics}(F_0) = \langle M_1(F_1), \dots, M_i(F_i) \rangle, \quad (1)$$

где S_{ics} – разрабатываемая система комплексного контроля (integrated control system) вычислительных процессов;

$M_1(F_1)$ – первый модуль системы, реализующий набор функций F_1 ;

$M_i(F_i)$ – i -й модуль системы, реализующий набор функций F_i .

Каждый модуль, в свою очередь, может быть представлен в виде математического описания, аналогичного (1), в соответствии с заданным деревом функций.

В соответствии с методологией функционально-структурного подхода [9] и на ос-

нове анализа технических материалов [1–5,7,13] сформируем дерево функций системы.

Функции 1-го уровня определяют основные показатели системы комплексного контроля вычислительных процессов, такие как производительность, надежность, функциональность, и оказывают первоочередное влияние на структуру системы комплексного контроля вычислительных процессов.

Дополнительные функции 2-го уровня расширяют функциональность системы. В данной статье ограничимся рассмотрением дерева функций 1-го уровня, поскольку они в первую очередь определяют структуру разрабатываемой системы.

Уровень 0. Целевая функция

F_0 – функционирование системы комплексного контроля вычислительных процессов с целью определения состояния вычислительного процесса и получения информации о сбое вычислительного процесса, а также выполнения прочих вспомогательных функций.

Функции уровня 1

Сформулируем функции уровня 1 системы диагностирования электронных модулей.

F_1 – функция сопряжения системы комплексного контроля с системной шиной объекта диагностирования.

F_2 – функция управления структурными модулями.

F_3 – функция информационного обмена с управляющим компьютером.

F_4 – функция цифровой обработки диагностической информации.

F_5 – функция интеллектуальной обработки диагностической информации.

F_7 – функция обнаружения и анализа сбоев вычислительного процесса.

Для реализации предложенного дерева функций система комплексного контроля вычислительных процессов должна состоять из следующих модулей (рис. 1):

M_1 – модуль сопряжения системы комплексного контроля с системной шиной объекта диагностирования;

M_2 – модуль управления;

M_3 – модуль обмена информацией с управляющим компьютером;

M_4 – модуль цифровой обработки диагностической информации;

M_5 – нейросетевой модуль интеллектуальной обработки диагностической информации;

M_6 – нейросетевой модуль обнаружения и анализа сбоев вычислительного процесса.

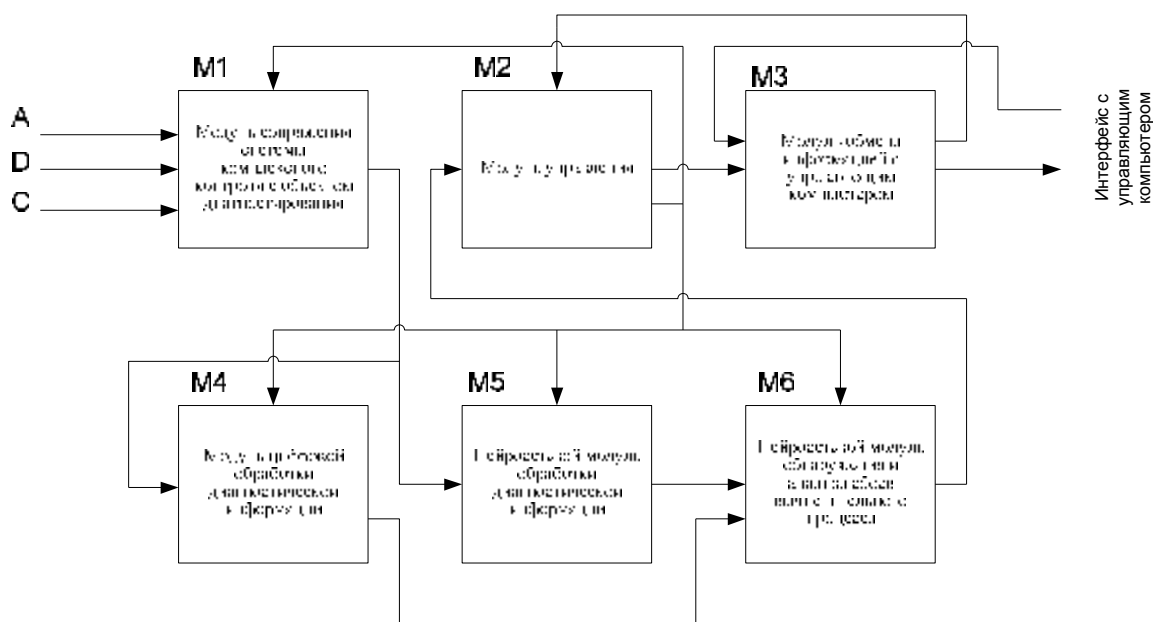


Рис. 1. Структура системы комплексного контроля выполнения вычислительных процессов

Выводы. Определены условия, определяющие исправное состояние вычислительного процесса.

Для интеллектуализации контроля вычислительного процесса предложено использовать нейронную сеть с ансамблевой организацией, что позволит не только обнаружить сбой правильного выполнения вычислительного процесса, но и определить причины и место сбоя, выполнить анализ причин, вызвавших сбой, спрогнозировать поведение вычислительного процесса во времени.

Сформировано дерево функций, на основе которого выполнен синтез структуры системы комплексного контроля вычислительного процесса, что позволит выполнить разработку схмотехнических и программных решений системы комплексного контроля выполнения вычислительных процессов.

Список литературы

1. Ленков С. В., Пашков С. А., Цыцарев В. Н., Березовская Ю. В. Автоматизированная система технического обслуживания сложного объекта радиоэлектронной техники: принципы построения. *Системи озброєння і військова техніка*: наук. журн. Харківський університет Повітряних Сил імені Івана Кожедуба. 2015. № 1 (41). С. 124–131.
2. Вакаренко А. В., Наконечний В. С., Голуб В. А., Матішєн Р. В. Конструкційні та функціональні аспекти вітчизняної апаратури для діагностування і ремонту електронних модулів зенітних ракетних комплексів. *Системи озброєння і військова техніка*: наук. журн. Харківський університет Повітряних Сил імені Івана Кожедуба. 2010. № 1 (21). С. 44–47.
3. Рудаков К. С., Деткин В. Г., Хрулёв Н. В., Титоренко И. С. Функции и структура специализированного диагностического процессора. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*. 2009. № 3. С. 8–11.
4. Деткин В. Г., Хрулёв Н. В. Методы комплексного контроля вычислительных процессов. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*. 2006. № 1. С. 76–79.
5. Уильямс Г. Б. Отладка микропроцессорных систем. Москва: Энергоатомиздат, 1988. 253 с.
6. Коваленко А. А., Петропавловский М. Д. Основы микроэлектроники: учеб. пособие для студ. высш. учеб. заведений. Москва: Изд. центр «Академия», 2006. 240 с.
7. Гольцев А. Д. Нейронные сети с ансамблевой организацией. Киев: Наукова думка, 2005. 200 с.
8. Куссуль Э. М. Ассоциативные нейродобные структуры АН Украины. Ин-т кибернетики. Киев: Наукова думка, 1992. 140 с.
9. Vega A., Baidyk T., Kussul E., Pérez Silva J. L. Digital implementation of LIRA Neural Classifier. *Proceedings of the 1st international congress on instrumentation and applied sciences*, October 2010. URL: <http://somi.ccadet.unam.mx/icias2010/memorias/31>
10. Рудницький В. Н., Хрулёв Н. В., Бабенко В. Г. Функции и структура нейросетевого модуля системы ЧПУ. *Системи обробки інформації*: зб. наук. праць Харківського університету Повітряних Сил. Харків, 2012. Вип. 2 (100). С. 96–100.
11. Strunz Bob. Design for testability in digital integrated circuits. Bob Strunz, Colin Flanagan, Tim Hall University of Limerick, Ireland. URL: http://www.cs.colostate.edu/~cs530/digital_testing.pdf
12. Зинченко Ю. Е. Методы и средства встроенного тестового диагностирования специализированных устройств сетей передачи данных реального времени: диссертация. Киев: ИПМЭ, 1989. 208 с.
13. Иванов Ю. П., Никитин В. Г., Чернов В. Ю. Контроль и диагностика измерительно-вычислительных комплексов: учеб. пособ. Санкт-Петербург, 2004. 98 с.
14. Балашов Е. П. Эволюционный синтез систем. Москва: Радио и связь, 1985. 328 с.

References

1. Lenkov, S. V., Pashkov, S. A., Tsyt-sarev, V. N., Berezovskaya, Yu. V. (2015) Automated system of servicing maintenance of a complex object of radioelectronic engineering: principles of construction. *Systemy ozbroiennia i viiskova tekhnika*: nauk. zhurn. Kharkiv: Kharkivskiy universytet Povitrianykh Syl imeni Ivana Kozheduba, No. 1 (41), pp. 124–131 [in Russian].

2. Vakarenko, A. V., Nakonechnyi, V. S., Holub, V. A., Matiishen, R. V. (2010) Structural and functional aspects of domestic equipment for diagnostics and repair of electronic modules of anti-aircraft rocket complexes. *Systemy ozbroiennia i viiskova tekhnika: nauk. zhurn.* Kharkiv: Kharkivskiy universytet Povitrianykh Syl imeni Ivana Kozheduba, No. 1 (21), pp. 44–47 [in Ukrainian].
3. Rudakov, K. S., Detkin, V. G., Khrulov, N. V., Titorenko, I. S. (2009) Functions and structure of specialized diagnostic processor. *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu. Seria: Tehnichni nauky*, No. 3, pp. 8–11 [in Russian].
4. Detkin, V. G., Khrulov, N. V. (2006) Methods of complex control of computational processes. *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu. Seria: Tehnichni nauky*, No. 1, pp. 76–79 [in Russian].
5. Uil'yams, G. B. (1988) Debugging of microprocessor systems. Moscow: Energoatomizdat, 253 p.
6. Kovalenko, A. A., Petropavlovskiy, M. D. (2006) Fundamentals of microelectronics. Moscow: Izd. tsentr «Akademiya», 240 p. [in Russian].
7. Gol'tsev, A. D. (2005) Neural networks with ensemble organization. Kiev: Naukova dumka, 200 p. [in Russian].
8. Kussul', E. M. (1992) Associative neurosimilar structures of Academy of Science of Ukraine. In: *t of cybernetics*. Kiev: Nauk. dumka, 140 s. [in Russian].
9. Vega, A., Baidyk, T., Kussul, E., Pérez Silva, J. L. (2010) Digital implementation of LIRA Neural Classifier. *Proceedings of the 1st international congress on instrumentation and applied sciences*, October. URL: <http://somi.ccadet.unam.mx/icias2010/memorias/31>
10. Rudnitskiy, V. N., Khrulov, N. V., Babenko, V. G. (2012) Functions and structure of neuronet module of numerical program control system. *Systemy obrobky informatsii: zb. nauk. prats Kharkivskoho universitetu Povitrianykh Syl.* Kharkiv, vyp. 2 (100), pp. 96–100 [in Russian].
11. Strunz, Bob. Design for testability in digital integrated circuits. Bob Strunz, Colin Flanagan, Tim Hall University of Limerick, Ireland. URL: http://www.cs.colostate.edu/~cs530/digital_testing.pdf
12. Zinchenko, Yu. Ye. (1989) Methods and means of built-in testing in specialized devices of networks for data transfer in real time: thesis. Kiev: IPME, 208 p. [in Russian].
13. Ivanov, Yu. P., Nikitin, V. G., Chernov, V. Yu. (2004) Control and diagnostics of measuring-calculating complexes. St. Petersburg, 98 p.
14. Balashov, Ye. P. (1985) Evolutional synthesis of systems. Moscow: Radio i svyaz', 328 p.

V. M. Rudnitskiy, *D.Tech.Sc., professor*,
e-mail: rvn_2008@ukr.net

V. G. Detkin, *Ph.D., associate professor*,
e-mail: ded@nensi.net

N. V. Khrulev, *Ph.D., associate professor*,
e-mail: hrulev@ukr.net

G. V. Krivous, *head of laboratories*
e-mail: krivous_gv@gmail.com

Cherkasy State Technological University
Shevchenko blvd., 460, Cherkasy, 18006, Ukraine

FUNCTIONS AND STRUCTURE OF THE SYSTEM OF COMPLEX CONTROL OF COMPUTING PROCESSES

The problems of the synthesis of the structure of computational processes complex control system are considered. The conditions for the correct execution of computational process are determined. To intellectualize the control of computational process, it is proposed to use a neural network with ensemble organization that will allow not only to detect the failure of computational process correct execution, but also to determine causes and location of the failure, to analyze causes of the failure,

and to predict the behavior of computational process in the time. It is offered to perform the system structure synthesis on the basis of functional-structural approach proposed in the works of E. P. Balashov. As a result of objective function decomposition, the function tree is formed. This function tree determines the main parameters of the system of computational processes complex control, such as performance, reliability, functionality, and has a primary impact on the structure. The results of the synthesis of the structure of computational processes complex control system on the basis of the proposed function tree are presented.

Keywords: *computational process, control, function tree, functional-structural approach, structure, neural network.*

Статтю представляє В. М. Рудницький, д.т.н., професор.

О. О. Харін, аспірант кафедри
інформаційної безпеки та комп'ютерної інженерії
e-mail: kharin_aa@mail.ua
Черкаський державний технологічний університет
б-р Шевченка, 460, Черкаси, 18006, Україна

ПОРІВНЯЛЬНА ОЦІНКА ФАКТОРІАЛЬНИХ КОДІВ

У роботі досліджено механізм утворення помилок декодування, їх зв'язок зі статистикою помилок та алгоритмами прийняття рішень у процесі декодування факторіальними кодами. Для виконання порівняльного оцінювання стійкості різних факторіальних кодів до впливу потоку помилок створено експериментально-розрахункові моделі для повного факторіального коду (ПФК), факторіального коду з відновленням даних (ФКВД), ФКВД з додатковими перевірними бітами (ФКВДд) та факторіального каскадного коду (ФКК). Для запропонованих кодів виконано оцінювання достовірності передачі даних, швидкості коду та величини енергетичного виграшу для однакових значень довжини інформаційного блоку та ймовірності бітової помилки в каналі зв'язку за біноміального розподілу помилок на вході декодера. Виконано аналіз механізму утворення помилок декодування. На основі отриманих результатів розроблено рекомендації щодо застосування кожного з факторіальних кодів для вирішення задач забезпечення контролю цілісності інформації (КЦІ) та її криптографічного захисту.

Ключові слова: факторіальний код, повний факторіальний код, факторіальний код з відновленням даних, достовірність передачі даних, енергетичний виграш, контроль цілісності інформації, криптографічний захист.

Постановка проблеми. На сучасному етапі розвитку комп'ютерних систем і мереж актуальною є задача комплексного захисту інформації, що передбачає:

- захист інформації від несанкціонованого читання;
- забезпечення цілісності інформації, що включає захист від помилок, які виникають у каналі зв'язку під час її передавання, і захист від нав'язування хибних даних.

Розробка нових методів вирішення задач криптографічного захисту та КЦІ, а також їх поєднання дозволяють підвищити ефективність засобів обробки інформації за рахунок суміщення операцій захисту інформації від несанкціонованого зчитування, підміни та каналного кодування і є актуальним напрямком досліджень.

Аналіз джерел і публікацій. Отримані в [1, 2, 3, 4, 5] результати показують ефективність використання факторіальних кодів для підвищення достовірності передавання інформації, а також для вирішення задач КЦІ та криптографічного захисту. Основною перевагою таких кодів є те, що вони поєднують у собі функції захисту від помилок у каналі зв'язку, захисту від нав'язування хибних даних, а також криптографічного захисту. В

основі принципів факторіального кодування лежить побудова перестановок на основі факторіальної системи числення. Це здійснюється за рахунок відображення точок на числовій осі, що відповідають інформаційному вектору, в точки числової осі, що відповідають перестановці або відповідній контрольній сумі. Крім того, відзначимо, що більшість розглянутих факторіальних кодів мають здатність до самосинхронізації і не потребують введення в формат кадру синхроблоку, що дозволяє зменшити внесену надлишковість. Це обумовлено тим, що символи перестановки $\{0; 1; \dots; M-1\}$ зустрічаються в ній рівно по одному разу, а їх сума дорівнює $\sigma = 0,5M(M-1)$ [3]. Оскільки факторіальні коди не завжди забезпечують повний комплекс засобів із захисту інформації, залежно від характеру вирішуваних задач, було розроблено декілька видів факторіального кодування.

В [1] розглядається метод захисту інформації від помилок та нав'язування хибних даних (імітозахисту) за рахунок додавання до k -бітної інформаційної послідовності перевірної частини, що представлена перестановкою чисел $\{0, 1, \dots, M-1\}$, де M – порядок перестановки.

новки. У результаті такої операції сформований блок даних містить $n = k + r$ біт, де $r = l_r \cdot M$, r – розмір перевірної частини, l_r – довжина кодової комбінації кожного елемента перестановки. Такий код отримав назву повного факторіального коду (ПФК). Його особливістю є те, що розмірність перевірної частини може бути довільною і залежить від необхідного рівня підвищення достовірності, а також необхідного рівня імітостійкості. Разом із тим, зі збільшенням розміру імітовставки зменшується швидкість коду. Крім того, слід зауважити, що інформаційна частина передається у відкритому вигляді і не захищена від несанкціонованого читання.

У [3] запропоновано повністю замінити інформаційну послідовність на перестановку, сформовану за цією послідовністю. Такий код отримав назву факторіального коду з відновленням даних за перестановкою (ФКВД). ФКВД являє собою нероздільний код, в якому носієм інформаційної послідовності з k біт є обчислена за всіма бітами інформаційної послідовності перестановка чисел порядку M , що обирається з умови $M! \geq 2^k$. При цьому частина перестановок відноситься до забороненої множини для забезпечення рівної потужності множини інформаційних векторів і множини перестановок. ФКВД забезпечує криптографічний захист та захист від помилок у каналі зв'язку. Значною перевагою такого коду є те, що він дозволяє виявляти всі помилки, що не призводять до трансформації одної перестановки в іншу з дозволеної множини перестановок. У роботах [4, 5] розглянуто методи, спрямовані на підвищення стійкості ФКВД до помилок, що призводять до трансформації перестановок за рахунок внесення додаткової надлишковості.

У [4] запропоновано метод підвищення достовірності передавання даних для ФКВД за рахунок зменшення розміру інформаційної послідовності і введення в неї додаткових перевірних біт. Такий метод отримав назву ФКВД з доповненням (ФКВДд). Додатково розглянуто код, в якому додаткові біти доповнювали вже сформовану перестановку і не змінювали початкову інформаційну послідовність. Такий метод кодування було названо факторіальним кодуванням з додатковими перевірними бітами (ФКДБ).

Інший метод підвищення достовірності передавання, розглянутий у [5], полягає у

каскадуванні декількох кодів – рівноважного коду та ФКВД. Такий код отримав назву факторіального каскадного коду (ФКК). Недоліком такого коду є те, що рівноважний код, так само як і ФКВД, вразливий до помилок парної кратності. Також слід відзначити, що реалізація такого коду вимагає значних обчислювальних ресурсів.

Мета роботи. Метою цієї роботи є оцінювання набору якостей та основних властивостей факторіальних кодів, а також формулювання рекомендацій щодо оптимального вибору коду для конкретного застосування. Для цього необхідно виконати оцінювання існуючих факторіальних кодів у системах передачі даних з вирішальним зворотним зв'язком та порівняти отримані характеристики. При цьому треба оцінити:

- швидкість коду;
- імовірність помилкового декодування блока даних;
- енергетичний виграш.

Рішення задачі. Слід зазначити, що всі факторіальні коди, в першу чергу, вирішують задачу захисту інформації від помилок, що виникають у каналі зв'язку. Але порівняння факторіальних кодів лише за показником достовірності передавання даних не дає об'єктивної оцінки, оскільки не враховуються додаткові властивості, притаманні кожному з цих кодів. Тому, крім порівняння факторіальних кодів за швидкістю коду, енергетичним виграшем і ймовірністю помилкового декодування блока даних, також слід зазначити, за яких умов необхідно застосовувати кожен із досліджуваних кодів.

З метою порівняння факторіальних кодів розроблено розрахунково-експериментальні моделі для таких кодів: ПФК[1], ФКВД [3], ФКВДд [4], ФКДБ, ФКК [5].

У першу чергу, розглянемо особливості реалізації ПФК. Відзначимо, що, хоча ПФК передбачає довільний розмір перевірної частини, під час побудови розрахунково-експериментальної моделі порядок перестановки, що являє собою перевірку частину коду, обирався за умови $M! \geq 2^k$. Виконання цієї умови дозволяє уникнути колізій, коли декільком інформаційним векторам відповідає одна перестановка, і забезпечує вищу достовірність передавання даних за рахунок зниження швидкості коду.

У цій роботі будемо досліджувати ФКВДд [4] з одним додатковим перевірним бітом, що являє собою ознаку парності конт-

рольної суми, розрахованої за всіма бітами інформаційної послідовності:

$$a_{add} = a_0 \oplus a_1 \oplus \dots \oplus a_{k-1},$$

де $\{a_0, a_1, \dots, a_{k-1}\}$ – біти інформаційного вектора.

Як випливає з [4], такий спосіб дає змогу значно підвищити достовірність передавання даних за рахунок незначного зниження швидкості коду, причому зі збільшенням довжини інформаційного вектора зниженням швидкості можна знехтувати, що дозволяє ввести декілька перевірних біт. Очевидним недоліком такого коду є необхідність зменшення інформаційної частини для збільшення надлишковості.

У свою чергу, ФКДБ як варіант модифікації ФКВДд передбачає додавання перевірних біт до вже сформованої перестановки, що за умови вибору довжини інформаційного вектора, рівної $k = \lceil \log_2 M \rceil$, дозволяє мінімізувати надлишковість і, як наслідок, отримати більшу швидкість коду. У цьому коді перевірні біти визначаються як ознаки парності суми всіх елементів синдрому та/або індексу перестановки [7]. Залежно від кількості та способу формування додаткових біт оцінюванню підлягають наступні варіанти побудови кодів ФКДБ.

1. Перестановка доповнюється одним перевірним бітом, який визначає парність числа інверсій перестановки, що розраховується як алгебраїчна сума всіх елементів синдрому за модулем 2:

$$check_bit = \left| \sum_{i=0}^{M-1} b_i \right|_2,$$

де $check_bit$ – перевірний біт, $\{b_{M-1}, b_{M-2}, \dots, b_0\}$ – факторіальні коефіцієнти (елементи синдрому перестановки S_f).

2. Перестановка доповнюється трьома перевірними бітами, які визначають парність числа інверсій перестановки і дублюють один одного:

$$\begin{aligned} check_bit_1 &= check_bit_2 = \\ &= check_bit_3 = \left| \sum_{i=0}^{M-1} b_i \right|_2. \end{aligned}$$

3. Перестановка доповнюється трьома перевірними бітами, перший з яких визначає парність числа інверсій, другий – індекс ін-

версної перестановки, третій – індекс взаємної перестановки.

4. Перестановка доповнюється трьома перевірними бітами, перший з яких визначає парність числа інверсій всієї перестановки, другий – парність числа інверсій за парними елементами синдрому, третій – парність числа інверсій за непарними елементами синдрому:

$$\begin{aligned} check_bit_1 &= \left| \sum_{i=0}^{M-1} b_i \right|_2, \\ check_bit_2 &= \left| \sum_{i=0}^{\left\lfloor \frac{M}{2} \right\rfloor} b_{2i} \right|_2, \\ check_bit_3 &= \left| \sum_{i=0}^{\left\lfloor \frac{M}{2} \right\rfloor} b_{2i+1} \right|_2. \end{aligned}$$

5. Перестановка доповнюється одним перевірним бітом, який визначає парність інформаційної частини (за аналогією з ФКВДд, за винятком того, що інформаційна частина вибирається з умови $k = \lceil \log_2 M \rceil$, а біт перевірки дописується в кінці блока):

$$check_bit = a_0 \oplus a_1 \oplus \dots \oplus a_{k-1}.$$

6. Перестановка доповнюється трьома перевірними бітами, що обчислюються аналогічно п. 3, але рішення про коректність прийнятого блока приймається за мажоритарним принципом (за більшістю голосів). Якщо хоча б двоє з трьох перевірних бітів, прийнятих з каналу зв'язку, збігаються з розрахованими на приймальній стороні за прийнятою перестановкою, то такий блок даних вважається прийнятим без помилок.

У результаті дослідження властивостей ФКДБ встановлено, що контроль парності алгебраїчної суми елементів синдрому дозволяє виявляти всі двократні помилки, що призводять до транспозиції елементів перестановки. Також очевидно, що за рахунок накладання помилок на перевірні біти мають місце два специфічні види помилок декодування, властивих для всіх варіантів побудови ФКДБ:

1) помилка призвела до трансформації однієї перестановки в іншу, що належить дозволений множині перестановок, а також відповідним чином змінила перевірні біти;

2) перестановка прийнята без помилок, але значення перевірних біт було спотворено помилкою. У цьому випадку має місце «хибна

помилка». Приймальна сторона вважає весь блок даних прийнятим з помилкою і формує сигнал на повторний запит блока.

Табл. 1 демонструє результати моделювання досліджуваних факторіальних кодів. Під час моделювання оцінювалися такі параметри, як: швидкість коду v , імовірність помилкового декодування блока даних P_{ud} та енергетичний виграш ΔP . Моделювання ви-

конувалося для біноміального закону розподілу помилок у каналі зв'язку, довжина інформаційного вектора k становила 15 біт, імовірність бітової помилки $p_0 = 1/15$. Порядок перестановки M обирається з умови $M! \geq 2^k$, довжина блока даних n залежить від способу кодування.

Таблиця 1

Результати моделювання факторіальних кодів

№	Код	k , біт	n , біт	M	P_{ud}	v	ΔP , дБ
1	ПФК	15	39	8	0,000036	0,385	8,166
2	ФКВД	15	24	8	0,011550	0,625	5,371
3	ФКВДд	14	24	8	0,002808	0,583	6,179
4	ФКДБ, варіант 1	15	25	8	0,001126	0,600	6,649
5	ФКДБ, варіант 2	15	27	8	0,000335	0,556	7,213
6	ФКДБ, варіант 3	15	27	8	0,000549	0,556	7,005
7	ФКДБ, варіант 4	15	27	8	0,000522	0,556	7,027
8	ФКДБ, варіант 5	15	25	8	0,005753	0,600	5,812
9	ФКДБ, варіант 6	15	27	8	0,004598	0,556	5,979
10	ФКК	15	36	9	0,001125	0,417	6,816

Результати, відображені в таблиці, дають змогу оцінити якісні характеристики досліджених факторіальних кодів та сформулювати рекомендації щодо їх використання:

1. ПФК має найбільший енергетичний виграш, а також найменшу швидкість коду, що обумовлено його великою надлишковістю. При цьому ПФК забезпечує імітозахист і захист від помилок каналу зв'язку;
2. ФКВД має найбільшу швидкість коду серед усіх розглянутих кодів та найменший енергетичний виграш. Але головною його перевагою є те, що він виконує функцію шифрування і забезпечує захист інформації від несанкціонованого читання. Тому ФКВД доречно використовувати для передавання конфіденційної інформації;
3. ФКВДд та ФКДБ є варіантами підвищення ефективності ФКВД за рахунок введення додаткових перевірних бітів і, як наслідок, зменшення швидкості коду. Очевидно, що ці коди, як і ФКВД, виконують функцію шифрування і більш стійкі до помилок каналу зв'язку;
4. ФКК є спробою поєднання факторіальних кодів з іншими з метою підвищити

стійкість факторіальних кодів до помилок парної кратності. У [5] запропоновано поєднання ФКВД та рівноважного кодів, що дало змогу отримати більший енергетичний виграш порівняно з ФКВД, але не дозволило виявити всі помилки парної кратності. Це обумовлено тим, що ФКВД сам по собі має властивість рівноважності, а підвищення достовірності передавання даних обумовлено попередньою обробкою інформаційного вектора. Варто зазначити, що ФКК зберігає властивість ФКВД із забезпечення захисту від несанкціонованого читання, а за умови збереження порядку перестановки M дає більший енергетичний виграш для сталої швидкості коду.

Висновки. Проведені дослідження дозволили проаналізувати та узагальнити інформацію про факторіальні коди. Виконано порівняння наступних факторіальних кодів: ПФК, ФКВД, ФКВДд, ФКК, ФКДБ – за критеріями:

- швидкість коду;
- імовірність помилкового декодування блока даних;
- енергетичний виграш.

Було розроблено розрахунково-експериментальні моделі, що дали змогу оці-

нити якісні характеристики факторіальних кодів. Окрім оцінювання кодів з точки зору достовірності передавання даних, розглянуто їх властивості по забезпеченню захисту від нав'язування хибних даних та криптозахисту. На основі отриманих результатів моделювання сформульовано рекомендації щодо застосування кожного з кодів.

Список літератури

1. Фауре Э. В., Швыдкий В. В., Щерба А. И. Контроль целостности информации на основе факториальной системы счисления. *Journal of Baku Engineering University. Mathematics and Computer Science*. 2017. № 1. Т. 2.
2. Фауре Э. В., Швыдкий В. В., Щерба А. И. Комбинированное факториальное кодирование и его свойства. *Радиоэлектроника, информатика, управління*. 2016. № 3. С. 80–86.
3. Фауре Э. В. Факториальное кодирование с восстановлением данных. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*. 2016. № 2. С. 33–39.
4. Фауре Э. В. Метод повышения эффективности факториального кодирования с восстановлением данных. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*. 2016. № 4. С. 57–61.
5. Харін О. О. Оцінка властивостей каскадного коду, що поєднує факторіальний та рівноважний код. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*. 2017. № 2. С. 86–90.
6. Кнут Д. Э. Искусство программирования. Т. 1. Основные алгоритмы. Москва: Вильямс, 2002. 720 с.
7. Кнут Д. Э. Искусство программирования. Т. 2. Получисленные алгоритмы. Москва: Вильямс, 2007. 832 с.
8. Прокис Д. Г. Цифровая связь; пер. с англ. под ред. Д. Д. Кловского. Москва: Радио и связь, 2000. 800 с.
9. Пат. 117004 Україна, МПК H03M 13/09 (2006.01), H04L 1/16 (2006.01), G04C 1/06 (2006.01). Спосіб факторіального кодування з відновленням даних / Фауре Е. В., Харін О. О., Швидкий В. В., Щерба А. І.; заявник та патентовласник Черкаський

державний технологічний університет. № u201613641; заявл. 30.12.2016; опубл. 12.06.2017, Бюл. № 11.

10. Пат. 106669 Україна, МПК G06F 21/64 (2013.01). Спосіб формування імітовставки / Фауре Е. В., Швидкий В. В., Щерба А. І.; заявник та патентовласник Черкаський державний технологічний університет. № a201505934; заявл. 16.06.2015; опубл. 10.05.2016, Бюл. № 9.

References

1. Faure, E. V., Shvydkiy, V. V., Shcherba, A. I. (2017) Information integrity control based on factorial number system. *Journal of Baku Engineering University. Mathematics and Computer Science*, No. 1, vol. 2 [in Russian].
2. Faure, E. V., Shvydkiy, V. V., Shcherba, A. I. (2016) Combined factorial coding and its properties. *Radioelektronika, informatyka, upravlinnya*, No. 3, pp. 80–86 [in Russian].
3. Faure, E. V. (2016) Factorial coding with data recovery. *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu. Seria: Tehnichni nauky*, No. 2, pp. 33–39 [in Russian].
4. Faure, E. V. (2016) The method of increasing the efficiency of factorial coding with data recovery. *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu. Seria: Tehnichni nauky*, No. 3, pp. 57–61 [in Russian].
5. Kharin, O. O. (2017) Estimation of properties of cascade code, which combines factorial and equilibrium codes. *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu. Seria: Tehnichni nauky*, No. 2, pp. 86–90 [in Ukrainian].
6. Knut, D. E. (2002) The art of computer programming. Vol. 1. Fundamental algorithms. Moscow: Vil'yams, 720 p. [in Russian].
7. Knut, D. E. (2007) The art of computer programming. Vol. 2. Seminumerical algorithms. Moscow: Vil'yams, 832 p. [in Russian].
8. Proakis, J. G. (2001) Digital communications. Boston: McGraw-Hill.
9. Faure, E. V., Kharin, O. O., Shvydkiy, V. V., Shcherba, A. I. (2017) The mode of factorial coding with data recovery. Cherkasy State

- Technological University, assignee. UA Patent 117004, printed June 12 [in Ukrainian].
10. Faure, E. V., Shvydkyi, V. V., Shcherba, A. I. (2016) The mode of staffing formation. Cherkasy State Technological University, assignee. UA Patent 106669, printed May 10 [in Ukrainian].

O. O. Kharin, *postgraduate student,*
postgraduate student of information security and computer engineering chair
e-mail: kharin_aa@mail.ua
Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine

COMPARATIVE EVALUATION OF FACTORIAL CODES

In the work, the mechanism of generation of decoding errors, their connection with error statistics and algorithms of decision making in the process of decoding by factorial codes are investigated in detail. To perform a comparative estimation of the stability of various factorial codes to the influence of the error flow, experimental-calculation models for full factorial code (FFC), factorial code with data recovery (FCDR), FCDR with additional verification bits (FCDRd) and factorial cascading code (FCC) were created. The reliability of the data transmission, the speed of the code and the value of the energy gain for proposed codes were evaluated with the same values of the length of the information block and the probability of a bit error in the communication channel in the binomial distribution of errors at the decoder input. An analysis of the mechanism of generation of decoding errors is performed. On the basis of the obtained results, recommendations were made for the use of each of the factorial codes when solving the problems of ensuring the control of the integrity of information and cryptographic protection.

Key words: *factorial code, full factorial code, factorial code with data recovery, reliability of data transmission, energy gain, integrity control of information, cryptographic protection.*

Рецензенти: В. М. Рудницький, д.т.н., професор,
С. В. Голуб, д.т.н., професор

С. Ю. Куницька, к.т.н.,

доцент кафедри інформаційної безпеки та комп'ютерної інженерії,

e-mail: kunitskaya33@gmail.com

Черкаський державний технологічний університет,

бульв. Шевченка, 460, м. Черкаси, 18006, Україна,

ТЕХНОЛОГІЯ ОБРОБКИ ІНФОРМАЦІЇ НОРМАЛІЗОВАНИХ СИСТЕМ

Для спрощення обчислювального процесу моделей будь-якої складності виникла необхідність розробити технологію обробки інформації у вигляді програмного алгоритму, який дозволяє обробляти, аналізувати та прогнозувати майбутній процес. Для перетворення вхідних даних у вихідну інформацію необхідно мати локальний алгоритм перетворення інформації, що ґрунтується на індуктивному методі синтезу цих алгоритмів. На першому етапі будь-якого ймовірного алгоритму синтезу описаний в статті алгоритм перетворення інформації - це представлення вхідних даних у вигляді перевизначеної системи умовних рівнянь. Надалі приведено системи до вигляду, який дозволяє визначити коефіцієнти системи. А потім введено поняття «нормалізації» системи, використовуючи метод найменших квадратів. Дослідження системи відбувається з точки зору її аргументів, що й дає змогу отримати необхідну навчену модель. Всі отримані модифікації навчених моделей перевірено на наявність похибки, що представляє собою середньоквадратичну похибку прогнозу для перевірки прогнозованої послідовності.

Ключові слова: умовні рівняння, експериментальні точки, система, нормалізація, модель, похибка, прогнозування.

Постановка проблеми. Побудова математичної моделі складного об'єкта або процесу є необхідністю для вирішення таких головних задач, як прогнозування або розпізнання образів. Під поняттям «математична модель» ми розуміємо систему рівнянь регресії, які використовуються для одноразового прогнозу майбутнього ходу процесу в складній системі.

Тобто, математична модель в задачах прогнозування може бути представлена як система рівнянь, що описує об'єкт з певним числом експериментальних точок, необхідних для подальшого спостереження.

Аналіз останніх досліджень. Історичне виникнення мови програмування C# починає свій розвиток з 60-х років, де початком була мова В, що є представником імперативних мов програмування. Головною метою розробки цієї мови – це реалізація операційної системи UNIX. Наступним кроком розвитку була мова програмування С, що розроблена в 1972 році, де мова В розширилася за рахунок наочного використання типів, структур та нових операцій. Надалі, в 1984 році, введено поняття класу, як об'єкту даних та набуває розвитку мова C++ вже як об'єктно-орієнтована мова програмування. На сьогодні, мова C# ґрунту-

ється на чітко побудованій компонентній архітектурі та реалізує механізми, що забезпечують принцип наслідування, побудову інтерфейсів, обробку виключних ситуацій і нитей (threads), а також безпеку динамічного завантаження кода при виконанні програми.

В цілому, корпорація Microsoft досить чітко реалізувала найважливіші задачі для програмування, що й відображені в мові програмування C#:

- компонентно-орієнтований підхід (що є характерним для ідеології Microsoft .NET);
- властивості, як засоби інкапсуляції даних;
- ситуаційна обробка (оператор `try`), делегати (`delegate`), індексатори – оператори індексу для звернення до елементів класу-контейнера (`indexer`), перезавантаженні оператори, оператори для обробки всіх елементів класів-колекцій (`foreach` – аналог Visual Basic), механізми для пере визначення типів (`boxing` і `unboxing`);
- атрибути, як засоби оперування метаданими в СОМ-моделі;
- прямокутні масиви;
- уніфікована система типізації, що відповідає ідеології Microsoft .NET в цілому.

Метою дослідження є нормалізація системи та отримання навченої моделі на основі

розробленого програмного алгоритму, що зв'язує певний набір експериментальних точок за обраним діапазоном з введених раніше табличних даних, що зосереджені в Excel. Тобто описано програмний обчислювальний процес нормалізованих систем рівнянь, що будуються в залежності від кількості невідомих аргументів в опорному вигляді моделі полінома Колмогорова-Габора 2 ступеня з можливістю прогнозування поведінки майбутнього процесу.

Виклад основного матеріалу. Експериментальні точки, незалежно від рівня знань людини, містять в собі інформацію о різноманітних факторах [1]. Математична модель може бути побудована на різних наборах аргументів. Це ніяким чином не впливає на об'єктивність прогнозуючої ситуації, але при цьому повинна бути забезпечена достатня свобода вибору наступних рішень.

1. Перша і основна задача, що направлена на розробку та освітлена в цій статті - це написання програмного продукту на обраній мові програмування, що буде містити реалізацію обчислювального процесу за допомогою обрахунку полінома Колмогорова-Габора методом найменших квадратів та приведення рівнянь до нормалізації з метою подальшого прогнозування [1].

Програмний продукт написано об'єктною мовою програмування C# з підтримкою інтегрованого середовища розробки Visual Studio Professional 2017 на платформі .NET, що має зручний інтерфейс користувача та містить необхідні для роботи кнопки управління.

Табличні значення за деякими двома рядками можуть бути як константи, так і введенні необхідні статистичні данні за необхідністю. Діапазон обчислення обирається також за необхідністю, при цьому обчислюються всі аргументи, що заносяться з таблиці для подальшого збереження інформації, аналізу та майбутнього прогнозування. Внесення даних та визначення діапазону експериментальних точок знаходяться в таблицях Excel, де зберігаються в різноманітних файлах.

Програмний продукт максимально автоматизовано, що значно мінімізує втручання користувача, що й робить рішення поставлених задач найбільш універсальним. Дії користувача зводяться до введення з клавіатури певних експериментальних точок в таблицю, або обрання діапазону констант точок для

переходу на наступний етап розробки. Чим більше буде введено експериментальних точок, тим складніше отримаємо майбутню навчену модель, але більш точніше отримаємо прогноз процесу [2]. Надалі необхідно обрати кількість невідомих аргументів по опорному вигляду полінома і на цьому втручання діяльності користувача обмежується. Далі обчислювальний процес автоматизовано.

2. Опишемо та обґрунтуємо другу поставлену задачу, яка полягає в рішенні обчислювального процесу.

Різноманітні модифікації многорядного алгоритму відрізняються один від одного по виду опорної функції F. В алгоритмі з лінійними поліномами використовують часний опис виду:

$$y_k = a_0 + a_1x_i + a_2x_j, \quad (1)$$

де $0 < i < m, 0 < j < m$

Ускладнення моделі відбувається тільки за рахунок збільшення числа використаних аргументів, тобто в першому рядку селекції синтезуються моделі, що містять по два аргумента, на другому рядку синтезуються моделі з трьома або чотирма аргументами, на третьому - може доходити до восьми аргументів.

Многорядні алгоритми при використанні нелінійних опорних функцій мають наступний вигляд:

$$y_k = a_0 + a_1x_i + a_2x_j + a_3x_ix_j \quad (2)$$

Вони дозволяють отримати моделі практично будь-якої складності, тому що в кожному рядку селекції ступень полінома подвіюється. Число коефіцієнтів моделі при цьому може наближатися до нескінченності.

Особливість прогнозування – кожному наступному набору точок прогнозування передують ряд рішень попереднього набору точок обраних для написання системи умовних рівнянь, їх нормалізації та отримання навченої моделі в результаті.

В роботі розглянуто алгоритм отримання регресійного, тобто за формальними ознаками відповідність першим двом загально відомим принципам самоорганізації [3]:

- дозволена повна свобода вибору як при включенні нових факторів в модель, так і при виключенні їх;

- граничне значення F-критерія є зовнішнім критерієм селекції, що обирається з таблиць із статистичними даними.

В свою чергу поняття самоорганізації щільно пов'язано з появою впорядкування в

будь-якій системі. При цьому система повинна мати структуру, при дослідженні якої і будуть виникати критерії для її аналізу, прогнозування та поліпшенню процесу.

Надалі виникає необхідність в дослідженні системи з точки зору її поведінки, що й дає змогу в результаті отримати необхідну

нам навчену модель. Це досягається за рахунок наступних етапів:

1. Спочатку обирається опорний вигляд полінома Колмогорова-Габора 2 ступеня [4]. Модель будь-якого динамічного процесу максимальної складності можна отримати із загального повного полінома (3):

$$\varphi = a_0 + \sum_{i=1}^m a_i x_i + \sum_{i=1}^m \sum_{j=1}^m a_{ij} x_i x_j + \sum_{i=1}^m \sum_{j=1}^m \sum_{k=1}^m a_{ijk} x_i x_j x_k + \dots \quad (3)$$

2. Далі вносимо данні в таблицю експериментальних точок, що й необхідні для подальшого обчислювального процесу;

3. Формуємо систему умовних рівнянь за обраним поліномом Колмогорова-Габора. Наприклад, для шести членів загальний вигляд полінома приймає наступний вид:

$$y = a_0 + a_1 x_1 + a_2 x_2 + a_3 x_1 x_2 + a_4 x_1^2 + a_5 x_2^2 \quad (4)$$

4. Наступний етап – це отримання системи нормальних рівнянь за принципом: беремо кожне умовне рівняння та перемножуємо на коефіцієнти при першому невідомому, далі всі умовні рівняння додаємо. Для отримання другого нормалізованого рівняння беремо умовне рівняння та перемножаємо на коефіцієнти при другому члені рівняння, знову додаємо. Цей процес повторюється до тих пір, поки кількість нормальних рівнянь не зрівняється з кількістю невідомих коефіцієнтів в системі умовних рівнянь.

5. Надалі нормалізована система рівнянь приводиться до матричного вигляду для подальшого її обрахунку методом Гауса

або методом найменшого квадрата. Рішення нормалізованої системи рівнянь надає нам результат у вигляді отримання значень необхідних аргументів, які необхідні в подальшому для аналізу поведінки процесу та прогнозування.

Таким чином, ми отримали навчену модель, яку необхідно обов'язково перевірити на наявність похибок [5].

Найбільш частіше використовують один з наступних критеріїв, що відповідає за визначення оптимальної моделі – це критерій регулярності [6, 7]. Він представляє собою середнє квадратичну похибку прогнозу для перевірки спрогнозованої послідовності за наступною формулою:

$$\delta^2 = \sum_{i=1}^{n_2} (y_{\phi i} - y_{\rho i})^2 / \sum_{i=1}^{n_2} y_{\phi i}^2, \quad (5)$$

де $y_{\rho i}$ – прогноз i -го значення для перевірки прогнозованої послідовності; $y_{\phi i}$ – фактичне значення цієї ж послідовності; n_2 – об'єм послідовності

Тобто, отримана модель дозволяє отримати найбільш точні кількісні значення вихідних змінних при однократному прогнозуванню майбутнього процесу. Але при збільшенні складності рівнянь регресії, такі як ступень полінома Колмогорова-Габора та число невідомих аргументів, похибка, що виникає в обчислювальному процесі поступово зменшує свої значення на всіх експериментальних точках [8, 9].

У випадку рівності кількості експериментальних точок числу коефіцієнтів рівняння в поліномі похибка майже наблизиться до нуля або буде дорівнювати нулю.

Висновки. Згідно сформованих задач розглянута та досліджена спрогнозована поведінка декількох математичних моделей, що отримані та навчені завдяки наступним крокам:

- в статті описан процес отримання моделі через поліном Колмогорова-Габора будь-якої складності із введенням діапазону деяких даних;

- отримано навчену модель, що задається зовнішніми критеріями, і яка вже досліджена на наявність похибок прогнозуючого процесу;

- для спрощення обробки моделей будь-якої складності розроблено технологію обробки інформації завдяки програмному алгоритму із зручним інтерфейсом користувача, що дозволяє не тільки автоматизувати процес обчислювання моделей, але й зберігати всю необхідну інформацію по отриманню навчених моделей різної складності таку як: кількість експериментальних точок, складність обраного поліному в залежності від невідомих аргументів, результати обчислення невідомих аргументів, модифікації навчених моделей та обчислення похибки прогнозуючого процесу [10].

Список літератури

1. Дайитбегов Д. М., Калмыкова О. В., Черепанов А. И. Программное обеспечение статистической обработки данных. М.: Финансы и статистика, 1984. 192 с.
2. Ивахненко А. Г. Долгосрочное прогнозирование и управление сложными системами. 1975. 312с.
3. Ивахненко А. Г. Индуктивный метод самоорганизации моделей сложных систем. Киев: Наук. Думка, 1982. 296 с.
4. Куницька С. Ю. Приведення системи умовних рівнянь до нормалізації. *Проблеми інформатизації*: тези доп. п'ятої міжнародн. наук.-техн. конф., Черкаси, 13-15 листопада 2017 року. Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ, 2017. С. 60.
5. Флейшман Б. С., Брусиловский П. М., Розенберг Г. С. О методах математического моделирования сложных систем. *Системные исследования. Ежегодник*. М.: Наука, 1982. С. 65–79.
6. Ивахненко А. Г. Самообучающиеся системы распознавания и автоматического. Киев: Техника, 1969. 392 с.
7. Ивахненко А. Г., Зайченко Ю. П., Димитрова В. Д. Принятие решений на основе самоорганизации. М.: Сов. Радио, 1976. 275 с.
8. Редкозубов С. А. Статистические методы прогнозирования в АСУ. М.: Энергоатомиздат, 1981. 150 с.
9. Шеннон К. Е. Имитационное моделирование систем – искусство и наука. М.: Мир, 1978. 418 с.
10. Лисичкин В. А. Теория и практика прогностики. М.: Наука, 1972. 224 с.

References

1. Daiitbegov, D., Kalmykova, O., Cherepanov, O. (1984) Software for Statistical Data Processing. M.: Finance and Statistics. 192 p.
2. Ivakhnenko, A. (1975) Long-term forecasting and management of complex systems. Kiev: Technics. 312 p.
3. Ivakhnenko, A. (1982) Inductive method of self-organization of models of complex systems. Kiev: Science. Opinion. 296 p.
4. Kunytska, S. (2017) Bringing the system of conditional equations to normalization. *Problems of informatization: theses of additional. fifth international. Sci.-Tech. Conf.*, Cherkasy, November 13-15, 2017. Cherkasy; Baku; Bielsko-Biala; Poltava. P. 60.
5. Fleischman, B., Brusilovsky, P., Rosenberg, G. (1982) About methods of mathematical modeling of complex systems. *System research. Yearbook*. M.: Science. P. 65–79.
6. Ivakhnenko, A. (1969) Self-learning recognition and automatic control systems. Kiev: Technics. 392 p.
7. Ivakhnenko, A., Zaychenko, Y., Dimitrova, V. (1976) Decision-making based on self-organization. M.: Sov. Radio. 275 p.
8. Rezkubov, S. (1981) Statistical methods of forecasting in ACS. M.: Energoatomizdat. 150 p.
9. Shannon, K. (1978) Imitation Modeling Systems – Art and Science. M.: Mir. 418 p.
10. Lisichkin, V. (1972) Theory and Practice of Prognostics. M.: Science. 224 p.

S. Kynytska, Ph.D,

associate professor of the department of information security and computer engineering

e-mail: kunitskaya33@gmail.com

*Cherkasy State Technological University,
Shevchenko blvd., 460, Cherkasy, 18006, Ukraine*

TECHNOLOGY OF INFORMATION PROCESSING OF NORMALIZED SYSTEMS

To simplify the computational process of models of any complexity, there was a need to develop a technology for processing information in the form of a software algorithm that allows you to process, analyze and predict the future process. To convert input data into source information, it is necessary to have a local information conversion algorithm based on the inductive method of synthesizing these algorithms. In the first stage of any probabilistic synthesis algorithm, the algorithm for information transformation is described in the article as the representation of the input data in the form of a predefined system of conditional equations. In the following, the system is presented in a form that allows you to determine the coefficients of the system. And then the concept of "normalization" of the system is introduced, using the method of least squares. The system's research takes place from the point of view of its arguments, which makes it possible to obtain the necessary trained model. All received modifications of the trained models were checked for an error, which is the mean square prediction error for checking the predicted sequence.

Keywords: *conditional equations, experimental points, system, normalization, model, error, forecasting*

Рецензенти: С.В. Голуб, д.т.н., професор,

Т.О. Прокопенко, д.т.н., доцент

Голуб М. В., викладач,
Брик С. М., магістр,
Гарасюта В. М., магістр,
Савченко В. І., магістр,
Сандига О. Ю., магістр

Черкаський державний технологічний університет
б-р Шевченка, 460, 18006, м. Черкаси, Україна, тел. (0472) 730261

ТЕХНІЧНІ, ТЕХНОЛОГІЧНІ УМОВИ ТА ТЕХНІКО ЕКОНОМІЧНІ КРИТЕРІЇ ЕЛЕКТРОННО-ПРОМЕНЕВОЇ МІКРООБРОБКИ ОПТИЧНИХ ВИРОБІВ МАЛИХ РОЗМІРІВ

В статті представлено технічні, технологічні умови та техніко економічні критерії електронно-променевої мікрообробки оптичних виробів малих розмірів (до $1 \cdot 10^{-3}$ м). Лінійні розміри та температурні режими роботи катоду дозволяють визначати вимоги до джерел енергії, електронно-променевої гармати, систем попереднього нагріву і охолодження виробів, систем керування потужністю електронного потоку, а значить і оптимізувати режими електронно-променевої мікрообробки виробів малих розмірів. Джерело нагріву повинно бути рухомим і забезпечувати локальний нагрів поверхні оптичного матеріалу з точністю 0.5%, а параметри, що регулюються, повинні змінюватися у межах 2...4 порядків.

Ключові слова: електронний потік, електронно-променева обробка (мікрообробка), оптичне скло, поверхневий шар скла, мікрооптика, інтегральна оптика, MOMS, MOEMS.

Актуальність. Різке зростання попиту користувачів до мікрооптичних виробів, мікрооптомеханічних систем (MOMS) та мікрооптоелектромеханічних систем (MOEMS) усе сильніше загострює проблему виготовлення плат малих розмірів (від 10...1000 мкм) для розташування на їх поверхні оптичних мікроелементів з лінійними розмірами у 0,47...0,75 мкм [1-3].

Вирішення цієї проблеми в умовах оптичного виробництва можливе через розробку та впровадження нового інструментарію, екологічно чистих технологічних середовищ, які б забезпечили створення матеріалів з новими фізико-хімічними властивостями, та виробів з максимальним ефектом взаємодії зі світловими хвилями.

Принципову можливість використання стрічкового електронного потоку для керування якістю поверхневого шару оптичних матеріалів та створення на поверхні оптичних матеріалів фокусуючих, відбиваючих та заломлюючих світло мікроструктур доведено у роботах професора Канашевича Г.В. [4,5].

Разом з тим, недослідженими та невисвітленими залишаються питання з технічних, технологічних умов та техніко економічних критеріїв цієї технології

Мета роботи. Дослідити та визначити технічні, технологічні умови та техніко еко-

номічні критерії електронно-променевої мікрообробки оптичних виробів малих розмірів, оптимізуючи результати попередніх робіт з поверхневої електронно-променевої мікрообробки оптичних матеріалів.

Обладнання, об'єкти обробки і інструмент для електронно-променевої обробки:

Обладнання. Електронно-променева установка виготовлена на базі вакуумної установки УВН74-ПЗ. Електронний термопарний регулятор температури РИФ-101 забезпечує необхідний температурний профіль печі з точністю $\pm 1^\circ\text{C}$. Максимальна робоча температура нагріву печі 800°C . Механізм переміщення забезпечує рух пластин в об'ємі вакуумної камери зі швидкістю 0...50 см/с, залишковий тиск у вакуумній камері складає 10^{-4} Па.

Об'єкти мікрообробки: мікролінзи, плоскопаралельні пластини, рис.1.



Рис. 1. Об'єкти обробки електронним потоком

Мікролінзи широко використовуються, як фокусуючі елементи волоконно-оптичних систем зв'язку, в мікроелектроніці, лазерній хірургії та терапії, мікрооб'єктивів ендоскопів, лазерних аналізаторах, в MOMS та MOEMS [6].

Інструмент обробки. Електронно-променева гармата Пірса генерує стрічковий електронний потік питомої потужності $10^1 \text{ Вт/см}^2 \leq P_{\text{пот}} \leq 10^5 \text{ Вт/см}^2$, який може пе-

реміщуватися по поверхні виробу зі швидкістю $v_{\text{ном}} = 0 \dots 20 \text{ см/с}$, b' – ширина стрічки $0,5 \dots 3 \text{ мм}$.

Отримані результати та їх обговорення.

Нами побудована схема, (рис.2), яка відображає еволюцію інструментарію (елементарного інструменту) та її взаємозв'язок зі зменшенням лінійних розмірів виробів мікрооптики, інтегральної оптики і волоконної оптики [2,7,8].

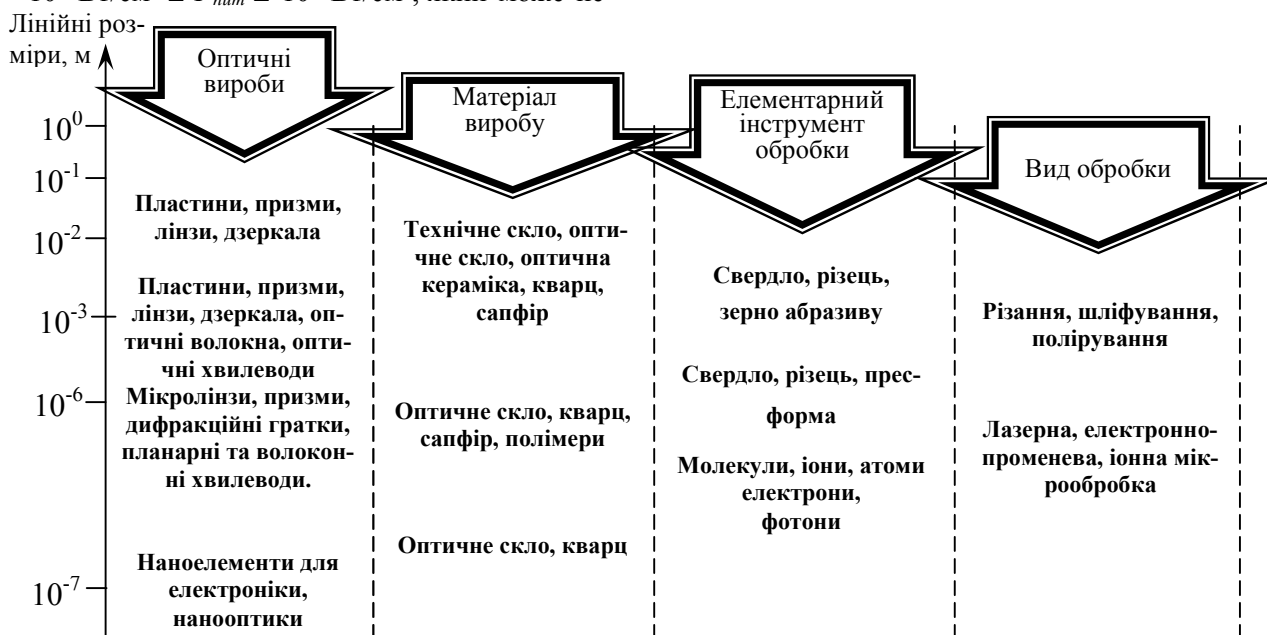


Рис. 2. Діапазони розмірів сучасних виробів оптики, мікрооптики, інтегральної та волоконної оптики а також матеріалу, елементарного інструменту та виду обробки

Суть методу низькоенергетичного ($E \leq 10 \text{ кеВ}$) полірування полягає в тому, що електронний потік фіксованої потужності при взаємодії з поверхнею оптичного матеріалу (скло, полікристал) здатний розігріти та розтопити тонкий, у десятки та сотні мікрометрів, поверхневий шар даного матеріалу [9, 10]. Робоча температура в зоні дії електронного потоку складає близько $1500 \text{ }^\circ\text{C}$, а час дії електронного потоку на матеріал не перевищує декількох секунд. В результаті взаємодії потоку електронів певної енергії з матеріалом низької теплопровідності на поверхні такого матеріалу виникає зона з рідинно-текучим станом. При використанні рухомого потоку електронів ця рідинна зона також буде рухомою. В залежності від режимів такої обробки (потужності потоку та часу дії на матеріал) після охолодження утворюється хвиляста або плоска поверхня. Застигла поверхня представляє собою тонкий шар, який відрізняється

від основного матеріалу своєю структурою та фізико-хімічними властивостями [9].

Аналізуючи концепцію [11] високоефективного керування процесом електронно-променевої мікрообробки для забезпечення прецизійності технології можна визначити такі технічні та технологічні умови електронно-променевої мікрообробки оптичних матеріалів малих розмірів.

До технічних умов належать:

1. Наявність спеціального технологічного вакуумного обладнання або адаптація існуючого вакуумного обладнання, які б забезпечили використання:

- термopечі у вакуумній камері (вакуум не менший за 10^{-3} Па) для попереднього нагріву і охолодження виробів з регульованим діапазоном робочих температур $20 \dots 640 \text{ }^\circ\text{C} \pm 1 \text{ }^\circ\text{C}$ на протязі 10 годин роботи установки;

- технологічної арматури, механізмів руху, які б забезпечили швидкість проходження електронного потоку $0,2 \dots 10 \text{ см/с}$;

- електронно-променевої гармати Пірса із стрічковою формою потоку з необхідним нахилом потоку до поверхні виробу, яка оброблюється.

2. Наявність джерел живлення електронно-променевої гармати Пірса, які б забезпечили стабільну роботу гармати в межах питомої потужності $P_{\text{пит}} = 0,5 \cdot 10^2 \dots 5 \cdot 10^4 \text{ Вт/см}^2$ та регульований нагрів ($20 \dots 1250$) $^{\circ}\text{C}$ і охолодження оптичних матеріалів зі швидкістю меншою за $8 \text{ }^{\circ}\text{C/хв}$ в умовах обробки.

3. Забезпечення на базі ПК автоматизованої системи зондування електронного потоку та керування режимами електронно-променевої обробки.

4. Наявність приладів та обладнання для забезпечення технологічного контролю якості виробів, отриманих поверхонь і функціональних шарів.

До технологічних умов належать:

1. Забезпечення оптимальних значень вакууму, температур попереднього нагріву виробів у вакуумній камері перед електронно-променевою обробкою.

2. Забезпечення оптимальних значень потужності і швидкості електронного потоку при поверхневій обробці оптичних матеріалів.

3. Забезпечення оптимальних режимів нагріву та охолодження виробів після електронно-променевої обробки.

4. Визначення характеристик якості (мікрорельєфу поверхонь, площинності, світлорозсіяння, залишкових термонапружень, чистоти оптичної поверхні тощо) оброблених деталей.

Оскільки процес обробки передбачає сильний локальний термічний вплив електронної стрічки на поверхню заготовки (градієнт температур на поверхні досягає значень $10^2 \dots 10^3 \text{ К/мм}$), і виходячи з розмірів електронної стрічки (довжина робочої частини катоду не перевищує 80 мм , а діаметр катоду не перевищує $0,8 \text{ мм}$) визнаємо, що ширина і довжина зони обробки будуть обмеженими. З урахуванням цих умов та необхідної номенклатури оптичних матеріалів проведено класифікацію виробів, які отримуються електронно-променевим методом, а саме:

- за матеріалом (скляні без металізації і з металізацією поверхні; керамічні без металізації і з металізацією поверхні);

- за розмірами: по довжині і ширині (малих розмірів – до 5 мм ; середніх розмірів – від 5 до 30 мм ; крупних розмірів – від 30 до 60 мм); по товщині (тонкі – до 3 мм ; середні – від 3 до 8 мм ; товсті – більше 8 мм);

- за формою поверхні (плоскі; з мікрорельєфом; опуклі; ввігнуті);

- за способом обробки (без оплавлення поверхні; з оплавленням поверхні).

Сукупність цих ознак буде визначати вимоги до джерел енергії, електронно-променевої гармати, систем попереднього нагріву і охолодження виробів, систем керування потужністю електронного потоку.

В залежності від форми і матеріалу виробу ці параметри можуть змінюватись у широкому діапазоні значень. При виборі обладнання необхідно оцінити ступінь його універсальності для отримання найбільшого техніко-економічного ефекту від його впровадження. Це можливо при оптимальній відповідності обладнання технологічним і економічним вимогам. Перші визначаються вищезгаданими характеристиками виробів та відповідними параметрами обробки. Інші вимоги визначаються необхідною якістю виробу (R_a ; R_z ; $h_{\text{пр}}$; p ; σ_p ; $\sigma_{\text{ст}}$ та інші) і його серійністю.

Для порівняння варіантів вакуумного обладнання з урахуванням технологічних і техніко-економічних особливостей, які виникають у конкретних ситуаціях, недостатньо відомих критеріїв, тому виникла необхідність доповнити їх показниками ефективності і техніко-економічними критеріями [12, 13]:

- $P_{\text{пр}} = \Sigma T_n / S_{\text{обр}}$, нормогодини/см² – питома трудомісткість процесу електронно-променевої обробки;

- $P_m = \Sigma C_m / S_{\text{обр}}$, грн/см² – питома матеріалоемність процесу електронно-променевої обробки;

- $C = \Sigma C_i / S_{\text{обр}}$, грн/см² – собівартість процесу електронно-променевої обробки;

- $P_k = \Sigma C_k / S_{\text{обр}}$, грн/см² – питомі капіталовкладення;

- $A = 1 - t_n / t_{\text{обр.с}}$ – критерій адаптивності обладнання,

- де t_n – час налагодження обладнання під електронно-променеву обробку серійного типорозміру виробу, $t_{\text{обр.с}}$ – час обробки всієї серії;

- $\text{Ш} = 1 - t_{\text{доп}} / t_{\text{обр}}$ – критерій швидкодії обладнання,

- де $t_{\text{доп}}$ – час на допоміжні операції; $t_{\text{обр}}$ – час на обробку;

- $\Gamma = 1 - t_r / t_{zm}$ – критерій готовності обладнання,

- де t_r – термін часу для приведення обладнання у робочий стан після повного відключення, t_{zm} – термін часу повної робочої зміни;

- $P_W = W_i / W_{i+1}$ – критерій точності регулювання потужності джерела енергії,

- де i – ступень регулювання;

- $P_{ww} = 1 - W_{\min} / W_{\max}$ – критерій діапазону потужності джерела енергії;

- $P_s = S_{n1} / S_{n1+1}$ – критерій точності регулювання площі нагріву під електронно-променевим потоком;

- $Y = \{ R_a; R_z; h_{пр}; n; \sigma_p; \sigma_{ст} \}$ – критерій якості виробів після електронно-променевої обробки, який може бути виражено абсолютним або питомим показником шорсткості поверхні, глибиною проплавлення, показником заломлення, напруженнями стиснення або розтягнення у матеріалі після термічної обробки;

- ΔG_{01} – критерій активності оточуючого середовища, який приймає два значення: 0 – при негативній дії середовища та 1 – при забезпеченні захисту матеріалів при обробці;

- $\eta_{теп}$ – критерій ефективності повної теплової обробки оптичних матеріалів (електронно-променевою гарматою і у термопечах при нагріві і охолодженні).

Одержані дані за результатами промислових і експериментальних порівнянь ефективності різних джерел енергії дозволяють сформулювати вимоги до оптимального джерела енергії при поверхневій мікрообробці оптичних матеріалів наступним чином:

- джерело нагріву повинно бути стрічковим, рухомим і повинно забезпечувати локальний нагрів оптичних матеріалів з точним регулюванням площі і форми технологічної зони нагріву матеріалу;

- параметри, що регулюються, повинні змінюватися у межах 2...4 порядків;

- загальна похибка джерела по інтенсивності у технологічній зоні повинна складати величину не більшу за 1%.

Висновки: за результатами проведених досліджень можна зробити висновки:

1. Сукупність ознак, що стосуються ступені вакууму в технологічній установці, лінійних розмірів та температурних режимів роботи катоду дозволяє визначати вимоги до джерел енергії, електронно-променевої гармати, систем попереднього нагріву і охолодження виробів, систем керування потужністю елект-

ронного потоку, а значить і оптимізувати режими електронно-променевої мікрообробки виробів малих розмірів (10...1000 мкм) з оптичних матеріалів.

2. Отримані критерії слід використовувати разом з аналізом особливостей поверхонь і приповерхневих шарів оброблених матеріалів.

3. Одержані дані за результатами промислових і експериментальних порівнянь ефективності різних джерел енергії дозволяють сформулювати вимоги до оптимального джерела енергії при поверхневій мікрообробці оптичних матеріалів наступним чином:

- джерело нагріву повинно бути стрічковим, рухомим і повинно забезпечувати локальний нагрів оптичних матеріалів з точним (0.5%) регулюванням площі і форми технологічної зони нагріву матеріалу;

- параметри, що регулюються, повинні змінюватися у межах 2...4 порядків;

- загальна похибка джерела по інтенсивності у технологічній зоні повинна складати величину не більшу за 1%.

Список літератури

1. <https://hi-tech.ua/mirovoy-ryinok-smartfonov-vyiros-pri-etom-dolya-samsung-i-apple-snizilas/>
2. <https://deps.ua/novosti/item/optychni-razvetviteli-v-setjah-dostupa.html>
3. https://itc.ua/articles/kremnievaya_fotonika_kak_alternativa_mednym_vnutrennim_soedineniyam_25541/
4. Канашевич Г. В. Фізичні явища і механізми за якими змінюється поверхня і поверхневий шар оптичного матеріалу від дії електронного потоку. *Збірник наукових праць Харківського університету Повітряних Сил*. 2014. №1. С. 184–189.
5. Канашевич Г. В. Термоелектричний вплив низькоенергетичного електронного потоку на дефектний шар оптичного скла. *Вісник НТУУ «КПІ», Серія Приладобудування*. Вип. 45. С. 123–130.
6. Оптика та оптичні прилади ДСТУ ISO 10110-1:2004 – ДСТУ ISO 10110-14:2004 [Чинний від 25-10-01]. – К.: Держспоживстандарт України, 2006. – IV, 231 с. – (Національний стандарт України)
7. Greenwod J., Dobre G. An optical pressures ensor for an aeronautical application using white light interferometry *Proc. SPIE*. 2000. Vol. 4075. P. 94–100.

8. Optomechatronic systems. *Proc. SPIE*. 2001. Vol. 4190. 350 p.
9. Канашевич Г. В. Термічна електронно-променева обробка скляних плат оптичних інтегральних схем: монографія. Укр. Деп. в ННІ ТЭХІМ, Черкаси, 2002. 165 с.
10. Канашевич Г. В. Технологічні умови і показники ефективності спеціальної електронно-променевої обробки поверхні оптичного скла. *Процеси механічної обробки в машинобудуванні: зб. наук. праць*. Житомир: ЖДТУ, 2013. Вип. 14. С. 62–74.
11. Канашевич Г. В., Щерба А. І., Дробот І. В. Алгоритм керування якістю поверхневого шару оптичних матеріалів при електронно-променевої мікрообробці. *Вісник національного технічного університету «Харківський політехнічний інститут» Тематичний випуск «Математичне моделювання в техніці та технологіях»*. 2012. Вип. 27. С. 231–239.
12. Шепелев А. Г., Юрченко Л. Д., Редкокаша А. П. Анализ информационных потоков по функциональным покрытиям на стеклах. *Сборник докладов Международного научно-практического симпозиума "Функциональные покрытия на стеклах"*. Харьков: ННЦ ХФТИ, "Константа", 2003. С. 8–10.
13. Григорович И. М., Мрочек Ж. А., Фигурин Б. Л., Селифанов С. О., Селифанов В. И., Рулинский В. И., Ресенчук В. В. Установка вакуумно-плазменной металлизации и пайки керамических изоляторов "Сапфир-10". *Электронная обработка материалов*. 1991. № 1.
5. Kanashkevych, H. V. (2013) The thermoelectric effect of low-energy electron beam to the defective layer optical glass. *Vestnik NTUU "KPI" series Instrument Series*. Vol. 45. P. 123–130.
6. Optics and optical instruments DSTU ISO 10110-1: 2004 - DSTU ISO 10110-14: 2004 [Effective from 25-10-01]. К.: Derzhspozhyvstandart of Ukraine, 2006. IV, 231 p. (National Standard of Ukraine)
7. Greenwood, J., Dobre, G. (2000) An optical pressures ensor for an aeronautical application using white light interferometry. *Proc. SPIE*. Vol. 4075. P. 94–100.
8. Optomechatronic systems. *Proc. SPIE*. 2001. Vol. 4190. 350 p.
9. Kanashkevych, H. V. (2002) Thermal electron-beam processing of glass fiber optic integrated circuits. Monograph. Ukr Dep. in the Research Institute of TEKHIM, Cherkasy. 165 p.
10. Kanashkevych, H. V. (2013) Technological conditions and indicators of the efficiency of special electron beam treatment of optical glass surface. *Processes of mechanical processing in mechanical engineering: Sb. sciences works*. Zhytomyr: ZHDТУ. Ed. 14, P. 62–74.
11. Kanashkevych, G. V., Shcherba, A. I., Drobot I. V. (2012) Algorithm for controlling the quality of the surface layer of optical materials under electron-beam microprocessing. *Bulletin of the National Technical University "Kharkiv Polytechnic Institute" Thematic issue "Mathematical modeling in technology and technologies"*. Vol. 27. P. 231–239.
12. Shepelev, A. G., Yurchenko, L. D., Radkoxa, A. P. (2003) Analysis of Information Flows on Functional Coatings on Glasses. *Collection of reports of the International Scientific and Practical Symposium "Functional coatings on glasses"*. Kharkov: NSC KhPTI, "Constant". P. 8–10.
13. Grigorovich, I. M., Mrochev, J. A., Figurin, B. L., Selifanov, S. O., Selifanov, V. I., Rulinsky, V. I., Reshenchuk, V. V. Installation of vacuum-plasma metallization and soldering of ceramic insulators "Sapphire-10". *Electronic processing of materials*. 1991. № 1.

References

1. <https://hi-tech.ua/mirovoy-ryinok-smartfonov-vyiros-pri-etom-dolya-samsung-i-apple-snizilas/>
2. <https://deps.ua/novosti/item/optychni-razvetviteli-v-setjah-dostupa.html>
3. https://itc.ua/articles/kremnievaya_fotonika_kak_alternativa_mednym_vnutrennim_soedeneniyam_25541/
4. Kanashkevych, H. V. (2014) Physical phenomena and mechanisms on which the surface and surface layer of the optical material change from the action of the electronic stream. *Collection of scientific*

M. V. Holub, *lecturer*

S. M., Bryk, *master*

V. M. Harasiuta, *master*

V. I. Savchenko, *master*

O. Yu. Sandyha, *master*

Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine

TECHNICAL, TECHNOLOGICAL CONDITIONS AND TECHNO-ECONOMIC CRITERIA OF ELECTRON-BEAM MICROPROCESSING OF OPTICAL PRODUCTS OF SMALL SIZES

The article presents the technical, technological conditions and techno-economic criteria of electron-beam microprocessing of optical products of small sizes (up to $1 \cdot 10^{-3}$ m). The linear dimensions and temperature modes of the cathode can determine the requirements for energy sources, electron beam gun, preheating and cooling systems, power control systems for electronic flow, and thus optimize the modes of electron beam microprocessing of small size products. The heating source must be mobile and provide local heating of the surface of the optical material with an accuracy of 0.5%, and the regulated parameters must vary within 2... 4 orders.

Keywords: *electronic flow, electron beam processing (microprocessing), optical glass, glass surface layer, microoptics, integral optics, MOMS, MOEMS.*

Рецензенти *Канашиевич Г.В., д.т.н., професор,
Поздєєв С.В., д.т.н., професор.*

Т. О. Прокопенко, д.т.н., доцент

e-mail: t.prokopenko@chdtu.edu.ua

Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна

ІМІТАЦІЙНА МОДЕЛЬ ПРИЙНЯТТЯ РІШЕНЬ В УПРАВЛІННІ ОРГАНІЗАЦІЙНО-ТЕХНОЛОГІЧНИМИ ОБ'ЄКТАМИ

В статті розглядається питання розробки імітаційної моделі прийняття рішень в управлінні організаційно-технологічними об'єктами та комплексами. Сучасний темп змін та розвитку технологій вимагає застосування адекватних методологій дослідження в режимі реального часу. На основі застосування мультиагентного підходу, автором запропонована імітаційна модель, що надасть можливості прогнозу динаміки досягнення цілей, динаміки зміни показників ефективності при прийнятті відповідного управлінського рішення та виборі на основі цього оптимального рішення.

Ключові слова: організаційно-технологічний об'єкт, прийняття рішень, імітаційна модель, мультиагентний підхід.

Вступ. Сучасні підприємства, корпорації, об'єднання в різних галузях промисловості характеризуються багатовимірністю, складністю організаційної та виробничої структури, наявністю та зміною багатьох цілей, активністю, нестаціонарністю технологічних процесів, необхідністю забезпечення мінімальних втрат цільового продукту при жорстких обмеженнях на енергоносії, не детермінованістю. Тісний взаємозв'язок організаційних та технологічних процесів, їх взаємна інтеграція, організація інноваційної діяльності, інтелектуальне керування виробничими процесами дає можливість розглядати сучасні виробництва як організаційно-технологічні об'єкти та комплекси [1]. Прийняття рішень в управлінні такими об'єктами має базуватись на комплексному поєднанні формалізованих методів, інтелектуальних методів та евристичних способів на основі оцінювання теперішнього стану та прогнозування майбутнього з врахуванням впливу факторів зовнішнього середовища та ризиків.

Такі властивості організаційно-технологічних об'єктів як наявність підсистем, що пов'язані між собою складними структурними та функціональними відношеннями; ієрархічна структура, що обумовлена існуванням глобальної цілі та локальних цілей підсистем; необхідність адаптації до зміни внутрішніх умов функціонування та зовнішнього середовища; велика розмірність задачі управління, залежність від якості сировини та навантажень, що характеризується виробничими

ситуаціями ускладнюють прийняття управлінських рішень в режимі реального часу. Тому для підвищення ефективності управління складними організаційно-технологічними об'єктами, особливо в умовах невизначеності та ризиків, доцільними є застосування комплексних методів та підходів, що нададуть можливості не тільки обробки значного обсягу інформації в режимі реального часу, а також автоматизованого управління певними процесами, але й прийняття рішень з врахуванням поточного стану, майбутніх перспектив та ризиків.

Аналіз останніх досліджень та публікацій. В управлінні організаційно-технологічними об'єктами актуальним є об'єднання всіх функцій управління та створення гнучких систем з елементами штучного інтелекту, які дозволяють оперативно здійснювати оцінку ефективності підприємства, планування і управління виробництвом, планування та управління матеріальними потоками, логістичний аналіз, розрахунок та аналіз собівартості продукції; а також планувати стратегічну діяльність в умовах невизначеності та ризиків.

Моделі прийняття рішень в управлінні організаційними, організаційно-технічними (технологічними) об'єктами та комплексами досліджуються в роботах вітчизняних та зарубіжних вчених. Так, в роботах [2, 3] вітчизняних вчених Ладанюка А.П., Українця А.І., Кишенько В.Д. та зарубіжних вчених A. Chochowski, I. Chernyshenko та ін. досліджу-

ється питання управління організаційно-технологічними процесами, зокрема біотехнологічними, на основі застосування методів ситуаційного аналізу та сценарного підходу. При цьому розглядається система моделей, що описує процеси зміни параметрів та умов функціонування біотехнологічних процесів, дискретно фіксуючи принципи з точки зору розробника системи управління біотехнологічними процесами моменти переходу на новий якісний рівень функціонування та режимів роботи. В роботі [4] вітчизняних вчених Грабовського Г.Г., Богаєнко І.М., Архангельського В.І. прийняття рішень в управлінні організаційно-технологічними об'єктами досліджено з точки зору інтегрованого підходу в управлінні залежно від ситуації з використанням об'єктивної інформації, що надходить та оброблюється в темпі протікання процесів. Робота [5] зарубіжних вчених Большакова О.А. та ін. присвячена дослідженню організаційно-технічних систем на основі застосування комбінованого інтелектуального методу. В роботі [6] прийняття управлінських рішень в організаційно-технічних системах досліджується на основі нечітких множин та нечіткої логіки. В роботі [7] описуються моделі прийняття рішень в управлінні організаційними системами на основі математичної теорії, теорії ігор, теорії активних систем.

Однак, для організаційно-технологічних об'єктів в процесі прийняття управлінських рішень важливим є врахування факторів швидкої зміни обставин, коли необхідно охопити великий обсяг інформації, що надходить, порівняти її з інформацією, яка вже є, врахувати досвід минулого, розібратися в різних ситуаціях, втрутитись в хід реалізації управлінського рішення [8]. Тобто важливого значення набуває фактор реального часу.

Метою даної статті є обґрунтування та дослідження імітаційної моделі прийняття рішень в управлінні організаційно-технологічними об'єктами, що базується та застосовує мультиагентного підходу, та забезпечить можливість визначення подальших перспектив з врахуванням поточного стану.

Викладення основного матеріалу дослідження. Швидкість і адекватність прийняття рішень в управлінні організаційно-технологічними об'єктами, а також їх реалізація в умовах зросту складності процесів

управління викликає необхідність використання сучасних методів управління, в тому числі інтелектуальних. Організаційно-технологічні процеси характеризуються та контролюються сотнями параметрів та показників, що впливають на ефективність управлінського рішення. Тому моделювання прийняття рішення та прогнозування результатів не певний інтервал часу доцільно реалізувати на основі застосування мультиагентного підходу, що поєднує досягнення системного аналізу і програмування та штучного інтелекту [9]. Така імітаційна модель є досить гнучкою та надасть можливості прийняття рішення з врахуванням фактору часу, оцінювати результати дій та використовувати різні варіанти сценаріїв рішень для досягнення різних цілей, що забезпечить підвищення ефективності організаційно-технологічного об'єкту.

В основі імітаційної моделі прийняття рішення на основі мультиагентного підходу є взаємодія агентів, що представляють собою організаційну та технологічну підсистеми, які характеризуються вхідними каналами, на які надходять ресурси (фінансові, інформаційні, матеріальні, енергетичні, людські та ін.), та вихідними каналами, що видають результати її роботи (продукцію) [10].

Модель агента задається наступними елементами:

- структурою цілей;
- структурою рішень;
- структурою показників ефективності.

Кожна структура задається за допомогою графів, вершини яких відповідають параметрам агента, а ребра – відносинам на множині параметрів (рис. 1–3).

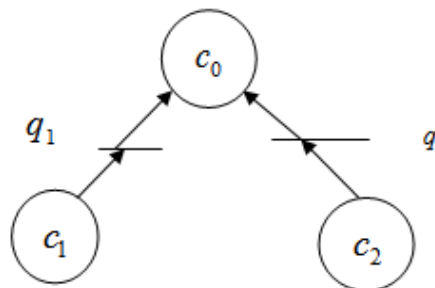


Рис. 1. Граф цілей

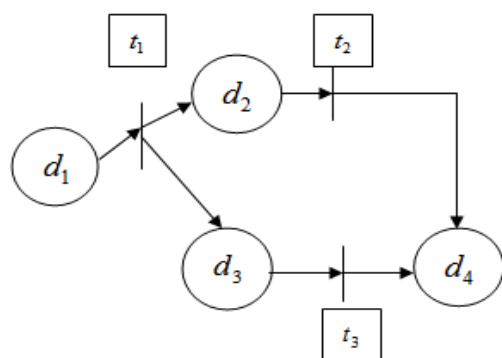


Рис. 2. Граф рішень

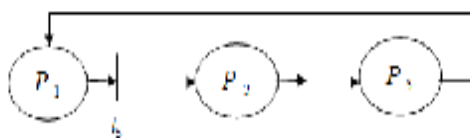


Рис. 3. Граф показників ефективності

Мультиагентна імітаційна модель прийняття рішень в управлінні організаційно-технологічними об'єктами представляє собою множину взаємопов'язаних агентів, діяльність яких може координуватися у часі, причому в певні моменти часу агенти можуть передавати один одному ресурси. Результатом індивідуальної діяльності агентів є досягнення певних колективних цілей і певна динаміка колективних показників. Мультиагентна система характеризується інтегральними цілями та показниками. Для технологічної складової організаційно-технологічних об'єктів такими цілями є максимізація кількості виготовленої продукції (C_0), максимізація коефіцієнту виробництва (C_1), мінімізація тривалості виробництва (C_2). В якості показників ефективності виступають показники кількості виготовленої продукції (P_1), коефіцієнт виробництва (P_2), тривалість виробництва (P_3). Процеси $d_1 \dots d_4$ характеризують рішення, що спрямовані на досягнення цілей C_i , результат виконання яких характеризується показниками ефективності P_i .

Імітаційне моделювання прийняття рішення реалізовано наступним чином. Здаються для кожного агента графові моделі цілей, рішень показників (рис. 1-3).

Вершини графа цілей відповідають цілям c_i , що з'єднані ребрами з переходами q_j . C_0 – інтегральна ціль для агента, що зображено на рис.1. Вершини c_i і переходи q_j складають комбінацію $c_i q_j$, що відповідає ребру та має певний номер, так наприклад номер 1 відповідає парі $q_1 c_1$. В позицію C_0 ведуть вхідні ребра 1 і 2.

Вершини графа рішень d_k відповідають певним рішенням, що повинні бути реалізовані для досягнення цілей c_i . Переходи t_n вказують на реалізацію відповідного рішення (рис. 2).

Вершини графа показників P_i відповідають показникам ефективності технологічної складової організаційно-технологічного об'єкту. Переходи r_m визначають можливе досягнення відповідних показників (рис. 3).

В кожен момент часу агент виконує дії, згідно наступного алгоритму:

Крок 1. Послідовно перевіряє умови для всіх продукційних правил переходів графів цілей, рішень і показників (з врахуванням свого стану та зовнішніх впливів).

Крок 2. Для тих продукційних правил "ЯК-ЩО.., ТО..", умови яких виконані, оператор обчислює і знаходить значення вихідних змінних (досягнення цілей, реалізація рішень, бальні значення показників ефективності та оцінку стану об'єкта управління при прийнятті певного рішення).

Крок 3. Виконує дії і оновлює поточні параметри стану. При цьому агент інформує систему як про свою нормальну поведінку, так і про порушення функціонування, які можуть виникнути: якщо виявлено момент часу, в який не виконується умова ні для одного переходу; при суперечливості, якщо деякому параметру в один і той же момент присвоюються різні значення; при виході параметра за межі допустимого для цього інтервалу значень.

Імітаційне моделювання дало можливість на першому кроці сформулювати рядок символів (позицій і переходів) у вигляді букв із нижніми індексами. На другому кроці розставляються стрілки, на третьому вводяться номери стрілок.

На рис. 4 показана схема взаємодії графів цілей, рішень, показників ефективності при прийнятті певного рішення, де стрілками

с, d, P позначено впливи кожного з трьох графів на два інших, стрілки V відповідають впливам подій зовнішнього середовища.

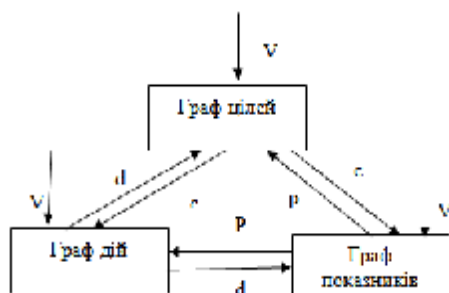


Рис. 4. Схема взаємодії графів цілей, рішень, показників ефективності

Моделювання динаміки індивідуального і колективного функціонування агента при прийнятті управлінського рішення реалізується на основі індикаторних виразів, у тому числі шляхом встановлення міжагентних часових і ресурсних зв'язків.

Динаміка прийняття рішення при імітаційному моделюванні визначається динамікою внутрішньої поведінки агентів і динамікою їх зовнішньої поведінки – взаємодій між агентами, а також агентами й зовнішнім середовищем, на заданому інтервалі дискретної часової шкали $\tau = 0, 1, \dots, N$. При цьому зміна параметрів (досягнення цілей, зміна рішень, зміна величини показників ефективності) відбувається в моменти спрацьовування вершин-переходів графа, а значення параметрів у проміжку між спрацьовуванням переходів фіксується у вершинах-позиціях. Переходи позначено продукційними правилами – виразами виду «ЯКЩО (виконання умови), ТО (реалізація оператора)», де умова й оператор описуються логічними формулами (ЛФ). Продукційні правила такого типу, зіставлені переходам графа відповідають логічним виразам та описуються формулами причинно-наслідкового зв'язку ЛФ1→ЛФ2.

Індикатор дорівнює 1, якщо співвідношення # виконується, і рівний 0, якщо не виконується. ЛФ формується на базі індикаторів шляхом застосування до них логічних операцій кон'юнкції, диз'юнкції, заперечення. Перехід графа спрацьовує в момент τ , якщо у відповідному йому індикаторному виразі ЛФ1 = 1. У результаті в момент $\tau+1$ буде виконува-

тися співвідношення ЛФ2=1, що ініціює реалізацію оператора переходу.

Так, наприклад вираз для переходу t_1 графа рішень і переходу t_5 графа показників ефективності агента має вигляд:

$$F(t_1): (d_1 = 1) \wedge (v = 0) \rightarrow (d_2 = 1) \wedge (d_3 = 1), \quad (1)$$

де v – булева змінна, що відповідає зовнішньому впливу,

$$F(t_5): (P_1(\tau) > 7) \rightarrow (P_1(\tau + 1) = P_1(\tau) - 1) \vee (P_2(\tau + 1) = P_2(\tau) - 1), \quad (2)$$

де значення показників представлене функцією дискретного часу τ . Оператор індикаторного виразу (1) при настанні моменту $\tau + 1$ зменшує на одиницю значення показників P_1 , P_2 у момент τ .

В результаті імітаційного моделювання можливо два варіанта імітаційного експерименту: або доходимо до кінцевого моменту часового інтервалу моделювання, не зустрічаючи порушень у поведінці агента, або фіксуємо порушення, наприклад:

не виявлено момент, коли не виконується умова ні для одного переходу;
суперечливість, якщо деякій змінній в один і той же момент привласнюються різні значення;
вихід змінної за межі припустимого для неї інтервалу значень.

При виявленні вищевказаних, а можливо й інших порушень у діяльності агентів здійснюється корегування комплексної моделі (керування моделлю) на рівні графів та індикаторних виразів. Далі цикл «імітаційне моделювання – управління» повторюється й т.д.

Висновки. Розглянутий підхід до побудови імітаційної моделі дає можливість розробки інформаційної технології прийняття рішень в управлінні організаційно-технологічними об'єктами. Організаційно-технологічний об'єкт представлено як множину взаємодіючих агентів зі своїми індивідуальними цілями, рішеннями і показниками ефективності, що у процесі прийняття рішення орієнтовані на досягнення інтегральних (колективних) цілей і характеризується інтегральними показниками. Взаємодії агентів при прийнятті рішення відбуваються у формі передачі ресурсу або/і інформаційних потоків. Взаємодії залежать від внутрішньої ситуації й

впливу зовнішнього середовища, і носять нерегулярний (випадковий) характер. Дана технологія дає можливість оцінити ефективність організаційно-технологічного об'єкту при прийнятті рішення, що забезпечує прийняття оптимального управлінського рішення.

Список літератури

1. Прокопенко Т. О., Ладанюк А. П. Інформаційні технології управління організаційно-технологічними системами: монографія. Черкаси: Вертикаль, видавець Кандич С.Г., 2015. 224 с.
2. Ладанюк А. П., Українець А. І., Кишенько В. Д. Управління автоматизованими технологічними комплексами харчових виробництва на основі сценарного підходу. *Автоматика. Автоматизация. Электро-технические комплексы и системы*. 2008. №2. С. 187–196.
3. Chochowski A., Chernyshenko I., Kozys-kyi V., Kyshenko V. Innovative energy-saving technologies in biotechnological objects control. K.: Tsentr Uchbovoi Literatyr, 2014. 240 p.
4. Архангельский В. И., Грабовский Г. Г., Рюшин Н. А., Богаенко И. В. Интегрированное управление производством: организационные и технологические аспекты менеджмента предприятиями. К.: «Техніка», 2005. 328 с.
5. Интеллектуальные системы управления организационно-техническими системами / под. ред. А.А. Большакова. М.: Горячая линия-Телеком, 2006. 160 с.
6. Борисов В. В., Сысков В. В. Мультиагентное моделирование сложных организационно-технических систем в условиях противоборства. *Информационные технологии*. 2012. № 4. С. 7–14.
7. Novikov D., Ashimov A., Sultanov B., Adilov Z., Borovskiy Y., Alshanov R., Ashimov A. Macroeconomic Analysis and Parametric Control of a National Economy. New York: Springer, 2013. 288 p.
8. Прокопенко Т.О., Куліш В.І. Моделювання оцінювання впливів факторів на показники ефективності організаційно-технологічних об'єктів з врахуванням сезонності виробництва. *Технологический аудит и резервы производства*. 2015. №6/6 (26). С. 15–17.
9. Юдицкий С.А. Моделирование динамики многоагентных триадных сетей. М.: СИНТЕГ, 2012. 112 с.

10. Прокопенко Т.А., Ладанюк А.П. Информационная модель управления технологическими комплексами непрерывного типа в классе организационно-технических систем. *Международный научно-технический журнал «Проблемы управления и информатики»*. 2014. №5. С. 64–70.

References

1. Prokopenko, T. O., Ladanyuk, A. P. (2015) Information technology management organizational and technological systems. Cherkasy: Vertical, publisher Kandych S. G., 224 p. [in Ukrainian].
2. Ladajuk, A. P., Ukrainian, A. I., Kishenko V. D. (2008) Management of automated technological complexes of food production on the basis of scenario approach. *Automatics. Automation. Electro-technical complexes and systems*, 2. pp.187–196 [in Ukrainian].
3. Chochowski, A., Chernyshenko, I., Kozys-kyi, V., Kyshenko, V. (2014) Innovative energy-saving technologies in biotechnological objects control. K.: Tsentr Uchbovoi Literatyr, 240 p. [in English].
4. Arkhangelsk, V. I., Bohaenko I. V., Grabowski, G. G., Ryumshyn, N. A. (2005) Yntehryrovannoe Production Management: Organizational and Technological aspects of enterprise management. K.: «Tekhnika». 328 p. [in Russian].
5. Bolshakov, A. A. (2006) Intellectual systems of management of organizational and technical systems. M.: Hot line-Telecom, 160 p. [in Russian].
6. Borisov, V. V., Syskov, V. V. (2012) Multiagent modeling of complex organizational and technical systems in the context of confrontation. *Information technology*, 4, pp.7–14.
7. Novikov, D., Ashimov, A., Sultanov, B., Adilov, Z., Borovskiy, Y., Alshanov, R., Ashimov, A. (2013) Macroeconomic Analysis and Parametric Control of a National Economy. New York: Springer, 288 p. [in English].
8. Prokopenko, T., Kulish, V. (2015) Modeling of estimation of factors influence on indicators of efficiency of organizational and technological objects taking into account seaso-

- ality of production. *Technological audit and production reserves*. 6/6 (26), pp. 15 – 17. [in Ukrainian].
9. Yuditsky, S. A. (2012) Modeling the dynamics of multi-agent triad networks. M.: SYNTHET, 112 p. [in Russian].
10. Prokopenko, T. O. (2014). Information model of control of the continuous type technological complexes in the class of organizational and technical systems. *Journal of Automation and Information*, 5, pp. 64–70 [in Russian].

T. O. Prokopenko, Dr.Tech.Sc, associate professor,
t.prokopenko@chdtu.edu.ua
Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine

IMMIGRATIONAL MODEL OF DECISION-MAKING IN MANAGEMENT BY ORGANIZATIONAL AND TECHNOLOGICAL OBJECTS

The article discusses the main question of the development of a simulation model for decision making in the management of organizational and technological objects and complexes. The current pace of change and technology development requires the use of adequate research methodologies in real time. Decision-making in the management of organizational and technological objects should be based on an integrated combination of formalized methods, intellectual methods and heuristic methods. To increase the efficiency of managing complex organizational and technological facilities, especially in conditions of uncertainty and risks, it is expedient to use complex methods and approaches. This will ensure the processing of a significant amount of information in real time, automated management of certain processes, decision making taking into account the current state, future prospects and risks. The author applied the multi-agent approach. The simulation model provides a forecast of the dynamics of achievement of goals, dynamics of changes in performance indicators when making the appropriate managerial decision. On the basis of the simulation model we implement the choice of the optimal solution.

This approach is recommended for application in the development of automated control systems for technological complexes of continuous type, including at enterprises, corporations of chemical, food, and other industries. Research results can also be applied in decision support systems for sugar industry enterprises.

Keywords: organizational and technological object, decision-making, imitation model, multi-agent approach.

Статтю представляє Т. О. Прокопенко, д.т.н., доцент.

О. М. Панаско, к.т.н., доцент,
e-mail: lena.pa@ukr.net

М. В. Хроленко, магістр з інформаційної безпеки,
e-mail: mkhrolenko@gmail.com

Черкаський державний технологічний університет,
б-р Шевченка, 460, м. Черкаси, 18006, Україна

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПАРОЛІВ КОРИСТУВАЧІВ В ПРОЦЕДУРАХ АУТЕНТИФІКАЦІЇ

Стаття присвячена дослідженню підходу щодо забезпечення захисту паролів користувачів, які відіграють визначальну роль при реалізації процедур аутентифікації, авторизації та аудиту систем захисту із використанням до парольної інформації хешування із додаванням так званої «солі» – рядка випадкових даних, який подається на вхід хеш-функції одночасно із вихідними даними. Проведено аналіз відомих способів атак на систему аутентифікації, що пов'язані із отриманням паролів при зламі системи за їх хеш-значеннями, до яких, зокрема, відносяться метод повного перебору (bruteforce), пошук за словником, застосування спеціальних структур даних – таблиць пошуку, різних їх модифікацій, зокрема, зворотніх таблиць пошуку, а також таких, що відомі як «rainbow» таблиці. Зважаючи на сучасні інформаційно-технічні можливості, повністю запобігти зазначеним атакам неможливо, але при цьому є доцільним впливати на те, щоб значно знижувати їх ефективність. На основі проведеного аналізу розглядається напрямок, що здатний забезпечити захист паролів користувачів внаслідок ускладнення відновлення вихідних паролів за їх хеш-значеннями за попередньо сформованими «rainbow» таблицями, який ґрунтується на використанні хешування із додаванням до пароля так званої «солі».

Ключові слова: аутентифікація, авторизація, системи захисту, пароль користувача, хешування, «rainbow» таблиці, застосування «солі».

Постановка проблеми. В еру інформаційних технологій та зростання ролі всесвітньої павутини для сучасного суспільства дуже гостро постає питання забезпечення захисту даних, що обумовлюють ідентифікацію користувача та відповідно перевірку та підтвердження прав його доступу до системи, даних та функцій (аутентифікація та авторизація).

Отримання доступу до системи є результатом представлення користувачем відповідних даних, зокрема, імені користувача та пароля, що являє собою секретне слово або певну послідовність символів, призначену для підтвердження особи або її прав. Сформований користувачем пароль в подальшому зберігається в системі і наразі постає питання доцільності зберігання пароля у відкритому – незахищеному вигляді, оскільки це обумовлює зловмиснику можливість отримати несанкціонований доступ до системи. В даній статті досліджується аспект зберігання паролів у хешованому вигляді з використанням так званої «солі», що на сьогоднішній день вважається розповсюдженим способом під-

вищення надійності збереження паролів та їх захисту.

Аналіз останніх досліджень і публікацій.

Дослідження в галузі забезпечення захисту інформації в комп'ютерних системах та мережах характеризуються надзвичайною актуальністю на сьогоднішній день. В цьому контексті слід відзначити роботи М.В. Гайворонського, В.С. Галатенка, О.М. Новікова, А.Ю. Щеглова та інших. Одним із загальноприйнятих підходів до забезпечення безпеки інформаційних ресурсів є виконання базових технічних вимог, що повинні бути впроваджені при розробці систем захисту: аутентифікації, авторизації та аудиту. В літературі цей підхід відомий як «Концепція трьох «А»». Будь-яка ефективна система захисту інформаційних ресурсів повинна мати відповідні засоби для реалізації зазначених процедур [1,2,4,5]. Важливим аспектом захисту інформації в комп'ютерних мережах є реалізація основних криптографічних алгоритмів для шифрування файлів та паролів [1]. Для пере-

дачі та зберігання паролів використовують шифрування із застосуванням хешування. Аналіз наукових джерел дозволяє стверджувати про різноманітність сфер застосування процедури хешування інформації, зокрема, при обчисленні контрольних сум від даних з метою подальшого виявлення в них помилок, при побудові асоціативних масивів, при пошуку дублікатів в серіях наборів даних, при реалізації електронного підпису, а також при зберіганні паролів інформації в системах захисту у вигляді хеш-коду тощо. Протягом останніх років здійснюється потужна робота з приводу розробки нових, а також вдосконаленню існуючих методів криптографічного хешування. В цьому напрямку слід відзначити роботи Лукецького В. А. та Баришева Ю. В., Бойка А. О. та Горбенка І. Д. Значний внесок у розвиток алгоритмів хешування також внесли Д. Кнут, У. Пітерсон та Ханс Петер Лун.

Метою даної роботи є дослідження підходу щодо забезпечення захисту паролів користувачів в процедурах аутентифікації на основі застосування хешування із додаванням

додаткового значення, так званої «солі», що здатний знизити ефективність відомих методів отримання паролів за їх хеш-значеннями.

Виклад основного матеріалу. Термін хешування пов'язаний із процедурою перетворення вхідного масиву даних довільної довжини у вихідний бітовий рядок фіксованої довжини. Це дає змогу зберігати паролі користувачів в системі чи на сервері в захешованому вигляді, що ускладнює можливість злоумисникам отримати несанкціонований доступ до даних, функцій чи програм.

Для процедури хешування використовуються хеш-функції, які будуються за ітеративною схемою, коли вихідне повідомлення розбивається на блоки певного розміру M_i , а над ними виконуються ряд перетворень з використанням як зворотних, так і незворотних операцій. На вхід кожного циклу хешування подається вихід попереднього циклу, а також черговий блок повідомлення, тобто $h_i = f(M_i, h_{i-1})$ (рис.1).



Рис. 1. Отримання хеш-значення

Розрізняють криптографічні та некриптографічні хеш-функції. Слід зазначити, що криптографічні функції хешування забезпечують дотримання наступних вимог:

– якщо відоме значення хеш-функції h , процес знаходження повідомлення M такого, що $H(M) = h$, повинен бути обчислювально складним;

– при заданому повідомленні M процес знаходження іншого повідомлення M' , такого, що $H(M) = H(M')$, повинен бути обчислювально складним [2].

Важливою особливістю хеш-функцій є те, що вони не допускають зворотного перетворення, що полягає в неможливості отримання вихідного повідомлення за його дайджестом (хеш-значенням). При зломі системи існує потенційна загроза викрадення паролів, що вимагає використання криптостійких хеш-функцій для зберігання паролів користувачів, якщо злоумисником ініційовано атаку на сис-

тему аутентифікації. До найрозповсюдженіших криптостійких хеш-функцій можна віднести, зокрема, SHA256, SHA512, RipeMD та WHIRLPOOL. Вибір тієї чи іншої хеш-функції визначається специфікою задачі, що розв'язується.

Для перевірки коректності введеного пароля система реалізує порівняння між паролем, що був збереженим при реєстрації користувача, а також введеним під час процедури аутентифікації користувача. Для протидії загрозі несанкціонованого доступу, внаслідок того, що ідентичні рядки даних мають однакові хеш-значення, існує можливість перевірки на відповідність збереженого хеш-значення пароля користувача та згенерованого хеш-значення, що відповідає введеному паролю.

Внаслідок цього при реєстрації, коли вводиться ім'я користувача (логін) та пароль, останній хешується та зберігається відповідно в системі чи на сервері. Під час процедури

аутентифікації користувача до введеного пароля застосовують процедуру хешування і порівняння із збереженим хеш-значенням, що відповідає введеному логіну. Користувач отримує доступ до системи (авторизується) у випадку збіжності хеш-значень.

Застосування хешування унеможливає визначення оригінального пароля для зломника і водночас надає можливість порівняння отриманого хеш-значення, що зберігається в системі, з хеш значенням введеного пароля користувача в процедурі аутентифікації. Внаслідок цього не можна стверджувати, що застосування криптографічних хеш-функцій для пароля користувача забезпечить його абсолютний захист.

Хоча хеш-функція і є односторонньою і відповідно неможливо провести зворотню хешуванню операцію та відновити вихідні дані, це не виключає здатність отримати необхідні дані іншим способом з урахуванням сучасних технологічних можливостей. З цього приводу можна навести бази даних, що сформовані з хеш-значень поширених слів і коротких фраз. Крім того прості паролі можна визначити за допомогою процедури повного перебору (bruteforce) або перебору за словником. Не слід виключати і можливість застосування пошукової системи для пошуку за хеш значенням – ввівши хеш-значення, з'являється ймовірність дізнатись відкритий пароль із напрацьованих на сьогоднішній день онлайн баз даних, в яких зберігаються хеші [3].

До відомих способів отримання паролів за їх хеш-значеннями, зокрема, належать:

- пошук хеш-значення за так званими «rainbow» (веселковими) таблицями – базами даних, де накопичуються заздалегідь визначені хеші для будь-яких можливих рядків;

- метод грубої сили (bruteforce), що полягає у переборі всіх можливих комбінацій символів і їхньому хешуванні доти, поки не отримано відповідне хеш-значення;

- пошук за словником, який подібний до попереднього способу, але для нього є характерним обмеження процедури перебору за рахунок того, що розглядаються не всі можливі комбінації символів, а їхня підмножина – всього декілька тисяч найпопулярніших паролів вигляду «qwerty», «asdf», «123», «password» та ін.

Найтривіальніший спосіб зламати хеш-код – це спробувати вгадати пароль, обчис-

люючи хеш-код для кожного з можливих варіантів і перевіряючи на збіжність отриманого хеш-коду із тим, що потрібно зламати.

Атака за словником заснована на використанні файлу, який представлено словами, фразами, поширеними паролями та іншими рядками, які з певною ймовірністю можуть бути використаними в якості пароля. Кожне слово в файлі захешовано з метою подальшого порівняння його хеш-значення із хеш-значенням пароля. Зазвичай, файли словників побудовані на основі «добування» слів з великих масивів тексту або з реальних баз даних паролів.

Сутність атаки повним перебором полягає у переборі всіх можливих комбінацій символів заданої довжини. Ці атаки вимагають дуже великих обчислювальних витрат, і, зазвичай, вони найменш ефективні за показником числа зламаних хеш-кодів по відношенню до часу виконання, а втім врешті-решт вони завжди знаходять пароль. В цілому, оскільки неможливо повністю запобігти атакам за словником або атакам повним перебором, доцільно намагатися знижувати їхню ефективність.

Достатньо оптимальним методом для дуже швидкого злому великої кількості хеш-кодів одного типу є застосування таблиць пошуку, в яких заздалегідь обчислені хеш-значення паролів зі словника паролів зберігаються в спеціальних структурах даних – таблицях пошуку. Особливість способу організації таблиць пошуку обумовлює високу швидкість процедури пошуку хеш-кодів.

Зворотні таблиці пошуку дозволяють зломисникові застосувати атаку за словником або повним перебором до багатьох хеш-кодів одночасно без наявності попередньо обчисленої таблиці пошуку. Спочатку зломисник створює таблицю пошуку, яка зіставляє кожен хеш-код пароля з скомпрометованої бази даних для користувача зі списком користувачів, які мали цей хеш-код, а потім – отримує хеш-значення кожного передбачуваного пароля і використовує таблицю пошуку для формування списку користувачів, чий пароль був визначений. Зазвичай кілька користувачів мають один і той же пароль, а тому цей вид атак особливо ефективний.

Найкращими таблицями пошуку вважаються «rainbow» таблиці, які набагато ефективніші за звичайні та зворотні таблиці пошуку, оскільки займають набагато менше

пам'яті при своїй побудові. «Rainbow» таблиці – це заздалегідь визначений набір даних, який містить хеш-функції, що відповідають множині комбінацій символів. Структура таблиць дозволяє дуже швидко знаходити відповідний пароль за відомим значенням хеш-функції. В основу механізму створення «rainbow» таблиць покладено побудову ланцюжків можливих паролів, початок яких – це певний випадковий пароль фіксованої довжини, а в середині – поперемінне застосування хеш-функції та функції редукції [7].

З огляду на можливість отримання відкритого пароля за його хеш-значенням за вище описаними методами, а також враховуючи сучасні інформаційно-технічні можливості доцільно зазначити, що для забезпечення захисту паролів користувачів від пошуку за «веселковими» таблицями для процедури хешування рекомендується використовувати деяку додаткову комбінацію символів, так звану «сіль» (salt) [3,6,8].

У криптографії з цим поняттям пов'язано рядок випадкових даних, який подається на вхід хеш-функції разом з вихідними даними, і зазвичай використовується для

подовження рядка пароля, що значно ускладнює відновлення вихідних паролів за допомогою попередньо побудованих «веселкових» таблиць. Слід відзначити, що «сіль» при цьому не здатна захистити від повного перебору для кожного пароля окремо – все залежить лише від затраченого для отримання потрібного результату часу. «Сіль» збільшить час підбору, що в свою чергу призведе до підвищення криптостійкості хеш-коду. Зберігати «сіль» обов'язково потрібно поруч з хеш-значенням, в якому її було додано до пароля, для подальшої перевірки вірності пароля при аутентифікації користувача. Для забезпечення унікальності кожного конкретного пароля «сіль» слід генерувати за допомогою генератора випадкових чисел.

Використання «солі» характеризується динамічністю: навіть при використанні двох однакових паролів із додаванням випадково згенерованої «солі» їхні хеш-значення будуть різні. Окресливши переваги використання «солі» доцільно розглянути механізм формування паролю користувача при реєстрації в системі на основі хешування із додаванням «солі» (рис.2).

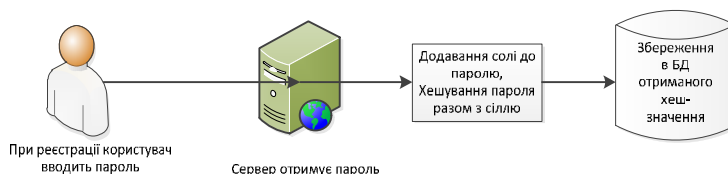


Рис. 2. Схема реєстрації користувача з використанням «солі» під час хешування

Наведений на рис.2 схемі реєстрації користувача відповідають окремі фрагменти програмних реалізацій мовою програмування C#.

Після введення користувачем імені та пароля для реєстрації відбувається генерація випадкової «солі»:

```

public string doSalt() {
    Random rnd = new Random();
    string salt = rnd.Next()
        .ToString();
    return salt;
}
  
```

Згенерована «сіль» додається до введеного користувачем пароля:

```

string saltPassw=password+doSalt();
  
```

В даному фрагменті password являє собою змінну, в яку записується пароль, а doSalt() – метод генерації «солі».

Виконання хешування пароля з «сіллю» відбувається на основі методу doHash(), який виконує процедуру хешування за допомогою алгоритму SHA512:

```

doHash(soltPassw);
public string doHash(string passw) {
    byte[] HashValue;
    byte[] password =
        System.Text.Encoding.UTF8
            .GetBytes(passw);
    SHA512 SHhash = new
        SHA512Managed();
    HashValue = Shhash
        .ComputeHash(password);
    string s =
        System.Text.Encoding
            .UTF8.GetString(
                HashValue, 0,
                HashValue.Length)
  }
  
```

В результаті формується рядок, який відповідає захешованому пароллю з «сіллю».

```
string hashPassw = doHash(soltPassw);
```

Отримане хеш-значення записується разом з відкритою «сіллю» та іменем користувача (в даному прикладі в базі даних MongoDB).

```
var client =
new MongoClient(
    "mongodb://localhost:27017");
var dbUsers = client.GetDatabase(
    "users");
var userData =
```

```
dbUsers.GetCollection<UserInfo>(
    "userData");
userData.InsertOne(uInfo);
```

В наведеному фрагменті `userData` являє собою об'єкт типу `UserInfo`, в якому зберігається ім'я користувача, отримане хеш-значення та «сіль».

Коли в подальшому користувачу потрібно повторно надавати свої ім'я та пароль, процедура аутентифікації відбуватиметься відповідно до блок-схеми (рис.3):

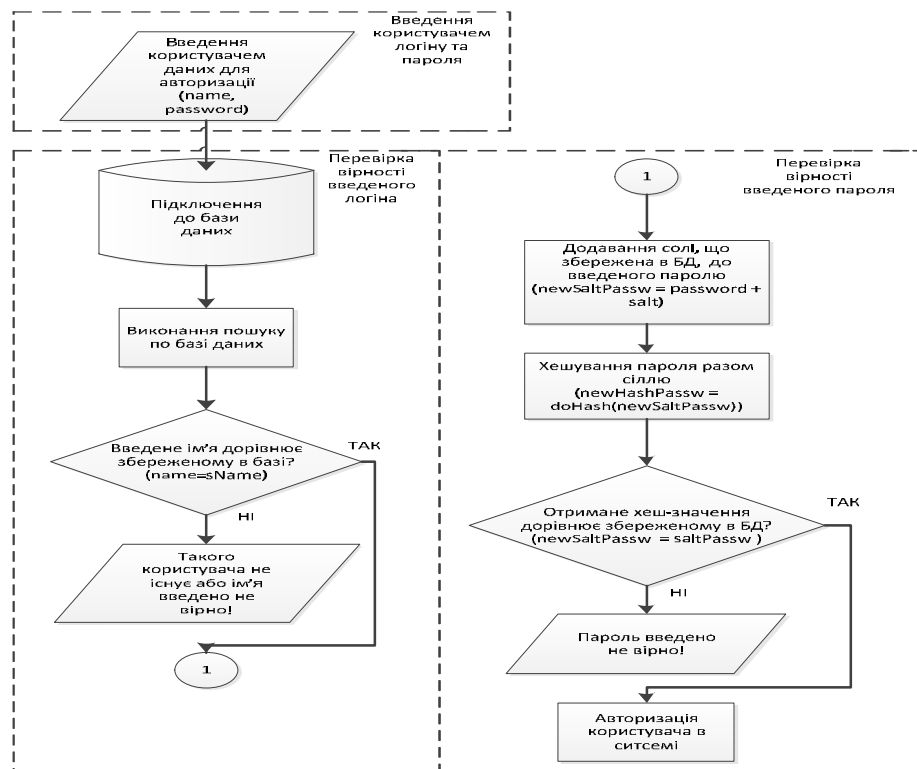


Рис. 3. Блок-схема процедури аутентифікації користувача

Після введення користувачем логіну та пароля відбувається перевірка вірності введеного пароля:

```
public void FindUsers(
    string userName, string pasw){
var client =
new MongoClient(
    "mongodb://localhost:27017");
var dbUsers =
    client.GetDatabase("users");
var userData =
    dbUsers.GetCollection<UserInfo>
        ("userData");
```

Відбувається пошук в базі даних (БД) інформації користувача за його іменем – захешованих пароля та «солі» та відкритої «солі»:

```
var filter1 = Builders<UserInfo>
    .Filter.Eq(
        c => c.Name,
        userName);
var users = userData.Find(filter1)
    .ToList();
```

До введеного пароля додається збережена в базі «сіль» та виконується процедура хешування (для знайденого запису користувача):

```
foreach (var doc1 in users){
    string paswSalt = pasw + doc1.Salt;
    Hashing hashPasw = new Hashing();
    String hashP = hashPasw.doHash(
        paswSalt);
}
```

Після отримання хеш-значення виконується пошук в БД об'єкта, захешовані пароль

з «сіллю» якого рівні попередньо отриманому хеш-значенню. Навіть якщо у різних користувачів паролі будуть однаковими, програма знайде лише одного користувача з ідентичними згенерованим хеш-значенням та збереженим, оскільки «сіль» у кожного користувача різна.

```
var filter2 = Builders<UserInfo>
    .Filter.Eq(c => c.Passw, hashP);
var usersPasw = usersData
    .Find(filter2).ToList();
foreach (var doc2 in usersPasw) {
    MessageBox.Show(doc2.Name +
        " Вас авторизовано!");
}
```

Користувача буде успішно авторизовано при знайденій відповідності в БД згенерованого хеш-значення та збереженого при реєстрації для введеного імені користувача. Це демонструє відповідний фрагмент програмної реалізації, в якому для введених даних (userName та password) за допомогою методу FindUsers() шукаються ідентичні ім'я та пароль в БД:

```
string userName = NewUser;
string password = password12345;
MongoDB mdb = new MongoDB();
mdb.FindUsers(userName, password);
```

В цілому, використання випадкової «солі», яка є унікальною для кожного користувача, забезпечить захист паролів користувачів в процедурах аутентифікації від атак на основі використання «rainbow» таблиць, оскільки кожному паролю відповідатиме своя унікальна «сіль» і це в свою чергу обумовить необхідність генерування зловмисником значної кількості окремих веселкових таблиць, що з практичної точки зору вважається недоцільним. Генерація «солі» не потребує затрат часу та додаткових ресурсів системи, порівняно із відомим методом подвійного хешування. Внаслідок того, що «сіль» можна зберігати у відкритому вигляді, процедура аутентифікації не передбачає додаткових витрат на маніпуляції з нею. В результаті для підвищення надійності збереження паролів користувачів та забезпечення їхнього захисту вважається доцільним проводити хешування із використанням додаткового значення – «солі».

Висновки. В процесі даного дослідження розглянуто підхід щодо забезпечення захисту паролів користувачів в процедурах аутентифікації на основі використання хешу-

вання із додаванням унікального параметру, так званої «солі», що в результаті проведення аналізу основних методів отримання паролів за їх хеш-значеннями здатно знизити ефективність застосування зазначених методів, зокрема, за попередньо сформованими «rainbow» таблицями.

Список літератури

1. Шнайер Б. Прикладная криптография: протоколы, алгоритмы и исходные тексты на языке Си. 2-е изд. Москва: Триумф, 2002. 688 с.
2. Горбенко И. Д. Функции хеширования. Понятия, требования, классификация, свойства и применение. *Радиоэлектроника и информатика*. 1998. № 1. С. 64–69.
3. «Соленое» хеширование паролей: делаем правильно. URL: http://www.internet-technologies.ru/articles/article_1807.html.
4. Чунарьова А. В. Аналіз існуючих шаблонів систем автентифікації в інформаційно-комунікаційних системах та мережах. *Безпека інформації*. 2012. № 2. С. 65–70.
5. Єсіна М. В., Горбенко І. Д. Багатофакторна аутентифікація: використання механізмів двофакторної автентифікації для захисту від несанкціонованого доступу. *Комп'ютерное моделирование в наукоемких технологиях (КМНТ-2014): труды научно-технической конференции с международным участием*, 28–31 мая 2014 г. Харьков: Харьк. нац. ун-т им. В. Н. Каразина, 2014. С. 159–162.
6. Хэширование паролей. URL: <http://phpfaq.ru/tech/ hashing>.
7. Словарные атаки на хэш-функции. URL: <http://www.panasenko.ru/articles/168/168.html>.
8. Pritesh N. A., Jigisha K., Paresh V. Cryptography Application using Salt Hash Technique. *International Journal of Application or Innovation in Engineering & Management*. 2013. № 6. С. 236–239.

References

1. Shnayer, B. (2002) Applied Cryptography: Protocols, Algorithms, and Source Code in C. Moscow: Triumf, 2002, 610 p.
2. Gorbenko, I. D. (1998) Hashing functions. Concepts, requirements, classification, properties and applications. *Radyoelektronika y unformatyka*, No. 1, pp. 64–69.

3. "Salty" hashing of passwords: we do it right. URL: http://www.internet-technologies.ru/articles/article_1807.html.
4. Chunarova, A. V. (2012) Analysis of existing patterns of authentication systems in information and communication systems and networks. *Bezpeka informatsii*, No. 2, pp. 65–70.
5. Yesina, M. V., Horbenko, I. D. (2014) Multi-factor Authentication: Using two-factor authentication mechanisms to protect against unauthorized access. *Kompyuternoe modelirovanie v naukoemkikh tekhnologiyah (KMNT-2014): Trudy nauchno- tekhnicheskoy konferentsii s mezhdunarodnyim uchastiem*, 28-31
6. Password hashing. URL: <http://phpfaq.ru/tech/hashing>.
7. Dictionary attacks on hash functions. URL: <http://www.panasenko.ru/articles/168/168.html>.
8. Pritesh, N. A, Jigisha, K., Paresh, V. (2013) Cryptography Application using Salt Hash Technique. *International Journal of Application or Innovation in Engineering & Management*, No. 6, pp. 236–239.

O. M. Panasko, *Ph.D., associate professor*,
e-mail: lena.pa@ukr.net,

M. V. Khrolenko, *Master in cybersecurity*
e-mail: mkhrolenko@gmail.com

Cherkassy State Technological University,
Shevchenko blvd., 460, Cherkassy, 18006, Ukraine

PROVISION OF USER PASSWORDS PROTECTION IN AUTHENTICATION PROCEDURES

The article is devoted to the study of the approach to ensuring the user passwords protection, which play a decisive role in the implementation of authentication, authorization and audit security systems of using password-based hashing with the addition of so-called "salt" – a string of random data that is submitted to the input of hash functions simultaneously with source data. The analysis of known methods of attack on the authentication system, which is associated with the receipt of passwords for their hash values, which include, in particular, the bruteforce method, dictionary search, the use of special data structures - search tables, various modifications, in particular, "rainbow" tables is shown in this article. Given the current information and technical capabilities, it is not possible to completely prevent these attacks, but it is advisable to reduce their effectiveness. On the basis of the analysis, a direction is considered that can provide protection of user passwords due to the difficulty of restoring output passwords on their hash values for pre-formed "rainbow" tables, which is based on the use of hashing with the additional value which is known as "salt".

Keywords: authentication, authorization, protection systems, user password, hashing, "rainbow" tables, Salt Hash Technique.

Статтю представляє О. М. Панаско, к.т.н., доцент

С. В. Сисоєнко¹, асистент

кафедри інформаційної безпеки та комп'ютерної інженерії,

e-mail: s.sysoienko@gmail.com,

О. Г. Мельник², к.т.н., ст. наук. співробітник,

доцент кафедри будівельних конструкцій,

e-mail: melnyk.olja.2014@gmail.com,

М. О. Пустовіт², старший викладач

кафедри техніки та засобів цивільного захисту,

e-mail: m.pustovit@gmail.com.

¹ Черкаський державний технологічний університет

б-р Шевченка, 460, м. Черкаси, 18006, Україна

² Черкаський інститут пожежної безпеки імені Героїв Чорнобиля

Національного університету цивільного захисту України

вул. Онопрієнка, 8, м. Черкаси, 18034, Україна

СИНТЕЗ ОПЕРАЦІЙ ОБЕРНЕНОГО ГРУПОВОГО МАТРИЧНОГО КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ

Одним із способів удосконалення існуючих та побудови нових систем захисту інформації є пошук та використання нових функцій криптографічного перетворення інформації. На сьогодні не достатньо вивчені операції оберненого групового матричного криптографічного перетворення інформації, що можуть застосовуватися для реалізації криптографічного кодування даних. В роботі досліджено можливість синтезу операцій оберненого перетворення на основі пошуку обернених групових та не групових дворозрядних операцій. Шляхом перебору даних перетворень знайдено алгоритм побудови оберненого групового криптографічного перетворення. За результатами досліджень формалізовано модель прямого та оберненого двохоперандного групового криптографічного перетворення. Запропонована модель забезпечує спрощення знаходження оберненого криптографічного перетворення, тому що для її реалізації необхідно знайти три обернених двохоперандних перетворення замість одного оберненого чотирьохперандного перетворення.

Ключові слова: криптографічне перетворення інформації, пряма та обернена операція, операція матричного перетворення, групові операції, коректність операції.

Актуальність дослідження. З кожним днем об'єм інформації, що обертається в телекомунікаційних мережах, збільшується в геометричній прогресії. При цьому вона потребує все більш кращого захисту від несанкціонованого доступу, що може призвести до її спотворення або викрадення [1]. Захист даних за допомогою методів криптографічного захисту інформації – одне з можливих рішень проблеми безпеки інформації [2].

Актуальним питанням сьогодення є вдосконалення існуючих та пошук нових функцій криптографічного перетворення інформації, що дозволять покращити властивості самих криптоалгоритмів та підвищити стійкість систем захисту інформації.

Вищевикладене зумовило актуальність досліджень, спрямованих на більш детальне дослідження операцій оберненого групового

матричного криптографічного перетворення інформації, що можуть застосовуватися для реалізації криптографічного кодування даних.

Аналіз останніх досліджень і публікацій. Серед останніх досліджень і публікацій варто виділити наукові праці, в яких досліджувався метод захисту інформаційних ресурсів на основі матричних операцій криптографічного перетворення [3-5]; в яких розглядалося питання підвищення якості псевдовипадкової послідовності [6, 7]; в яких доведено, що використання матричних операцій криптографічного перетворення в поєднанні з груповими операціями криптографічного перетворення забезпечує підвищення якості шифрування (отриманої псевдовипадкової послідовності), а також забезпечує можливість розшифрування інформації, тому що забезпечує використання умови отримання невироджено-

го перетворення [8], та роботу, в якій було вивчено питання підвищення стійкості комп'ютерних криптографічних алгоритмів за рахунок використання операцій криптоперетворення та алгоритмів криптографічного перетворення двох блоків змінних [9].

Проте в даних дослідженнях не достатньо вивчено питання щодо можливості синтезу операцій оберненого перетворення на основі пошуку обернених групових та не групових дворозрядних операцій.

Мета статті полягає в дослідженні можливості побудови оберненого групового криптографічного перетворення, якщо відоме пряме групове перетворення, та формалізації моделі прямого та оберненого двооперандного групового криптографічного перетворення.

Виклад основного матеріалу. Дослідимо можливість побудови оберненого групового криптографічного перетворення, якщо відоме пряме групове перетворення.

В [9] для перевірки невідродженості результатів виконання групових операцій криптографічного перетворення інформації використовували метод синтезу матричних операцій оберненого криптографічного перетворення.

Проте при використанні дворозрядних групових операцій відповідно до розглянутих прикладів необхідно знаходити чотирирозрядну матрицю оберненого перетворення. Дослідимо можливість синтезу операцій оберненого перетворення на основі пошуку обернених групових та не групових дворозрядних операцій. Знаходження даних закономірностей приведе до значного зменшення обчислювальної складності розшифрування інформації.

Для побудови оберненого групового криптографічного перетворення, якщо відоме пряме групове перетворення, використаємо прямі та обернені групові й не групові перетворення. Шляхом перебору даних перетворень знайдемо алгоритм побудови оберненого групового криптографічного перетворення, якщо він існує.

При проведенні досліджень необхідно розглянути наступні випадки:

1. Пряма та обернена групова операція співпадають, пряма та обернена не групові операції співпадають.

2. Пряма та обернена групова операція співпадають, пряма та обернена не групові операції не співпадають.

3. Пряма та обернена групова операція не співпадають, пряма та обернена не групові операції співпадають.

4. Пряма та обернена групова операція не співпадають, пряма та обернена не групові операції не співпадають.

Розглянемо перший випадок, коли пряма та обернена групова операція співпадають, пряма та обернена не групові операції співпадають.

$$\text{Нехай} \quad G = G_{3,6}^k = G_{3,6}^d,$$

$$F_1 = F_2 = F_{3,6}^k = F_{3,6}^d, \text{ тоді:}$$

$$G_{3,6}^k = \begin{bmatrix} F_1 \\ F_1 \oplus F_2 \end{bmatrix} = \begin{bmatrix} F_{3,6}^k(z_1) \\ F_{3,6}^k(z_1) \oplus F_{3,6}^k(z_2) \end{bmatrix} = \begin{bmatrix} z_{1,1} \\ z_{1,1} \oplus z_{1,2} \\ z_{1,1} \oplus z_{2,1} \\ z_{1,1} \oplus z_{1,2} \oplus z_{2,1} \oplus z_{2,2} \end{bmatrix}.$$

Тоді

$$G_{3,6}^d = \begin{bmatrix} F_1 \\ F_1 \oplus F_2 \end{bmatrix} = \begin{bmatrix} F_{3,6}^d(w_1) \\ F_{3,6}^d(w_1) \oplus F_{3,6}^d(w_2) \end{bmatrix} = \begin{bmatrix} w_{1,1} \\ w_{1,1} \oplus w_{1,2} \\ w_{1,1} \oplus w_{2,1} \\ w_{1,1} \oplus w_{1,2} \oplus w_{2,1} \oplus w_{2,2} \end{bmatrix}.$$

Підставивши результати прямого перетворення в операцію оберненого перетворення, отримаємо:

$$G_{3,6}^d = \begin{bmatrix} w_{1,1} \\ w_{1,1} \oplus w_{1,2} \\ w_{1,1} \oplus w_{2,1} \\ w_{1,1} \oplus w_{1,2} \oplus w_{2,1} \oplus w_{2,2} \end{bmatrix} = \begin{bmatrix} z_{1,1} \\ z_{1,1} \oplus z_{1,1} \oplus z_{1,2} \\ z_{1,1} \oplus z_{1,1} \oplus z_{2,1} \\ z_{1,1} \oplus z_{1,1} \oplus z_{1,2} \oplus z_{1,1} \oplus z_{2,1} \oplus z_{1,1} \oplus z_{1,2} \oplus z_{2,1} \oplus z_{2,2} \end{bmatrix} = \begin{bmatrix} z_{1,1} \\ z_{1,2} \\ z_{2,1} \\ z_{2,2} \end{bmatrix}.$$

Так як підтверджено коректність оберненої операції, то будуть справедливими наступні твердження.

Якщо $G_{3,6}^k = \begin{bmatrix} F_{3,6}^k(z_1) \\ F_{3,6}^k(z_1) \oplus F_{3,6}^k(z_2) \end{bmatrix}$, то

$$G_{3,6}^d = \begin{bmatrix} F_{3,6}^d(w_1) \\ F_{3,6}^d(w_1) \oplus F_{3,6}^d(w_2) \end{bmatrix}$$

або $G_{3,6}^d = \left(G_{3,6}^k = \begin{bmatrix} F_{3,6}^k(z_1) \\ F_{3,6}^k(z_1) \oplus F_{3,6}^k(z_2) \end{bmatrix} \right)$,

або $G_{3,6}^d = \left(G_{3,6}^k = \begin{bmatrix} F_{3,6}^d(w_1) \\ F_{3,6}^d(w_1) \oplus F_{3,6}^d(w_2) \end{bmatrix} \right)$,

або $G_{3,6}^d = \left(G_{3,6}^d = \begin{bmatrix} F_{3,6}^d(w_1) \\ F_{3,6}^d(w_1) \oplus F_{3,6}^d(w_2) \end{bmatrix} \right)$,

або $G_{3,6}^d = \left(G_{3,6}^d = \begin{bmatrix} F_{3,6}^k(z_1) \\ F_{3,6}^k(z_1) \oplus F_{3,6}^k(z_2) \end{bmatrix} \right)$,

або і т.п.

Виходячи з отриманого результату, можна констатувати, що при співпаданні прямого та оберненого перетворення для декодування інформації необхідно брати обернені (прямі) операції криптоперетворення та обернені (прямі) групові операції перетворення.

Нехай $G = G_{6,5}^k = G_{6,5}^d$, $F_1 = F_2 = F_{6,5}^k = F_{6,5}^d$.

$$G_{6,5}^k = \begin{bmatrix} F_1 \oplus F_2 \\ F_2 \end{bmatrix} = \begin{bmatrix} F_{6,5}^k(z_1) \oplus F_{6,5}^k(z_2) \\ F_{6,5}^k(z_2) \end{bmatrix} =$$

$$= \begin{bmatrix} z_{1,1} \oplus z_{1,2} \oplus z_{2,1} \oplus z_{2,2} \\ z_{1,2} \oplus z_{2,2} \\ z_{2,1} \oplus z_{2,2} \\ z_{2,2} \end{bmatrix}.$$

Тоді

$$G_{6,5}^d = \begin{bmatrix} F_1 \oplus F_2 \\ F_2 \end{bmatrix} = \begin{bmatrix} F_{6,5}^d(w_1) \oplus F_{6,5}^d(w_2) \\ F_{6,5}^d(w_2) \end{bmatrix} =$$

$$= \begin{bmatrix} w_{1,1} \oplus w_{1,2} \oplus w_{2,1} \oplus w_{2,2} \\ w_{1,2} \oplus w_{2,2} \\ w_{2,1} \oplus w_{2,2} \\ w_{2,2} \end{bmatrix}.$$

Підставивши результати прямого перетворення в операцію оберненого перетворення, отримаємо:

$$G_{6,5}^d = \begin{bmatrix} w_{1,1} \oplus w_{1,2} \oplus w_{2,1} \oplus w_{2,2} \\ w_{1,2} \oplus w_{2,2} \\ w_{2,1} \oplus w_{2,2} \\ w_{2,2} \end{bmatrix} =$$

$$= \begin{bmatrix} z_{1,1} \oplus z_{1,2} \oplus z_{2,1} \oplus z_{2,2} \oplus z_{1,2} \oplus z_{2,2} \oplus z_{2,1} \oplus z_{2,2} \oplus z_{2,2} \\ z_{1,2} \oplus z_{2,2} \oplus z_{2,2} \\ z_{2,1} \oplus z_{2,2} \oplus z_{2,2} \\ z_{2,2} \end{bmatrix} =$$

$$= \begin{bmatrix} z_{1,1} \\ z_{1,2} \\ z_{2,1} \\ z_{2,2} \end{bmatrix}.$$

Перевірка даного факту на повній множині симетричних операцій підтвердила коректність зробленого висновку.

Нехай $G = G_{6,5}^k = G_{6,5}^d$, $F_1 = F_{6,5}^k = F_{6,5}^d$, $F_2 = F_{3,6}^k = F_{3,6}^d$.

Тоді

$$G_{6,5}^k = \begin{bmatrix} F_1 \oplus F_2 \\ F_2 \end{bmatrix} = \begin{bmatrix} F_{6,5}^k(z_1) \oplus F_{3,6}^k(z_2) \\ F_{3,6}^k(z_2) \end{bmatrix} = \begin{bmatrix} z_{1,1} \oplus z_{1,2} \oplus z_{2,1} \\ z_{1,2} \oplus z_{2,1} \oplus z_{2,2} \\ z_{2,1} \\ z_{2,1} \oplus z_{2,2} \end{bmatrix}.$$

Тоді

$$G_{6,5}^d = \begin{bmatrix} F_1 \oplus F_2 \\ F_2 \end{bmatrix} = \begin{bmatrix} F_{6,5}^d(w_1) \oplus F_{3,6}^d(w_2) \\ F_{3,6}^d(w_2) \end{bmatrix} = \begin{bmatrix} w_{1,1} \oplus w_{1,2} \oplus w_{2,1} \\ w_{1,2} \oplus w_{2,1} \oplus w_{2,2} \\ w_{2,1} \\ w_{2,1} \oplus w_{2,2} \end{bmatrix}.$$

Підставивши результати прямого перетворення в операцію оберненого перетворення, отримаємо:

$$G_{6,5}^d = \begin{bmatrix} w_{1,1} \oplus w_{1,2} \oplus w_{2,1} \\ w_{1,2} \oplus w_{2,1} \oplus w_{2,2} \\ w_{2,1} \\ w_{2,1} \oplus w_{2,2} \end{bmatrix} =$$

$$= \begin{bmatrix} z_{1,1} \oplus z_{1,2} \oplus z_{2,1} \oplus z_{1,2} \oplus z_{2,1} \oplus z_{2,2} \oplus z_{2,1} \\ z_{1,2} \oplus z_{2,1} \oplus z_{2,2} \oplus z_{2,1} \oplus z_{2,1} \oplus z_{2,2} \\ z_{2,1} \\ z_{2,1} \oplus z_{2,1} \oplus z_{2,2} \end{bmatrix} =$$

$$= \begin{bmatrix} z_{1,1} \oplus z_{2,1} \oplus z_{2,2} \\ z_{1,2} \oplus z_{2,1} \\ z_{2,1} \\ z_{2,2} \end{bmatrix}.$$

Обернене перетворення побудовано за умови

$$G_{3,6}^d = \left(G_{3,6}^d = \begin{bmatrix} F_{6,5}^d(w_1) \oplus F_{3,6}^d(w_2) \\ F_{6,5}^d(w_1) \end{bmatrix} \right) \text{ не коректне.}$$

Отриманий не коректний результат можна розглядати як виняток з правила, робити висновок про хибність даного підходу можна лише тоді, коли буде повторно виявлено не коректність даного підходу.

Розглянемо другий випадок коли пряма та обернена групова операція співпадають, пряма та обернена не групові операції не співпадають.

$$\text{Нехай } G = G_{3,6}^k = G_{3,6}^d, \quad F_1 = F_{5,6}^k \neq F_{6,3}^d,$$

$$F_2 = F_{6,5}^k = F_{6,5}^d.$$

$$G_{3,6}^k = \begin{bmatrix} F_1 \\ F_1 \oplus F_2 \end{bmatrix} = \begin{bmatrix} F_{5,6}^k(z_1) \\ F_{5,6}^k(z_1) \oplus F_{6,5}^k(z_2) \end{bmatrix} = \begin{bmatrix} z_{1,2} \\ z_{1,1} \oplus z_{1,2} \\ z_{1,2} \oplus z_{2,1} \oplus z_{2,2} \\ z_{1,1} \oplus z_{1,2} \oplus z_{2,2} \end{bmatrix}.$$

Тоді

$$G_{3,6}^d = \begin{bmatrix} F_1 \\ F_1 \oplus F_2 \end{bmatrix} = \begin{bmatrix} F_{6,3}^d(w_1) \\ F_{6,3}^d(w_1) \oplus F_{6,5}^d(w_2) \end{bmatrix} = \begin{bmatrix} w_{1,1} \oplus w_{1,2} \\ w_{1,1} \\ w_{1,1} \oplus w_{1,2} \oplus w_{2,1} \oplus w_{2,2} \\ w_{1,1} \oplus w_{2,2} \end{bmatrix}.$$

Підставивши результати прямого перетворення в операцію оберненого перетворення, отримаємо:

$$G_{3,6}^d = \begin{bmatrix} w_{1,1} \oplus w_{1,2} \\ w_{1,1} \\ w_{1,1} \oplus w_{1,2} \oplus w_{2,1} \oplus w_{2,2} \\ w_{1,1} \oplus w_{2,2} \end{bmatrix} = \begin{bmatrix} z_{1,2} \oplus z_{1,1} \oplus z_{1,2} \\ z_{1,2} \\ z_{1,2} \oplus z_{1,1} \oplus z_{1,2} \oplus z_{1,2} \oplus z_{2,1} \oplus z_{2,2} \oplus z_{1,1} \oplus z_{1,2} \oplus z_{2,2} \\ z_{1,2} \oplus z_{1,1} \oplus z_{1,2} \oplus z_{2,2} \end{bmatrix} = \begin{bmatrix} z_{1,1} \\ z_{1,2} \\ z_{2,1} \\ z_{1,1} \oplus z_{2,2} \end{bmatrix}.$$

Обернене перетворення побудовано за умови

$$G_{3,6}^d = \left(G_{3,6}^d = \begin{bmatrix} F_{6,3}^d(w_1) \\ F_{6,3}^d(w_1) \oplus F_{6,5}^d(w_2) \end{bmatrix} \right) \text{ не коректне.}$$

Розглянемо можливість побудови оберненого групового перетворення на основі використання прямих і обернених перетворень. Так як $G_{3,6}^d = G_{3,6}^k$, то необхідно розглянути:

$$G_{3,6}^d = \left(G_{3,6}^d = \begin{bmatrix} F_{5,6}^k(z_1) \\ F_{5,6}^k(z_1) \oplus F_{6,5}^d(w_2) \end{bmatrix} \right).$$

$$G_{3,6}^d = \begin{bmatrix} F_1 \\ F_1 \oplus F_2 \end{bmatrix} = \begin{bmatrix} F_{5,6}^k(z_1) \\ F_{5,6}^k(z_1) \oplus F_{6,5}^d(w_2) \end{bmatrix} = \begin{bmatrix} w_{1,2} \\ w_{1,1} \oplus w_{1,2} \\ w_{1,2} \oplus w_{2,1} \oplus w_{2,2} \\ w_{1,1} \oplus w_{1,2} \oplus w_{2,2} \end{bmatrix} = \begin{bmatrix} z_{1,1} \oplus z_{1,2} \\ z_{1,2} \oplus z_{1,1} \oplus z_{1,2} \\ z_{1,1} \oplus z_{1,2} \oplus z_{1,2} \oplus z_{2,1} \oplus z_{2,2} \oplus z_{1,1} \oplus z_{1,2} \oplus z_{2,2} \\ z_{1,2} \oplus z_{1,1} \oplus z_{1,2} \oplus z_{1,1} \oplus z_{1,2} \oplus z_{2,2} \end{bmatrix} = \begin{bmatrix} z_{1,1} \oplus z_{1,2} \\ z_{1,1} \\ z_{2,1} \oplus z_{1,2} \\ z_{1,2} \oplus z_{2,2} \end{bmatrix}.$$

Обернене перетворення не коректне.

Дослідження можливості побудови оберненого групового перетворення на основі використання прямих і обернених перетворень для випадків:

$$G_{3,6}^d = \left(G_{3,6}^d = \begin{bmatrix} F_{6,3}^d(w_1) \\ F_{5,6}^k(z_1) \oplus F_{6,5}^d(z_2) \end{bmatrix} \right) \text{ та}$$

$$G_{3,6}^d = \left(G_{3,6}^d = \begin{bmatrix} F_{5,6}^k(z_1) \\ F_{6,3}^d(w_1) \oplus F_{6,5}^d(w_2) \end{bmatrix} \right),$$

також показали їх некоректність. Шляхом перебору прямих та обернених групових і не групових перетворень побудувати обернене групове криптографічне перетворення для всіх випадків не вдалося.

Спробуємо для відомого групового криптографічного перетворення по аналогії з [10] знайти обернене перетворення і привести його до оберненого групового криптографічного перетворення.

$$\text{Якщо } G = G_{3,6}^k = G_{3,6}^d, \quad F_1 = F_{6,5}^k = F_{6,5}^d, \\ F_2 = F_{5,6}^k \neq F_{6,3}^d.$$

$$G_{3,6}^k = \begin{bmatrix} F_1^k(z_1) \\ F_1^k(z_1) \oplus F_2^k(z_2) \end{bmatrix} = \begin{bmatrix} F_{6,5}^k(z_1) \\ F_{6,5}^k(z_1) \oplus F_{5,6}^k(z_2) \end{bmatrix} = \begin{bmatrix} z_{1,1} \oplus z_{1,2} \\ z_{1,2} \\ z_{1,1} \oplus z_{1,2} \oplus z_{2,2} \\ z_{1,2} \oplus z_{2,1} \oplus z_{2,2} \end{bmatrix}.$$

Тоді

$$G_{3,6}^d = \begin{bmatrix} w_{1,1} \oplus w_{1,2} \\ w_{1,2} \\ w_{1,1} \oplus w_{1,2} \oplus w_{2,1} \oplus w_{2,2} \\ w_{1,1} \oplus w_{2,1} \end{bmatrix} = \begin{bmatrix} F_{6,5}^d(w_1) \\ F_{6,3}^d(w_1) \oplus F_{6,3}^d(w_2) \end{bmatrix} = \\ = \begin{bmatrix} F_1^d(w_1) \\ F_2^d(w_1) \oplus F_2^d(w_2) \end{bmatrix}.$$

Перевіримо коректність отриманого оберненого перетворення:

$$G_{3,6}^d = \begin{bmatrix} F_1^d(w_1) \\ F_2^d(w_1) \oplus F_2^d(w_2) \end{bmatrix} = \begin{bmatrix} w_{1,1} \oplus w_{1,2} \\ w_{1,2} \\ w_{1,1} \oplus w_{1,2} \oplus w_{2,1} \oplus w_{2,2} \\ w_{1,1} \oplus w_{2,1} \end{bmatrix} = \\ = \begin{bmatrix} z_{1,1} \oplus z_{1,2} \oplus z_{1,2} \\ z_{1,2} \\ z_{1,1} \oplus z_{1,2} \oplus z_{1,2} \oplus z_{1,1} \oplus z_{1,2} \oplus z_{2,2} \oplus z_{1,2} \oplus z_{2,1} \oplus z_{2,2} \\ z_{1,1} \oplus z_{1,2} \oplus z_{1,1} \oplus z_{1,2} \oplus z_{2,2} \end{bmatrix} = \begin{bmatrix} z_{1,1} \\ z_{1,2} \\ z_{2,1} \\ z_{2,2} \end{bmatrix}.$$

Обернене перетворення отримано коректно.

Перевірка обернених перетворень для випадків:

$$1) \quad G = G_{3,6}^k = G_{3,6}^d, \quad F_1 = F_{5,6}^k \neq F_{6,3}^d,$$

$$F_2 = F_{6,5}^k = F_{6,5}^d;$$

$$2) \quad G = G_{3,6}^k = G_{3,6}^d, \quad F_1 = F_{5,6}^k \neq F_{6,3}^d,$$

$$F_2 = F_{6,3}^k \neq F_{5,6}^d \text{ також показала їх коректність.}$$

Розглянемо третій випадок, коли пряма та обернена групова операція не співпадають, пряма та обернена не групові операції співпадають.

$$\text{Нехай } G = G_{5,6}^k \neq G_{6,3}^d, \quad F_1 = F_{6,5}^k = F_{6,5}^d, \\ F_2 = F_{3,6}^k = F_{3,6}^d.$$

$$G_{5,6}^k = \begin{bmatrix} F_2^k(z_2) \\ F_1^k(z_1) \oplus F_2^k(z_2) \end{bmatrix} = \begin{bmatrix} F_{3,6}^k(z_2) \\ F_{6,5}^k(z_1) \oplus F_{3,6}^k(z_2) \end{bmatrix} = \\ = \begin{bmatrix} z_{2,1} \\ z_{2,1} \oplus z_{2,2} \\ z_{1,1} \oplus z_{1,2} \oplus z_{2,1} \\ z_{1,2} \oplus z_{2,1} \oplus z_{2,2} \end{bmatrix}.$$

Тоді

$$G_{6,3}^d = \begin{bmatrix} w_{1,1} \oplus w_{1,2} \oplus w_{2,1} \oplus w_{2,2} \\ w_{1,2} \oplus w_{2,2} \\ w_{1,1} \\ w_{1,1} \oplus w_{1,2} \end{bmatrix} = \begin{bmatrix} F_{6,5}^d(w_1) \oplus F_{6,5}^d(w_2) \\ F_{3,6}^d(w_1) \end{bmatrix} = \\ = \begin{bmatrix} F_1^d(w_1) \oplus F_1^d(w_2) \\ F_2^d(w_1) \end{bmatrix}.$$

Перевіримо коректність отриманого оберненого перетворення:

$$G_{6,3}^d = \begin{bmatrix} F_1^d(w_1) \oplus F_1^d(w_2) \\ F_2^d(w_1) \end{bmatrix} = \begin{bmatrix} w_{1,1} \oplus w_{1,2} \oplus w_{2,1} \oplus w_{2,2} \\ w_{1,2} \oplus w_{2,2} \\ w_{1,1} \\ w_{1,1} \oplus w_{1,2} \end{bmatrix} = \\ = \begin{bmatrix} z_{2,1} \oplus z_{2,1} \oplus z_{2,2} \oplus z_{1,1} \oplus z_{1,2} \oplus z_{2,1} \oplus z_{1,2} \oplus z_{2,1} \oplus z_{2,2} \\ z_{2,1} \oplus z_{2,2} \oplus z_{1,2} \oplus z_{2,1} \oplus z_{2,2} \\ z_{2,1} \\ z_{2,1} \oplus z_{2,1} \oplus z_{2,2} \end{bmatrix} = \begin{bmatrix} z_{1,1} \\ z_{1,2} \\ z_{2,1} \\ z_{2,2} \end{bmatrix}.$$

Обернене перетворення отримано коректно.

Перевірка оберненого перетворення для випадку: $G = G_{6,3}^k \neq G_{5,6}^d$, $F_1 = F_{3,6}^k = F_{3,6}^d$,

$$F_2 = F_{6,5}^k = F_{6,5}^d \text{ також показала його коректність.}$$

Розглянемо четвертий випадок, коли пряма та обернена групова операція не співпадають, пряма та обернена не групові операції не співпадають.

$$\text{Нехай } G = G_{5,6}^k \neq G_{6,3}^d, \quad F_1 = F_{6,3}^k \neq F_{5,6}^d, \\ F_2 = F_{5,6}^k \neq F_{6,3}^d.$$

$$G_{5,6}^k = \begin{bmatrix} F_2^k(z_2) \\ F_1^k(z_1) \oplus F_2^k(z_2) \end{bmatrix} = \begin{bmatrix} F_{5,6}^k(z_2) \\ F_{6,3}^k(z_1) \oplus F_{5,6}^k(z_2) \end{bmatrix} = \\ = \begin{bmatrix} z_{2,2} \\ z_{2,1} \oplus z_{2,2} \\ z_{1,1} \oplus z_{1,2} \oplus z_{2,2} \\ z_{1,1} \oplus z_{2,1} \oplus z_{2,2} \end{bmatrix}.$$

Тоді

$$G_{6,3}^d = \begin{bmatrix} w_{1,2} \oplus w_{2,2} \\ w_{1,1} \oplus w_{1,2} \oplus w_{2,1} \oplus w_{2,2} \\ w_{1,1} \oplus w_{1,2} \\ w_{1,1} \end{bmatrix} = \begin{bmatrix} F_{5,6}^d(w_1) \oplus F_{5,6}^d(w_2) \\ F_{6,3}^d(w_1) \end{bmatrix} = \\ = \begin{bmatrix} F_1^d(w_1) \oplus F_1^d(w_2) \\ F_2^d(w_1) \end{bmatrix}.$$

Перевіримо коректність отриманого оберненого перетворення:

$$G_{6,3}^d = \begin{bmatrix} F_1^d(w_1) \oplus F_1^d(w_2) \\ F_2^d(w_1) \end{bmatrix} = \begin{bmatrix} w_{1,2} \oplus w_{2,2} \\ w_{1,1} \oplus w_{1,2} \oplus w_{2,1} \oplus w_{2,2} \\ w_{1,1} \oplus w_{1,2} \\ w_{1,1} \end{bmatrix} = \\ = \begin{bmatrix} z_{2,1} \oplus z_{2,2} \oplus z_{1,1} \oplus z_{2,1} \oplus z_{2,2} \\ z_{2,2} \oplus z_{2,1} \oplus z_{2,2} \oplus z_{1,1} \oplus z_{1,2} \oplus z_{2,2} \oplus z_{1,1} \oplus z_{2,1} \oplus z_{2,2} \\ z_{2,2} \oplus z_{2,1} \oplus z_{2,2} \\ z_{2,2} \end{bmatrix} = \begin{bmatrix} z_{1,1} \\ z_{1,2} \\ z_{2,1} \\ z_{2,2} \end{bmatrix}.$$

Обернене перетворення отримано коректно.

Дослідження оберненого перетворення для випадку: $G = G_{5,6}^k \neq G_{6,3}^d$, $F_1 = F_{5,6}^k \neq F_{6,3}^d$, $F_2 = F_{6,3}^k \neq F_{5,6}^d$ також показало його коректність.

Отримані результати дозволяють узагальнити результати дослідження та формалізувати модель прямого та оберненого двохоперандного групового криптографічного перетворення.

$$\text{Якщо } G^k = \begin{pmatrix} a_{11}F_1^k(z_1) \oplus a_{12}F_2^k(z_2) \\ a_{21}F_1^k(z_1) \oplus a_{22}F_2^k(z_2) \end{pmatrix},$$

$$\text{тоді } G^d = \begin{pmatrix} b_{11}F_1^d(w_{1+k}) \oplus b_{12}F_1^d(w_{2+k}) \\ b_{21}F_2^d(w_{1+k}) \oplus b_{22}F_2^d(w_{2+k}) \end{pmatrix},$$

де $a_{ij} \in [0,1]$ – коефіцієнти матриці прямого групового криптографічного перетворення; $b_{ij} \in [0,1]$ – коефіцієнти матриці оберненого групового криптографічного перетворення; F_i^k – операції не групових двохоперандних криптографічних перетворень; F_i^d – операції обернених не групових двохоперандних криптографічних перетворень; $\oplus$ – операція «сума за mod 2»; k – коефіцієнт вибору аргумента функції: $w_i = \begin{cases} w_i & \text{якщо } k = 0 \\ w_j & \text{якщо } k = 1 \end{cases}$ за умови, що $j \neq i$. I, j – номер аргументу, а коефіцієнт визначено з: $k = \begin{cases} 0 & \text{якщо } G^k = G^d \\ 1 & \text{якщо } G^k \neq G^d \end{cases}$.

Висновок. Запропонована модель забезпечує спрощення знаходження оберненого криптографічного перетворення, тому що для її реалізації необхідно знайти три обернених двохоперандних перетворення замість одного оберненого чотирихоперандного перетворення.

Список літератури

1. Богуш В. М., Юдін О. К. Інформаційна безпека держави. Київ : МК-Прес, 2005. 432 с.
2. Рудницький В. Н., Мильчевич В. Я., Бабенко В. Г., Мельник Р. П., Рудницький С. В., Мельник О. Г. Криптографическое кодирование: методы и средства

- реализации (часть 2) : монография. Краснодар, 2014. 224 с.
3. Рудницький В. М., Бабенко В. Г., Рудницький С. В. Метод синтезу матричних моделей операцій криптографічного перекодування інформації. *Захист інформації: наук.-практ. журнал*. 2012. № 3 (56). С. 50–56.
4. Рудницький В. М., Бабенко В. Г., Рудницький С. В. Метод синтезу матричних моделей операцій криптографічного кодування та декодування інформації. *Збірник наукових праць Харківського університету Повітряних Сил*. 2012. Вип. 4 (33). С. 198–200.
5. Бабенко В. Г., Рудницький С. В. Реалізація методу захисту інформації на основі матричних операцій криптографічного перетворення. *Системи обробки інформації*. 2012. № 9 (107). С. 130–139.
6. Фауре Е. В., Сисоєнко С. В., Миронюк Т. В. Синтез і аналіз псевдовипадкових послідовностей на основі операцій криптографічного перетворення. *Системи управління, навігації та зв'язку*. 2015. № 4 (36). С. 85–87.
7. Рудницький В. М., Фауре Е. В., Сисоєнко С. В. Оцінка якості псевдовипадкових послідовностей на основі додавання за модулем. *Вісник інженерної академії України*. 2016. № 3. С. 219–221.
8. Наукоемкие технологии в инфокоммуникациях: обработка информации, кибербезопасность, информационная борьба: монография / под общ. ред. В. М. Безрука, В. В. Баранника. Харьков: Лидер, 2017. 600 с.
9. Сисоєнко С. В., Мельник О. Г. Використання операцій та алгоритмів криптоперетворення двох блоків змінних в криптографії. *Інноваційні тенденції сьогодення в сфері природничих, гуманітарних та точних наук*: мат.-ли міжнар. наук.-практ. конф. (17 жовтня 2017 р.). Івано-Франківськ, 2017. С. 47–49.
10. Рудницький В. М., Бабенко В. Г., Рудницький С. В. Метод синтезу матричних моделей операцій криптографічного кодування та декодування інформації. *Збірник наукових праць Харківського університету Повітряних Сил*. 2012. Вип. 4 (33). С. 198–200.

References

1. Bogush, V. M. and Yudin, O. K. (2005) Information security of the state. Kyiv : MK-Pres, 432 p. [in Ukrainian].
2. Rudnytsky, V. N., Mylchevych, V. Y., Babenko, V. G., Melnyk, R. P., Rudnytsky, S. V. and Melnyk, O. G. (2014) Cryptographic coding: methods and means of realization (part 2): monograph. Krasnodar, 224 p. [in Russian].
3. Rudnytsky, V. M., Babenko, V. G. and Rudnytsky, S. V. (2012) Method of synthesis of matrix models of operations of cryptographic information reencoding. *Zaxyst informaciyi: nauk.-prakt. zhurnal*, No. 3 (56), pp. 50–56 [in Ukrainian].
4. Rudnytsky, V. M., Babenko, V. G. and Rudnytsky, S. V. (2012) Method of synthesis of matrix models of operations of cryptographic encoding and decoding of information. *Zbirnyk naukovykh prats Kharkivskoho universytetu Povitrianykh Syl*, No. 4 (33), pp. 198–200 [in Ukrainian].
5. Babenko, V. G. and Rudnytsky, S. V. (2012) Realization of the method of information protection on the basis of matrix operations of cryptographic transformation. *Systemy obrobky informatsii*, No. 9 (107), pp. 130–139 [in Ukrainian].
6. Faure, E. V., Sysoyenko, S. V. and Myronyuk, T. V. (2015) Synthesis and analysis of pseudorandom sequences based on cryptographic transformation operations. *Systemy upravlinnya, navihatsiyi ta zvyazku*, No. 4 (36), pp. 85–87 [in Ukrainian].
7. Rudnytsky, V. M., Faure, E. V. and Sysoyenko, S. V. (2016) Assessing the quality of pseudorandom sequences based on the addition of a module. *Visnyk inzhenernoyi akademiyi Ukrayiny*, No. 3, pp. 219–221 [in Ukrainian].
8. High technology in infocommunications: information processing, cybersecurity, information struggle: monograph / pod obshchey red. V. M. Bezruka, V. V. Barannyka. Kharkov: Lyder, 2017, 600 p. [in Ukrainian].
9. Sysoyenko, S. V. and Melnyk, O. G. (2017) Using of the operations and algorithms of cryptographic transformation of two blocks of variables in cryptography. *Innovatsiyni tendentsiyi sohodennya v sferi pryrodnychyykh, humanitarnyykh ta tochnyykh nauk: mat-ly mizhnar. nauk.-prakt. konf.*, (17 zhovtnya 2017 r.). Ivano-Frankivsk, pp. 47–49 [in Ukrainian].
10. Rudnytsky, V. M., Babenko, V. G. and Rudnytsky, S. V. (2012) Method of synthesis of matrix models of operations of cryptographic encoding and decoding of information. *Zbirnyk naukovykh prats Kharkivskoho universytetu Povitrianykh Syl*, No. 4 (33), pp. 198–200 [in Ukrainian].

S. V. Sysoyenko,

Department of Information Security and Computer Engineering, Assistant

e-mail: s.sysoyenko@gmail.com,

O. G. Melnyk, Ph.D., Senior Researcher,

Department of Building Constructions, Associate professor,

e-mail: melnyk.olja.2014@gmail.com

M. O. Pustovit,

Department of Engineering and Civil Defense Equipment, Senior lecturer,

e-mail: m.pustovit@gmail.com.

¹ Cherkasy State Technological University,

Shevchenko blvd., 460, Cherkasy, 18006, Ukraine

² Cherkasy Institute of Fire Safety named after

Chornobyl Heroes of National University of Civil Protection of Ukraine,

Onoprienko Str., 8, Cherkasy, 18034, Ukraine

SYNTHESIS OF OPERATIONS OF REVERSE GROUP MATRIX CRYPTOGRAPHIC TRANSFORMATION OF INFORMATION

One way to improve existing and build new information security systems is to find and use new functions of cryptographic transformation of information. At present, operations of inverse group ma-

trix cryptographic transformation of information, which can be used to implement cryptographic data coding, are not sufficiently studied. The possibility of synthesizing inverse transformation operations based on the search for inverse group and non-group two-bit operations is investigated. By looking through the transformation data, an algorithm for constructing an inverse group cryptographic transformation was found. Based on the research results, the model of direct and inverse two-operand group cryptographic transformation is formalized. The proposed model provides a simplification of finding the reverse cryptographic transformation, since for its implementation it is necessary to find three inverse two-operand transformations instead of one inverse four-operand transformation.

Keywords: *cryptographic transformation of information, direct and reverse operation, operation of matrix transformation, group operations, correctness of operation.*

*Рецензенти: Рудницький В. М., д.т.н., професор,
Кириченко О. В., д.т.н., с.н.с.*

І. В. Миронець, к.т.н., доцент,

доцент кафедри інформаційної безпеки та комп'ютерної інженерії,

e-mail: irenmir30@gmail.com

В. О. Кобрін, магістрант,

e-mail: vitaliy.kobrin@gmail.com

Черкаський державний технологічний університет,

бульв. Шевченка, 460, м. Черкаси, 18006, Україна

АНАЛІЗ МЕТОДІВ РЕАЛІЗАЦІЇ АУТЕНТИФІКАЦІЇ НА ОСНОВІ МАРКЕРІВ ДОСТУПУ ДЛЯ КОРПОРАТИВНОЇ СИСТЕМИ ЗБЕРЕЖЕННЯ ТА ОБМІНУ ДАНИМИ

Стаття присвячена аналізу методів аутентифікації користувача в інформаційній системі, а саме аутентифікації на основі маркерів доступу. В процесі дослідження проаналізовано принцип роботи методу аутентифікації, його ключові особливості, сферу застосування та стандарт, що його описує. Також досліджено переваги даного методу у порівнянні з іншими методами аутентифікації.

В інформаційній системі для ідентифікації користувач надає свої особисті електронні дані для перевірки з метою отримання доступу до певного ресурсу. На етапі аутентифікації особисті електронні дані користувача перевіряються за допомогою певних протоколів. На кінцевому етапі, в результаті успішної перевірки електронних даних користувача на достовірність, користувач отримує права доступу до запитуваного ресурсу. Електронні системи передачі інформації мають і складніші методи аутентифікації та авторизації, такі як багатофакторна аутентифікація або аутентифікація з одноразовими паролями.

Дослідивши переваги та недоліки розглянутого протоколу аутентифікації користувача в інформаційних системах, було визначено основні проблеми, що виникають в процесі розробки додатку на його основі. Запропоновані рішення проблем розширюють функціональні можливості аутентифікації на основі маркерів доступу та підвищують ступінь захисту системи від несанкціонованого доступу.

Ключові слова: ідентифікація, аутентифікація, маркер доступу, інформаційні системи, конфіденційні дані, захист інформації, несанкціонований доступ.

Постановка проблеми. В продовж останніх років спостерігається стрімке зростання популярності односторінкових веб-додатків, мобільних програм та веб-сервісів. Як результат, істотно змінюється підхід до створення таких додатків. За допомогою сучасних технологій та фреймворків на розробку веб-додатку витрачається набагато менше часу, а якість та продуктивність додатків зростає. Відповідно, приділяється більше уваги до побудови серверної частини додатку, створення більш потужного та продуктивного API. Зона відповідальності серверної частини додатку обмежується опрацюванням бізнес-логіки та реалізацією рівня доступу до даних, а логіка відображення є винятково відповідальністю веб або мобільного додатку. Ці зміни призвели до нових шляхів впровадження аутентифікації в сучасних додатках.

Аутентифікація – це одна з найважливіших частин будь-якого веб-додатку. Досить

тривалий час найпростішим та найпопулярнішим вирішенням проблеми аутентифікації були файли cookie та аутентифікація на базі серверів. Проте, обробка аутентифікації в сучасних додатках для мобільних пристроїв та односторінкових додатків може бути складнішою та вимагати іншого підходу. Одне з найбільш відомих рішень для реалізації аутентифікації для веб-сервісів – аутентифікація на основі маркерів доступу.

Для корпоративної системи збереження та обміну даними захист від несанкціонованого доступу є винятково важливим атрибутом, що, наряду з іншими найбільш важливими компонентами системи (оптимізовані алгоритми обробки великих об'ємів даних, файлова система, реалізація розмежування прав доступу до ресурсів та ін.), забезпечує надання інформаційною системою високоякісних послуг.

Будь-яка система збереження даних, крім документів користувачів, може також

зберігати базу даних особистої інформації користувачів: фізичні адреси, телефонні номери, адреси електронної пошти, приватні повідомлення. Зловмисники є зацікавленими у заволодінні такими інформаційними ресурсами.

Корпоративна система збереження даних може використовуватися для збереження інтелектуальної власності, результатів діяльності компанії, електронних версій юридичних документів тощо. Цінність таких даних істотно перевищує цінність звичайних документів, відповідно збільшуються і вимоги до системи захисту.

Аналіз останніх досліджень та публікацій. Аналіз науково-технічної літератури [1-10] доводить актуальність досліджень методів і протоколів аутентифікації та зростання зацікавленості відомих корпорацій у пошуку новітніх рішень для реалізації аутентифікації. У публікаціях останніх років описано постійно зростаючу інтенсивність удосконалення засобів злому інформаційних систем з метою заволодіння інформаційними ресурсами. У зв'язку з цим удосконалюються і методи захисту інформації від несанкціонованого доступу. В процесі функціонування інформаційної системи здійснюється постійна обробка даних, їх передача в мережі та зберігання. Захист інформації повинен забезпечувати надійність виконання всіх операцій з даними.

Науковцем Дасгупта Д. розглянуто процес перевірки автентичності, а також типи механізмів аутентифікації та їх особливостей. В його книзі [2] розглянуто використання цих механізмів в експлуатаційному середовищі, що змінюється у часі, включаючи такі сторонні фактори, як пристрої, засоби масової інформації та навколишнє середовище.

Малюком А.А. [9] розглянуто проблеми вразливості інформації в системах обробки даних, описано принципи роботи протоколів аутентифікації, а також їх взаємодія з веб-серверами та веб-додатками.

Чапмен Н. [1] надав опис способів вирішення проблеми видачі інформаційною системою дозволу на виконання операції над даними на вимогу від певного користувача або програми.

За результатами проведеного аналізу публікацій було визначено основні існуючі протоколи та засоби аутентифікації.

Мета даної роботи полягає у дослідженні методів реалізації аутентифікації на

основі маркерів доступу для корпоративної системи збереження та обміну даними, їх доцільності використання, а також переваг та недоліків.

Виклад основного матеріалу. Існує два основні типи аутентифікації користувача в інформаційній системі:

- аутентифікація на основі файлів cookie;
- аутентифікація на основі маркерів доступу.

Аутентифікація на основі файлів cookie на даний час є застарілою у зв'язку з недосконалістю реалізації механізму аутентифікації користувача. Такий тип аутентифікації передбачає, що сесія користувача повинна зберігатися як на сервері, так і на стороні клієнта. Сервер повинен відстежувати активні сесії в базі даних, тоді як на стороні клієнта створюється файл cookie, який містить ідентифікатор сеансу, тобто аутентифікацію на основі файлу cookie.

Аутентифікація на основі маркерів доступу навпаки не передбачає збереження сесії користувача. Немає необхідності реалізовувати на сервері механізм обліку користувачів, що авторизуються у системі. В такому випадку кожен запит на сервер супроводжується маркером доступу, який сервер використовує для перевірки автентичності запиту.

Маркер (токен) доступу – це фрагмент даних, що містить облікові дані для сеансу входу та ідентифікує користувача, групи користувачів, привілеї користувача та, у деяких випадках, певну програму. Маркер доступу може використовуватись клієнтською частиною додатку для доступу до прикладного програмного інтерфейсу (Application programming interface (англ.) або API) сервера. Мета маркера доступу полягає в інформуванні API про те, що носій цього маркера отримав дозвіл на доступ до API та виконання певних дій (в межах наданого доступу).

Функція аутентифікації на основі маркерів доступу забезпечує, що кожен запит на сервер супроводжується підписаним маркером, який сервер перевіряє на достовірність, а потім відповідає на запит в залежності від результатів перевірки.

Маркер доступу створюється на етапі аутентифікації користувача у системі у разі її успішного завершення.

Розглянемо процес створення та використання маркера доступу (рис. 1):

- користувач вводить свої реєстраційні дані;
- сервер перевіряє правильність облікових даних і повертає підписаний маркер;
- отриманий від сервера маркер зберігається на стороні клієнта, найчастіше в локальному сховищі браузера, але також може зберігатися в пам'яті або файлі cookie;
- наступні запити на сервер містять цей маркер як додатковий заголовок (Authorization) запиту, також додатково може бути відправлений в тілі запиту POST або як параметр запиту;
- сервер здійснює валідацію маркера і в разі, якщо він дійсний, здійснює обробку запиту, інакше – повертає відповідь з помилкою;
- коли користувач виходить з системи, маркер знищується на стороні клієнта, взаємодія з сервером не потрібна.

Аутентифікація на основі маркерів доступу має наступні переваги:

- відсутність механізму керування сесіями;
- кросдоменність;
- збереження даних в маркері;
- біль висока продуктивність;
- адаптація для використання у мобільних додатках;
- стандартизованість.

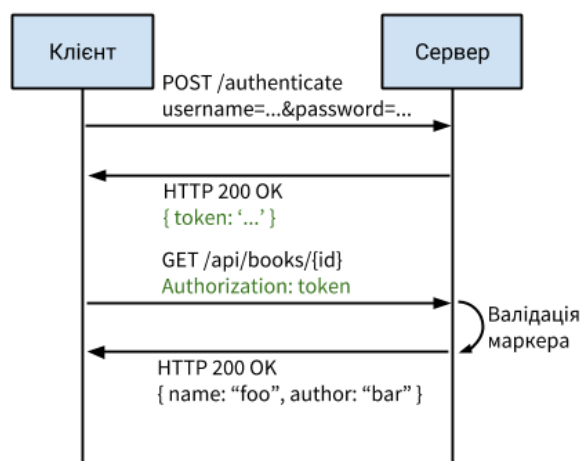


Рис. 1. Послідовність отримання та використання маркера доступу

Розглянемо ці пункти детальніше.

Перевагою використання маркерів у порівнянні з файлами cookie є те, що при використанні маркерів немає необхідності у збереженні сесії користувача на стороні сервера.

Кожен маркер є самостійною одиницею, що містить всі дані, необхідні для перевірки його дійсності, а також передачі інформації про користувача.

В такому випадку робота сервера полягає у підписуванні маркерів у випадку успішного виконання запиту на авторизацію користувача і перевірці правильності вхідних маркерів. Використовуючи сторонні сервіси для підпису маркерів, задачею сервера є лише підтвердження валідності маркера.

Аутентифікація на основі cookies працює коректно з сингулярними доменами та субдоменами. У випадках необхідності керування файлами cookie в різних доменах, процес реалізації аутентифікації стає набагато складнішим. Аутентифікація на основі маркерів доступу не вимагає додаткових налаштувань, оскільки маркер доступу перевіряється з кожним запитом на стороні сервера.

Використовуючи підхід, заснований на файлі cookie, передбачає збереження ідентифікатора сесії користувача у цьому файлі. Підхід на основі маркерів доступу дозволяє зберігати будь-який тип метаданих безпосередньо у маркері, якщо дані можуть бути представлені у форматі JSON.

Під час використання аутентифікації на основі файлів cookie є необхідність у виконанні пошукових запитів до бази даних для вилучення даних про сесію користувача. В залежності від типу СУБД, що використовується, такі запити можуть бути більш тривалими, ніж процес декодування маркера.

Наприклад, якщо є ресурс, що доступний за запитом на адресу /api/books, але доступ для перегляду даних за цією адресою мають лише користувачі з роллю «адміністратор». При використанні файлів cookie, під час виконання запиту буде здійснено принаймні три запити до бази даних:

1. перевірка, що сесія є дійсна;
2. пошук даних користувача та перевірка, що користувач має роль адміністратора;
3. пошук запитуваних даних.

За допомогою підходу на основі маркерів доступу роль користувача може бути збережена всередині маркера. Тому після валідації маркера і підтвердження, що користувач має роль адміністратора, буде виконано один запит до бази даних з метою отримання запитуваних даних.

В ролі клієнта по відношенню до сервера може виступати як браузер так і мобільний додаток. Мобільні платформи не мають підтримки файлів cookie. Також існує ряд обмежень щодо використання файлів cookie на мобільних платформах пов'язані з вразливістю системи захисту даних користувача. Для реалізації аутентифікації на основі маркерів доступу не потрібно мати підтримки на рівні платформи. Даний підхід повністю придатний для реалізації на платформах iOS та Android.

Існує стандарт JSON Web Token (RFC 7519), що описує структуру маркера доступу, способи його використання, процедури кодування та підпису тощо. Існує підтримка стандарту для більшості популярних платформ програмування (.NET, Ruby, Java, Python, PHP, NodeJS та ін.). Стандарт використовується багатьма сервісами наряду із стандартами OAuth та OAuth 2.0.

Стандарт JSON Web Token (JWT) визначає компактний та автономний спосіб безпечного передавання інформації між сторонами як об'єкт у форматі JSON. Цю інформацію можна перевірити на достовірність, оскільки вона підписана цифровим способом. JWT можна підписати, використовуючи секрет (з алгоритмом HMAC) або пару публічний/приватний ключ з асинхронними алгоритмами шифрування.

JWT передбачає компактність маркера, оскільки він надсилається через HTTP-запити. Крім того, менший розмір означає більшу швидкість передачі.

Автономність означає, що маркер містить у собі всю необхідну інформацію про користувача.

JWT складаються з трьох частин, розділених крапками:

- заголовок (header),
- вміст (payload),
- підпис (signature).

Заголовок, як правило, складається з двох атрибутів: «typ» (тип маркера, в даному випадку JWT), та «alg» (алгоритм хешування, що використовується, наприклад HMAC SHA256 або RSA).

Друга частина маркера містить набір тверджень (claims). Твердження – це інформація про суб'єкт (як правило, користувача) та додаткові метадані. Всього використовується три типи тверджень:

- Зареєстровані твердження – це набір попередньо визначених тверджень, які не є обов'язковими, але рекомендовані для включення їх до набору тверджень (див. табл. 1).

- Публічні твердження – твердження, які можна визначити за бажанням тих, хто використовує JWT. Щоб уникнути колізій, вони повинні бути визначені в реєстрі IANA JSON Web Token або бути визначеними як URI, що містить конфліктну зону імен.

- Приватні твердження – це спеціальні вимоги, створені для обміну інформацією між сторонами, які погоджуються на їх використання.

Звернімо увагу, що назви тверджень, як правило, складаються лише з трьох символів, оскільки одна із вимог до побудови JWT – забезпечення його компактності.

Таблиця 1

Зареєстровані твердження вмісту JWT

Поле	Назва	Значення
iss	Issuer	Ідентифікатор сервісу, що видав маркер
sub	Subject	Ідентифікатор суб'єкта, якого стосуються твердження.
exp	Expiration Time	Час закінчення терміну дії маркера в форматі Unix.
iat	Issued At	Час, коли маркер був виданий (в форматі Unix)

Заголовок та вміст маркера кодуються у форматі Base64Url, що дозволяє перетворити набір даних в компактну послідовність символів і утворити маркер.

Підпис є результатом криптографічного перетворення перших двох частини маркера (заголовку та вмісту у форматі Base64Url та розділених крапкою). Шифрування відбувається за алгоритмом, вказаним у заголовку. Отримана в результаті перетворення послідовність символів (хеш) додається до перших двох частин та відокремлюється крапкою.

Наприклад, підписаний алгоритмом HMAC SHA256 маркер, може мати наступний вигляд: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0Ij06MTYyOTQwMDAwfQ.TJVA95OrM7E2cBab30RMHrHDcEfxjoYZgeFONFh7Hg.

Підпис призначений для ідентифікації джерела маркера та підтвердження цілісності даних, які він містить.

Під час валідації маркера здійснюється операція, подібна до операції підпису маркера: створюється хеш на основі перших двох частин маркера та порівнюється із третьою частиною маркера. Якщо обидва хеши співпадають, маркер вважається валідним. В протилежному випадку система генерує помилку і подальша обробка маркера припиняється.

Одним із найпопулярніших способів отримання хешу для JWT є використання механізму HMAC (Hash-based message authentication code (англ.) або хеш-код аутентифікації повідомлень).

HMAC – це група алгоритмів, які забезпечують спосіб підписування повідомлень за допомогою спільного ключа. У випадку HMAC використовується криптографічна хеш-функція (наприклад, SHA256). Потужність залежить від алгоритму хешування, що використовується.

Основним завданням при проектуванні алгоритму було досягти можливості комбінувати ключ з повідомленням, одночасно надаючи гарантії проти несанкціонованого втручання і модифікації повідомлення. Спеціальні рішення (наприклад, додавання ключа до повідомлення, а потім хешування результату) мають математичні недоліки, які дозволяють потенційним зломисникам підробляти підпис. Алгоритм HMAC розроблений з урахуванням цих недоліків.

HMAC використовується з JWT, коли є необхідним простий спосіб для створення та валідації JWT в різних компонентах інформаційної системи. Будь-який компонент системи, якому відомий ключ, може створювати нові JWT. Іншими словами, перехопивши ключ, зломисник може видати себе за іншого: JWT на основі HMAC не надає гарантій щодо сторони, на якій було створено JWT. Для запобігання цього доцільніше використовувати асиметричні алгоритми для побудови хешу, а саме RSA.

RSA – асиметричний алгоритм шифрування та цифрового підпису. Даний алгоритм надає можливість перевірки або дешифрування повідомлення без можливості створення нового. Сторона, яка видає маркер, використовує приватний ключ для підписання JWT. Сторона, що отримує маркер, використовує відкритий ключ, що поширюється відкритим

джерелом. Приймаючі сторони не можуть створювати нові JWT за допомогою відкритого ключа відправника.

Алгоритм RSA є більш складним у реалізації, ніж HMAC. Але використання цього алгоритму істотно зменшує шанс підробки маркера доступу.

Наступним важливим кроком у валідації маркера доступу після ідентифікації автора маркера та підтвердження його цілісності – це перевірка терміну його дії.

Як зазначалось раніше, одним із рекомендованих тверджень вмісту маркера є exp (Expiration Time), що містить дату та час завершення дії маркера. За реалізації аутентифікації на основі маркерів доступу відсутній механізм контролю сесій користувачів. В даному випадку доцільним є перевірка терміну дії маркера.

Термін дії маркера – термін закінчення дії умовної сесії користувача, тобто час, протягом якого користувач може взаємодіяти із системою без необхідності виконання повторної процедури авторизації у системі.

Існують рекомендації щодо терміну підтримки сесій користувачів активними (від 10 годин до 1 доби), недотримання яких може призвести до поганого впливу на досвід користування системою.

Оскільки механізм контролю сесій користувачів відсутній, є неможливим відстеження та анулювання маркерів, що були видані. Якщо став відомий факт перехоплення маркера доступу користувача та його несанкціонованого використання, система не в змозі виявити даний маркер та заборонити доступ до системи стороні, що його використовує, навіть якщо користувач здійснить вихід із системи. Збереження у базі даних будь-яких міток або реєстру маркерів суперечить принципам реалізації аутентифікації на основі маркерів доступу та нівелює існуючі переваги такого підходу.

Вирішенням даної проблеми є використання маркера оновлення (refresh token). Даний підхід вимагає впровадження додаткових кроків в процеси авторизації та аутентифікації користувачів, але дозволяє підвищити контроль над використанням існуючих маркерів.

Використання маркерів оновлення дозволяє генерувати маркери доступу з короткотривалим терміном дії (до 1 год.). Маркер оновлення – JWT, з терміном дії, що еквівале-

нтний терміну дії сесії користувача в системі та з відображенням у базі даних.

Розглянемо процес аутентифікації з використанням маркера оновлення (рис. 2):

- користувач вводить свої реєстраційні дані;
- сервер перевіряє правильність облікових даних і повертає підписані маркери доступу та оновлення;
- отримані від сервера маркери зберігаються на стороні клієнта;
- наступні запити на сервер містять маркер доступу;
- сервер здійснює валідацію маркера доступу і в разі, якщо він дійсний, здійснює обробку запиту, інакше – повертає відповідь з помилкою;
- якщо отримано помилку від сервера, надсилається запит на оновлення маркера доступу, відповідно запит містить маркер оновлення;
- сервер здійснює валідацію маркера оновлення і в разі, якщо він дійсний, повертає новий маркер доступу;
- коли користувач виходить з системи, маркери знищуються на стороні клієнта, сервер повідомляється про завершення сесії.

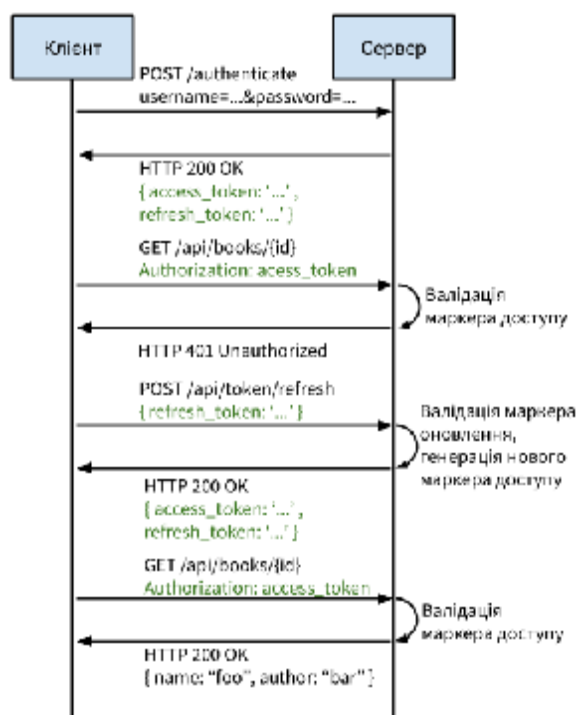


Рис. 2. Процес аутентифікації користувача з використанням маркера оновлення

Якщо маркер оновлення є невалідним або термін його дії закінчився, новий маркер доступу не буде виданий.

Як видно, даний процес аутентифікації передбачає виконання додаткових запитів до бази даних, але лише у разі запиту на оновлення маркера.

Якщо користувач здійснив вихід із системи або його сесія була автоматично завершена у випадку виявлення факту несанкціонованого використання маркера доступу, сесія фактично буде активною до завершення терміну дії маркера доступу. Новий маркер доступу не буде виданий навіть у випадку перехоплення маркера оновлення.

Даний підхід не гарантує абсолютного захисту від несанкціонованого доступу, але є значно надійнішим у порівнянні з підходом без використання маркера оновлення.

Також даний підхід дозволяє вирішити іншу проблему, пов'язану з неможливістю анулювати маркер доступу. Якщо в системі передбачено механізм управління правами доступу користувачів до певних даних, може виникнути ситуація, коли адміністратором інформаційної системи буде вирішено заблокувати або частково обмежити конкретному користувачеві доступ до певного ресурсу. З використанням лише маркера доступу, даний користувач буде мати доступ до забороненого для нього ресурсу протягом терміну дії сесії. Проте, під час валідації маркера оновлення можливо здійснити додаткову перевірку на можливі зміни у правах доступу користувача та запобігти його доступу до захищеного ресурсу.

Як вже зазначалось, заголовок JWT містить параметр, що вказує алгоритм, що використовувався для підпису маркера. Крім назви алгоритму, даний параметр може містити нульове значення (none). Нульове значення використовується в ситуаціях, коли цілісність маркера вже підтверджена.

В разі використання сторонніх реалізацій механізмів валідації JWT необхідно передбачити додатковий ступінь перевірки маркера на назву алгоритму, що міститься в заголовку маркера. Така процедура є необхідною, оскільки в сторонніх реалізаціях може бути відсутнім механізм валідації для маркерів, які містять в заголовку нульовий алгоритм. Це надає зловмисникам можливість підміни маркера доступу на будь-який інший та отримати несанкціонований доступ до захищених ресурсів.

Також однією із проблем використання JWT є Формат Base64, що передбачає лише кодування вмісту маркера. Дані, що містяться в маркері, не є захищеними та можуть бути розкодованими третіми особами. В інформаційних системах, вимогою до яких є передача в маркері інформації, недоступної для третіх осіб, використання JWT не є прийнятним рішенням. Замість цього можна використовувати модифікацію JWT – JWE (JSON Web Encryption). JWE, на відміну від JWT, містить зашифровані дані. JWE має структуру, відмінну від структури JWT, і має більш складні процеси генерації та валідації.

Використання JWE замість JWT потребує додаткового аналізу для виявлення відповідно переваг та недоліків аутентифікації на основі JWE.

Висновки. В процесі даного дослідження було розглянуто основні методи реалізації аутентифікації, виявлено переваги та недоліки аутентифікації на основі маркерів доступу. Здійснено покроковий аналіз можливих алгоритмів роботи системи аутентифікації.

Проведено дослідження особливостей використання маркерів доступу, проблеми, пов'язані з їх використанням, та способи їх вирішення. Розглянуто один із стандартів побудови маркерів доступу, внутрішню структуру маркерів, особливості передачі даних в середині маркерів. Також проаналізовано способи шифрування вмісту маркерів та створення цифрового підпису, що дозволяє ідентифікувати джерело маркера та підтвердження цілісності даних, які він містить.

Список літератури

1. Chapman N., Chapman J. Authentication and Authorization on the Web. MacAvon Media. 2012. 236 с.
2. Dasgupta D., Arunava R., Nag A. Advances in User Authentication. Springer International Publishing AG. 2017. 233 с.
3. Topol B., Nash H., Martinelli S. Identity, Authentication, and Access Management in OpenStack. O'Reilly Media, Inc. 2015. 130 с.
4. Афанасьев А. А., Веденев Л. Т., Воронцов А. А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. 2-е изд. Москва: Горячая линия-Телеком, 2012. 570 с.
5. Барабанов А. В., Дорофеев А. В., Марков А. С., Цирлов В. Л. Семь безопасных информационных технологий. Москва: ДМК Пресс, 2017. 224 с.
6. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации. Учеб. пособ. 3-е изд., перераб. и доп. Москва: Инфра-М, 2017. 324 с.
7. Баричев С. Г., Гончаров В. В., Серов Р. Е. Основы современной криптографии. 3-е изд. Москва: Горячая линия-Телеком, 2017. 176 с.
8. Горбатов В. Г., Полянская О. Ю. Основы технологии PKI. Москва: Горячая линия-Телеком, 2004. 248 с.
9. Малюк А. А., Пазизин С. В., Погужин Н. С. Введение в защиту информации в автоматизированных системах. Москва: Горячая линия-Телеком, 2001. 148 с.
10. Малюк А. А., Горбатов В. С., Королев В. И. Введение в информационную безопасность. Москва: Горячая линия-Телеком, 2011. 288 с.

References

1. Chapman, N. Chapman, J. (2012) Authentication and Authorization on the Web. MacAvon Media, 236 p.
2. Dasgupta, D., Arunava, R., Nag, A. (2017) Advances in User Authentication. Springer International Publishing AG, 233 p.
3. Topol, B., Nash, H., Martinelli, S. (2015) Identity, Authentication, and Access Management in OpenStack. O'Reilly Media, 130 p.
4. Afanas'ev, A. A., Veden'ev, L. T., Voroncov, A. A. (2012) Authentication. The theory and practice of research of secure access to the information resources. Moscow: Goryachaya liniya-Telekom [in Russian].
5. Barabanov, A. V., Dorofeev, A. V., Markov, A. S., Cirlov, V. L (2017) Seven secured information technologies. Moscow: DMK Press [in Russian].
6. Baranova, E. K., Babash, A. V. (2017) Information security and protection. Moscow: Infa-M [in Russian].
7. Barichev, S. G., Goncharov, V. V., Serov, R. E. (2017) Basics of modern cryptography. Moscow: Goryachaya liniya-Telekom [in Russian].

8. Gorbatov, V. G., Polyanskaya, O. YU. (2004) Basics of PKI technology. Moscow: Goryachaya liniya-Telekom [in Russian].
9. Malyuk, A. A., Pazizin, S. V., Pogozhin, N. S. (2001) Introduction into information protection in automated systems. Moscow: Goryachaya liniya-Telekom [in Russian].
10. Malyuk, A. A., Gorbatov, V. S., Korolev, V. I. (2011) Introduction into information security. Moscow: Goryachaya liniya-Telekom [in Russian].

I. V. Myronets, *Ph.D., associate professor,*
associate professor of information security and computer engineering chair,
e-mail: irenmir30@gmail.com,

V. O. Kobrin, *master,*
e-mail: vitaliy.kobrin@gmail.com,
Cherkasy State Technological University,
Shevchenko blvd., 460, Cherkasy, 18006, Ukraine

ANALYSIS OF METHODS FOR AUTHENTICATION IMPLEMENTATION BASED ON TOKENS OF ACCESS FOR CORPORATE SYSTEM OF DATA STORAGE AND SHARING

In recent years, the population of single page applications, mobile applications and web services is growing rapidly. As a result, the approaches to developing such applications are changing significantly. Usage of new approaches brings new implementation methods of authentication in modern applications. The objectives of this research are implementation methods of token based authentication for corporate system of data storage and sharing, investigation of such method usage expediency, research for existing solutions and analyzing their advantages and disadvantages. A protection from unauthorized access is the most important attribute for corporate system of data storing and sharing. This is the one of the most important components which guarantees providing high quality service. The intensity of improvements of ways to hack information systems are growing significantly. So, the information security system should provide reliable performing of data processing, transferring and storing. The results of the research on the use of the token based authentication system are presented in this article. This type of authentication was compared with cookie based authentication. The main advantages and disadvantages of this approach were described.

Access token is a fragment of a data contained user claims. Token allows server to identify the user, group of the users and/or application. Token is used by client side application as a key to the API. The main goal of the access token is to inform that the bearer of this token has access to the API. Function of a token based authentication is to provide every request to the server with signed access token. This token is checked by server on authenticity. After that the server responds to request depending on the results of the checking. There is a JSON Web Token (JWT) standard that describes access token structure, ways of it usage and caching procedures.

This article contains the detailed description of the JWT usage scenarios. There is a description of the authentication process based on refresh token usage that brings more control over user sessions. The ways to sign the token described as well.

The result of this research is defined implementation methods of authentication. Advantages and disadvantages of token based authentication were defined. Step-by-step analysis of possible working algorithms of authentication system was performed.

Keywords: *identification, authentication, access token, information system, confidential data, information security, unauthorized access.*

*Рецензенти: С. В. Голуб, д.т.н., професор,
Т. О. Прокопенко, д.т.н., доцент.*

І. В. Миронець, к.т.н., доцент,

доцент кафедри інформаційної безпеки та комп'ютерної інженерії,

e-mail: irenmir30@gmail.com

А. В. Маламуж, магістрант,

e-mail: andrey.malamuzh.1994@gmail.com

Черкаський державний технологічний університет,

б-р Шевченка, 460, м. Черкаси, 18006, Україна

ДОСЛІДЖЕННЯ ТА ОПТИМІЗАЦІЯ СИСТЕМИ УПРАВЛІННЯ КОНТЕНТОМ ДЛЯ ОРГАНІЗАЦІЇ ПЕРСОНАЛЬНОГО САЙТУ

Стаття присвячена дослідженню та оптимізації системи управління контентом для організації персонального сайту. В процесі дослідження проаналізовано проблему створення системи управління контентом, сферу застосувань, розглянуто основні аналоги системи та проаналізовано основні завдання та функції. Система управління контентом – інформаційна система, яка використовується для організації веб-сайтів чи інших інформаційних ресурсів в Інтернеті. Необхідність такої системи управління контентом з'явилася в той момент, коли кількість матеріалу на веб-сайтах почала стрімко зростати, а введення даних на сайт потребувало знання технологій HTML/CSS. Оперативне оновлення (додавання, редагування, видалення) змісту повинне виконуватися не розробниками, а людьми, чийі знання в сфері інформаційних технологій можна охарактеризувати як "користувач ПК". Сайт побудований на основі такої системи в ідеальному випадку перетворюється в інструмент, яким можуть легко керувати безпосередньо контент-менеджери та піар-фахівці. З повсякденної роботи над ресурсом практично повністю виключаються технічні фахівці, що призводить до реального зниження вартості підтримки сайту.

Ключові слова: система управління контентом, персональний сайт, web, інтернет-технології, організація веб-сайту, HTML, CSS, користувач ПК, підтримка сайту.

Постановка проблеми. З появою Web-технологій комп'ютер починають використовувати абсолютно нові верстви населення. Можна виділити дві найбільш характерні групи, які були стрімко залучені в нову технологію. З однієї сторони це були представники елітарних груп – керівники великих організацій, президенти банків, чиновники. З іншої сторони, це були представники найширших верст населення – викладачі, домогосподарки, діти і т.д.

Спектр соціальних груп, які підключаються до мережі Інтернет та шукають інформацію в WWW, весь час розширюється за рахунок користувачів, які не відносяться до категорії спеціалістів в області інформаційних технологій.

Web-технології повністю перевернули наше бачення про роботу з інформацією та з комп'ютером в цілому. Тоді, коли інтерфейс між людиною та комп'ютером став спрощеним до звичайного сприйняття звичайною людиною, розпочався вибух зацікавленості до можливостей обчислювальної техніки.

З розвитком технології гіпертекстової розмітки в Інтернеті з'явилося все більше сайтів, тематика яких зовсім різна – від сайтів великих компаній, до звичайних персональних сайтів.

Система управління контентом – засіб для створення та організації сайтів. В цій системі можуть знаходитися різноманітні дані: документи, фотографії, номери телефонів, наукові роботи, тощо. Така система часто використовується для збереження, управління, перегляду та публікації документації.

Існує проблема в тому, що не кожний користувач вміє створювати сайт та підтримувати його. Саме тому, було вирішено розробити таку систему управління контентом (CMS), яка забезпечить кожного користувача можливістю створювати та постійно підтримувати свій власний сайт.

Аналіз останніх досліджень та публікацій. В світі існує сотні систем управління контентом для різних цілей, різної якості, перспективності розвитку, вартості, тощо. Завдяки їх функціональності ці системи можна використовувати в різних компаніях. Най-

популярнішими системами на сучасному етапі розвитку інформаційних технологій є: Joomla!, 1С-битрикс, Wordpress [7].

Joomla! – займає перше місце серед безкоштовних систем. Особливість даної системи є мінімальна кількість інструментів при встановленні. Всі модулі та шаблони розробник може написати сам та додати до встановленої версії. Але недоліком Joomla! є те, що при некомпетентному налаштуванні, вона перетворюється в складну систему стосовно використання та гальмує в цілому загрузку сайту [4].

1С-битрикс – займає перше місце серед платних систем. В силу своєї ціни та складності, вона в основному користується попитом серед власників великих інтернет-порталів. Архітектура адміністративної панелі не інтуїтивна та потребує вивчення [5].

WordPress – система управління контентом сайту з відкритим кодом. Потрібно відмітити її гнучкість і велику кількість шаблонів для персоналізації. Також слід зауважити – в ній можливе використання відкритого коду на мові PHP, що корисно для фахівців у сфері розробки програмних додатків. Крім того, для професійного використання сайту необхідні додаткові налаштування системи. Дана система використовується в основному для блогів та інтернет-магазинів [3].

Метою даної роботи є дослідити та проаналізувати варіативність оптимізації системи управління контентом для організації персонального сайту.

Виклад основного матеріалу. Першим етапом розробки будь-якого програмного продукту є постановка задачі. Ядром системи управління контентом для організації персонального сайту є база даних, що містить інформацію про структуру та наповнення сайту, а також про користувачів [6]. Маючи точно сформульовані цілі та задачі, можна приступати до проектування структури бази даних та всього продукту в цілому [1].

Створювана система для організації персонального сайту повинна задовольняти наступним вимогам:

- редагування категорій та записів;
- перегляд та редагування коментарів;
- редагування сторінок;
- редагування категорій користувачів;
- можливість додавання та зміни засобів зв'язку;
- перегляд статистики.

Створення системи управління контентом для організації персонального сайту – це трудомісткий та відносно тривалий процес, який відбувається в декілька етапів. По мірі проходження цих етапів, ідея перетворюється в реальну функціональну систему.

Щоб проект був успішним, необхідно як мінімум визначити:

- які задачі покладаються на систему управління контентом;
 - на яких користувачів розрахована система управління контентом;
 - яку функціональність потрібно закласти в свою систему, як вона буде працювати;
- Процес розробки системи управління контентом можна розділити на наступні етапи:
- маркетингове планування;
 - планування структури майбутньої системи управління контентом (модулі, навігація і т.д.);
 - розробка дизайну системи управління контентом;
 - розробка програмних модулів;
 - тестування системи управління контентом.

Розглянемо кожен з наведених етапів детальніше.

Маркетингове планування. На даному етапі виділяються основи створюваної системи управління контентом: що вона повинна робити, чого ми хочемо досягнути з її допомогою та ін.. Ці та інші питання допомагають визначити, якою саме буде система.

Планування структури. На цьому етапі варто особливу увагу приділити тому, в якому режимі працюватимуть модулі та особливості роботи навігації. Тому створюваній системі управління контентом було вирішено надати наступну структуру: на боковій панелі є перехід до всіх функцій системи, а верхня панель дає можливість перейти до сайту або вийти із системи взагалі [1-2].

Розробка дизайну. Більшість із користувачів першу увагу звертає на зовнішній вигляд самого сайту, тому він повинен бути максимально привабливий та зручний [8].

Тестування системи. Не дивлячись на те, що проміжне тестування проходить на кожному етапі реалізації проекту, кінцеве тестування є найважливішим. Воно дає можливість остаточно перевірити всі основні моменти функціонування створеної системи

управління контентом для організації персонального сайту та систематизувати основні функції її організації.

Оптимізація. Оптимізація – модифікація системи для покращення її ефективності. Для оптимізації даної системи управління контентом було вирішено залишити у системі основні модулі для керування сайтом, а інші зробити в якості плагінів. Користувач обирає сам, встановлювати ці плагіни чи ні. Саме тому спочатку система управління контентом займає мінімальну кількість пам'яті та не навантажує систему. До основних модулів, які за замовчуванням є у системі управління контентом відносяться додавання та редагування записів, додавання та редагування сторінок, додавання медіа файлів, додавання користувачів. У системі управління контентом існують плагіни, які користувач може додати до своєї системи відносяться коментарі, перегляд статистика, створення засобів зв'язку та інші.

Також для оптимізації системи управління контентом для організації персонального сайту використовується кешування даних. Кешування даних – це процес збереження часто запитуваних даних на комп'ютері користувача, завдяки чому значно прискорюється завантаження сторінок. Після налаштування кешування браузер або звертається до локально збереженої копії документа (сторінки), замість того, щоб завантажувати його знову і знову при наступних відвідуваннях. Таким чином, кешування дозволяє уникнути повторного формування сторінок, опрацьованих при обробці попередніх запитів. В результаті зменшується час прийому-передачі, виключаються численні HTTP запити і знижується навантаження на сервер.

Висновки. Дане дослідження дало можливість проаналізувати існуючі аналоги систем управління контентом, дослідити їх основні переваги та недоліки.

В процесі дослідження було розглянуто основні вимоги, завдання та функції, які має виконувати створювана система управління контентом для організації персонального сайту, а також визначено етапи її створення та організації.

Результатом проведеного дослідження є створена система управління контентом, яка працює в усіх сучасних браузерах. При чому тестування показало, що всі зарезервовані функції працюють вдало, як і було заплановано.

Список літератури

1. Веллинг Л. Разработка WEB-приложений с помощью PHP и MySQL. М.: «Вильямс», 2009. 800 с.
2. Зандстра М. PHP: объекты, шаблоны и методики программирования. М.: «Вильямс» 2011. 528 с.
3. Документація CMS Wordpress URL: <https://wordpress.org/>.
4. Документація CMS Joomla URL: <http://joomla.ru/>.
5. Документація CMS 1С-битрикс URL: <https://www.bitrix.ua/>.
6. PHP, MySQL и другие веб-технологии URL: <http://www.php.su>.
7. Сравнение CMS URL: <http://sitepark.ua/luchshaya-cms>
8. Мак-Дональд М. HTML5: недостающие руководство. 2012. 479 с.
9. Макконнелл С. Совершенный код - 2010. 867 с.
10. Стефанов С. Java Script: шаблоны. 2011. 263 с.

References

1. Welling, L. (2009) Development of WEB applications using PHP and MySQL M.: Williams. 800 p.
2. Zandstra, M. (2011) PHP: Objects, Patterns and Programming Techniques. M.: Williams. 528 p.
3. CMS Wordpress documentation URL: <https://wordpress.org/>.
4. CMS Joomla documentation URL: <http://joomla.ru/>.
5. CMS 1С-битрикс documentation URL: <https://www.bitrix.ua/>.
6. PHP, MySQL and other web technologies URL: <http://www.php.su>.
7. Comparison of CMS URL: <http://sitepark.ua/luchshaya-cms>
8. McDonald, M. (2012) HTML5: Missing Guide 479 pp.
9. McConnell, S. (2010) Perfect code. 867 s.
10. Stefanov, S. (2011) Java Script: Templates. 263 p.

I. V. Myronets, *Ph.D., associate professor,*
associate professor of information security and computer engineering chair,
e-mail: irenmir30@gmail.com,

A. V. Malamuzh, *master,*
e-mail: andrey.malamuzh.1994@gmail.com
Cherkasy State Technological University,
Shevchenko blvd., 460, Cherkasy, 18006, Ukraine

RESEARCH AND OPTIMIZATION OF CONTENT MANAGEMENT SYSTEM FOR PERSONAL SITE ORGANIZATION

The article is devoted to the research and optimization of the content management system for the organization of a personal site. In the course of the research, the cause of the creation of a content management system, application area was analyzed, the main analogs of the system were considered and the main tasks that this system should perform is analyzed. Content Management System is an information system used to organize web sites or other information resources on the Internet. The need for a content management system began to emerge at a time when the amount of material on the websites began to grow rapidly, and inputting the data to the site required the knowledge of HTML / CSS technologies. The operational update (adding, editing, deleting) content should be performed not by developers, but by people whose knowledge in IT can be described as "PC user". The site, built on the basis of such a system ideally turns into a tool that can easily be directly managed by content managers and PR specialists. Of the daily work on the resource practically completely excluded technical specialists, which leads to a real reduction in the cost of maintaining the site.

Keywords: *content management system, personal website, web, Internet-technologies, website organization, HTML, CSS, PC user, website support.*

*Рецензенти: Кириченко О. В., д.т.н., с.н.с.,
Прокопенко Т. О., д.т.н., доцент.*

Т. В. МIRONIYUK, к.т.н.,

доцент кафедри інформаційної безпеки та комп'ютерної інженерії,

e-mail: tanjamiron85@gmail.com,

Л. Т. ДУДА, магістрант,

e-mail: lyubomir-duda@ukr.net.

Черкаський державний технологічний університет,

бульв. Шевченка 460, м. Черкаси, 18006, Україна

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ОНЛАЙН СПІЛКУВАННЯ

В даній статті розглядаються основні методи захисту он-лайн спілкування на прикладі програм та програмних комплексів для обміну повідомленнями. Розкривається проблема надмірного поширення персональних даних користувачами. Досліджуються основні технології захисту особистої інформації в мережі Інтернет. Особлива увага приділяється огляду спеціалізованих програмних продуктів для безпечного обміну повідомленнями інформацією, які присутні зараз на ринку. Сформульовано базові правила для користувачів, при дотриманні яких, спілкування та обмін контентом в мережі Інтернет стане більш захищеним, і не призведе до втрати особистої інформації і розголошення персональних даних. Описано створення експериментального онлайн-чату на основі узагальнених потреб та побажань користувачів з урахуванням недоліків подібних програм по безпечності, комфорту користування та надійності. Виділено найбільш важливі проблеми, які потрібно було вирішити при реалізації програмного продукту.

Ключові слова: онлайн спілкування, чати, соцмережі, методи захисту інформації, інтернет простір, інтернет.

Постановка проблеми. Інтернет – важливий елемент сьогодишнього людського життя. Навчання, спілкування з друзями, відпочинок завдяки необмеженим ресурсам глобальної мережі Інтернет стає цікавішим та змістовнішим. Інтернет вміщує великий навчальний, розважальний та інформаційний потенціал, який може становити певну небезпеку та нести деякий ризик. Особливо важливим є захист онлайн-спілкування та особистої інформації в онлайн-чатах.

Метою даної роботи є визначити та охарактеризувати найоптимальніші методи захисту для спілкування в он-лайн.

Виклад основного матеріалу. Як показує практика, в останні роки відбулося значне зростання кількості правопорушень в інформаційній галузі. Ірраціональне поширення суб'єктами персональних даних – причина більшості з них [1].

Окрім цього, одним з важливих аспектів порушення норм захисту особистих даних в інформаційних системах стало незаконне розповсюдження персональної інформації. Ця сторона суспільних відносин на сьогодні досліджена дуже мало. Захист персональних даних - надзвичайно важливе питання, науково-

практичну актуальність якого важко переоцінити. То ж розглянемо детальніше це питання, зробимо спробу проаналізувати його та знайти методи і шляхи вирішення [2].

Виділимо найбільш популярні сервіси та протоколи захисту спілкування в онлайн чатах та соціальних мережах.

Для пересилання захищених повідомлень розроблений криптографічний протокол OTR. Для створення надійного шифрування протокол використовує комбінацію алгоритмів AES, симетричного ключа, алгоритму Діффі - Хеллмана і хеш-функції SHA-1.

Основна перевага OTR перед іншими засобами шифрування це його застосування на льоту, а не після підготовки повідомлення. Він був розроблений Микитою Борисовим і Яном Голдбергом. Для використання в сторонніх додатках розробники протоколу створили клієнтську бібліотеку. Тому, щоб захистити передачу даних по ІМ-каналах, можна скористатися спеціально призначеними для захисту додатками.

Ще один з подібних проектів – Cryptocat [3, 4]. Це додаток з відкритим вихідним кодом, написаний на JavaScript. Розширення можна встановлювати в Chrome, Firefox

і Safari. Крім цього, є клієнтська програма, але тільки для macOS. Cryptocat шифрує повідомлення на стороні клієнта і передає їх довіреному серверу. Для цього на стороні клієнта використовується симетричне шифрування повідомлень і файлів з використанням AES-256 і обраного ключа. Для кожного чату генерується новий ключ.

Інші учасники розмови (до 10 чоловік в кімнаті) зможуть прочитати їх, тільки якщо самі вірно введуть той же самий ідентифікатор. Для надійної передачі ключів використовується алгоритм Діффі – Хеллмана, для генерації унікальних відбитків при аутентифікації – хеш-функція Whirlpool, а для перевірки цілісності повідомлень HMAC-WHIRLPOOL. Метод роботи з ключами перетворює Cryptocat в систему секретності, в якій навіть втрата закритого ключа не може скомпрометувати ключ сесії. Листування видаляється через півгодини відсутності активності, а сам сервіс працює з постійним SSL-шифруванням [2].

Ще один проект подібного роду Bitmessage [5], написаний Джонатаном Уорреном на Python. Bitmessage це децентралізована P2P-програма для обміну зашифрованими повідомленнями між двома або декількома користувачами. Вона використовує сильну криптографію, яка надійно захищає абонентів від прослуховування на рівні інтернет-провайдера або на сервері. Варто зауважити, що криптографічна система практично в точності копіює схему, яка використовується в P2P-системі Bitcoin, однак спрямована на обмін повідомленнями. Особливість Bitmessage полягає в тому, що факт спілкування двох користувачів практично неможливо довести: повідомлення передається не безпосередньо від користувача А до Б, а розсилкою всім учасникам мережі (подібний підхід реалізований в Tor). При цьому прочитати його може тільки той користувач, з яким встановлено з'єднання і який володіє коректним ключем для розшифровки [6].

Останнім проектом цього ряду, який буде розглянуто, буде Tor Chat [7]. Мережа Tor Chat є вільною децентралізованою високоанонімною криптозахищеною системою обміну миттєвими повідомленнями і файлами з відкритим кодом. Tor Chat в основі своїй використовує анонімну мережу Tor, але це повністю відокремлений проект. Анонімність передачі даних в більшості покладена на приховані сервіси Tor, Tor Chat, по суті, лише

надбудова до них, що займається обробкою повідомлень. Криптозахист з'єднання двох користувачів також забезпечується прихованими сервісами Tor за допомогою асиметричного шифрування за стандартом RSA. Спочатку Tor Chat був написаний на Python, а клієнт для macOS, відповідно, на Objective C. На початку 2012 року був запущений проект jTorChat, що розробляється на Java. Поки в ньому не реалізована вся функціональність оригінального Tor Chat, наприклад, відсутня передача файлів.

Також доцільно буде розглянути захищені сервіси для відео конференцій. Одним з таких проектів став Tox відкрита і вільна заміна Skype. Він використовує схожу на Skype модель організації взаємодії в мережі для поширення повідомлень, що використовує криптографічні методи для ідентифікації користувача і захисту транзитного трафіку від перехоплення. Підтримується обмін текстовими повідомленнями, голосовий зв'язок, відеодзвінки і передача файлів. Робота організована через простий і типовий для ІМ-клієнтів графічний інтерфейс.

Одне з ключових завдань проекту забезпечити приватність і таємницю листування, в тому числі захист від можливого аналізу трафіку хакерами. Для забезпечення адресації користувачів використовується розподілена хеш-таблиця (DHT), робота з якою організована в стилі BitTorrent. Канал зв'язку організовується за допомогою надбудови над протоколом UDP з реалізацією сеансового рівня (Lossless UDP).

Для ідентифікації кожного користувача використовується спеціальний публічний ключ, який також застосовується як відкритий ключ для шифрування. Окремо генерується закритий ключ для розшифровки повідомлень, зашифрованих з використанням ідентифікатора / відкритого ключа. Для організації комунікацій потрібно з'єднання до піру (англ. peer-to-peer), який може бути визначений вручну, або знайдений автоматично (доступна функція пошуку пірів в локальній мережі).

Код Tox написаний на мові C і поширюється під ліцензією GPLv3. Підтримуються платформи Linux, Windows і macOS. Для організації шифрування використовується бібліотека libsodium. Функціональність розробки поки знаходиться на рівні серії тестових прототипів, консольного клієнта, написаного з використанням бібліотеки ncurses, і графічного клієнта на базі Qt5.

Крім того, в операційній системі GNU[8] створюється альтернатива під назвою GNU Free Call. Цей проект націлений на розробку і впровадження по всьому світу безпечних і самоорганізованих комунікаційних сервісів. В якості базового протоколу в GNU Free Call буде використовуватися SIP, підтримка якого забезпечена за допомогою VoIP-сервера GNU SIP Witch. Комунікаційна мережа побудована з використанням P2P-технологій і має топологію mesh-мережі, в якій кожна клієнтська точка мережі пов'язана через сусідні клієнтські точки. Кінцевою метою проекту є формування VoIP-мережі, що нагадує Skype за можливостями і зручністю використання.

З технічного боку для реалізації проекту в GNU SIP Witch, крім функції маршрутизації SIP-дзвінків, буде забезпечена підтримка роботи в ролі захищеного VoIP-проксі, додана можливість зберігання кеша хостів і виконання функцій обміну маршрутами з сусідніми вузлами mesh-мережі. Підтримка VoIP-проксі дозволить спростити побудову призначених для користувача інтерфейсів і створення додатків для мобільних пристроїв, оскільки забезпечить підтримку прийому і здійснення дзвінків з будь-яких SIP-сумісних програмних телефонів.

Клієнтське ПЗ для роботи в мережі GNU Free Call буде підтримувати широкий спектр різноманітних програмних платформ. Мережа буде мати повністю децентралізовану структуру, не прив'язану до окремих керуючим серверів.

Взагалі, поняття соціальні мережі слабо в'яжуться з концепцією анонімності та конфіденційності листування. Ці сервіси стали джерелом інформації про осіб різного віку: люди пишуть в соцмережі все про себе, своїх близьких і друзів, викладають життєві фото і відео. Можна обмежити доступ до цих відомостей, але це не перешкода для спецслужб. Відомі випадки, коли за запитом влади їм передавалися цікаві для них дані про користувачів. Безумовно, соцмережі це не найкращий спосіб для спілкування. Але іноді хочеться поділитися чимось з рідними або розповісти про досягнення близьким друзям. Тому, навіть, соцмережі відіграють позитивну роль.

Щоб захистити свої приватні дані від шахраїв, хакерів або спецслужб, можна скористатися вільними захищеними аналогами. У них, звичайно, набагато менше користувачів, але тим краще. І чим більше користувачів

будуть розуміти значущість приватності інформації, а до цього все йде, тим більше їх число буде переходити в захищені соцмережі.

Одна з таких мереж Friendica. Проект було розпочато в 2011 році Майком Макгрівіном. Friendica вільна соціальна мережа з відкритим вихідним кодом, що дислокується на GitHub. Вона надає широкий вибір конекторів для різноманітних соціальних мереж: як традиційних (Facebook, Twitter), так і нових (Diaspora, Identi.ca). Крім того, за допомогою Friendica можна обмінюватися листами і читати RSS-стрічки. Якщо в Friendica зробити фото закритим, то воно насправді буде в публічному чаті і ніхто (крім, природно, власника і обраних ним осіб) не зможе отримати до нього доступ.

В даний час йде розробка наступної версії соцмережі під назвою Red (що з іспанського означає «мережу»). За словами авторів, під час розробки Friendica були усвідомлені деталі і обкатані механізми розробки соцмереж, тому наступний проект стане ще кращим і буде позбавлений від фундаментальних недоліків першої версії.

Ще одна захищена соціальна мережа, на яку можна звернути увагу, – це Diaspora [9]. Дана мережа базується на трьох базових принципах. На відміну від традиційних соцмереж, де дані зберігаються в одному дата-центрі, в Diaspora, як і в багатьох захищених в Інтернеті продуктах, дані зберігаються децентралізовано. У цьому випадку дані зберігаються не на центральному сервері, а на подах (pod) - комп'ютерах тих користувачів, хто надав їх для цієї мети. Другий принцип, звичайно ж, свобода. Третій принцип - секретність. Ніхто, крім вас, не має доступу до ваших даних, а хто може їх переглядати, визначаєте ви самі, встановлюючи дозволи. Дані принципи діють глобально, тобто ніхто їх не порушить.

На основні дослідження методів захисту спілкування, розглянутих вище, можливо сформувати алгоритм роботи для учасників онлайн-чатів.

1. На веб-сайті чату чи соціальної мережі потрібно читати положення політики приватності (іноді її називають "політикою конфіденційності") і читати пункти, що відносяться до безпеки ваших даних. Скажімо, чи залишає власник мережі за собою право використовувати цю інформацію в маркетингових дослідженнях.

2. З'ясовуємо, які програмні способи пропонує власник мережі для захисту даних. Наприклад, при заповненні профілю користувача, чи можна поставити потрібну помітку, щоб ця інформація не показувалася іншим користувачам.

3. Якщо планується проведення якоїсь онлайн-акції, можливо, слід завести для цього інший аккаунт, а не той, який був використаний в попередній акції або хоча б інший псевдонім (нік).

4. При обранні онлайн чату потрібно бути обережним, якщо є потреба користуватися своїм акаунтом з чужого комп'ютера. Не забувати очищати історію і кеш браузера і видаляти збережений ним пароль.

5. По можливості використовувати захищений (SSL) доступ ([https: // ...](https://...)). Таким чином можна шифрувати сеанси зв'язку між вашим браузером і мережею.

Онлайн чат може містити інструменти для інтеграції з іншими подібними мережами або сервісами. Наприклад, при публікації чого-небудь в Twitter, ця новина автоматично з'являється на сторінці користувача в Facebook. Потрібно бути обережним з інтеграцією. На будь-якому ресурсі можна діяти анонімно і відчувати себе захищеним, але лише до певного часу. Автоматична інтеграція може розкрити особистість користувача [10].

6. Не потрібно використовувати чат або інший подібний сервіс в якості основного сховища інформації. Це не особистий сайт певного користувача, а резервне копіювання, зазвичай, не входить в набір стандартних інструментів. Якщо рішенням власника (а може, і під тиском уряду) сторінка користувача виявиться заблокованою або видаленою, відновити її буде неможливо. Потрібно пам'ятати, що власнику мережі простіше позбутися від "незручного" користувача, ніж вступати в конфлікт з урядом, ризикуючи втратити набагато більше [11].

У багатьох соціальних мережах можна поспілкуватися з друзями в реальному часі. Мабуть, немає менш безпечного способу обмінюватися інформацією в інтернеті, ніж цей. Якщо все-таки без чату не обійтися, потрібно переконатися, що всі учасники розмови увійшли на сайт з використанням захищеного протоколу ([https: // ...](https://...)), а краще скористатися якою-небудь незалежною програмою для обміну миттєвими повідомленнями.

На основі проведеного дослідження було спроектовано та розроблено експериментальний чат з урахуванням всіх недоліків подібних програм та побажань користувачів. Для розробки було обрано мову програмування PHP. Графічний інтерфейс оформлено за допомогою мови розмітки HTML та мови стилів CSS. Також в інтерфейсі присутні функції, що реалізовані на JS та JQuery. Це додає програмі динамічності та швидкості. Чат має стандартну для подібних програм архітектуру «клієнт - сервер» та посилений декількома сторонніми сервісами авторизації використовуючи API цих сервісів.

Одним з таких сервісів є SMS авторизація. Цей сервіс є доволі поширеним, але мало хто використовує його в своїх продуктах так як більшість таких сервісів є платними. В розробленому чаті SMS авторизація представлена зв'язком профілю користувача з номером його телефону. При кожній авторизації, крім введення логіну та пароля, користувач буде отримувати код підтвердження на свій мобільний телефон. Це називається двофакторною авторизацією.

База даних користувачів зашифрована два рази підряд використовуючи алгоритм шифрування MD5 з додаванням додаткового слова (salt). Якщо припустити, що база даних буде викрадена, то на розшифрування даних піде дуже багато часу, або дані розшифрувати буде взагалі неможливо.

Також важливою частиною таких чатів є обмін файлами з різноманітними розширеннями. Це є доволі проблемною частиною тому, що файли можуть містити прихований код який може бути використаний щоб нанести шкоду системі. Таким способом можна викрасти особисті дані користувачів або навіть базу даних. Ця проблема вирішена використанням стандартних функцій мови PHP для розпізнавання та очистки файлів та повідомлень від вставок програмного коду. Статистичні дані показують, що дані функції працюють доволі непогано і їх можна використовувати для розробки. Додатково потрібно зазначити, що сьогодні у більшості хостинг-провайдерів є функції які додатково захищають системи від вставок шкідливого коду.

В результаті було розроблено експериментальний онлайн-чат, в якому враховано більшість потреб користувачів по комфорту, безпеці та надійності. Система, звичайно, не є ідеальною але повністю підходить для вико-

ристання в корпоративних цілях для невеликих компаній, що не хочуть використовувати глобальні сервіси. При наявності ресурсів, даний програмний продукт можна поширювати та використовувати для більшої кількості користувачів.

Висновки. Було розглянуто декілька програм та програмних комплексів для обміну повідомленнями та спілкування в мережі.

Розглянуто методи захисту при он-лайн спілкуванні та сформульовано найоптимальніший алгоритм роботи для учасників онлайн-чатів.

В результаті дослідження було розроблено експериментальний онлайн-чат, в якому враховано та вдосконалено недоліки існуючих програмних продуктів.

Список літератури

1. Мироненко А. В. Темпоральні виміри Інтернет-реальності. *Психологічні та педагогічні проблеми Інтернет-реальності : наук.-практ. сем., 14 лютого 2012 р.*: тези доп. Київ, 2012. URL: http://ispp.org.ua/podiy_37.htm – Назва з екрану.
2. Удалова О. А., Швед О. В., Євсюкова М. В. та ін. Безпечне користування сучасними інформаційно-комунікативними технологіями: методичні рекомендації. К.: Україна, 2010. 72 с. URL: http://static.klasnaocinka.com.ua/uploads/editor/4916/401901/sitepage_71/files/bezpechne_koristuvannya_ikt.pdf – Назва з екрану.
3. Greenberg A. Crypto.cat Aims To Offer Super-Simple Encrypted Messaging. *Forbes*. URL: <https://www.forbes.com/sites/andygreenberg/2011/05/27/crypto-cat-aims-to-offer-super-simple-encrypted-messaging> – Назва з екрану.
4. Kirk J. Cryptocat Aims for Easy-to-use Encrypted IM Chat. *IDG News Service*. URL: https://www.pcworld.com/article/251837/cryptocat_aims_for_easytouse_encrypted_im_chat.html – Назва з екрану.
5. Cawrey D. Bitmessage is the Bitcoin of online communication. *CoinDesk*. URL: <https://www.coindesk.com/bitmessage-is-the-bitcoin-of-online-communication/> – Назва з екрану.
6. Павленко Д. Як захистити персональні дані. URL: <http://www.epravda.com.ua/>

- columns/2011/09/30/300156/ – Назва з екрану.
7. Interview with Bernd Kreuss of TorChat. *Free Software Foundation*. URL: <https://www.fsf.org/blogs/licensing/interview-with-bernd-kreuss-of-torchat> – Назва з екрану.
8. Ru.wikipedia.org. GNU. URL: <https://ru.wikipedia.org/wiki/GNU>.
9. Vernon A. Striking back at Facebook, the open-source way. *Network World*. URL: <https://www.networkworld.com/article/2230713/microsoft-subnet/striking-back-at-facebook--the-open-source-way.html> – Назва з екрану.
10. Обуховська Т. І., Шуляк В. П. Персональні дані: теорія та реальність. *Електронне урядування*. 2011. № 2. С. 76–88.
11. Обуховська Т. І. Нормативно-правове забезпечення обробки та циркуляції персональних даних. *Вісн. НАДУ*. 2011. № 4. С. 119–126.

References

1. Myronenko, A. (2012) Temporalni vymiry Internet-realnosti. In: *Psychologichni ta pedagogichni problemy Internet-realnosti*. [online] Kiev. URL: http://ispp.org.ua/podiy_37.htm [Accessed 2 Nov. 2017].
2. Udalova O. and Shved O. and Yevsyukova M. (2010) *Bezpechne korystuvannya suchasnyimi informacijno-komunikatyvnymy tekhnologiyamy: metodychni rekomendaciyi* [online] Kiev. URL: http://static.klasnaocinka.com.ua/uploads/editor/4916/401901/sitepage_71/files/bezpechne_koristuvannya_ikt.pdf [Accessed 2 Nov. 2017].
3. Greenberg, A. (2011) Crypto.cat Aims To Offer Super-Simple Encrypted Messaging. [online] Forbes.com. URL: <https://www.forbes.com/sites/andygreenberg/2011/05/27/crypto-cat-aims-to-offer-super-simple-encrypted-messaging> [Accessed 2 Nov. 2017].
4. Kirk, J. (2012) Cryptocat Aims for Easy-to-use Encrypted IM Chat. [online] PCWorld. URL: https://www.pcworld.com/article/251837/cryptocat_aims_for_easytouse_encrypted_im_chat.html [Accessed 2 Nov. 2017].
5. Cawrey, D. (2013). Bitmessage is the Bitcoin of online communication - CoinDesk.

- [online] CoinDesk. URL: <https://www.coindesk.com/bitmessage-is-the-bitcoin-of-online-communication/> [Accessed 3 Nov. 2017].
6. Pavlenko, D. (2011). Yak zaxystyty personalni dani. [online] epravda.com. URL: <http://www.epravda.com.ua/columns/2011/09/30/300156> [Accessed 3 Nov. 2017].
7. Fsf.org. (2017). Interview with Bernd Kreuss of TorChat — Free Software Foundation — working together for free software. [online] URL: <https://www.fsf.org/blogs/licensing/interview-with-bernd-kreuss-of-torchat> [Accessed 3 Nov. 2017].
8. Ru.wikipedia.org. (2017). GNU. [online] URL: <https://ru.wikipedia.org/wiki/GNU> [Accessed 4 Nov. 2017].
9. Vernon, A. (2017). Striking back at Facebook, the open-source way. [online] Network World. URL: <https://www.networkworld.com/article/2230713/microsoft-subnet/striking-back-at-facebook--the-open-source-way.html> [Accessed 5 Nov. 2017].
10. Obuxovska, T. and Shulyak, V. (2011). Personalni dani: teoriya ta realnist. *Elektronne uryaduvannya*, (2), pp.76-88.
11. Obuxovska, T. (2011). Normativno-pravove zabezpechennya obrobky ta cyrkulyaciyi personalnyx danyx. *Visnyk NADU*, (4), pp.119-126.

T. V. Myronyuk, Ph.D.,

associate professor of information security and computer engineering chair,

e-mail: tanjamiron85@gmail.com,

L. T. Duda, master,

e-mail: lyubomir-duda@ukr.net,

Cherkasy State Technological University,
Shevchenko blvd., 460, Cherkasy, 18006, Ukraine

RESEARCH OF ONLINE COMMUNICATION PROTECTION METHODS

This article discusses the basic methods of protecting online communication on the example of applications and software systems for messaging. The problem of excessive dissemination of personal data by users is revealed. The main technologies of protection of personal information on the Internet are investigated. Particular attention is paid to the review of specialized software for the secure exchange of messages on the information currently available on the market. Basic rules are formulated for users whose adherence to, communication and content sharing on the Internet will become more secure and will not result in loss of personal information and disclosure of personal data. Describes the creation of an experimental online chat based on the general needs and wishes of users, taking into account the drawbacks of similar programs for safety, comfort and reliability. Highlights the most important issues that need to be addressed when implementing a software product.

Keywords: online communication, chats, social networks, methods of information security, internet space, internet.

Рецензенти: Т. О. Прокопенко, д.т.н., доцент,

О. В. Кириченко, д.т.н., с.н.с.

Ю. Г. Лега, д.т.н., професор,
О. С. Гавриш, к.ф.-м.н., доцент,
А. О. Іващенко, аспірант,
О. В. Бурдукова, аспірант,
М. О. Багрій, студент

Черкаський державний технологічний університет
бул. Шевченка, 460, Черкаси, 18006, Україна

АНАЛІЗ ПОТЕНЦІЙНИХ ХАРАКТЕРИСТИК КВАДРАТИЧНОГО АЛГОРИТМУ ВИМІРЮВАННЯ АМПЛІТУДИ ГАРМОНІЧНОГО СИГНАЛУ З ФЛУКТУЮЧОЮ ЧАСТОТОЮ ПРИ КОГЕРЕНТНОМУ ПРИЙОМІ

В роботі досліджуються потенційні точнісні характеристики лінійного та квадратичного алгоритмів вимірювання амплітуди гармонічного сигналу з флуктуючою частотою при когерентному прийомі, за умови впливу асиметрично-ексцесної завади. Показано, що при синтезі поліноміальних алгоритмів методом максимізації поліному, їх точність може зростати за рахунок врахування тонкої структури завади у вигляді кумулянтів вищих порядків. Обґрунтовано, що точність квадратичного алгоритму вимірювання амплітуди гармонічного сигналу з флуктуючою частотою може бути максимальною за умови, що кумулянтні коефіцієнти 3-го та 4-го порядків, що описують адитивну заваду, прагнуть до грані ОДЗ.

Ключові слова: *точнісні характеристики, метод максимізації поліному, дисперсія оцінки, кількість добутої інформації про параметр, амплітуда, флуктуація частоти, гармонічний сигнал, когерентний прийом, коефіцієнти асиметрії та ексцесу.*

Вступ. В багатьох сучасних системах зв'язку їх параметри та характеристики напряму залежать від стабільності частоти сигналу. Проте флуктуація параметрів сигналу є невід'ємною частиною процесу передачі інформації по каналу зв'язку і закладена в самій природі цих явищ [1, 2]. Наприклад, у РЛС нестабільність частоти гетеродина впливає на точність опрацювання доплерівської інформації, а у системах зв'язку з цифровою модуляцією нестабільність частоти призводить до зростання амплітуди вектора помилок (EVM), що відображається на пропускній здатності систем [3].

В роботах [4-7] наведено результати оцінки параметрів гармонічного сигналу з флуктуючою частотою, коли в якості математичного опису випадкової величини використовуються щільність розподілу. Такий підхід забезпечує оптимальність отримуваних результатів, проте не є гнучким для широкого класу завад. В роботі [8] синтезовано обчислювальні алгоритми вимірювання амплітуди гармонічного сигналу за умови впливу адитивної негауссівської завади, яка описується кінцевою послідовністю кумулянтів [9].

Для аналізу поліноміальних алгоритмів оцінки амплітуди гармонічного сигналу також доцільно використовувати метод максимізації поліному (ММПл) [10, 11].

Постановка задачі. В даній роботі ставиться задача дослідити асимптотичні властивості квадратичного алгоритму вимірювання амплітуди гармонічного сигналу з флуктуючою частотою при когерентному прийомі, який було синтезовано в роботі [8], в умовах дії негауссівських завад. Особливістю моделей завад, що використовуються в роботі [8], є їх моментно-кумулянтне представлення, що зумовлює накладання певних обмежень на їх параметри при поліноміальній обробці сигналу, що приймається. Так, при квадратичній обробці сигналу модель завади описується кінцевою послідовністю кумулянтів χ_2 , χ_3 , χ_4 . Згідно з класифікацією випадкових величин, наведеною в роботах [10, 11], така завада називається асиметрично-ексцесною випадковою величиною. Лінійний алгоритм, синтезований методом максимізації поліному при $s=1$ співпадає з алгоритмом, отриманим при використанні методу максимальної правдопо-

дібності, і є оптимальним для гауссівської завади. Для з'ясування впливу негауссовості завади у вигляді кумулянтів 3-го та 4-го порядків на точнісні властивості досліджуваного алгоритму необхідно провести порівняння точнісних характеристик квадратичного та лінійного алгоритмів.

Метою роботи є аналіз точнісних характеристик квадратичного алгоритму вимірювання амплітуди A гармонічного сигналу з флуктуючою частотою при когерентному прийомі при різних параметрах асиметрично-ексцесної завади і визначення умов, за яких виграш в точності оцінювання при квадратичному опрацюванні буде максимальним порівняно з лінійним алгоритмом.

Результати роботи. Дослідимо точнісні властивості алгоритмів вимірювання амплітуди гармонічного сигналу з флуктуючою частотою при когерентному прийомі, отриманих ММПл при $s = 1, 2$ [8]. Згідно методу максимізації поліному, дисперсія оцінки параметру дорівнює величині, зворотній кількості добутої інформації про скалярний параметр

$$\sigma_{(A)s}^2 = J_{sn}^{-1}, \quad (1)$$

де

$$J_{sn} = \sum_{i=1}^s \sum_{v=1}^n k_{iv}(A) \frac{dm_{iv}(A)}{dA}. \quad (2)$$

Використовуючи оптимальний коефіцієнт $k_{1v}(A)$, знайдений в роботі [8], а також вираз для похідної від початкового моменту 1-го порядку за параметром A , легко знайти вираз для кількості добутої інформації про шуканий параметр A при $s = 1$

$$J_{1n} = \sum_{v=1}^n \frac{b^2 \cos^2 \alpha}{\frac{A^2}{2}(1 + b^4 \cos 2\alpha - 2b^2 \cos^2 \alpha) + \chi_2}. \quad (3)$$

Очевидно, що дисперсія оцінки амплітуди гармонічного сигналу, знайденої методом максимізації поліному при $s = 1$, прийме вид

$$\sigma_{(A)1}^2 = \frac{\chi_2}{\sum_{v=1}^n \frac{q}{2} \frac{b^2 \cos^2 \alpha}{(1 + b^4 \cos 2\alpha - 2b^2 \cos^2 \alpha) + 1}}, \quad (4)$$

де $q = A^2 / \chi_2$ відношення сигнал-завада за потужністю.

З останнього виразу видно, що дисперсія лінійної оцінки амплітуди гармонічного сигналу з флуктуючою частотою при когерентному прийомі прямо пропорційна дисперсії завади χ_2 і відношенню сигнал-завада q .

Використовуючи оптимальні коефіцієнти $k_{1v}(A)$ і $k_{2v}(A)$ [8], можна знайти кількість добутої інформації про параметр A при степені поліному $s=2$

$$J_{2n} = \sum_{v=1}^n \frac{1}{\Delta_2} (A^4 a_{4i} + A^2 \chi_2 a_{2i} + A a_{1i} \chi_2^{\frac{3}{2}} \gamma_3 + \chi_2^2 b^2 \cos^2 \alpha (2 + \gamma_4)), \quad (5)$$

де

$$\begin{aligned} a_{4i} &= \frac{1}{2} b^{12} \cos^3 2\alpha + \frac{3}{2} b^4 \cos 2\alpha + \frac{3}{2} b^8 \cos^2 2\alpha - \frac{1}{4} b^{10} \cos^2 \alpha \cos^2 2\alpha - \frac{3}{2} b^6 \cos^2 \alpha \cos 2\alpha + \\ &+ \frac{1}{2} - \frac{11}{8} b^2 \cos^2 \alpha + \frac{1}{8} b^{18} \cos^2 \alpha \cos 4\alpha - \frac{1}{2} b^{10} \cos \alpha \cos 3\alpha - \frac{1}{2} b^{14} \cos \alpha \cos 2\alpha \cos 3\alpha; \\ a_{2i} &= -2b^6 \cos^2 \alpha \cos 2\alpha + 2b^4 \cos 2\alpha + b^8 \cos^2 2\alpha + 1 - 2b^2 \cos^2 \alpha; \\ a_{1i} &= -2b^5 \cos \alpha \cos 2\alpha - 2b \cos \alpha + 4b^3 \cos^3 \alpha. \end{aligned}$$

Використовуючи вираз (5) можна знайти дисперсію оцінки амплітуди гармонічного сигналу при степені поліному $s=2$

$$\sigma_{(A)2}^2 = \frac{\chi_2}{\sum_{v=1}^n \frac{q^2 a_{4i} + q a_{2i} + \sqrt{q} a_{1i} \gamma_3 + (2b^2 \cos^2 \alpha + b^2 \cos^2 \alpha \gamma_4)}{\frac{1}{16} q^3 a_{60} + q^2 a_{40} + q^{1.5} \gamma_3 a_{30} + q a_{20} + (2 - \gamma_3 + \gamma_4)}}. \quad (6)$$

Для порівняння дисперсій оцінок виду (6) і (4) знайдемо коефіцієнт ефективності оцінки:

$$g_{21} = \frac{\sigma_{2(A)}^2}{\sigma_{1(A)}^2} = \frac{\sum_{v=1}^n \frac{b^2 \cos^2 \alpha}{\frac{q}{2}(1+b^4 \cos 2\alpha - 2b^2 \cos^2 \alpha) + 1}}{\sum_{v=1}^n \frac{q^2 a_{4i} + q a_{2i} + \sqrt{q} a_{1i} \gamma_3 + (2b^2 \cos^2 \alpha + b^2 \cos^2 \alpha \gamma_4)}{\frac{1}{16} q^3 a_{60} + q^2 a_{40} + q^{1.5} \gamma_3 a_{30} + q a_{20} + (2 - \gamma_3^2 + \gamma_4)}}. \quad (7)$$

Коефіцієнт ефективності оцінки залежить не лише від параметрів завади, а й від відношення сигнал/завада. Фіксуємо параметр $q = A^2 / \chi_2$, можна побудувати залежність коефіцієнта ефективності від коефіцієнта асиметрії γ_3 при фіксованих значеннях γ_4 . На рис.1 наведено графіки коефіцієнта ефективності g_{21} для різних значень сигнал/завада $q = \{0,25; 1; 9\}$, з яких видно, що криві накладаються одна на іншу, отже величина виграшу g_{21} не залежить від співвідношення сигнал/завада. Графік має симетричний характер відносно осі ординат, оскільки функція g_{21} є парною відносно параметра γ_3 .

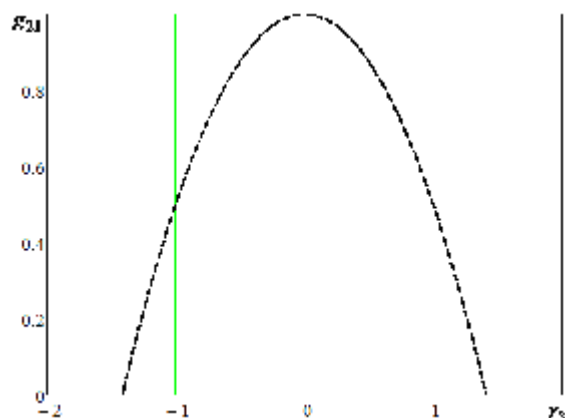


Рис. 1. Залежність коефіцієнта ефективності оцінки від коефіцієнта асиметрії при $\gamma_4 = 0$ при різних значеннях сигнал/завада

На рис. 2 досліджено залежність коефіцієнта ефективності оцінки від коефіцієнта асиметрії при фіксованому значеннях коефіцієнта ексцесу $\gamma_4 = \{-1,5; 0; 1,5; 4\}$. Для кожного значення γ_4 коефіцієнт асиметрії має інтервал допустимих значень. Якщо коефіцієнт асиметрії прагне до границі своєї області визначення, то виграш в точності вимірювання може значно зростати (одиниці та десятки разів). У разі, якщо сигнал приймається на тлі симетричних завад ($\gamma_3 = 0$), то точність дисперсії не

змінюватиметься, навіть якщо коефіцієнт ексцесу відмінний від нуля.

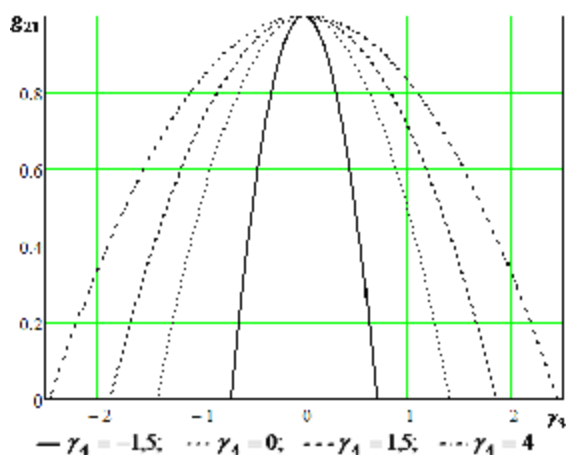


Рис. 2. Залежність коефіцієнта ефективності оцінки від коефіцієнта асиметрії при фіксованих значеннях коефіцієнта ексцесу

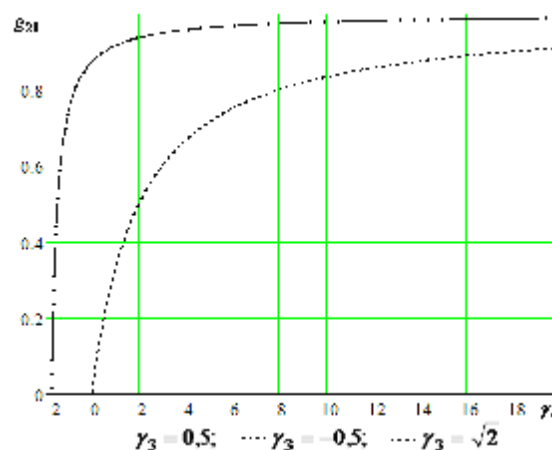
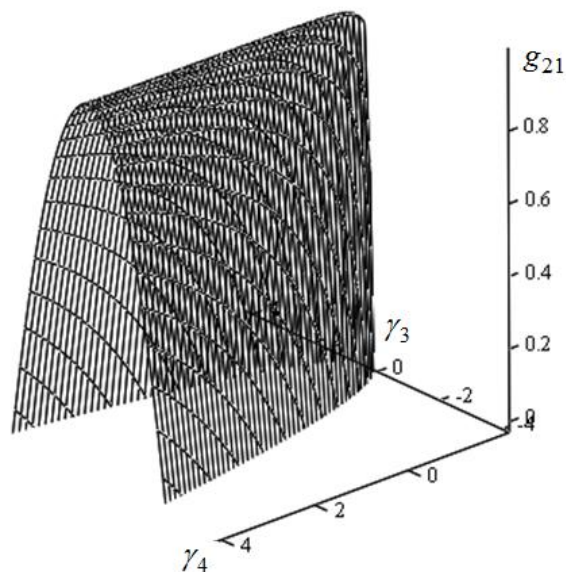


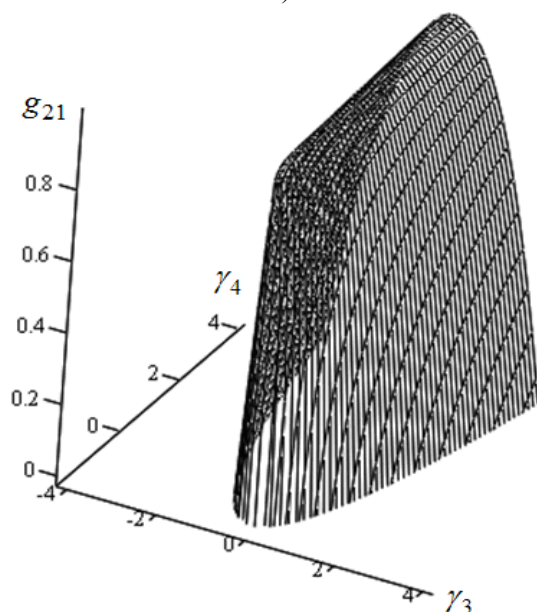
Рис. 3. Залежність коефіцієнта ефективності оцінки від коефіцієнта ексцесу γ_4 при фіксованих значеннях коефіцієнта асиметрії

На рис. 3 наведено залежність коефіцієнта ефективності оцінки від коефіцієнта ексцесу γ_4 при фіксованих значеннях коефіцієнта асиметрії $\gamma_3 = \{-0,5; 0,5; \sqrt{2}\}$. З графіку видно, що чим ближчий розподіл завади до си-

метричного ($|\gamma_3| \rightarrow 0$) тим ближчою до сходинкоподібної є форма графіку функції коефіцієнта ефективності оцінки. Це вказує на те, що виграш в оцінці параметру можливий лише при найменших значеннях коефіцієнту ексцесу $\gamma_4 \rightarrow -2$. Для великих значень коефіцієнта асиметрії (наприклад, $|\gamma_3| = \sqrt{2}$) ефективність оцінок зростає ($g_{21} \leq 0,8$) для широкого діапазону значень коефіцієнта ексцесу $\gamma_4 \in (0; 8)$.



а)



б)

Рис. 4. Різні ракурси тривимірного графіка коефіцієнта ефективності оцінки

Загальне уявлення про характер зменшення коефіцієнта ефективності оцінки при одночасній зміні коефіцієнтів асиметрії та ексцесу можна отримати з рис.4, на якому для наочності, наведені різні ракурси тривимірного зображення функціональної залежності. Зміна коефіцієнту асиметрії можлива в діапазоні $\gamma_3 \in (-\infty; \infty)$, а коефіцієнт ексцесу змінюється в інтервалі $\gamma_4 \in (-2; \infty)$.

Висновки. Отримані результати вказують на те, що точність поліноміальних алгоритмів, синтезованих методом максимізації поліному, може покращуватися з ростом степеня поліному. Показано, що для певного сполучення значень параметрів негауссівської задачі квадратичний алгоритм має потенційно вищі точнісні характеристики, порівняно з характеристиками класичного лінійного алгоритму, оптимального при гауссівських задачах. За допомогою побудованих графіків можна оцінити для задач з якими параметрами можна отримати максимальний виграш в точності оцінювання порівняно з лінійним алгоритмом.

Список літератури

1. https://ru.wikibooks.org/wiki/Понятие_о_помехах_и_методы_борьбы_с_ними. Понятие о помехах и методы борьбы с ними.
2. Семенов А.А., Арсеньян Т.И. Флуктуации электромагнитных волн на приземных трассах. М.: Наука, 1978. 272 с.
3. <https://literature.cdn.keysight.com/litweb/pdf/5991-4797RURU.pdf?id=2508814> – Keysight Technologies Анализ стабильности частоты в частотной и временной областях.
4. Гришин Ю. П., Ипатов В. П., Казаринов Ю. М. и др. Радиотехнические системы: учеб. для вузов по спец. «Радиотехника» / под ред. Ю. М. Казаринова. М.: Высш. шк., 1990. 496 с.
5. Патюков В. Г., Патюков Е. В., Силантьев А. А. Оценка отношения сигнал/шум на основе фазовых флуктуаций сигнала. Журнал радиоэлектроники. 2013. №4. 10 с. URL: <http://jre.cplire.ru/iso/apr13/1/text.html>
6. Лезин Ю. С. Введение в теорию и технику радиотехнических систем. М.: Радио и связь, 1986. 280 с.
7. Сосулин Ю. Г. Теоретические основы радиолокации и радионавигации. М.: Радио и связь, 1992. 304 с.

8. Гавриш О. С., Бурдукова О. В., Івашченко А. О., Безпалій Р. О. Поліноміальні алгоритми вимірювання амплітуди гармонічного сигналу з флюктуючою частотою і когерентному прийомі при асиметрично-експоненційній заваді. *Вісник Черкаського державного технологічного університету*. 2017. №1. С. 45–49.
9. Малахов А. Н. Кумулянтный анализ негауссовских случайных процессов и их преобразований. М.: Сов. радио, 1978. 376 с.
10. Кунченко Ю. П. Полиномиальные оценки параметров близких к гауссовским случайных величин. Часть 1. Стохастические полиномы, их свойства и применение для нахождения оценок параметров. Черкассы: ЧИТИ, 2001. 133 с.
11. Kunchenko Yu. Polynomial parameter estimations of close to Gaussian random variables. Germany, Aachen : Shaker Verlag, 2002. 396 p.
5. Patiukov, V. H., Patiukov, E. V., Syantev A.A. (2013) Signal/noise ratio estimation based on signal phase fluctuation. *Zhurnal radioelektroniki*. №4. 10 p. URL: <http://jre.cplire.ru/iso/apr13/1/text.html> [in Russian]
6. Lezin, Yu.S. (1986), *Introduction to the theory and technique of radio systems*. Moscow: Radio i svyaz' [in Russian].
7. Sosulin, Yu. G. (1992) Theoretic bases of radiolocation and radionavigation. Moscow: Radio i svyaz', 304 p. [in Russian].
8. Havrysh, O. S., Burdukova, O. V., Ivashchenko, A. O., Bezpalii, R. O. (2017) Polynomial algorithms for measurement of the amplitude of a harmonic signal with fluctuated frequency and coherent detection at skewness-kurtosis interference. *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu. Seria: Tehnichni nauky*, (1), pp. 45–49 [in Ukrainian].
9. Malahov, A. N. (1978) *Cumulant analysis of the non-Gaussian random processes and their transformations*. M.: Sov. radio, 376 p. [in Russian].
10. Kunchenko, Yu. P. (2001) *Polynomial estimations of parameters of close to Gaussian random variables. Part 1. Stochastic polynomials, their properties and application for parameters estimations*. Cherkassy: CHITI, 133 p. [in Russian].
11. Kunchenko, Yu. (2002) Polynomial parameter estimations of close to Gaussian random variables. Germany, Aachen: Shaker Verlag, 396 p.

References

Yu. G. Lega, *Dr. Tech. Sc., professor*,
O. S. Havrysh, *Ph.D., associate professor*,
A. O. Ivashchenko, *Ph. D.*,
O. V. Burdukova, *Ph. D.*,
M. O. Bagrii, *student*

Cherkasy State Technological University
 Shevchenko blvd, 460, Cherkasy, 18006, Ukraine

ANALYSIS OF POTENTIAL CHARACTERISTICS OF THE QUADRATED ALGORITHM OF MEASUREMENT OF HARMONIC SIGNAL AMPLITUDE WITH FLUCTUATED FREQUENCY IN COHERENT DETECTION

In the paper, an analysis of the exact characteristics of linear and quadratic algorithms for measuring the amplitude of a harmonic signal with a fluctuating frequency with coherent reception, under the influence of an asymmetric and high-frequency noise is carried out. The analytical expres-

sions for the amount of information obtained and the variance of the estimation of the amplitude under the polynomial degree $s=1$ and 2 are obtained. It is shown that with the growth of the polynomial degree, the exact characteristics of the polynomial algorithms can increase with the asymmetric distribution of the additive interference. The gain in the accuracy of the estimation depends on the combination of values of cumulative coefficients of the 3rd and 4th orders. The closer the value of the coefficients of asymmetry and excess to the limit of the range of admissible values, the higher the accuracy of computational algorithms.

Keywords: precision characteristics, polynomial maximization method, dispersion, amount of information about parameter, amplitude, frequency fluctuation, harmonic signal, coherent detection, coefficient of skewness-kurtosis.

Статтю представляє Ю. Г. Лега, д.т.н., професор.

ВІСНИК
Черкаського державного
технологічного університету

СЕРІЯ: ТЕХНІЧНІ НАУКИ
4 • 2017

VISNYK
Cherkaskogo derzhavnogo
tehnologichnogo universitetu

SERIA: TEHNICHNI NAUKY
4 • 2017

COLLECTION OF RESEARCH PAPERS
of Cherkasy State
Technological University

SERIES: ENGINEERING SCIENCES
4 • 2017

Статті друкуються в авторській редакції.

*За точність посилань та достовірність фактичного матеріалу
відповідальність несуть автори. Редакція може не поділяти погляди авторів.
Матеріали друкуються з максимальним збереженням авторської стилістики
та орфографії.*

*Технічний редактор Давиденко К. В.
Комп'ютерна обробка Вознюк Т. І., Костенко О. А.
Коректура Костенко Т. В.*

Видавець – Черкаський державний технологічний університет
бульвар Шевченка, 460, м. Черкаси, 18006.
Свідоцтво про державну реєстрацію ДК № 896 від 16.04.2002 р.

Виготівник – ФОП ГОРДІЄНКО Є.І.
Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру видавців,
виготівників і розповсюджувачів видавничої продукції Серія ДК № 4518 від 04.04.2013 р.
Україна, 18000, м. Черкаси тел./факс: (0472) 56-56-12, (067) 444-28-94
e-mail: book.druk@gmail.com

Формат 60x84 1/8. Гарнітура Times New Roman.
Умовн. друк. арк. 17,20. Обл.-вид. арк. 18,6. Наклад 100 прим. Зам. № 17-240.