НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ І ГЛОБАЛЬНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ

ІНСТИТУТ КІБЕРНЕТИКИ ім. В.М. ГЛУШКОВА

ІНСТИТУТ ЕКОНОМІКИ ТА ПРОГНОЗУВАННЯ

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ В ЕКОНОМІЦІ

№ 3 (16), липень-вересень 2019 р.

Міжнародний науковий журнал

Заснований у липні 2014 р.
Виходить 4 рази на рік

Журнал включено до Переліку наукових фахових видань України, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора і кандидата наук за напрямами фізико-математичні, технічні та економічні науки
(Наказ Міністерства освіти і науки України від 09.03.2016. № 241)

Свідоцтво про реєстрацію журналу КВ № 20259-10659 Р від 14.07.2014

КИЇВ 2019

Рекомендовано до друку Вченою радою Інституту телекомунікацій і глобального інформаційного простору НАН України (протокол № 12 від 20.09.2019 р.)

Журнал публікує оригінальні та оглядові статті, матеріали проблемного та дискусійного характеру, науково-практичні матеріали з питань математичного моделювання в різних сферах господарювання, інформаційного забезпечення процесу моделювання і прогнозування, розвитку кібернетичної складової і застосування сучасних програмно-апаратних засобів для математичного моделювання.

ОСНОВНІ ТЕМАТИЧНІ РОЗДІЛИ ЖУРНАЛУ

- Інформаційні технології в економіці
- Математичні та інформаційні моделі в економіці
- Аналіз, оцінка та прогнозування в економіці
- Дискусійні повідомлення

ЗМІСТ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ

МАТЕМАТИЧНІ ТА ІНФОРМАЦІЙНІ МОДЕЛІ В ЕКОНОМІЦІ

АНАЛІЗ, ОЦІНКА ТА ПРОГНОЗУВАННЯ В ЕКОНОМІЦІ

CONTENTS

INFORMATION TECHNOLOGY IN ECONOMY

MATHEMATICAL AND INFORMATIONAL MODELS IN ECONOMY

ANALYSIS, EVALUATION AND FORECASTING IN ECONOMY

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ

УДК 004.056.53:303.732.4

https://orcid.org/0000-0001-9642-7006
https://orcid.org/0000-0002-0346-0390

А.Б. КАЧИНСЬКИЙ, І.В. СТЬОПОЧКІНА

ІНФОРМАЦІЙНИЙ І КІБЕРНЕТИЧНИЙ ПРОСТОРИ ЯК ДЖЕРЕЛО СУЧАСНИХ ЗАГРОЗ

Анотація. *Виділено найбільш небезпечні тенденції розвитку сучасних загроз, проаналізовано історію вживання термінів "інформаційний простір", "кібернетичний простір" науковим суспільством на основі онлайнових баз публікацій із використанням математичного апарату, зокрема вперше обчислено статистичні характеристики, які дозволяють зробити висновки про взаємозалежність категорій при існуванні водночас суттєвих відмінностей. Для цього здійснено підрахунок кількості наукових публікацій за джерелами JSTOR, ScienceDirect, GoogleScholar, в яких вживаються або цитуються категорії «інформаційний простір», «кіберпростір» (за період 1950-2018 рр.), побудовано відповідні залежності, що ілюструють динаміку змін. Відмічено наявність трьох часових періодів в характері розвитку вживання категорій інформаційного та кібернетичного просторів, які тісно пов'язані із усвідомленням суспільством відповідних класів загроз.*

Ключові слова: *інформаційний простір, кібернетичний простір, веб-колекції публікацій, термінологія, кібербезпека, інформаційна безпека*

DOI: 10.35350/2409-8876-2019-16-3-5-17

Вступ

Однією з важливих науково обґрунтованих категорій загальної теорії безпеки є поняття «джерело загроз». Воно є методологічною базою кількісного виміру стану захищеності об'єктів захисту і віддзеркалює взаємини та протиріччя між особистістю, суспільством, державою, людською спільнотою загалом та оточуючим їх середовищем.

Під джерелом загроз ми розуміємо будь-яку людську діяльність або стан довкілля, що здатні призвести до реалізації загрози і появи в оточуючому їх середовищі вражаючих факторів [1]. На сучасний момент поряд з інформаційним простором, який є джерелом інформаційних загроз [2], виділяється поняття кіберпростору, що породжує клас кібернетичних загроз.

Взаємозалежність між поняттями “інформаційний простір” та “кіберпростір” породжує значні суперечності у їх трактуванні, що негативно впливає на формування і розуміння законодавчої бази у сфері інформаційної та кібернетичної безпеки, а відповідно, впливає і на всі сфери людської діяльності, які керуються відповідними законами.

Питання дослідження змістовного наповнення термінів “інформаційний простір” та “кіберпростір” розглядались в ряді робіт, в тому числі [3-9], авторами яких, зокрема, проаналізовано нормативну базу, законодавче та практичне підґрунтя для відповідних термінів і надано відповідні рекомендації щодо уточнення існуючих визначень.

Однак, дослідження історичних засад становлення та вживаності даних термінів із використанням математичного апарату, який може надати нові висновки щодо їх сутності, проведено не було.

В даній роботі виконано огляд потенційного впливу інформаційного простору та кіберпростору як джерел загроз на сучасне суспільство та сфери діяльності, розглянуто існуючі визначення цих категорій; виконано аналіз вживаності та цитування термінів “інформаційний простір” і “кібернетичний простір” на основі веб-колекцій наукових публікацій JSTOR, Science Direct, Google Scholar; обчислено необхідні статистичні характеристики, які дозволяють зробити висновки про тенденції вживання відповідних термінів науковцями та перспективи їх розвитку. Одержані в даній статті результати є передумовою для подальшого системного аналізу явищ інформаційного та кібернетичного просторів та породжуваних ними загроз.

1. Вплив інформаційного та кібернетичного просторів як джерела загроз на різні сфери діяльності

Вплив кібернетичних та інформаційних загроз на інформаційно-комунікаційні системи, об’єкти критичної інфраструктури і, власне, на саме суспільство постійно ускладнюється і розвивається.

Інформаційне наповнення будь-яких технологій, природно, є складовими кібернетичного чи інформаційного просторів. На часі велика кількість технологій, що тільки народжуються – робототехніка, штучний інтелект, адитивні технології виробництва, синтетична біологія, – глибоко впливатимуть на нас і одночасно будуть породжувати серйозні можливості для шпигунської, кримінальної та терористичної діяльності.

Особливо виділяється нова обчислювальна парадигма Інтернет речей (IoT), як глобальне навколишнє мережеве середовище, створене завдяки постійному розповсюдженню інтелектуальних датчиків, камер і відповідного програмного забезпечення, баз даних в інфраструктурі, що охоплює світ. Як тільки ця парадигма разом із Big Data і хмарними обчисленнями буде остаточно запроваджена, то світ, в якому ми живемо, остаточно і назавжди зміниться.

На думку [10], перед нами – майбутній ураган, що назріває, і несе у собі всі ознаки глобальної катастрофи. Тому аналіз джерел загроз для інформаційної та кібернетичної безпеки на разі є вкрай важливим. За таких умов поняття «інформаційний простір» і «кібернетичний простір» мають вкрай важливе значення для інформаційної та кібернетичної безпеки.

Інформаційний та кібернетичний простори є джерелом загроз і для людської свідомості та людства в цілому. Поява Інтернету призвела до появи нових моделей соціальної взаємодії. З одного боку, віртуальні спільноти, які головним чином базуються на комунікації онлайн, стали тлумачитися як кульмінація історичного процесу у формуванні спільноти загалом [11]. З іншого боку, критики Інтернету доводять, що нові, вибіркові моделі соціальних стосунків можуть стати потужним джерелом злочинів майбутнього [10]. Іншими словами, ми будуємо цивілізацію, що водночас і глибоко взаємопов'язана, і технологічно небезпечна. Ми створюємо світ, пов'язаний зі злочинністю і цілим арсеналом нових загроз особі, суспільству загалом і державі [1].

2. Загальна постановка задачі, об'єкт, предмет та мета досліджень

Швидкість змін у характері та кількості загроз, джерелами яких є інформаційний і, особливо, кібернетичний простори, призводить до необхідності надання чітких визначень, в яких буде окреслено, в чому полягає відмінність між цими двома феноменами, що сприятиме несуперечливому розумінню фахівцями відповідних понять.

Об'єкт досліджень – кібернетичний простір та інформаційний простір. Мета досліджень – виявлення сучасних тенденцій у вживанні категорій "кіберпростір" та "інформаційний простір", пов'язаних із усвідомленням науковим суспільством відповідних загроз. Метою досліджень є встановлення наявності чи відсутності об'єктивних взаємозалежностей та відмінностей у категоріях "інформаційний простір" та "кіберпростір" та одержання необхідних статистичних даних, вибору необхідних інструментів подальшого об'єктивного аналізу явищ інформаційного простору та кібернетичного простору.

3. Визначення інформаційного та кібернетичного простору

Як уже зазначалося, попри всю теоретичну та практичну важливість зазначених вище категорій, в науковій літературі досі не розроблено єдиного підходу щодо їх визначення. Поняття «інформаційний простір» і «кібернетичний простір» розглядаються у великій кількості робіт [3-9, 12-18].

В першу чергу це стосується поняття "інформаційний простір". Окрім того, у низці публікацій як синонім інформаційного простору вживають словосполучення "інформаційне середовище". В деяких роботах ці поняття дещо відрізняють між собою, а саме: "інформаційне середовище" є більш загальним і включає загальнолюдські, психологічні та соціокультурні аспекти, а "інформаційний простір" є більш технічно-орієнтованим поняттям, що передбачає насамперед наявність інформаційних взаємодій із використанням комп'ютерних мереж чи інформаційних технологій різних видів.

На наш погляд, найбільш типовими визначеннями терміну «інформаційний простір», що дають про нього чітке уявлення, є наступні:

Глосарій з інформаційної безпеки України: "Інформаційний простір – інформаційне середовище, в якому здійснюються інформаційні процеси та інформаційні відносини щодо створення, збирання, відображення, реєстрації,

накопичення, зберігання, захисту і поширення інформації, інформаційних продуктів та інформаційних ресурсів, на яке розповсюджується юрисдикція держави" [19].

Лабораторія штучного інтелекту MIT (MIT Artificial Intelligence Laboratory): "Інформаційний простір – це тип інформаційної конструкції, в якому представлення інформаційних об'єктів розташовані в принциповому просторі. В принциповому просторі мають значення місцеположення та напрямок, таким чином є можливими карти та навігація по них" [20].

Кембріджський словник (Cambridge dictionary): "Інформаційний простір – це місце, головним чином веб-ресурс, де інформація доступна" [21].

Фінансовий словник: "Інформаційний простір – сукупність банків і баз даних, технологій їх супроводу та використання, інформаційних телекомунікаційних систем, функціонуючих на основі загальних принципів, і таких що забезпечують інформаційну взаємодію організацій та громадян, задоволення їх інформаційних потреб" [22].

Довідник технічного перекладача: "Інформаційний простір це:

1. Інтегральний електронний інформаційний простір, який утворюється при використанні електронних мереж.

2. Сфери в сучасному суспільному житті світу, в яких інформаційні комунікації відіграють провідну роль. (Тут категорія "інформаційний простір" наближається до категорії "інформаційне середовище").

3. Простір, в якому циркулюють інформаційні потоки.

4. Форма існування інформаційних систем, що характеризується структурністю, протяжністю та диференційованістю" [23].

Навчальна література: "Інформаційне середовище (information environment) – сфера діяльності суб'єктів, що пов'язана зі створенням, перетворенням і використанням інформації. Інформаційне середовище умовно розділяється на три основні складові: створення та поширення інформації, формування інформаційних ресурсів, підготовки продуктів та надання інформаційних послуг, споживання інформації та дві допоміжні складові: створення та використання інформаційних систем, технологій і засобів їх забезпечення; створення і використання засобів і механізмів інформаційної безпеки" [24].

Попри велику зацікавленість міжнародної спільноти, окремих держав в керуванні процесами в кіберпросторі подібна тенденція спостерігається і у визначенні терміну «кібернетичний простір».

Міжнародний стандарт: "Кібернетичний простір це – середовище існування, що виникло в результаті взаємодії людей, програмного забезпечення та послуг в Інтернеті за допомогою технологічних пристроїв і мереж, що під'єднані до них, і якого не існує в будь-якій іншій формі" [12].

США: "Кібернетичний простір це – сфера, що характеризується можливістю використання електронних і електромагнітних засобів для запам'ятовування, модифікування та обміну даними в мережевих системах і пов'язана з ними фізична інфраструктура" [13].

"Кібернетичний простір це – операційний домен, або базова адміністративна одиниця в Інтернеті, форматована для застосування електронним обладнуванням з метою використання інформації за допомогою взаємопов'язаних систем і зв'язаним з ними мережевим устаткуванням" [25].

Євросоюз: “Кібернетичний простір це – віртуальний простір, у якому циркулюють електронні дані світових персональних комп’ютерів. Оскільки теорія систем і системний аналіз в основному орієнтовані на методологічні питання вивчення та опису систем різної природи, можна скористатися методами системної методології наукових досліджень” [13].

Великобританія: “Кібернетичний простір це – всі форми мережевої цифрової активності, що включають у себе контент і дії, здійснювані через цифрові мережі” [13].

Німеччина: “Кібернетичний простір це – вся інформаційна інфраструктура, що доступна через Інтернет поза будь-якими територіальними кордонами” [13].

Україна: “Кібернетичний простір це – віртуальний простір, що отриманий у результаті взаємодії користувачів, програмного й апаратного забезпечення, мережевих технологій (у т.ч. Інтернет) для підтримки та управління процесами перетворення інформації (електронних інформаційних ресурсів) з метою забезпечення інформаційних потреб суспільства” [17].

“Кібернетичний простір це – віртуальне комунікаційне середовище, що утворене системою зв’язків між користувачами та об’єктами інформаційної інфраструктури, такими як електронний інформаційний ресурс, системи та мережі всіх форм власності, керовані автоматизованими системами управління, що використовуються не лише для перетворення та передачі інформації, що в них циркулює, з метою забезпечення інформаційних потреб суспільства, а й для впливу на аналогічні об’єкти протиборчої сторони” [26].

Очевидно, що вищенаведені визначення термінів «інформаційний простір» (інформаційне середовище) та «кібернетичний простір» мають достатньо широкий характер, від загально-філософського до суто технічного.

Попри те, що джерела інформаційних і кібернетичних загроз є реальним чинником неприйнятного ризику, нині існує значна невизначеність щодо цих термінів. Таке ставлення до них зберігається як у наукових виданнях, так і в засобах масової інформації. Це також підтверджується цікавими результатами, в контексті дослідження нашої проблеми, що одержані за допомогою онлайн-словнику [26], де найбільш релевантними синонімами словосполучення “інформаційний простір”(“information space”) є наступні: computer network; information technology; web; Internet; WWW; communications; email. А найбільш релевантними синонімами словосполучення “кібернетичний простір” (“cybernetic space”) є такі: World Wide Web; data bank; data network; electronic highway; electronic mail; global village; infobahn; information superhighway; online community; virtual community; virtual library; virtual reality. Знайдені слова свідчать про розмитість меж між поняттями “інформаційний простір” та “кіберпростір” (cyberspace), для яких даний ресурс надає практично ідентичний перелік релевантних слів.

3. Методика і результати досліджень тенденцій вживання термінів “інформаційний простір” та “кібернетичний простір”

Нині пошукові системи є одним з основних інструментів наукових досліджень, що включає пошук, вибір і збір інформації зі загальнодоступних джерел, з наступним її аналізом. Веб-простір, заснований на фізичній

інфраструктурі мережі Інтернет, об'єднує сотні мільйонів веб-серверів, під'єднаних до мережі Інтернет [27], і може дати необхідну інформацію щодо вживання будь-яких термінів, в тому числі й тих, що розглядаються в даній роботі.

Для аналізу вживаності та цитування термінів "інформаційний простір" і "кібернетичний простір" англійською й українською мовами були використані веб-колекції наукових публікацій JSTOR, Science Direct, Google Scholar. На разі, обсяги публікацій, доступні цим веб-колекціям, включають більшість рецензованих онлайн-журналів Європи й Америки провідних наукових видань.

Здійснений аналіз показав, що згідно з JSTOR (аналогічно Science Direct і Google Scholar) перша згадка терміну "інформаційний простір" припадає на 1959 рік. Попри те, що частота цитування у веб-ресурсах різна, загальна тенденція його використання однакова (рис. 1) – можна виокремити три різні періоди. Перший період повільного зростання припадає на кінець 50-х і початок 60-х років до середини 80-х років минулого століття. Другий період стрімкого зростання припадає на середину 80-х років минулого століття до 2013-2015 років цього століття. Нарешті, третій період стрімкого падіння починається з 2016 р. й продовжується до нині.

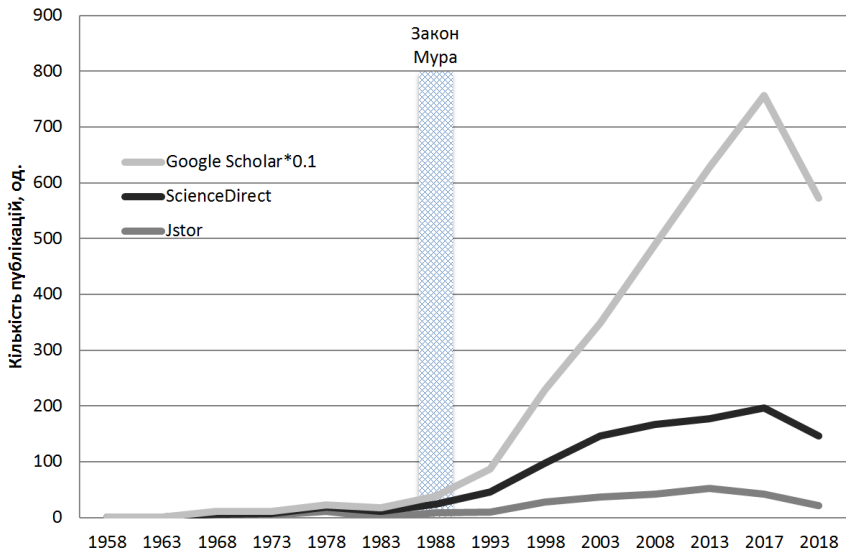

Рисунок 1 – Динаміка використання терміну "Інформаційний простір" в наукових джерелах

Термін «кіберпростір» вперше був введений у вжиток письменником Вільямом Гібсоном у 1982 р. в новелі «Палаючий Хром», а в 1984 році цей термін більш докладно був ним розкритий у творі «Нейромант». Одначе, як можна побачити (рис. 2), термін "кібернетичний простір" починає активно використовуватися в науковій сфері в 1992-1997 роках і досягає піку популярності в 2012-2013 роках.

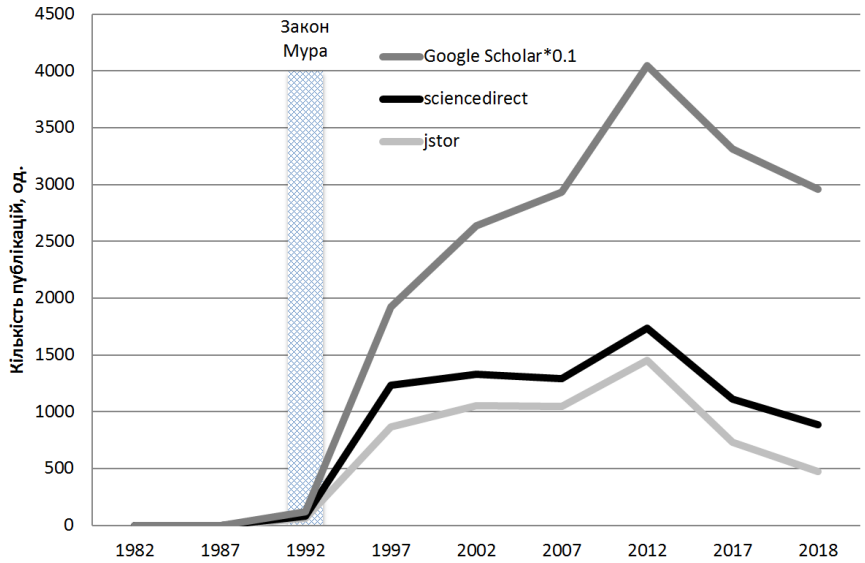

Рисунок 2 – Динаміка використання терміну “Кіберпостір” в наукових джерелах

Попри незначні відмінності, частота цитування терміну “кібернетичний простір” у веб-ресурсах JSTOR, Science Direct і Google Scholar подібна. Також співпадає й загальна тенденція використання цього терміну. Можна виокремити три різні періоди частоти цитування цього терміну: перший період повільного зростання припадає на кінець 80-х і початок 90-х років минулого століття. Другий період стрімкого зростання припадає на початок 90-х і продовжується до 2013 року цього століття. Нарешті, третій період стрімкого падіння починається з 2013 р. й продовжується нині.

Отже, що нам дає інформація про частоту цитування термінів “інформаційний простір” і “кібернетичний простір” у згаданих веб-ресурсах? З одного боку, ми дізнаємося, що термін “інформаційний простір” почав використовуватися раніше терміну “кібернетичний простір” – відповідно кінець 50-х і початок 90-х років. Також можна зазначити загальний характер становлення та розвитку частоти вживання цих термінів, якому властиві три подібні періоди: повільного зростання, стрімкого зростання, стрімкого падіння.

З іншого боку, візуальний аналіз даних (рис. 3) показує, що вони мають різні статистичні характеристики. В першу чергу це стосується медіани, враховуючи специфіку наших рядів, коли відносно невелике число елементів суттєво відрізняється від загальної маси спостережень. Так, медіана терміну “кібернетичний простір” значно більша за медіану терміну “інформаційний простір”. Нагадаємо, що медіана (x_{50}) – це число, яке більше або дорівнює і одночасно менше або дорівнює половині значень ряду розподілу. Міжквартильний інтервал (x_{75} - x_{25}), що дорівнює різниці між 75-м і 25-м процентилями терміну “кібернетичний простір” значно більший терміну “інформаційний простір”. “Вуса”, що йдуть від квартилів до статистично значимих точок x_1 і x_2, де

$$x_1 = \max(x_{min}, x_{25} - 1{,}5\,(x_{75} - x_{25}))$$
$$x_2 = \max(x_{min}, x_{25} + 1{,}5\,(x_{75} - x_{25}))$$

показують, що ряди спостережень не містять викидів, що не входять в статистично значимий діапазон.

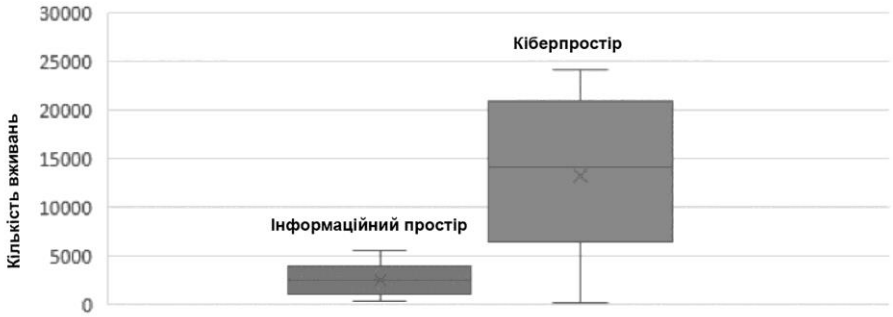

Рисунок 3 – Статистичні характеристики частоти цитування термінів "інформаційний простір" і "кібернетичний простір" в Google Scholar (скринька Тьюкі)

Але є висновок набагато глибший вищенаведених: маємо констатувати, що частота вживання термінів "інформаційний простір" і "кібернетичний простір" у різних сферах життєдіяльності взаємозалежна. На рисунку 4 наведена лінійна регресійна модель частоти вживання цих термінів. Високе значення коефіцієнта детермінації моделі $R^2 = 0{,}94$ підтверджує це припущення. Очевидно, що становлення та розвиток цих взаємопов'язаних термінів "інформаційний простір" і "кібернетичний простір" є історичним явищем, що залежить від розвитку техніки, свідомості людини та психіки.

Першим виникло поняття інформаційний простір тоді, коли з'явився знак (знакові системи). Поняття кібернетичний простір – після того як народилася наука кібернетика, коли теорія керування з'єдналася з теорією інформації, породивши категорію інформаційного контуру зворотного зв'язку. Даний етап розуміння нами цих термінів й частота їх вживання відповідали законам лінійного мислення. З часом кібернетична перспектива оголосила, що два потужні чинники – інформація та керування разом з Інтернетом як новим комунікаційним середовищем є її основними складовими. Тому на разі частота вживання цих термінів перестає відповідати законам лінійного мислення (верхня частина рисунку 4). Очевидно одне: обчислювальна потужність зростає, а наша здатність розуміти глобальну інформаційну мережу – падає. Це також стосується й розуміння термінів "інформаційний простір" і "кібернетичний простір", що знаходить своє відображення у падінні частоти їх використання (рис. 1, 2). Очевидно, що зазначені вище чинники безпосередньо впливають на стан «ментальних» моделей – моделей світу суб'єктів пізнання.

Під моделями світу суб'єктів пізнання розуміють активно використовувану ними сукупність уявлень про сутності та процеси реального світу у результаті накопичення й аналізу індивідуального та соціального досвіду [28].

Більш того, відомий футуролог Р. Курцвейл [29], відзначаючи постійне подвоєння комп'ютерної цінової динаміки і потужностей, пророкує момент у часі, де матиме місце «технологічна сингулярність»: комп'ютерний прогрес

настільки прискориться, що випередить спроможність людства осягнути його і машинний інтелект перевершить людський розум.

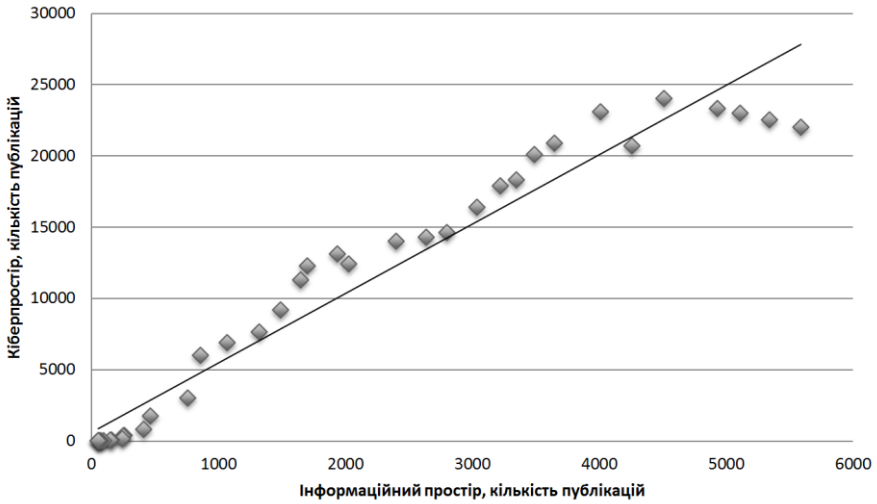

Рисунок 4 – Лінійна регресійна модель частоти цитування термінів “інформаційний простір” і “кібернетичний простір”

Необхідно зазначити, що використання термінів “інформаційний простір” і “кібернетичний простір” в україномовній науковій літературі почалося значно пізніше англомовної літератури і їй притаманний досить несистемний характер.

Підсумковий висновок, який слід відзначити – це те, що частота вживання цих термінів слідує сталому збільшенню (подвоєнню) обчислювальних потужностей комп’ютерів і постійно зростаючій присутності інформаційних технологій в нашому житті, передбаченим аксіомою технології, відомою як «закон Мура» і його наслідками [10]. Ці наслідки також поширюються за межі науки, на всі сфери людської діяльності, в тому числі й на предмет наших досліджень. Вони слідують невблаганній логіці становлення кібернетики як науки, що складається з трьох фаз [30, 31]: гомеостазу, рефлективності кібернетичної парадигми та самоорганізації. А це означає, що криві розвитку всіх комп’ютерних технологій є експоненційними, а не лінійними.

Завдяки комплексності явищ інформаційного та кібернетичного просторів, вирішенню проблеми адекватного визначення термінів «інформаційний простір» (інформаційне середовище) та «кібернетичний простір» може сприяти системна методологія, зокрема структурний підхід до аналізу систем. Будучи різновидом цілеспрямованої дослідницької діяльності, що здійснюється з метою створення оптимального за формою, змістом, а також рівнем деталізації і формалізації представлення наявних даних про складні системи, він може допомогти дати адекватні, адаптовані до предметної області визначення цих понять, що буде предметом наших подальших досліджень.

Висновки

Як показали результати досліджень, першим виникло поняття інформаційний простір, тоді як поняття кібернетичний простір виникло після появи науки кібернетики. Також можна зазначити загальний характер становлення та розвитку частоти вживання цих термінів, якому властиві три подібні періоди: повільного зростання, стрімкого зростання, стрімкого падіння. При цьому вони мають різні статистичні характеристики: медіана терміну "кібернетичний простір" значно більша за медіану терміну "інформаційний простір", а міжквартильний інтервал "кібернетичний простір" значно більший терміну "інформаційний простір".

Лінійний регресійний аналіз показав, що частота вживання термінів "інформаційний простір" і "кібернетичний простір" у різних сферах життєдіяльності взаємозалежна – коефіцієнт детермінації моделі дорівнює 0,94, що підтверджує це припущення.

Очевидно, що становлення та розвиток взаємопов'язаних термінів "інформаційний простір" і "кібернетичний простір" є історичним явищем, що залежить від розвитку техніки, свідомості людини та психіки, і тісно пов'язано із усвідомленням відповідних загроз. Частота вживання цих термінів слідує збільшенню обчислювальних потужностей комп'ютерів і постійно зростаючій присутності інформаційних технологій в нашому житті, що передбачено «законом Мура» і його наслідками. Попри те, що закон Мура в чистому виді через деякий час перестане виконуватись внаслідок технологічних обмежень класичної нейманівської архітектури, обчислювальні можливості, скоріше за все, зростатимуть з рахунок ускладнення підходів до їхньої організації, а отже, кіберпростір та інформаційний простір стануть джерелами все більш складних загроз людству.

На разі поняття «інформаційний простір» і «кібернетичний простір» розглядаються у великій кількості робіт, але попри всю теоретичну та практичну важливість зазначених вище категорій, в науковій літературі досі не розроблено єдиного підходу щодо їх визначення. Вирішенню проблеми адекватного визначення термінів «інформаційний простір» та «кібернетичний простір» може сприяти системна методологія.

Автори вважають своїм приємним обов'язком висловити подяку студентам Фізико-технічного інституту НТТУ "КПІ" ім. Ігоря Сікорського Сьомаку Р. та Яскалу Н. за активну участь в підготовці й оформленні статті до друку.

СПИСОК ЛІТЕРАТУРИ

1. Качинський А.Б. Безпека складних систем // А.Б. Качинський. – К.: ТОВ «Юстон», 2017. – 494 с.
2. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. К.: Видавнича група BHV, 2009. 608 с.
3. Безкоровайный М.М., Татузов А.Л. Кибербезопасность – подходы к определению понятия. Вопросы кибербезопасности. № 1(2), 2014. С. 22-27.
4. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва. К. : НІСД, 2014. 328 с.

5. Архипов А.Е. Приставка кибер- : все ли очевидно? Захист інформації. Т. 18, № 3. 2016. С. 203-209.
6. Грайворонський М.В. Сучасні підходи до забезпечення кібернетичної безпеки. Матеріали XVII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених "Теоретичні і прикладні проблеми фізики, математики та інформатики", НТУУ "КПІ". 2015. С. 1-8.
7. Корченко О.Г., Бурячок В.Л., Гнатюк С.О. Кібернетична безпека держави: характерні ознаки та проблемні аспекти. Безпека інформації. Т.19, №1. 2013. С. 40-44.
8. Марущак А.І. Щодо поняття «інформаційні ресурси держави». Інформаційна безпека людини, суспільства, держави. 2009. №1 (1). С. 11-15.
9. Грищук Р.В. Основи кібернетичної безпеки. Житомир : ЖНАЕУ, 2016. 636 с.
10. Гудмен М. Злочини майбутнього: усе взаємопов'язане, усі вразливі, і що ми можемо з цим зробити. Харків: Вид-во «Ранок»: «Фабула», 2019. 592 с.
11. Кастельс М. Інтернет-галактика – міркування щодо інтернету, бізнесу і суспільства. К.: Ваклер, 2006. 290 с.
12. ISO/IEC 27032. Information technology — Security techniques — Guidelines for cybersecurity. 2012. 50 p. (Інформаційна технологія – Техніки безпеки – Настанови щодо кібербезпеки. Міжнародний стандарт)
13. Присяжнюк М.М., Цифра Є.І. Особливості забезпечення кібербезпеки. Реєстрація, зберігання і обробка даних. Т.19, № 2. 2017. С. 61-68.
14. Шеломенцев В.П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення. Боротьба з організованою злочинністю і корупцією (теорія і практика). №2(28). 2012. С. 299-309
15. Діордіца І.В. Система забезпечення кібербезпеки: сутність та призначення. Підприємництво, господарство і право. №7. 2017. С. 109-116.
16. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека». Правова інформатика. №2(42). 2014. С. 54-62.
17. Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. Безпека інформації. Т. 19, № 2. 2013. С. 118–129.
18. Бурячок В.Л., Толубко Б., Хорошко В.О., Толюпа С.В. Інформаційна і кібербезпека: соціотехнічний аспект. К.:ДУТ. 2015. 288 с.
19. Харченко Л.С. Інформаційна безпека України: Глосарій / Л.С. Харченко, В.А. Ліпкан, О.В. Логінов. К.: Текст. 2004. 136 с.
20. The JAIR Information Space, MIT Artificial Intelligence Laboratory. [Електронний ресурс]. – Режим доступу: http://www.ai.mit.edu/projects/infoarch/jair/jair-space.html
21.Cambridge dictionary. [Електронний ресурс]. – Режим доступу: https://dictionary.cambridge.org/dictionary/english/information-space
22.Финансовый словарь. [Електронний ресурс]. – Режим доступу: https://dic.academic.ru/dic.nsf/fin_enc/23454
23. Справочник технического переводчика. [Електронний ресурс]. – Режим доступу: https://technical_translator_dictionary.academic.ru/78752/информационное_пространство
24. Юдін О.К., Бучик С.С. Державні інформаційні ресурси. Методологія побудови класифікатора загроз. К. : НАУ. 2015. 214 с.
25. Kuehl D.T. From Cyberspace to Cyberpower: Defining the Problem. Cyberpower and National Security. Washington, DC: National Defense University Press. 2009. P. 26-28. (Від Кіберпростору до Кібервлади: визначення проблеми. Кібервлада та національна безпека)
26. Thesaurus [електронний ресурс]. – Режим доступу: https://www.thesaurus.com
27. Додонов А.Г. Распознавание информационных операций / А.Г. Додонов, Д.В. Ланде, В.В. Цыганок, О.В. Андрейчук, С.В. Каденко, А.Н. Грайворонская. К.: ООО «Инжиниринг». 2017. 282 с.
28. Курносов Ю.В. Аналитика: методология, технология и организация информационно-аналитической работы / Ю.В. Курносов, П.Ю. Конотопов. М.: РУСАКИ. 2004. 512 с.

29. Курцвейл Р. Эволюция разума: Как расширение границ нашего разума позволит решать многие мировые проблемы. М.: Эксмо. 2016. 448 с.
30. Хейлз К. Н. Як ми стали постлюдством: Віртуальні тіла в кібернетиці, літературі та інформатиці. К.: Ніка-Центр. 2013. 426 с.
31. Глик Дж. Информация. История. Теория. Поток. М.: Изд-во АСТ: CORPUS. 2016. 576 с.

REFERENCES

1. Kachynskyy A.B. Bezpeka skladnykh system [Security of complex systems] // A.B. Kachynskyy. – K .: Yuston LLC, 2017. – 494 p. (in Ukrainian)
2. Graivoronskyy M.V., Novikov O.M. Bezpeka informatsiyno-komunikatsiynykh system [Security of information and communication systems]. K.: BHV Publishing Group, 2009. 608 p. (in Ukrainian)
3. Bezkorovaynyi M.M., Tatuzov A.L. Kiberbezopasnost – podhody k opredeleniyu poniatiia. [Cybersecurity – approaches to defining a concept]. Voprosy kiberbezopasnosi. No. 1 (2), 2014. P. 22-27. (in Russian)
4. Dubov D.V. Kiberprostir yak novyi vymir geopolitychnogo supernytstva. [Cyberspace as a new dimension of geopolitical rivalry]. K.: NISD, 2014. 328 p. (in Ukrainian)
5. Arkhipov A.E. Pristavka kiber-: vsio li ochevidno? [Prefix cyber: is everything obvious?] Zakhyst infomatsii. Vol. 18, No. 3. 2016. P. 203-209. (in Russian)
6. Graivoronskyy M.V. Suchasni pidkhody do zabezpechennia kibernetychnoyi bezpeky [Current approaches to cyber security]. Materials of the XVII All-Ukrainian scientific-practical conference of students, graduate students and young scientists "Theoretical and applied problems of physics, mathematics and informatics", NTUU "KPI". 2015. P. 1-8. (in Ukrainian)
7. Korchenko O.G., Buryachok V.L., Gnatyuk S.O. Kibernetychna bezpeka derazhavy: kharakterni oznaky ta problemni aspekty [State Cyber Security: Characteristics and Problem Aspects]. Bezpeka informatsii. Vol. 19, No. 1. 2013. P. 40-44. (in Ukrainian)
8. Marushchak A.I. Shchodo poniattia “informatsiyni resursy derzhavy” [On the concept of "information resources of the state."]. 2009. №1 (1). P. 11-15. (in Ukrainian)
9. Grishchuk R.V. Osnovy kibernetychnoyi bezpeky. [Fundamentals of cyber security]. Zhytomyr: ZhNAEU, 2016. 636 p. (in Ukrainian)
10. Goodman M. Zlochyny maybutniogo: vse vzayemopoviazane, usi vrazlyvi, i shcho my mozhemo z tsym zrobyty. [The crimes of the future: everything is interconnected, everything is vulnerable, and what we can do about it]. Kharkiv: Ranok: Fabula, 2019. 592 p. (in Ukrainian)
11. Castels M. Internet-galaktyka – mirkuvannia shchodo internetu, biznesu I suspilstva. [Internet Galaxy – reflections on the Internet, Business and Society]. K .: Wackler, 2006. 290 p. (in Ukrainian)
12. ISO / IEC 27032. Information technology – Security techniques – Guidelines for cybersecurity. 2012. 50 p. (in English)
13. Prysiazhniuk M.M., Tsyphra E.I. Osoblyvosti zabezpechennia kiberbezpeky. [Cybersecurity Features. Registration, storage and processing of data]. Vol. 19, No. 2. 2017. P. 61-68. (in Ukrainian)
14. Shelomentsev V.P. Sutnist organizatsiynogo zabezpechennia systemy kibernetychnoyi bezpeky Ukrainu ta napriamy yogo udoskonalennia [The essence of organizational support of the cyber security system of Ukraine and directions of its improvement]. Borotba z organizovanoyu zlochynnistiu I kiruptsiyeiu (theoriia i praktyka). No. 2 (28). 2012. P. 299-309. (in Ukrainian)
15. Diorditsa I.V. Systema zabezpechennia kiberbezpeky: sutnist ta pryznachennia. [Cybersecurity system: essence and purpose]. Pidpruyemnytstvo, gospodarstvo i pravo. No.7. 2017. P. 109-116. (in Ukrainian)

16. Baranov O.A. Pro tlumachennia ta vyznachennia poniattia “kiberbezpeka”. [About interpreting and defining the concept of cybersecurity]. Pravova informatyka. No. 2 (42). 2014. P. 54-62. (in Ukrainian)
17. Gnatyuk S. Kiberteroryzm: istoriia rozvytku, suchasni tendentsii ta kontrzakhody. [Cyberterrorism: history of development, current trends and countermeasures]. Bezpeka informatsii. Vol. 19, No. 2. 2013. P. 118–129. (in Ukrainian)
18. Buryachok V.L., Tolubko B., Khoroshko V., Tolyupa S.V. Informatsiyna I kiberbezpeka. [Information and Cyber Security: The Sociotechnical Aspect]. K.: DUT. 2015. 288 p. (in Ukrainian)
19. Kharchenko L.S. Informatsiyna bezpeka Ukrainy: Glosariy. [Information Security of Ukraine: Glossary / Kharchenko L.S., Lipkan V.A., Loginov O.V.] K .: Text. 2004. 136 p. (in Ukrainian).
20. The JAIR Information Space, MIT Artificial Intelligence Laboratory. [Electronic resource]. – Access mode: http://www.ai.mit.edu/projects/infoarch/jair/jair-space.html (in English).
21.Cambridge dictionary. [Online resource]. – Access mode: https://dictionary.cambridge.org/dictionary/english/information-space. (in English).
22.Phinansovyi slovar`. [Financial Dictionary]. [Electronic resource]. – Access mode: https://dic.academic.ru/dic.nsf/fin_enc/23454. (in Russian).
23. Spravochnyk tekhnicheskogo perevodchika. [Handbook of technical translator]. [Electronic resource]. – Access mode: https://technical_translator_dictionary.academic.ru/ 78752/information_space. (in Russian).
24. Yudin O.K., Buchik S.S. Derzhavni informatsiyni resursy. Metodologiya pobudovy klasyfikatora zagroz. [State information resources. Methodology for building a threat classifier]. K.: NAU. 2015. 214 p. (in Ukrainian).
25. Kuehl D.T. From Cyberspace to Cyberpower: Defining the Problem. Cyberpower and National Security. Washington, DC: National Defense University Press. 2009. P. 26-28. (in English)
26. Thesaurus [electronic resource]. – Access mode: https://www.thesaurus.com
27. Dodonov A.G. Raspoznavaniie informatsionnykh operatsiy. [Recognition of information operations / A.G. Dodonov, D.V. Lande, V.V. Tsyganok, O.V. Andreychuk, S.V. Kadenko, A.N. Grayvoronskaya.]. K .: “Engineering” LLC. 2017. 282 p. (in Russian)
28. Kurnosov Yu.V. Analitika: metodologiia, tekhnologiia, I organizatsiia informatsionno-analiticheskoy raboty [Analytics: methodology, technology and organization of information-analytical work / Yu.V. Kurnosov, P.Yu. Konotopov]. M .: RUSAKI. 2004. 512 p. (in Russian)
29. Kurzweil R. Evolutsiia razuma: kak rasshoreniie granits nashego razuma pozvolit reshat` mnogiie mirovye problemy. [The Evolution of the Mind: How expanding the boundaries of our minds will solve many world problems]. M .: Exmo. 2016. 448 p. (in Russian)
30. Hales K.N. Yak my staly postliudstvom: virtualni tila v kibernetytsi, literature ta informatytsi. [How We Became Posthumous: Virtual Bodies in Cybernetics, Literature and Informatics]. K .: Nika-Centr. 2013. 426 p. (in Ukrainian)
31. Glick J. Informatsiiya. Istoriia. Teoriia. Potok. [Information. History. Theory. Flow]. M .: AST: CORPUS. 2016. 576 p. (in Russian)

Стаття надійшла до редакції 01.07.2019.

УДК 519.1, 514.128

https://orcid.org/0000-0002-3232-1787
https://orcid.org/0000-0002-2138-2357

О.С. ПУСТОВІТ, В.О. УСТИМЕНКО

ПРО НОВІ ПОТОКОВІ АЛГОРИТМИ СТВОРЕННЯ ЧУТЛИВИХ ДАЙДЖЕСТІВ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

Анотація. *Для прийняття обґрунтованих планових рішень у суспільно-економічній сфері спеціалісти повинні користуватися перевіреними документами. До засобів перевірки документів належать криптографічно стабільні алгоритми компресії великого файлу в дайджест визначеного розміру, чутливий до будь-якої зміни символів на вході. Пропонуються нові швидкі алгоритми компресії, криптографічна стабільність яких пов'язується зі складними алгебраїчними проблемами, такими як дослідження систем алгебраїчних рівнянь великої степені та задача розкладу нелінійного відображення простору за твірними. Запропоновані алгоритми створення чутливих до змін дайджестів документів будуть використані для виявлення кібератак та аудиту усіх файлів системи після зареєстрованого втручання.*

Ключові слова: *кібербезпека, хеш-функції, аудентифікаційні коди повідомлень, гомоморфізм компресії, високо нелінійна криптографія від багатьох змінних, некомутативна криптографія.*

DOI: 10.35350/2409-8876-2019-16-3-18-35

Вступ

У статті пропонується новий швидкий метод формування компресованого дайджесту великих електронних документів, представлених у бінарному алфавіті у вигляді меншого бінарного файлу, розмір якого визначається користувачем. Створений дайджест виявився чутливим до змін. Так, зміна поєдиного символу в оригінальному документі приводить до зміни більше ніж 98% символів у дайджесті. Алгоритм є симетричним та залежним від ключа, що задовольняє вимогам криптографічної стабільності. Вважаємо, що розробка може бути ефективно використана для розв'язання наступних двох задач:

1. Захисту великих сховищ даних від кібератак за наступним алгоритмом: створюються дайджести як закодованих, так і не закодованих електронних документів в обраний початковий час. В поточний момент часу створюються нові дайджести та порівнюються з початковими. Присутність будь-яких змін означає ушкодження файлів (кібератака, комп'ютерний вірус, відмова апаратури, помилка персоналу та інше).

2. Перевірка цілісності електронних документів при пересиланні. Кореспондент створює дайджест оригінального файлу та цього ж файлу у зашифрованому вигляді. Після пересилання створюється дайджест отриманого файлу та декодованого документа. Кореспонденти порівнюють дайджести та роблять висновок щодо наявності пошкодження.

1. Про верифікацію електронних документів

Спрощену модель глобального інформаційного простору можна уявляти як велику, зростаючу в часі мережу зареєстрованих віртуальних користувачів (фізичні особи або установи), які обмінюються інформацією та можуть її зберігати в електронних сховищах, що розташовані в мережі або знаходяться в ізоляції від неї.

Розмір файлів для обміну (електронних документів) має тенденцію зростати. Важливою категорією інформаційного простору є довіра до документів. Користувачі можуть використати симетричний алгоритм із приватним ключем для шифрування документів та протоколу обміну ключів для підтримки безпеки процедури кодування. Для зміни ключа також можуть використовуватися і сертифіковані алгоритми з публічним ключем. Ці методи забезпечують безпеку каналів обміну.

Легко побачити, що навіть користування надійними засобами шифрування не забезпечує повної довіри до документів, тому що треба рахуватися із шумами у каналах та проблемами безпечного збереження файлів в електронних сховищах, де документи можуть бути підроблені, пошкоджені комп'ютерними вірусами, технічними помилками в роботі обчислювальної техніки та інше.

Зазначимо, що останнім часом постійно зростає загроза потужних кібертерористичних атак на сховища електронної інформації різного призначення, їх наслідки – це не тільки витік інформації, але й ушкодження або фальсифікування документів. Зрозуміло, що після виявлення кібератаки на корпоративне сховище інформації потрібно робити аудит усіх файлів системи. Протидія цій загрозі вимагає розробки нових програмних засобів.

Довіра до документів є важливою категорією інформаційного простору. Легко побачити, що навіть користування надійними засобами шифрування не забезпечує повної довіри до документів, тому що треба рахуватися із шумами у каналах та проблемами безпечного збереження файлів у електронних сховищах, де документи можуть бути підроблені, пошкоджені комп'ютерними вірусами, технічними помилками в роботі обчислювальної техніки та інше. Для задач виявлення кібератак, верифікації та автентифікації документів потрібні так звані залежні від ключів хеш-функції (автентифікаційні коди повідомлень або МАСи), які залежать від гасла [2]. Хеш-функція потрібна для генерації скомпенсованої форми оригінального документа довільно обраного розміру. Таку форму називають хешем або дайджестом документа, її використовують у різних криптографічних застосуваннях. Хеш-функція h працює з файлом довільного розміру n, її значення має фіксований розмір.

Для інших задач захисту інформації потрібна загальна хеш-функція, що не потребує ключа або ж гасла. Нещодавно було сертифіковано загальну хеш-функцію Купина як новий державний стандарт України [1].

2. Вимоги до дайджесту документів

Криптографічно стабільна функція хешування f повинна забезпечувати: практичну неможливість вибору пари посилань x та z таким самим значенням хеш-функції. Для дайджесту документа, створеного залежною від ключа

хеш-функцією (MAC), використовують символ HMAC. Коли користувачі хочуть безпечно обмінятися кореспонденцією, перевіряючи хто є дійсним автором листа, так і відсутність змін при пересилці, вони разом обирають спільний MAC. При цьому користуються спільною схемою симетричного шифрування.

Крім криптографічної стабільності дуже важлива швидкодія та високий показник аваланч ефекту. Цей ефект вимірюється таким чином. Обчислюється HMAC для генерованого файлу, змінюється довільний його біт та обчислюється HMAC для зміненого файлу, після цього робиться побітове порівняння отриманих дайджестів. Для практичного вживання MACу потрібно, щоб статистичні дослідження показали, що поєдина зміна символу приводить до зміни 40% бітів HMACу незалежно від розміру файлів, що генеруються [9].

3. Про некомутативну криптографію та її застосування до задач симетричного шифрування і побудови хеш-функцій

Некомутативна криптографія є активною областю криптології, яка досліджує криптографічні примітиви та системи, засновані на алгебраїчних структурах, таких як групи, напівгрупи та некомутативні кільця (див. [18-29]). Одним з найбільш ранніх застосувань некомутативної алгебраїчної структури для криптографічних цілей було використання груп для розробки криптографічних протоколів. Пізніше декілька інших некомутативних структур, таких як групи Томпсона та групи Григорчука, були визначені як потенційні кандидати для криптографічних постквантових додатків. Стандартним способом представлення груп і напівгруп є використання генераторів і зв'язків (Теорія комбінаторних груп). Криптографія на основі напівгрупи складається із загальних криптографічних схем, визначених у термінах широких класів напівгруп і їх реалізацій для вибраних напівгруп сімей (так звані платформи напівгруп). Звичайна техніка використання пам'яті комп'ютера для представлення групи і напівгрупи заснована на методі генераторів і відношень.

У роботах [3, 14, 30, 32, 33] автори розглядають альтернативний метод представлення групи платформ G як підгрупи афінної напівгрупи Кремони S(Kn) над скінченним комутативним кільцем K всіх поліноміальних перетворень і припускається, що кожен елемент подається у стандартній формі багатовимірної криптографії. Отже, напівгрупа операцій відображень композицій індукує групові операції перетворень. Це спроба поєднати методи некомутативної криптографії та багатовимірної криптографії.

Некомутативну криптографію створено для дослідження проблем асиметричної криптографії, таких як алгоритми відкритих ключів, протоколи обміну ключами та криптосистеми типу Ель Гамаля. У випадку коротко представленого вище підходу до використання спеціальних підгруп афінних методик напівгрупи Кремони некомутативної криптографії у симетричній криптографії, таких як розробка потокових шифрів (див. [6, 34] та інші посилання) і конструкції HMAC (див., наприклад, [35], де використовувалися спеціальні лінійні групи), ми використовуємо нелінійні підгрупи афінних напівгруп Кремони. Метод генерування афінних перетворень у термінах спеціальних графів, заданих рівняннями (так звані лінгвістичні графи),

використовується замість методу генераторів і відношень (див. [13, 14] і розділ 6 нижче). Інші застосування теорії графів до криптографії розглядаються в [31].

Дослідження HMAC (і пов'язаних з ними HMACами) – гаряча галузь. Повний огляд опублікованих результатів з розробки цих засобів та їх криптоаналізу просто не можливий, ми звертаємося лише до декількох останніх робіт [36-45].

Зверніть увагу, що будь-яка криптографічна хеш-функція, така як MD5 або SHA-1, може бути використана при обчисленні HMAC; отриманий алгоритм MAC називається HMAC-MD5 або HMAC-SHA-1 відповідно. Криптографічна ефективність HMAC залежить від криптографічної ефективності основної хеш-функції, розміру її хеш-виходу, а також від розміру і якості ключа.

4. Математичне підґрунтя хеш-функції, що пропонується

Нехай $F(K)$ – простір потенційно нескінченних текстів в алфавіті K, який являє сукупність всіх кортежів виду $(a_1,a_2,...,a_k), a_i \in K$ різної довжини k. Будемо вважати, що K є скінченним комутативним кільцем та ототожнювати $F(K)$ з напівгрупою із наступним множенням $(a_1,a_2,...,a_k)\circ(b_1,b_2,...,b_s)=(a_1,a_2,...,a_k,b_1+a_k,b_2+a_k,b_s+a_k)$. Нехай $F'(K)$ буде піднапівгрупою всіх слів парної довжини. Позначимо через $S(K^n)$ скінченну напівгрупу всіх поліноміальних відображень простору K^n в себе.

Наш алгоритм ґрунтується на наступному математичному твердженні.

Теорема [3]. Для кожного натурального m≥2 існує гомоморфне відображення $\psi: F'(K)\to S(K^m)$ таке, що його образ $\psi(F'(K))$ утворює групу G кубічних поліноміальних відображень ступеня 3.

Нагадаємо, що властивість гомоморфного відображення для $\psi=\psi_m$ записується як $\psi(a\circ b)=\psi(a)\circ\psi(b)$.

Відображення, що задовольняє умовам теореми, будується конструктивно в термінах теорії дискретних динамічних систем, визначених за алгебраїчними графами з екстремальними властивостями [4]. Ці методи дозволяють одержати таку нижню оцінку порядку конструктивно побудованої групи: $|G|\geq 2^{4n}$. Зазначимо, що твердження визначає рідкісний математичний об'єкт. Суперпозиція двох кубічних відображень з великою ймовірністю буде мати ступінь 9, трьох – 27, чотирьох – 81, а у побудованій групі всі ці добутки обмежені числом 3. Ця група вже вживалася для побудови криптографічних алгоритмів з приватним ключем ([5, 6] та подальші посилання) та протоколів обміну ключами [4, 7, 10, 11].

Для створення MACу [9] було використано не саму групу G, а відображення ψ, що її визначає, разом з афінними A та B перетвореннями групи Кремони за правилом $g: x\to A\psi(x)B$. Не важко побачити, що ψ – природний оператор компресії даних, який відображає нескінченну множину $F'(K)$ усіх слів парної довжини в алфавіті K на скінченну множину $S(K^m)$. На вихід подається список координат g(x), до яких двічі застосовано оператор

повного диференціалу. Комп'ютерна симуляція дозволила обчислити дуже високий аваланч ефект у межах 97-99%. Для прикладу в МАСу російських дослідників інтервал аваланч ефекту оцінюється як 47-50% [8]. Конструктивна побудова гомоморфізмів компресії визначається у термінах теорії лінгвістичних графів, елементи якої представлені у розділі 5. При цьому застосовуються відомі лінгвістичні графи A(n,K) та D(n,K), побудовані при розв'язанні задач екстремальної теорії графів (розділ 6).

5. Пришвидшення алгоритмів

У цьому розділі буде представлено модифікацію описаного вище алгоритму, що дозволяє зберегти (або ж поліпшити) рівень аваланч ефекту при значному підвищенні швидкодії. Зазначимо, що алгоритм визначається «за модулем» процедури обчислення значень гомоморфізму з теореми 1 попереднього розділу. Конструктивне визначення гомоморфізму ψ буде описане у розділі 6 у термінах відомих алгебраїчних графів з екстремальними властивостями. При цьому використана концепція лінгвістичних родин графів, що дозволяє вивчати спеціальні напівгрупу та групу, пов'язані з графами заданими системами алгебраїчних рівнянь.

Нехай $(a_1, a_2, ..., a_n)$ – документ, представлений в алфавіті K після перемішування з деяким псевдовипадковим словом сталої довжини. Будемо вважати, що число n парне. Користувачі обирають розмір дайджесту $m, m < n$ та $m = O(1)$ або ж $m = O(n)$ разом з ключем, що складається зі зростаючої послідовності натуральних чисел $i(1), i(2), ..., i(m-1)$ та невиродженої матриці M, складеної з елементів кільця лишків Z_{256}. Вони утворюють вектор $u = (v_1, v_2, ..., v_m)$, де $v_1 = a_1 + a_2 + ... + a_n, ..., v_j = v_{j-1} - a_{i(j-1)}$. Потім обчислюється кубічне відображення $F = \psi_m(a_1, a_2, ..., a_n)$, яке кореспонденти застосовують до вектора u. Отриманий вектор-рядок $F(u)$ множиться на матрицю M. Вектор $w = F(u)M$ вважаємо дайджестом документа.

Зазначимо, що значення $F(u)$ обчислюється за допомогою рекурсивного алгоритму, його складність визначається як $O(mn)$ і співпадає зі складністю створення дайджесту.

Цей базовий алгоритм легко модифікувати без змінення складності обчислень. Зокрема:

1) Можна представити слово $(a_1, a_2, ..., a_n)$ у вигляді конкатенації скінченної кількості слів $z_1, z_2, ..., z_t$ парної довжини. Потім обрати послідовність слів вигляду $u_1, u_2, ..., u_k$, де $u_i \in \{z_1, z_2, ..., z_t\}$ таку, що кожне z_i у цій послідовності зустрічається не менше ніж один раз. Далі обчислюється значення у добутку $u_1, u_2, ..., u_k$ у розглянутій вище напівгрупі слів $F'(K)$. Алгоритм модифікується заміною кубічного відображення $\psi(a)$ на $\psi(y)$. При умові всім відомого розбиття файлу криптографічна стабільність такого дайджесту буде залежною від проблеми розкладу $\psi(y)$ у добуток перетворень $\psi(z_i)$ з аффінної групи Кремони. Зазначимо, що поліноміального алгоритму для розв'язання цієї проблеми на звичайному або квантовому комп'ютері на сьогоднішній день не знайдено. Насправді ця

задача виникає за умов неповної визначеності, бо відоме тільки значення $\psi(y)$ на деякому залежному від файлу векторі. Зрозуміло, що розбиття a на підслова z_i та послідовність u_j слід вважати частиною спільного ключа для кореспондентів.

2) Можна обчислювати v_1 як добуток виразів $2a_i+1$ та одержувати v_i діленням v_{i-1} на $2a_{i(j-1)}+1$.

3) У варіанті 2 можна замінювати v_i на його непарні степені $k, k<128$. Тоді ці степені слід вважати параметрами ключа.

Імплементовані випадки (див. розділ 7) зручні для їх використання у технології blockchain, де потрібні дайджести у вигляді послідовності бітів або ж нулів та одиниць.

Зазначимо, що добрі властивості функції компресії ґрунтуються на конструкціях гомоморфізмів нескінченної півгрупи слів парної довжини у півгрупи Кремони, визначені родинами алгебраїчних графів з екстремальними властивостями.

6. Про лінгвістичні графи та пов'язані з ними напівгрупи афінних перетворень

Відсутні визначення теорії графів, які з'являються у даній статті, можна знайти у [12]. Всі графи, які ми розглядаємо, є простими графами, тобто неорієнтованими без петель та кратних ребер. Нехай через V(G) і E(G) позначимо множину вершин та множину ребер G відповідно.

Коли буде зручно, ми будемо ототожнювати G з відповідним антирефлексивним бінарним відношенням на V(G), тобто E(G) є підмножиною V(G)◦V(G), і запишемо v G u для суміжних вершин u і v (чи сусідніх).

Позначимо |{ x ϵ V(G)| xGv }| як ступінь вершини v.

Структура інцидентності є множина V з розділеними множинами P (точок) і L (прямих) і симетричного бінарного відношення I, такого що належність двох елементів означає, що один із них буде точкою, а інший – прямою. Ми будемо ідентифікувати I з простим графом цього відношення інцидентності або дводольного графа. Пара x, y, x ϵ P, yє L, така що x I y, називається прапором структури інцидентності I.

Нехай K – скінченне комутативне кільце. Позначимо структуру інцидентності з множини точок $P = P_{s,m} = K^{s+m}$ і множини прямих $L = L_{r,m} = K^{r+m}$ як лінгвістичну структуру інцидентності I_m, якщо точка $x = (x_1, x_2,\ldots, x_s, x_{s+1}, x_{s+2}, \ldots, x_{s+m})$ належить прямій $y = [y_1, y_2, \ldots, y_r, y_{r+1}, y_{r+2}, \ldots, y_{r+s}]$ тоді і тільки тоді, коли виконується співвідношення:

$$
\begin{aligned}
&a_1x_{s+1}+b_1\mathbf{y}_{r+1}=f_1(x_1, x_2,\ldots, x_s, y_1, y_2, \ldots, y_r)\\
&a_2x_{s+2}+b_2\mathbf{y}_{r+2}=f_2(x_1, x_2,\ldots, x_s, x_{s+1}, y_1, y_2, \ldots, y_r, y_{r+1})\\
&\qquad\qquad\ldots\\
&a_mx_{s+m}+b_m\mathbf{y}_{r+m}=f_m(x_1, x_2,\ldots, x_s, x_{s+1},\ldots, x_{s+m}, y_1, y_2, \ldots, y_r, y_{r+1}, \ldots, y_{r+m}),
\end{aligned}
$$

де a_j, і b_j, j = 1,2,…,m не є дільниками нуля і f_j – багатовимірні многочлени з коефіцієнтами з K [13]. Квадратні та круглі дужки дозволяють відрізняти точки від прямих.

Колір $\rho(x) = \rho((x))$ ($\rho(y) = \rho([y])$) точки x (прямої [y]) визначається як проекція елемента (x) (відповідно [y]) від вільного модуля на його початок s (відносно r) координат. Як випливає із визначення лінгвістичної структури інцидентності, для кожної вершини графа існує єдиний сусід вибраного кольору.

Позначимо $\rho((x))=(x_1, x_2, \dots, x_s)$ для $(x)=(x_1, x_2, \dots, x_{s+m})$ і $\rho([y])=(y_1, y_2, \dots, y_r)$ для $[y]=[y_1, y_2, \dots, y_{r+m}]$ як колір точки та колір прямої відповідно. Для кожного $b \in K^r$ і $p=(p_1, p_2, \dots, p_{s+m})$ існує єдиний сусід точки $[l]=N_b(p)$ кольору b. Так само для кожного $c \in K^s$ і прямої $l=[l_1, l_2, \dots, l_{r+m}]$ існує єдиний сусід прямої $(p)= N_c([l])$ кольору c. Потрійні параметри s,r,m визначають тип лінгвістичного графа.

Розглядаються також лінгвістичні структури інцидентності, визначені нескінченним числом рівнянь.

У випадку лінгвістичного графа Г шлях, що складається з його вершин $v_0, v_1, v_2, \dots, v_k$, однозначно визначається початковою вершиною v_0 і кольорами $\rho(v_i,)$, i=1, 2,..., k інших вершин зі шляху. Розглянемо відношення еквівалентності на множинах розбиття такі, що $(p)\approx(p')$ ($[l] \approx [l']$), якщо $p_{i+s}=p'_{i+s}$ ($l_{i+r}=l'_{i+r}$) для $i \in \{1,2,..m\}$.

Визначимо оператор стрибка $J(p, a)$, $a \in K^s$ на множині розбиття P ($J(l,a)$, $a \in K^r$ на множині розбиття L) умовами $J(p,a)\approx(p)$ та $\rho(J(p,a))=a(J([l],a)\approx[l]$ та $\rho(J([l],a))=a)$.

Оператор обчислення сусіда (чи оператор ковзання) N(v, a), діє на PUL за правилами $N(p, a)=[l]$, де $(p)I[l]$, $\rho([l])=a$ і $N([l],a)=(p)$, де $(p)I[l]$, $\rho((p))=a$.

Розглянемо ланцюги ковзання лінгвістичного графа з початковою точкою p, яка є послідовністю $(p, p_0, l_1, l_2, p_3, p_4, \dots, l_{t-3}, l_{t-2}, p_{t-1}, p_t)$, $t=4k$, $k\geq 0$ таке, що $p\approx p_0, l_{2i+1}\approx l_{2i+2}$, $i\geq 0$, $p_{2i+1}\approx p_{2i+2}$ і $p_{2i} I l_{2i+1}$ для $i \geq 0$.

Кольори елементів стрічок ковзання і початкова точка визначають цю послідовність. Очевидно, що послідовність обчислюється застосуваннями операторів стрибка J_a і ковзання, що чергуються. Насправді термін ланцюг ковзання вибирається, тому що його обчислення нагадує послідовності стрибків та поверхневих ковзань у фігурному катанні (або ж різних змаганнях на скейтбордах).

Конструкції напівгруп та груп.

Розглянемо напівгрупу $S(K^s)$ і сукупність $S^{s,r}(K)$ відображень вигляду $G:(y_1, y_2,\dots, y_r)\rightarrow(f_1(x_1, x_2,\dots, x_s), f_2(x_1, x_2,\dots, x_s),\dots, f_r(x_1, x_2,\dots, x_s))$. Якщо $H \in S(K^s)$ тоді $G(H)$ для $G \in S^{s,r}(K)$ існує відображення $(y_1, y_2,\dots, y_r)\rightarrow(f_1(H(x_1),H(x_2),\dots, H(x_s)), f_2(H(x_1),H(x_2),\dots, H(x_s)),\dots, f_r(H(x_1),H(x_2),\dots, H(x_s)))$.

Для зручності будемо ототожнювати елементи множини $S(K^s)$ з кортежами у $K[x_1, x_2,\dots, x_s]^s$ і елементи $S^{s,r}(K)$ кортежами у $K[x_1, x_2,\dots,x_s]^r$.

Розглянемо сукупність ${}^sBS_r(K)$ послідовностей виду $u=(H_0, G_1, G_2, H_3, H_4, G_5, G_6,\dots, H_{t-1}, H_t)$, $t=4i$, де $H_k \in S(K^s)$, $G_j \in S^{s,r}(K)$. Будемо називати ${}^sBS_r(K)$ сукупністю смугастих символьних стрічок.

Будемо визначати добуток u з $u'=(H'_0, G'_1, G'_2, H'_3, H'_4, G'_5, G'_6,\dots, H'_{l-1}, H_l)$ як $w=(H_0, G_1, G_2, H_3, H_4, G_5, G_6,\dots, H_{t-1}, H'_0(H_t), G'_1(H_t), G'_2(H_t), H'_3(H_t), H'_4(H_t), G'_5(H_t), G'_6(H_t), \dots, H'_{l-1}(H_t), H'_l(H_t))$.

Легко побачити, що ця операція перетворює ${}^sBS_r(K)$ у напівгрупу з одиничним елементом $(H_0)=(E_0)$, де E_0 – тотожне перетворення з $S(K^s)$.

Розглянемо гомоморфізм групи ${}^{s}BS_r(K)$ у напівгрупу Кремони $S(K^{s+m})$, визначених у термінах лінгвістичного графа $I=I^{m}(K)$. Зверніть увагу на те, що ми можемо розглядати граф $I^{m}(K')$ над розширенням K' кільця K з використанням тих самих рівнянь у визначенні.

Візьмемо кільце $K'=K[x_1, x_2,\ldots, x_{m+s}]$, де x_i є формальними змінними, і розглянемо нескінченний граф $I^{m}(K[x_1,x_2,\ldots,x_n])$, $n=m+s$ з множинами точок і прямих $P'=K[x_1, x_2,\ldots, x_{m+s}]^{m+s}$ та $L'=K[x_1, x_2,\ldots, x_{m+s}]^{m+r}$. Після цього беремо смугасту стрічку $u=(H_0, G_1, G_2, H_3, H_4, G_5, G_6,\ldots, H_{t-1}, H_t)$, утворену сукупністю поліномів з кільця $K[x_1, x_2,\ldots,x_s]$, і точку $(x)=(x_1, x_2,\ldots, x_n)$, утворену твірними елементами K'. Ці дані однозначно визначають ланцюг ковзання (x), $J((x),H_0)=({}^{1}x)$, $N(({}^{1}x), G_1)=[{}^{2}x]$, $J([{}^{2}x],G_2)=[{}^{3}x]$, $N([{}^{3}x], H_3)=({}^{4}x)$, $J(({}^{4}x),H_4)=({}^{5}x),\ldots$, $J([{}^{t-2}x],G_{t-2})=[{}^{t-1}x]$, $N([{}^{t-1}x], H_{t-1})=({}^{t}x)$, $J(({}^{t}x),H_t)=({}^{t}x)$.

Нехай $({}^{t}x)$ – кортеж $(H_t, F_2, F_3,\ldots, F_n)$ де $F_i \in K[x_1, x_2,\ldots, x_n]$. Ми визначаємо ${}^{I}\Psi(u)$ як відображення $(x_1, x_2,\ldots, x_n)\rightarrow(H_t, F_2, F_3,\ldots, F_n,)$, $n=m+s$.

Твердження, наведені нижче (див. [14]), випливають з визначення відображення.

Лема 1. Відображення $\boldsymbol{\psi}={}^{I}\boldsymbol{\psi}$**:** ${}^{s}BS_r(K)\rightarrow S(K^{n})$ є гомоморфізмом напівгруп.

Посилаємося на ${}^{I}\boldsymbol{\psi}({}^{s}BS_r(K))={}^{I}SR(K)$ як напівгрупу ланцюгових перетворень лінгвістичного графа I.

Ми визначаємо піднапівгрупу ${}^{s}S_r(K)$ гладких стрічок як сукупність смугастих стрічок $u=(H_0, G_1, G_2, H_3, H_4, G_5, G_6,\ldots, H_{t-1}, H_t)$ z ${}^{s}BS_r(K)$ з $H_0=E_0$, $G_1=G_2$, $H_3=H_4$, $G_5=G_6,\ldots$, $H_{t-1}=H_t$. Будемо називати образ цієї напівгрупи ${}^{I}\boldsymbol{\psi}({}^{s}S_r(K)={}^{I}SW(K)$ напівгрупою символічних переходів на лінгвістичному графі I.

Припустимо, що H_t є бієктивним відображенням і його обернене є поліноміальним відображенням (у випадку нескінченного кільця K). Тоді ми можемо розглядати зворотню бінарну стрічку $Rev(u)= (H_{t-1}(H_t^{-1}), G_{t-2}(H_t^{-1}), G_{t-3},(H_t^{-1}), H_{t-4}(H_t^{-1}), H_{t-5}{}^{1}(H_t), \ldots, G_2(H_t^{-1}), G_1(H_t^{-1}), H_0(H_t^{-1}), H_t^{-1})$.

Зверніть увагу, що сукупність бінарних стрічок u з H_t^{-1} поліноміальної природи утворює піднапівгрупу ${}^{s}BC_r(K)$. Будемо називати її напівгрупою реверсійних бінарних стрічок

Лема 2. Гомоморфне зображення ${}^{I}\boldsymbol{\psi}({}^{s}BC_r(K))= IR_I(K)$ – підгрупа групи Кремони $C(K^{n})$.

Дійсно, ${}^{I}\psi(u\cdot Rev(u))$, $u\in {}^{s}BC_r(K)$ – тотожне відображення.

Ми називаємо $IR_I(K)$ підгрупою реверсійних символічних переходів лінгвістичного графа I.

7. Деякі алгебраїчні конструкції екстремальної теорії графів, відповідні гомоморфізми компресії та нелінійні групи перетворень

7.1. Деякі означення екстремальної теорії графів

Обхват графа Г, позначаємо g = g(Г), – довжина найкоротшого циклу у Г. Діаметр d= d(Г) графа Г – максимальна довжина найкоротшого проходу між двома його вершинами.

Нехай $g_x = g_x(Г)$ – довжина мінімального циклу через вершину x з множини V (Г) вершин графа Г. Позначимо $Cind(Г) = \max\{g_x, x \in V (Г)\}$ як індикатор циклу графа Г.

Якщо Γ_i – сім'я k-регулярних зв'язних графів зростаючого порядку зі зростаючим індикатором циклу, для якого добре визначено проективну границю $\Gamma = \lim \Gamma_i$, $i \to \infty$, тоді Γ – дерево, тобто нескінченний зв'язний граф без циклів. Сім'я Γ_i k-регулярних зв'язних графів постійного ступеня є родиною графів малого світу, якщо $d(\Gamma_i) \leq \text{clog}_k (v_i)$, для деякої константи c, $c > 0$.

Нагадаємо, що сімейство регулярних графів Γ_i ступеня k і зростаючого порядку v_i є сім'єю графів великого обхвату, якщо $g(\Gamma_i) \geq \text{clog}_k (v_i)$, для деякої незалежної константи c, $c > 0$.

Назвемо сімейство регулярних простих графів Γ_i ступеня k і порядку v_i як сімейство графів з великим індикатором циклу, якщо $\text{Cind}(\Gamma_i) \geq \text{clog}_k (v_i)$ для деякої незалежної константи c, $c > 0$.

Зверніть увагу, що для вершинно-транзитивного графу його обхват та індикатор циклу збігаються. Визначені вище родини відіграють важливу роль в екстремальній теорії графів, теорії LDPC кодів та криптографії (див. [15] та подальші посилання).

7.2. Алгебраїчні графи A(n, K) і D(n,K), деякі результати і відкриті питання

Нижче буде визначено сімейства графів A(n,K) і D(n,K), для кожного натурального числа n, $n > 2$ та комутативного кільця K. У випадку $K = F_q$ позначатимемо ці графи як A(n, q) і D(n, q), відповідно. Ці графи виникають як гомоморфні зображення нескінченних дводольних графів A(K) і D(K), для яких множини точок та прямих P і L ототожнюються з копіями декартової степені K^N, де K – комутативне кільце і N – множина натуральних чисел. Щоб відрізняти точки від прямих, будемо використовувати круглі та квадратні дужки. Якщо $x \in V$, тоді $(x) \in P$ і $[x] \in L$.

Опис ґрунтується на побудові цих графів у термінах множини коренів розширеної діаграми Динкіна A_1 та відповідної їй алгебри Лі, що належить до класу алгебр Каца-Муді.

Вершини D(K) – нескінченні розмірні кортежі над K, ми запишемо їх наступним чином $(p)=(p_{0,1}, p_{1,1}, p_{1,2,} p_{21}, p_{22}, p'_{22}, p_{23}, \dots, p_{i,i}, p'_{i,i}, p_{i,i+1}, p_{i+1,i}, \dots)$, $[l]=[l_{1,0}, l_{1,1}, l_{1,2,,} l_{21}, l_{22}, l'_{22}, l_{23}, \dots, l_{i,i}, l'_{i,i}, l_{i,i+1}, l_{i+1,i}, \dots]$. Будемо вважати, що майже всі компоненти точок і прямих нулі. Умова належності точки (p) і прямої [l] ((p)I[l]) може бути записана за допомогою переліку нижченаведених рівнянь:

$l_{i,i} - p_{i,i} = l_{1,0} p_{i-1,i}$; $l'_{i,i} - p'_{i,i} = l_{i,i-1} p_{0,1}$; $l_{i,i+1} - p_{i,i+1} = l_{i,i} p_{0,1}$; $l_{i+1,i} - p_{i+1,i} = l_{1,0} p'_{i,i}$. Ці чотири співвідношення визначені для $i \geq 1$, ($p'_{1,1} = p_{1,1}$, $l'_{1,1} = l_{1,1}$).

Аналогічно, визначимо графи A(K) на множині вершин, що складаються з точок та прямих $(p) = (p_{0,1}, p_{1,1}, p_{1,2,} p_{21}, p_{22,,} p_{23}, \dots, p_{i,i}, p_{i,i+1,\dots})$.

$[l] = [l_{1,0}, l_{1,1}, l_{1,2,,} l_{21}, l_{22}, l_{23}, \dots, l_{i,i}, l_{i,i+1, \dots}]$ таких, що точка (p) належить прямій [l] ((p)I[l]), якщо між їх координатами виконуються наступні співвідношення: $l_{i,i} - p_{i,i} = l_{1,0} p_{i-1,i}$; $l_{i,i+1} - p_{i,i+1} = l_{i,i} p_{0,1}$.

Зрозуміло, що множина індексів A={(1; 0), (0; 1), (1; 1), (1; 2), (2; 2), (2; 3), … , (i-1, i), (i, i),… } є підмножиною D={(1, 0), (0; 1), (1, 1), (1, 2), (2; 2), (2, 2)',…, (i- 1, i); (i; i - 1); (i, i); (i, i)',…}. Точки і прямі D(K) є функціями від $K^{D-\{(1,0)\}}$ і $K^{D-\{(0,1)}$, їхні обмеження на A-{(1,0)} і A-{(0,1)} визначає гомоморфізм Ψ графа D(K) на A(K).

Для кожного додатного цілого $m \geq 2$ розглядаємо підмножини A(m) і D(m), що містять перші m+1 елементів A і D щодо визначених порядків. Обмеження точок і прямих D(K) на D(m)-{(1,0)} і D(m)-{(0,1)} визначають граф гомоморфізму ${}^{D}\Delta(m)$ із зображенням, позначеним як D(n, K). Аналогічно обмеження точок і прямих A(K) на A(m) -{(1,0)} і A(m)-{(0,1)} визначають гомоморфізм ${}^{A}\Delta(m)$ графа A(K) на граф, визначений як A(m, K).

Розглянемо також відображення Δ(m) на вершинах графу D(m, K), посилаючись на його точку $(p)\epsilon K^{D(m)-\{(1,0)\}}$, обмежену у $D(m)\cap A-\{(1,0)\}$, і його пряму $[l]\ \epsilon K^{D(m)-\{(0,1)\}}$, обмежену у $D(m)\cap A-\{(0,1)\}$. Це відображення є гомоморфізмом D(m, K) на A(n, k), $n=|D(m)\cap A|-1$.

Граф $D(q)=D(F_q)$, де q-регулярний ліс. Його частки D(n,q) є крайовими транзитивними графами. Тому їхні зв'язні компоненти є ізоморфними. Символ D(n,q) означає граф, ізоморфний одній з таких зв'язних компонентів.

Сімейство CD(n, q), n=2,3,… є сімейством великого обхвату для кожного параметра q, q>2 (див. [16] і подальші посилання). Питання «Чи є CD(n, q) сімейством графів малого світу?» залишається відкритим. Граф A(q), q>2 є q-регулярним деревом. Графи A(n, q) не мають транзитивних вершин.

Вони утворюють сімейство графів з великим індикатором циклу, який q-регулярний сімейства графів малого світу [17]. Питання «Чи є A(n,q), n=2,3,…сімейством великого обхвату?» залишається відкритим.

7.3. Про лінгвістичні та екстремальні графи і стабільні нелінійні підгрупи афінної групи Кремони

Всі графи, визначені у 2 розділі, належать до класу L лінгвістичних графів Γ=Γ(K) типу (1, 1, n-1), $n\epsilon N$ або $n=\infty$. Визначаються над комутативним кільцем K, яке містить дводольні графи з множиною точок $P=K^n$ і множиною прямих $L=K^n$ таких, що $(p)=(p_1, p_2, \dots, p_n)\epsilon P_n$ і $[l]=[l_1, l_2, \dots, l_n]\epsilon L_n$. утворює ребро Γ, якщо виконуються наступні умови ${}^{2}ap_2 - {}^{2}bl_2={}^{2}f(l_1, p_1)$, ${}^{3}ap_2-{}^{3}bl_2={}^{3}f(p_1, p_{12}, l_1, l_2)$, … , ${}^{n}ap_n-{}^{n}bl_n={}^{n}f(p_1, p_2, \dots, p_n, l_1, l_2, \dots, l_n)$, де ${}^{i}a$ і ${}^{i}b$, $i\geq 2$ елементи мультиплікативної групи K*, f_i поліноми від багатьох змінних. Визначимо кольори ρ((p)) і ρ([l]) точки (p) і прямої [l] як їх перші координати p_1 і l_1. Введемо добре визначений оператор N(v, a), який обчислює сусіда вершини v кольору $a\epsilon K$.

Нехай $S(K^n)$ означає напівгрупу Кремони поліноміальних перетворень вільного модуля K^n і $C(K^n)$ – афінна група Кремони обернених елементів $S(K^n)$ з поліноміальною інверсією. Ці алгебраїчні структури є важливими об'єктами алгебраїчної геометрії. Одна зі складних проблем полягає в побудові сімей стабільних підгруп G_n з $C(K^n)$ (чи напівгрупи S_n з $S(K^n)$) групи поліноміальних перетворень з максимальним ступенем, який дорівнює константі c. Зауважимо, що для більшості пара f ,g ϵ $C(K^n)$ ступенів r і s їх наборів має ступінь rs. Тому ця проблема складна, вона має сильні криптографічні мотивації.

Розглянемо сукупність St(K) рядків виду $(f_1, f_2, \dots, f_k)$ де $f_i \epsilon K[x]$. Позначимо поліном f і відображення $x\rightarrow f(x)$ з S(K). Добуток двох послідовностей $(f_1, f_2, \dots, f_k)$ і $(g_1, g_2, \dots, g_t)$ є послідовність $(f_1, f_2, \dots, f_k, g_1(f_k), g_2(f_k), \dots, g_t(F_k))$. Порожній рядок – це одиниця з напівгрупи St(K). Фактично St(K) є напівпрямим добутком вільної напівгрупи над алфавітом K[x] і напівгрупи Кремони S(K). Ми посилаємося на St(K) як напівгрупу поліноміальних

рядків. Нехай St'(K) означає напівгрупу рядків парної довжини з St(K) і ∑(K) – підгрупа рядків парної довжини з координатами виду x+c, cєK.

У випадку лінгвістичного графу Г=Г(K) типу (1,1,n-1) шлях, що складається з його вершин v_0, v_1, v_2, …,v_k, однозначно визначається початковою вершиною v_0, і кольори $\rho(v_i,)$, i=1, 2,..., k – іншими вершинами зі шляху. Ми можемо розглядати граф Г'=Г(K[x_1, x_2, …, x_n]), визначений тими самими рівняннями з Г, але над комутативним кільцем K[x_1, x_2, …, x_n].

Отже, можна визначити наступне символічне обчислення. Візьмемо символічну точку x=(x_1, x_2, …, x_n), де x_i є загальними змінними з K[x_1, x_2, …, x_n] і поліноміальним рядком CєSt'(K), який є кортежем многочленів f_1,, f_2,, ... , f_k, з K[x_1] з парним параметром k. (x=x_1). Утворюємо шлях вершин v_0,=x, v_1 так, що v_1Iv_o і $\rho(v_1)=f_1(x_1)$, v_2 так, що v_2Iv_1 і $\rho(v_2)=f_2(x_1)$, ..., v_k так, що v_kIv_{k-1} і $\rho(v_k)=f_k(x_1)$. Вибираємо параметр k як парне число. Так v_k – точка з множини K[x_1, x_2,…, x_n]^n графа Г'.

Зауважимо, що обчислення кожної координати v_i залежить від змінних x_1, x_2, …, x_n і многочленів f_1,, f_2,, ... , f_k, потребує лише арифметичних операцій додавання та множення. Як випливає з визначення лінгвістичного графа, остання вершина v_k (точка) має координати ($h_1(x_1)$, $h_2(x_1,x_2)$, $h_3(x_1,x_2,x_3)$,...,$h_n(x_1,x_2,…, x_n)$), де $h_1(x_1)=f_k(x_1)$. Розглянемо відображення ^{Г}H(C): $x_i\rightarrow h_i(x_1, x_2,…, x_n)$, i=1, 2,..., n яка відповідає поліноміальному рядку C.

Наступні твердження наведені у [14].

Теорема 1. Відображення $^{Г}\eta$:C → ^{Г}H(C) є гомоморфізмом St'(K) у напівгрупі Кремони S(K^n).

Ми називаємо $^{Г}\eta$ лінгвістичним відображенням стиснення. Якщо K скінченне, то відображення перетворює сукупність потенційно нескінченних рядків у скінченну напівгрупу.

Неважко побачити, що St'(K) збігається з напівгрупою $^{s}S_r$(K) гладких стрічок для випадку s=r=1, що була визначена у розділі 5. Лі образ $^{Г}\eta$(St'(K)) співпадає з напівгрупою ^{I}SW(K) символічних переходів на лінгвістичному графі I.

Неважко побачити, що ця напівгрупа ∑(K) є ізоморфною напівгрупі F'(K), визначеній у 1 розділі.

Теорема 2. Якщо Г – один з графів D(n, K) і A(n,K), то $^{Г}\eta$(∑(K)) є стабільною підгрупою C(K^n) ступеня 3.

Як наслідок із цього твердження одержуємо теорему з розділу 1. При цьому виникає дві ефективні конструкції гомоморфізму ψ, а саме ψ= $^{D(n,K)}\eta$ та ψ= $^{A(n,K)}\eta$

Позначимо $^{Г}\eta$(∑(K)) для Г=D(n,K) і Г=A(n,K) як GD(n,K) і GA(n,K). Ці групи вже використовувалися в усіх криптографічних додатках графів D(n,K) і A(n,K).

Таким чином, представлений вище алгоритм створення дайджесту, визначений у розділі 4 «за модулем процедури обчислення гомоморфізму», поповнюється описом цієї процедури. Дві різні версії конструктивного визначення гомоморфізму ψ визначають два різні алгоритмічні пакети створення чутливих дайджестів документів.

Зазначимо, що групи GD(n,K) і GA(n,K) є підгрупами груп ^{I}**ψ(**^{s}BC$_r$(K))= IR$_I$(K), I=D(n,K) та A(n,K).

Розглянемо підгрупу $SIR_I(K)$, переходів зсуву групи $IR_I(K)$, реверсійних символічних переходів лінгвістичного графа I, що складається з образів стрічок з координатами вигляду x+c, c∈K. Елементи груп $SIR_I(K)$, I=D(n,K), I=A(n,K) можна вживати в алгоритмах створення дайджестів замість груп GD(n,K) і GA(n,K). При цьому кольори, що відповідають стрибкам, слід вважати елементами гасла.

8. Про імплементацію алгоритмів створення дайджесту

Програми імплементовано на мові C++. Час її роботи залежить від параметрів комп'ютера. Ми використали звичайний персональний комп'ютер з процесором Pentium 3.00 GHz, 2GB пам'яті RAM та системи Windows 7. Для провадження комп'ютерних експериментів з базовим алгоритмом, описаним у розділі 4, було обрано групу GA(n,K) та розширені матриці M, які обчислюються за час O(m), де m – розмір дайджесту.

Для вимірювання аваланч ефекту дайджест представлявся у символах бінарного алфавіту. Швидкодія алгоритму в секундах, виміряна на файлах різного типу, подається нижче.

Таблиця 1 – Швидкодія алгоритму створення дайджестів

Розмір файлу, Мегабайт	Розмір дайджесту (у бітах)						
	256	384	512	640	768	896	1024
4,0	1,36	2,03	2,74	3,43	4,12	4,81	5,52
16,1	4,94	7,40	9,90	11,09	14,88	16,99	19,82
38,7	11,60	17,39	23,20	29,03	34,84	40,65	46,46
62,3	18,54	27,80	37,10	46,38	55,68	64,94	74,22
121,3	36,24	54,35	72,52	90,63	108,76	126,89	145,02
174,2	51,22	77,72	103,66	129,40	155,53	181,42	207,34

Комп'ютерний експеримент показав, що при зміні одного бінарного символу електронного документа змінюється щонайменше 98% символів дайджесту.

Частину модифікації базового алгоритму, описану у розділі 4, та деякі алгоритми з використанням груп $SIR_I(K)$, визначені у розділі 5, вже імплементовано. Проводяться комп'ютерні експерименти для оптимізації параметрів у відповідних програмах.

Висновки

Поточна робота підприємства, корпорації, фінансової установи потребує довгострокової праці спеціалістів із великою кількістю електронних документів. Для прийняття обґрунтованих планово-фінансових рішень,

спеціалісти повинні користуватися перевіреною інформацією. Інструментом перевірки можуть бути алгоритми компресії великого файлу і дайджест визначеного розміру, чутливий до будь-якої зміни символів на вході.

Запропоновано нову родину залежних від ключа швидких алгоритмів створення дайджестів електронних документів. Комп'ютерна симуляція дозволяє дослідити високий рівень аваланч ефекту, що виникає. Нехай K – вільно обране скінченне комутативне кільце, m – додатне ціле число. Алгоритми використовують нещодавньо знайдені гомоморфні відображення компресії напівгрупи потенційно нескінченних текстів у алфавіті K на скінченну групу кубічних поліноміальних перетворень m вимірного аффінного простору K^m.

Криптографічна стабільність функцій хешування пов’язується зі складними алгебраїчними проблемами, такими як дослідження систем алгебраїчних рівнянь великої степені та задача розкладу нелінійного відображення вільного модуля за заданими твірними.

Алгоритми імплементовано у випадках скінченних полів $F_2^8, F_2^{16}, F_2^{32}$, кілець Z_{256} та B(32) (булеве кільце порядку 2^{32}). Комп'ютерна симуляція демонструє, що швидкість алгоритму зростає зі збільшенням розміру базового комутативного кільця.

Пропоновані алгоритми можуть працювати з даними у вигляді тексту, відео- та аудіофайлів, фільму тощо. Розроблені методи створення дайджестів мають потоковий характер – швидкодія при сталому m лінійно залежить від n. Зростання n збільшує криптографічну стабільність. Імплементація у блоковому режимі можлива, але не вмотивована, бо розмір блоку обмежує кількість змінних системи нелінійних рівнянь.

Необхідність подальших досліджень і технологічних розробок зі створення нових залежних від ключа швидких хеш-функцій пов’язана із викликами кібербезпеки, зростанням глобального інформаційного простору, очікуванням появи квантового комп’ютера та розвитком технологій bitcoins, де потрібно хешувати вхідні дані довільного розміру, перетворюючи їх у послідовність бітів, що є дайджестом так званих blockchains. Запропоновані швидкі алгоритми створення чутливих до змін дайджестів документів вже зараз будуть практично використані для виявлення кібератак та аудиту усіх файлів системи після зареєстрованого втручання. Це перша вдала спроба по застосуванню ідеї некомутативної криптографії для створення HMACів. Вважаємо, що потрібна подальша робота з оптимізації побудованих алгоритмів, їх порівняння із відомими раніше HMACами та криптоаналітичні дослідження.

СПИСОК ЛІТЕРАТУРИ

1. Oliynykov R., Gorbenko I., Kazymyrov O., Ruzhentsev V., Kuznetsov O., Gorbenko Yu., Dyrda O., Dolgov V., Pushkaryov A., Mordvinov R., Kaidalov D. Data Security. Symmetric block transformation algorithm. Ministry of Economical Development and Trade of Ukraine. DSTU 7624:2014. National Standard of Ukraine. Information technologies. Cryptographic. – 2015.

2. Aumasson J.Ph., Serious Cryptography: A Practical Introduction to Modern Encryption, No Starch Press. – 2017. – 312 p.

3. V. Ustimenko, On new symbolic key exchange protocols and cryptosystems based on hidden tame homomorphism,. Dopov. Nac. akad. nauk Ukraine. – 2018, n 10. – pp. 26-36.
4. Устименко В.А. Об экстремальной теории графов и символьных вычислениях // Докл. НАН Украины, 2012 – №11 – С. 15-21.
5. Пустовіт О., Устименко В., Про застосування алгебраїчної комбінаторики до проблем кодування та криптографії // Математичне моделювання в економіці, № 1-2. – Київ. – 2017. – С. 31-46.
6. Ustimenko V., Roma´nczuk-Polubiec U., Wr´oblewska A., Polak M., Zhupa E., On the implementation of new symmetric ciphers based on non-bijective multivariate maps, Proceedings of the 2018 Federated Conference on Computer Science and Information Systems, M. Ganzha, L. Maciaszek, M. Paprzycki (eds). ACSIS, Vol. 15. – pp. 397-405 (2018).
7. Устименко В.О., Пустовіт О.С. Про нову концепцію електронного підпису та засоби її реалізації, Колективна монографія за матеріалами XVI Міжнародно-практичної конференції. – м. Київ (Пуща-Водиця). – 2017. – С. 86-89.
8. Krendelev S., Sazonova P., Parametric Hash Function Resistant to Attack by Quantum Computer, Based on Problem of Solving a System of Polynomial Equations in Integers, Proceedings of the 2018 Federated Conference on Computer Science and Information Systems, M. Ganzha, L. Maciaszek, M. Paprzycki (eds). ACSIS. – Vol. 15. – pp. 387-390 (2018).
9. Устименко В.О., Пустовіт О.С. Про нові алгоритми аудиту електронних документів, їх імплементацію та застосування у кібербезпеці, Колективна монографія за матеріалами XVII Міжнародно-практичної конференції. – м. Київ (Пуща-Водиця). – 2018. – С. 170-174.
10. V. Ustimenko, M. Klisowski, On Noncommutative Cryptography with cubical multivariate maps of predictable density, Proceedings of the 2019 Computing Conference. – London. – July, 2019 (to appear)
11. U. Roma´nczuk-Polubiec, V. Ustimenko. On new key exchange multivariate protocols based on pseudorandom walks on incidence structures, Dopovidi NAN Ukrainy, N1, 2015, pp. 41-49.
12. B. Bollob´as, ”Extremal graph theory”, Academic Press, London, 1978.
13. V. Ustimenko, Maximality of affine group, hidden graph cryptosystem and graph's stream ciphers, Journal of Algebra and Discrete Mathematics, 2004, v.10, pp. 51-65.
14. V. Ustimenko, On desynchronised multivariate algorithms of El Gamal type for stable semigroups of affine Cremona group, Theoretical and Applied Cybersecurity, KPI, N1, 2019 (to appear).
15. M. Polak, U. Romańczuk, V. Ustimenko, A. Wróblewska, On the applications of Extremal Graph Theory to Coding Theory and Cryptography, Electronic Notes in Discrete Mathema Discrete Mathematics, N 43, pp. 329-342.
16. F. Lazebnik, V. Ustimenko, A. J. Woldar, A new series of dense graphs of high girth, Bull. Amer. Math. Soc. (N.S.) 32 (1995), no. 1, 73–79.
17. V. Ustimenko. On extremal graph theory and symbolic computations, Dopovidi National Academy of Sci, Ukraine, 2013, N2, pp. 42-49.
18. Alexei Myasnikov, Vladimir Shpilrain and Alexander Ushakov (2008), Group-based Cryptography, Berlin: Birkhäuser Verlag.
19. Zhenfu Cao (2012), New Directions of Modern Cryptography. Boca Raton: CRC Press, Taylor & Francis Group. ISBN 978-1-4665-0140-9.
20. Benjamin Fine, et. al. "Aspects of Non abelian Group Based Cryptography: A Survey and Open Problems", arXiv:1103.4093.
21. Alexei G. Myasnikov; Vladimir Shpilrain and Alexander Ushakov (2011), Non-commutative Cryptography and Complexity of Group-theoretic Problems, American Mathematical Society.

22. Alexei G. Myasnikov; Vladimir Shpilrain and Alexander Ushakov (2011), Non-commutative Cryptography and Complexity of Group-theoretic Problems, American Mathematical Society.
23. I. Anshel, M. Anshel and D. Goldfeld, An algebraic method for public-key cryptography. Math. Res.Lett. 6(3–4), 287–291 (1999).
24. S.R. Blackburn and S.D. Galbraith, Cryptanalysis of two cryptosystems based on group actions. In: Advances in Cryptology – ASIACRYPT '99. Lecture Notes in Computer Science, vol. 1716, pp. 52–61. Springer, Berlin (1999).
25. K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J.S. Kang and C. Park, New public-key cryptosystem using braid groups. In: Advances in Cryptology – CRYPTO 2000, Santa Barbara, CA. Lecture Notes in Computer Science, vol. 1880, pp. 166–183. Springer, Berlin (2000).
26. G. Maze, C. Monico and J. Rosenthal, Public key cryptography based on semigroup actions, Adv.Math. Commun. 1(4), 489–507 (2007)
27. P.H. Kropholler and S.J. Pride, W.A.M. Othman K.B. Wong, P.C. Wong, Properties of certain semigroups and their potential as platforms for cryptosystems, Semigroup Forum (2010) 81: 172–186.
28. A. Lopez Ramos, J. Rosenthal, D. Schipani and R. Schnyder, Group key management based on semigroup actions, Journal of Algebra and its applications, vol.16 (to appear in 2019).
29. Gautam Kumar and Hemraj Saini, Novel Noncommutative Cryptography Scheme Using Extra Special Group, Security and Communication Networks,Volume 2017, Article ID 9036382, 21 pages, https://doi.org/10.1155/2017/9036382
30. V. Ustimenko, On the families of stable transformations of large order and their cryptographical applications, Tatra Mt. Math. Publ., 70 (2017), 107 =117.
31. Priyadarsini P.L.K., A Survey on some Applications of Graph Theory in Cryptography, Journal of Discrete Mathematical Sciences and Cryptography, 18:3, 209-217 (2015).
32. V. Ustimenko, On semigroups of multiplicative Cremona transformations and new solutions of Post Quantum Cryptography, Cryptology ePrint Archive, 133, 2019.
33. U. Romańczuk-Polubiec, V. Ustimenko, On Multivariate Cryptosystems Based on Polynomially Compressed Maps with Invertible Decompositions, Cryptography and Security Systems, Third International Conference, CSS 2014, Lublin, Poland, September 22-24, 2014. Proceedings, Communications in Computer and Information Science, 448, p. 23-37.
34. V. Ustimenko, U. Romanczuk-Polubiec, A. Wroblewska, M. Polak, E. Zhupa, On the constructions of new symmetric ciphers based on non-bijective multivariate maps of prescribed degree, Security and Communication Networks, 2019 (to appear)
35. Mathew Cary, Ramarathnam Venkatesam, A Message Authentication Code Based on Unimodular Matrix Groups, Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings, Lecture Notes in Computer Science.
36. Mihir Bellare, Daniel J. Bernstein, and Stefano Tessaro. Hash-function based PRFs:AMAC and its multi-user security. LNCS, pages 566-595. Springer, Heidelberg, 2016.
37. Kan Yasuda. A Double-Piped Mode of Operation for MACs, PRFs and PROs: Security beyond the Birthday Barrier. In Antoine Joux, editor, EUROCRYPT, volume 5479 of Lecture Notes in Computer Science, pages 242-259. Springer, 2009.
38. Xiaoyun Wang, Hongbo Yu, WeiWang, Haina Zhang, and Tao Zhan. Cryptanalysis on HMAC/NMACMD5 and MD5-MAC. In Antoine Joux, editor, EUROCRYPT, volume 5479 of Lecture Notes in Computer Science, pages 121{133. Springer, 2009.
39. Gaetan Leurent, Thomas Peyrin, and Lei Wang. New Generic Attacks against Hash-Based MACs. In Kazue Sako and Palash Sarkar, editors, Advances in Cryptology-ASIACRYPT 2013, volume 8270, pages 11-20. 2013.

40. Neal Koblitz and Alfred Menezes. Another look at HMAC. Cryptology ePrint Archive, Report 2012/074, 2012.
41. Yevgeniy Dodis, Eike Kiltz, Krzysztof Pietrzak, and Daniel Wichs. Message authentication, revisited. In David Pointcheval and Thomas Johansson, editors, EUROCRYPT 2012, volume 7237 of LNCS, pages 355{374. Springer, Heidelberg, April 2012.
42. Yevgeniy Dodis and John P. Steinberger. Domain Extension for MACs Beyond the Birthday Barrier.In Kenneth G. Paterson, editor, EUROCRYPT, volume 6632 of Lecture Notes in Computer Science, pages 323-342. Springer, 2011.
43. Yevgeniy Dodis, Thomas Ristenpart, John P. Steinberger, and Stefano Tessaro. To Hash or Not to Hash Again?, (In) Difererentiability Results for H2 and HMAC. In Reihaneh Safavi-Naini and Ran Canetti,editors, CRYPTO, volume 7417 of Lecture Notes in Computer Science, pages 348-366. Springer, 2012.
44. Pierre-Alain Fouque, Gaetan Leurent, and Phong Q. Nguyen. Full Key-Recovery Attacks onHMAC/NMAC-MD4 and NMAC-MD5. In Alfred Menezes, editor, CRYPTO, volume 4622 of Lecture Notes in Computer Science, pages 13-30. Springer, 2007.
45. Jongsung Kim, Alex Biryukov, Bart Preneel, and Seokhie Hong. On the Security of HMAC and NMAC Based on HAVAL, MD4, MD5, SHA-0 and SHA-1 (Extended Abstract). In Roberto De Prisco and Moti Yung, editors, SCN, volume 4116 of Lecture Notes in Computer Science. Springer, 2006.

REFERENCES

1. Oliynykov R., Gorbenko I., Kazymyrov O., Ruzhentsev V., Kuznetsov O., Gorbenko Yu., Dyrda O., Dolgov V., Pushkaryov A., Mordvinov R., Kaidalov D. Data Security. Symmetric block transformation algorithm. Ministry of Economical Development and Trade of Ukraine. DSTU 7624:2014. National Standard of Ukraine. Information technologies. Cryptographic. – 2015.
2. Aumasson J.Ph., Serious Cryptography: A Practical Introduction to Modern Encryption, No Starch Press. – 2017. – 312 p.
3. V. Ustimenko, On new symbolic key exchange protocols and cryptosystems based on hidden tame homomorphism, Dopov. Nac. akad. nauk Ukraine. – 2018, n 10. – pp. 26-36.
4. Ustimenko V.A. Ob ekstremalnoy teorii grafov i simvolnyih vyichisleniyah [On extremal graph theory and symbolic calculations] // Dokl. NAN Ukrainyi, 2012 – №11 – s. 15-21.
5. Pustovit O., Ustymenko V., Pro zastosuvannia alhebraichnoi kombinatoryky do problem koduvannia ta kryptohrafii [On the application of algebraic combinatorics to the problems of coding and cryptography] //Matematychne modeliuvannia v ekonomitsi, № 1-2. – Kyiv. – 2017. – s. 31-46.
6. Ustimenko V., Roma´nczuk-Polubiec U., Wr´oblewska A., Polak M., Zhupa E., On the implementation of new symmetric ciphers based on non-bijective multivariate maps, Proceedings of the 2018 Federated Conference on Computer Science and Information Systems, M. Ganzha, L. Maciaszek, M. Paprzycki (eds). ACSIS, Vol. 15. – pp. 397-405 (2018).
7. Ustymenko V.O., Pustovit O.S. Pro novu kontseptsiiu elektronnoho pidpysu ta zasoby yii realizatsii [A new concept of electronic signature and means of its implementation], Kolektyvna monohrafiia za materialamy XVI Mizhnarodno-praktychnoi konferentsii. – m. Kyiv (Pushcha-Vodytsia). – 2017. – s. 86-89.
8. Krendelev S., Sazonova P., Parametric Hash Function Resistant to Attack by Quantum Computer, Based on Problem of Solving a System of Polynomial Equations in Integers, Proceedings of the 2018 Federated Conference on Computer Science and Information Systems, M. Ganzha, L. Maciaszek, M. Paprzycki (eds). ACSIS. – Vol. 15. – pp. 387-390 (2018).

9. Ustymenko V.O., Pustovit O.S. Pro novi alhorytmy audytu elektronnykh dokumentiv, yikh implementatsiiu ta zastosuvannia u kiberbezpetsi [A new algorithms for audit of electronic documents, their implementation and application in cybersecurity], Kolektyvna monohrafiia za materialamy XVII Mizhnarodno-praktychnoi konferentsii. – m. Kyiv (Pushcha-Vodytsia). – 2018. – s. 170-174.
10. V. Ustimenko, M. Klisowski, On Noncommutative Cryptography with cubical multivariate maps of predictable density, Proceedings of the 2019 Computing Conference. – London. –July, 2019 (to appear).
11. U. Roma nczuk-Polubiec, V. Ustimenko. On new key exchange multivariate protocols based on pseudorandom walks on incidence structures, Dopovidi NAN Ukrainy, N1, 2015, pp. 41-49.
12. B. Bollob´as, "Extremal graph theory", Academic Press, London, 1978.
13. V. Ustimenko, Maximality of affine group, hidden graph cryptosystem and graph's stream ciphers, Journal of Algebra and Discrete Mathematics, 2004, v.10, pp. 51-65.
14. V. Ustimenko, On desynchronised multivariate algorithms of El Gamal type for stable semigroups of affine Cremona group, Theoretical and Applied Cybersecurity, KPI, N1, 2019 (to appear).
15. M. Polak, U. Romańczuk, V. Ustimenko A. Wróblewska, On the applications of Extremal Graph Theory to Coding Theory and Cryptography, Electronic Notes in Discrete Mathema Discrete Mathematics, N 43, pp. 329-342.
16. F. Lazebnik, V. Ustimenko, A. J. Woldar. A new series of dense graphs of high girth, Bull. Amer. Math. Soc. (N.S.) 32 (1995), no. 1, 73–79.
17. V. Ustimenko. On extremal graph theory and symbolic computations, Dopovidi National Academy of Sci, Ukraine, 2013, N2, pp. 42-49.
18. Alexei Myasnikov, Vladimir Shpilrain and Alexander Ushakov (2008), Group-based Cryptography, Berlin: Birkhäuser Verlag.
19. Zhenfu Cao (2012), New Directions of Modern Cryptography. Boca Raton: CRC Press, Taylor & Francis Group. ISBN 978-1-4665-0140-9.
20. Benjamin Fine, et. al. "Aspects of Non abelian Group Based Cryptography: A Survey and Open Problems", arXiv:1103.4093.
21. Alexei G. Myasnikov; Vladimir Shpilrain and Alexander Ushakov (2011), Non-commutative Cryptography and Complexity of Group-theoretic Problems, American Mathematical Society.
22. Alexei G. Myasnikov; Vladimir Shpilrain and Alexander Ushakov (2011), Non-commutative Cryptography and Complexity of Group-theoretic Problems, American Mathematical Society.
23. I. Anshel, M. Anshel and D. Goldfeld, An algebraic method for public-key cryptography. Math. Res.Lett. 6(3–4), 287–291 (1999).
24. S.R. Blackburn and S.D. Galbraith, Cryptanalysis of two cryptosystems based on group actions. In: Advances in Cryptology—ASIACRYPT '99. Lecture Notes in Computer Science, vol. 1716, pp. 52–61. Springer, Berlin (1999).
25. K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J.S. Kang and C. Park, New public-key cryptosystem using braid groups. In: Advances in Cryptology—CRYPTO 2000, Santa Barbara, CA. Lecture Notes in Computer Science, vol. 1880, pp. 166–183. Springer, Berlin (2000).
26. G. Maze, C. Monico and J. Rosenthal, Public key cryptography based on semigroup actions, Adv.Math. Commun. 1(4), 489–507 (2007).
27. P.H. Kropholler and S.J. Pride, W.A.M. Othman K.B. Wong, P.C. Wong, Properties of certain semigroups and their potential as platforms for cryptosystems, Semigroup Forum (2010) 81: 172–186.
28. A. Lopez Ramos, J. Rosenthal, D. Schipani and R. Schnyder, Group key management based on semigroup actions, Journal of Algebra and its applications, vol.16 (to appear in 2019).

29. Gautam Kumar and Hemraj Saini, Novel Noncommutative Cryptography Scheme Using Extra Special Group, Security and Communication Networks,Volume 2017, Article ID 9036382, 21 pages, https://doi.org/10.1155/2017/9036382
30. V. Ustimenko, On the families of stable transformations of large order and their cryptographical applications, Tatra Mt. Math. Publ., 70 (2017), 107 =117.
31. Priyadarsini P.L.K., A Survey on some Applications of Graph Theory in Cryptography, Journal of Discrete Mathematical Sciences and Cryptography, 18:3, 209-217 (2015).
32. V. Ustimenko, On semigroups of multiplicative Cremona transformations and new solutions of Post Quantum Cryptography, Cryptology ePrint Archive, 133, 2019.
33. U. Romańczuk-Polubiec, V. Ustimenko, On Multivariate Cryptosystems Based on Polynomially Compressed Maps with Invertible Decompositions, Cryptography and Security Systems, Third International Conference, CSS 2014, Lublin, Poland, September 22-24, 2014. Proceedings, Communications in Computer and Information Science, 448, p. 23-37.
34. V. Ustimenko, U. Romanczuk-Polubiec, A. Wroblewska, M. Polak, E. Zhupa, On the constructions of new symmetric ciphers based on non-bijective multivariate maps of prescribed degree, Security and Communication Networks, 2019 (to appear)
35. Mathew Cary, Ramarathnam Venkatesam, A Message Authentication Code Based on Unimodular Matrix Groups, Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings, Lecture Notes in Computer Science.
36. Mihir Bellare, Daniel J. Bernstein, and Stefano Tessaro. Hash-function based PRFs:AMAC and its multi-user security. LNCS, pages 566-595. Springer, Heidelberg, 2016.
37. Kan Yasuda. A Double-Piped Mode of Operation for MACs, PRFs and PROs: Security beyond the Birthday Barrier. In Antoine Joux, editor, EUROCRYPT, volume 5479 of Lecture Notes in Computer Science, pages 242-259. Springer, 2009.
38. Xiaoyun Wang, Hongbo Yu,WeiWang, Haina Zhang, and Tao Zhan. Cryptanalysis on HMAC/NMACMD5 and MD5-MAC. In Antoine Joux, editor, EUROCRYPT, volume 5479 of Lecture Notes in Computer Science, pages 121{133. Springer, 2009.
39. Gaetan Leurent, Thomas Peyrin, and Lei Wang. New Generic Attacks against Hash-Based MACs. In Kazue Sako and Palash Sarkar, editors, Advances in Cryptology-ASIACRYPT 2013, volume 8270, pages 11-20. 2013.
40. Neal Koblitz and Alfred Menezes. Another look at HMAC. Cryptology ePrint Archive, Report 2012/074, 2012.
41. Yevgeniy Dodis, Eike Kiltz, Krzysztof Pietrzak, and Daniel Wichs. Message authentication, revisited. In David Pointcheval and Thomas Johansson, editors, EUROCRYPT 2012, volume 7237 of LNCS, pages 355{374. Springer, Heidelberg, April 2012.
42. Yevgeniy Dodis and John P. Steinberger. Domain Extension for MACs Beyond the Birthday Barrier.In Kenneth G. Paterson, editor, EUROCRYPT, volume 6632 of Lecture Notes in Computer Science, pages 323-342. Springer, 2011.
43. Yevgeniy Dodis, Thomas Ristenpart, John P. Steinberger, and Stefano Tessaro. To Hash or Not to Hash Again?, (In) Difererentiability Results for H2 and HMAC. In Reihaneh Safavi-Naini and Ran Canetti,editors, CRYPTO, volume 7417 of Lecture Notes in Computer Science, pages 348-366. Springer, 2012.
44. Pierre-Alain Fouque, Gaetan Leurent, and Phong Q. Nguyen. Full Key-Recovery Attacks onHMAC/NMAC-MD4 and NMAC-MD5. In Alfred Menezes, editor, CRYPTO, volume 4622 of Lecture Notes in Computer Science, pages 13-30. Springer, 2007.
45. Jongsung Kim, Alex Biryukov, Bart Preneel, and Seokhie Hong. On the Security of HMAC and NMAC Based on HAVAL, MD4, MD5, SHA-0 and SHA-1 (Extended Abstract). In Roberto De Prisco and Moti Yung, editors, SCN, volume 4116 of Lecture Notes in Computer Science. Springer, 2006.

Стаття надійшла до редакції 06.08.2018.

УДК 004.942: 052:056

https://orcid.org/0000-0002-8698-0972
https://orcid.org/0000-0002-7860-9663
https://orcid.org/0000-0002-3014-5521

В.Г. ІВАНОВ, В.О. ЛИФАР, О.К. ЛИФАР

ТЕОРЕТИКО-МЕТОДИЧНІ АСПЕКТИ КОНЦЕПЦІЇ ЗАБЕЗПЕЧЕННЯ НЕОБХІДНОГО РІВНЯ ПОВНОТИ БЕЗПЕКИ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ ОБ'ЄКТАМИ ПІДВИЩЕНОЇ НЕБЕЗПЕКИ

Анотація. *Представлені аспекти сучасних підходів до вирішення науково-технічної проблеми щодо забезпечення необхідного рівня повноти безпеки технічних засобів АСУ ТП об'єктами підвищеної небезпеки. Сформульовано завдання досліджень і теоретико-методична концепція визначення показників надійності і безпеки апаратних і програмних засобів АСУТП. Розглянуто існуючі та запропоновано оригінальні методи визначення нормуючих показників надійності при проведенні SIL-аналізу. Розглянуто проблеми підготовки фахівців до забезпечення необхідного рівня SIL при розробці АСУТП.*

Ключові слова: *рівень повноти безпеки, функціональна безпека, електричні/електронні/програмовані електронні пристрої, надійність, безпека, інженерія програмного забезпечення, комп'ютерна інженерія, комп'ютерні науки, моделі процесорів, інформаційні технології.*

DOI: 10.35350/2409-8876-2019-16-3-36-48

Вступ

Оцінка і профілактика техногенних ризиків, попередження великих аварій при експлуатації промислових об'єктів підвищеної небезпеки вимагають зваженого підходу, нормуються національним і міжнародним законодавством і є актуальною науково-технічною проблемою. Рішення такої проблеми у вигляді теоретично обґрунтованих методів і моделей оцінки рівня надійності та класифікації небезпеки наслідків відмов для автоматизованих систем управління технологічними процесами (АСУТП), а також реалізації комплексної інформаційної технології підтримки прийняття рішень по забезпеченню інтегрального рівня безпеки АСУТП становить значний інтерес для розробників і користувачів таких систем для великих промислових підприємств. До них відносяться: хімічні і нафтохімічні заводи, засоби транспортування небезпечних вантажів і речовин.

На жаль, цій проблемі приділяється мало уваги в науково-технічній сфері, так як аналіз великих промислових аварій і катастроф найчастіше завершується висновком причини технологічних відмов, зовнішніх впливів або людських факторів. Іноді причинами таких небезпечних аварій є не діагностована відмова АСУТП. Однак, це слабо доказові припущення, особливо в умовах зростаючої складності і інтеграції технологічних процесів.

Дослідники і вчені, які займалися питаннями SIL: Michael A. Mitchell, Кулямін В.В., Glisente Landrini, Ковальов І.В., Буй Д.Б., Скобелєв В.Г., Гайдамакін Н.А., Wong Y.K., Eriksson J., Grindal M. та інші.

Незважаючи на безліч стандартних методів і підходів щодо забезпечення необхідного рівня повноти безпеки (РПБ) для АСУТП, існує велика кількість протиріч, неточностей, проблем формалізації і невирішених питань оцінки ризику відмов елементів управління технологічними процесами, що представляє значні складності при прийнятті рішень і сертифікації управляючих комплексів на відповідність інтегральному рівню безпеки (Safety integrity level – SIL) для систем з використанням електричних, електронних, програмованих електронних пристроїв (Е/Е/ПЕ – E/E/PE). Особливі труднощі відчувають розробники базових електронних, електричних, електронних програмованих пристроїв і програмного забезпечення АСУТП. Так як для центральної електронної частини управління спочатку невідомі функціональні призначення вхідних сигналів, їх інформаційна значимість і відповідність певним видам негативних наслідків у разі їх спотворення, істотно ускладнюється інтерпретація небезпеки таких відмов. Це саме можна сказати і до обробки інформації процесорами і вироблення керуючих сигналів. Завдання спрощується в разі, коли АСУТП представлена повним замкнутим контуром від датчиків і вимірювальних пристроїв, структурою прийому, обробки сигналів і видачі керуючих сигналів аж до виконавчих пристроїв і механізмів. В цьому випадку можлива більш-менш певна інтерпретація і аналіз небезпеки наслідків відмов системи або спотворення інформації в ній.

Проте, проблема проведення SIL аналізу і оцінка рівня повноти безпеки для центральних частин розроблюваних АСУТП (див. на рис. 1) є актуальною для встановлення верхньої межі РПБ, а також прийняття рішень щодо технологій розробки таких систем.

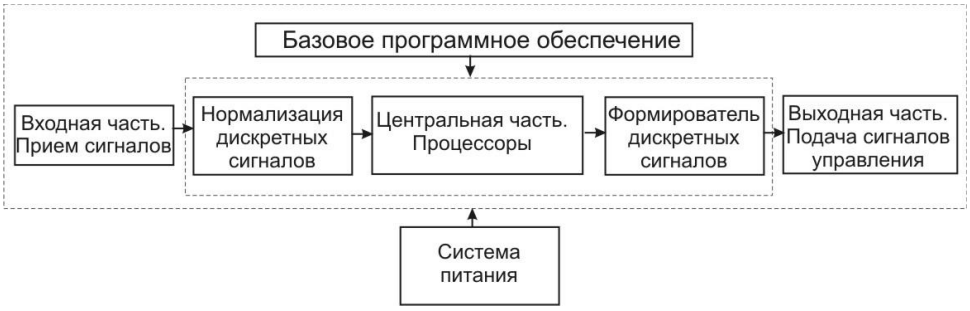

Рисунок 1 – Типова структура базової частини АСУТП

Оцінка рівня повноти безпеки для апаратних частин АСУТП регламентована в повному обсязі [1-4] і передбачає проведення аналізу причин і наслідків відмов (Failure modes and effects analysis – FMEA), а також їх критичності. За результатами аналізу визначаються види наслідків відмов елементів розглянутих блоків АСУТП або її центральної частини, і далі, з використанням методів оцінки ризику, обчислюються кількісні показники ймовірностей відмов.

Найбільш складною частиною вирішення проблеми оцінки РПБ для розроблюваних комплексів є визначення надійності і безпеки програмного забезпечення. Відомі і регламентовані методи [1-3] засновані в основному на рангових оцінках, що у великій мірі нівелює вірогідність визначення рівня надійності програмного забезпечення і представляє велику трудність для розробників базового програмного забезпечення (ПО) центральних частин комплексів АСУТП.

Необхідність розробки методів оцінки кількісних показників надійності програмних засобів, що забезпечують функціональну, експлуатаційну та технічну безпеку роботи АСУТП, обумовлена практичною відсутністю таких методів і проблемою узгодження якісних і кількісних критеріїв, що характеризують рівень повноти безпеки розроблюваних комплексів.

1. Аналіз даних і постановка задачі досліджень

Рівень повноти безпеки відображає ступінь ризику експлуатації об'єктів критичної області експлуатації. У цьому сенсі під «ризиком» мається на увазі настання певних наслідків з певною ймовірністю (або частотою для заданого періоду експлуатації). Проблема профілактики техногенного ризику об'єктів підвищеної небезпеки, обумовленого відмовами АСУТП, може бути розв'язана в результаті послідовного вирішення декількох задач:

1) аналіз виникнення і розвитку процесів відмов елементів АСУТП і оцінка ймовірності таких подій;

2) аналіз наслідків розглянутих відмов і віднесення їх до певної категорії (небезпечні; безпечні; діагностуються; що не діагностуються; критичні; що не критичні; які не впливають на безпеку) на підставі оцінки масштабів таких наслідків;

3) оцінка надійності програмного забезпечення АСУТП (показників ймовірності відмов: середня ймовірність відмови на запит виконання функції безпеки за час T1 (Probability of Failure on Demand) – PFDavg (T1); середня частота небезпечних відмов у годину (Hazardous Failure Probability) – PFH;

4) розробка вимог до діагностики і методів верифікації ПЗ для всіх стадій життєвого циклу;

5) аналіз отриманих показників надійності програмної і апаратної частини АСУТП і вироблення рішень (рекомендацій) за технологією розробки АСУТП на основі порівняльного аналізу нормативних і поточних показників надійності.

Розглядається дві ситуації, для яких може проводитися аналіз і визначення РПБ з метою сертифікації системи управління:

1. При розробці базового комплексу АСУТП без конкретної прив'язки до об'єкта управління. При цьому необхідно визначити нижню межу РПБ, яка забезпечує інтегральний рівень безпеки не гірше заявленого рівня.

2. При створенні АСУТП з повною прив'язкою до об'єкта управління і оцінкою показників ризику, обумовленого експлуатаційною безпекою АСУТП. При цьому функціональна і технічна безпека програмного забезпечення відноситься до внутрішньої складової експлуатаційної безпеки ПЗ.

Вхідними даними для визначення показників надійності апаратної частини АСУТП є показники надійності (напрацювання на відмову,

паспортні дані про ймовірність відмов на запит і на період експлуатації та ін.) окремих елементів Е/Е/ПЕ пристроїв. У першому випадку до таких елементів відносяться тільки фізичні елементи базового комплекту АСУТП (без вимірювальних і виконавчих пристроїв). У другому випадку аналізуються всі Е/Е/ПЕ елементи, включаючи датчики, що передають, і виконавчі пристрої. Завдання оцінки SIL для цих двох ситуацій також відрізняються тим, що в першому випадку апріорі встановлюється поняття «безпечного стану» як відмова системи або припинення її працездатності за умови повного і однозначного діагностування такого стану і нормально безаварійного відключення АСУТП. При цьому такі відмови або зупинки вважаються безпечними. Всі відмови елементів АСУТП, що призводять до спотворення або припинення виконання закладених функцій системи управління, вважаються апріорі небезпечними. У другому випадку рівень небезпеки відмови елемента системи управління встановлюється на підставі аналізу наслідків такої відмови для функціонування технологічних елементів об'єкта управління.

Теорія надійності програмного забезпечення отримала розвиток одночасно з розповсюдженням програмного забезпечення в керуючих комплексах [9, 11]. Для отримання кількісних показників надійності програмного забезпечення необхідно отримати велику кількість статистичного матеріалу, що містить інформацію про динаміку виявлення помилок в закінчених програмних утвореннях. Особливі труднощі представляє взаємодія цих утворень, так як область визначення повного функціоналу програмного комплексу навіть середньої складності найчастіше не може бути визначена повною мірою.

2. Об'єкт, мета та завдання розробок

Об'єкт дослідження – інформаційна підтримка процесів прийняття рішень при створенні керуючих комплексів АСУТП, спрямованих на досягнення необхідного рівня повноти безпеки.

Дана розробка проводиться з метою створення методів, моделей (їх композицій) і програмних засобів інформаційних технологій, які могли б забезпечити процес підтримки рішень при розробці автоматизованих систем управління об'єктами підвищеної небезпеки. Вивчення і розв'язання проблеми забезпечення необхідного рівня повноти безпеки завдань можливо на основі застосування методів оцінки надійності та ймовірності відмов окремих апаратних і програмних складових АСУТП з урахуванням їх взаємного впливу в інтегральному ризику.

Предметом дослідження є моделі, методи, інформаційна технологія оцінки і порівняльного аналізу рівня повноти безпеки на всіх стадіях життєвого циклу створення, експлуатації та ліквідації керуючих комплексів.

3. Існуючі методи і підходи до оцінки рівня повноти безпеки

Оцінка рівня повноти безпеки для апаратних частин АСУТП досить повно регламентована міжнародними стандартами [1-6] і рядом інших керівних документів, в тому числі створених провідними компаніями в області розробки керуючих комплексів. Наприклад, Глізенте Ландрін [12]

представляє ряд статей, в яких детально і дохідливо пояснює підходи і методи визначення кількісних показників, якісних характеристик і критерії вибору компонент для застосування в розподілених системах управління і спеціальних системах забезпечення безпеки з різними рівнями SIL, які рекомендовані в стандартах МЕК 61508 та 61511. Розглядаються також практичні приклади використання таких критеріїв. У статтях М. А. Мітчела [13] зроблено спробу роз'яснити узагальнені підходи до визначення SIL і застосування методів, описаних в стандартах до конкретних систем безпеки. В основі таких підходів лежать методи диференційованого аналізу причин і наслідків відмов FMEA (Failure modes and effects analysis) або з урахуванням їх критичності (FMECA). При цьому враховується принцип ALARP (As Low as Reasonable Practible - низький, наскільки це можливо) для зниження ризику реалізації небезпек, що викликаються відмовами до прийнятної величини.

Найбільшу трудність і невизначеність при такому підході викликають: визначення та формалізація функцій безпеки і встановлення однозначних зв'язків між значущими видами відмов елементів керуючої системи і впливом таких відмов на масштаби небезпечних наслідків.

На рис. 2 представлені відношення різних етапів створення системи функціональної безпеки заданого рівня з дотриманням стандартів IEC.

Рисунок 2 – Області застосування стандартів IEC для оцінки надійності АСУТП

Найбільш поширеними методами є якісні і напівякісні методи ранжирування ризику при оцінці поточного і необхідного рівня SIL. Однак уявна простота застосування таких методів значно нівелюється рівнем їх недостовірності.

Первинна проблема виникає при застосуванні HAZOP з подальшим поділом функцій безпеки. Аналіз небезпеки і працездатності систем безпеки проводиться методами експертних оцінок і не дозволяє в повній мірі виділити функціонал безпеки з функцій засобів подвійного призначення або навіть засобів захисту. Формалізація причинно-наслідкових зв'язків відмов систем управління і наслідків таких відмов без кількісних показників надійності і ризику є в значній мірі профанацією. У зв'язку з цим актуальною

є розробка методів і моделей, що комбінують HAZOP і FMEA з можливістю формалізації причинно-наслідкових зв'язків відмов і подій, ними викликаних, до рівня графів або дерев відмов і дерев подій. При цьому важливо вийти на кількісні показники надійності і небезпеки, а не тільки на рангові оцінки.

Безпеку програмних засобів необхідно оцінювати на всіх стадіях життєвого циклу: при системному аналізі проекту, проектуванні, розробці, тестуванні, верифікації та валідації, тестових випробуваннях, експлуатації та супроводі, модифікації і створенні нових версій, виведенні з експлуатації. На всіх стадіях будь-які впливи можуть мати наслідки для безпеки і змінюють показники надійності.

Ця обставина сприяла появі деяких технологій [14-16]:

1. Microsoft Solutions Framework (MSF). Методики призначені для створення проектів та прийняття рішень на принципах адаптованої моделі колективної розробки засобами Microsoft Visual Studio. Розробка ПО реалізується поетапно з використанням розподілених контрольних точок («водоспад»), а етапи розробки можуть повторюватися («спіраль»).

2. Rational Unified Process (RUP). Проект оформляється у вигляді розподіленої Web бази знань з використанням засобів пошуку та виділення подій. Методи забезпечують розподіл ролей та обов'язків у команді програмістів і реалізуються засобами автоматизації окремих етапів створення.

3. EXtreme Programming (XP). Методи орієнтовані на підвищення ефективності взаємодії як команди програмістів, так і постановників і замовників за рахунок циклів погоджень і перевірок чергових частин вимог замовника.

Основні проблеми, які виникають при використанні зазначених технологій і можуть призводити до відмов функціонування ПО, є помилки програмування і алгоритмізації, що може бути усунуто в достатній мірі методами комплексного тестування, перевірки та затвердження при розробці і супроводі ПЗ.

При цьому використовуються наступні види тестування:

– модульне тестування – для груп незалежних модулів із замкнутою повнотою функціонування;

– інтеграційне тестування – враховує функціональні зв'язки між групами модулів;

– системне тестування – перевірка коректності всього пакету ПО, відповідності продуктивності, критичним навантаженням, помилок користувача, стійкості до програмних і апаратних збоїв.

Верифікація та валідація ПО передбачена стандартами [17-19].

Етапи розробки систем захисту ПО передбачають [20-23]:

– пошук і виділення функцій безпеки ПЗ;
– визначення принципів безпеки функціонування ПЗ;
– види і критерії відмов ПЗ;
– рівні безпеки функціонування ПЗ;
– перелік зовнішніх і внутрішніх впливів, які становлять загрозу безпеці;
– ресурси, необхідні для забезпечення РПБ;
– формування і реалізація систем захисту ПЗ.

Категоріювання видів відмов і їх виявлення є трудомісткою функцією і вимагає високої кваліфікації і глибокого аналізу функціональних зв'язків усередині системи безпеки.

Виділення ресурсів необхідно виконувати з дотриманням принципів надмірності як ресурсів пам'яті, так і часу виконання елементів робочого циклу. При цьому важливо забезпечити:

– контроль зовнішніх даних на відповідність області визначення і застосування ПО;

– кошти on-line котроля правильності виконання програм і трансляції даних;

– засоби реагування на загрози національній безпеці (пастки);

– оперативні процедури відображення виявлення дефектів (визначуваних) і відновлення обчислень після збоїв.

При цьому більш дієвими є системи безпеки, інтегровані у вихідний код до компіляції. Однак такий підхід суттєво ускладнює код і процедури верифікації.

Засоби забезпечення безпеки повинні протистояти зовнішнім і внутрішнім загрозам з заданим рівнем надійності, більш ефективним, ніж це передбачено заявленим РПБ. При цьому необхідно враховувати, що повне усунення будь-яких проявів таких загроз нездійсненно.

Для реалізації систем захисту зазвичай необхідно формувати команду таких фахівців:

– менеджер безпеки проекту (лідер), який зобов'язаний забезпечити вимоги замовника з безпеки засобів АСУТП;

– архітектори систем захисту і розробки базової специфікації функціоналу ПС при критичних рішеннях;

– фахівці, які розробляють весь функціонал компонентів захисту і зв'язок деталей функціоналу (алгоритмізація) для коректного створення вихідного коду і його верифікації;

– програмісти, рівень яких відповідає вибраній специфікації коду;

– фахівці, які здійснювали фонову перевірку і тестування коду;

– фахівці, здатні розробити підсумкові документи з експлуатації систем безпеки відповідно до вимог стандартів.

Верифікація ПЗ проводиться різними методами, які повинні бути обрані на початковій стадії розробки.

Одним з найбільш поширених і недорогих методів є експертні оцінки. Наприклад, оцінка по Фагану (Fagan software inspection) [24] заснована на використанні наскрізного технічного контролю (brainstorming). Додатково можуть використовуватися методи інспекції інтерфейсу користувачів [25] і експертизи якості архітектури і захисту ПО [26-27].

Застосування статичного аналізу вихідного коду і його архітектури. Однак цей метод пов'язаний зі значними труднощами в застосуванні керуючих систем критичного значення в зв'язку з неможливістю прямого транслювання коду таких систем в загальноприйняті мови високого рівня, що обмежує можливості автоматизації перевірки компонент функціонального ПЗ.

Формальні і напівформальні методи верифікації ПЗ засновані на розробці вимог до логіко-алгебраїчних моделей і абстрактних моделей. Такі моделі в деяких випадках можуть бути формалізовані до логічного рівня і

забезпечити розробку інструментальних засобів автоматизованого процесу дозволу ряду завдань верифікації ПЗ. Приклад побудови предикат в деяких випадках логічних обчислень з отриманням кількісних показників ймовірності відмови наводиться в цій статті.

4. Пропозиції та методи комплексної оцінки ризику і РПБ АСУТП

В результаті проведеного аналізу та вивчення нормативної бази можна запропонувати окремі методи визначення кількісних показників РПБ на основі стохастичних показників надійності дискретних елементів керуючої системи і якісних показників програмного забезпечення АСУТП.

Визначення РПБ досліджуваної апаратної частини складової АСУТП пропонується здійснювати гібридними методами експертного аналізу, що поєднує стандартний підхід до визначення області небезпеки наслідків відмов окремих елементів апаратного забезпечення на базі HAZOP аналізу і автоматизованих методів оцінки ймовірності таких відмов. Аналіз небезпеки і працездатності необхідно проводити з використанням спеціальних протоколів, в яких відображаються причинно-наслідкові зв'язки між можливими причинами відмов вихідних елементів, їх впливом на працездатність системи управління і наслідками втрати функцій системи в результаті відмов. Використання структурованих записів таких причинно-наслідкових зв'язків, оформлених, наприклад, засобами мови структурованої розмітки (xml), дозволяє автоматизувати процес створення узагальненої математичної моделі оцінки SIL для заявленої системи управління. Така модель представляється кортежем (або графом) рівня надійності та безпеки і може бути формалізована до стану згортки / розгортки дерев відмов (FTA) і дерев подій (ETA). Причому в якості вихідних (ініціюючих) відмов або подій можуть розглядатися і елементи програмного забезпечення, що застосовується в АСУТП.

Авторами статті були виконані дослідження при постановці завдань, розробці алгоритмів, верифікації та впровадженні програмних засобів підтримки прийняття рішень при оцінці ризику великих промислових підприємств [28-29]. Перевірені можливості вищеописаного протоколу і достовірність результатів обчислень автоматизованих побудов FTA і ETA на базі логічних відносин причинно-наслідкових зв'язків аналізованих елементів АСУТП. Використання логічних операцій І (Заборона), АБО (див. Таб. 1) [30] для низхідного методу розгортки дерев відмов і бінарного розгалуження подій при впливах засобів захисту, представлених в деревах подій, дозволяє здійснити кількісні оцінки ймовірності виникнення негативних наслідків відмов елементів АСУ ТП.

Таблиця 1 – Відповідність формул визначення ймовірності логічних операцій

І ($\wedge$)	АБО ($\vee$)	виключає АБО ($\oplus$)
$P_e = \prod_{i=1}^{n} P_i$	$P_e = 1 - \prod_{i=1}^{n} (1 - P_i)$	$P_e = \sum_{i=1}^{n} P_i$

Програмні засоби (приклад наведено на рис. 3.) підтримки автоматизованого процесу формування FTA, ETA на основі використання протоколу аналізу HAZOP дозволяють в повній мірі здійснити проект кількісної оцінки SIL і виділити і сортувати поєднання відмов, які впливають на критичність наслідків у міру їх значущості, що дає можливість оптимізувати прийняті рішення.

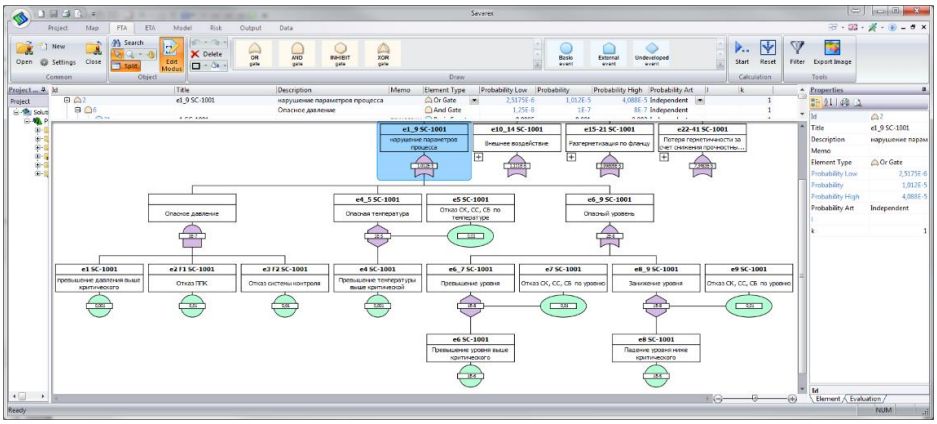

Рисунок 3 – Приклад автоматичної розгортки дерева відмов з графа протоколу HAZOP

Автономне тестування модулів програмного забезпечення базових частин АСУТП об'єктів підвищеної небезпеки може бути виконано на основі абстрактних синтаксичних побудов деревовидної форми [31-33].

Висновки

Існуючі моделі і методи, що дозволяють встановити рівень повноти безпеки систем управління об'єктами підвищеної небезпеки, не в повній мірі відповідають сучасним вимогам проведення сертифікаційних процедур. Науково-технічна проблема комплексної системної підтримки прийняття рішень в області створення систем безпеки АСУТП є актуальною.

Зниження суб'єктивної складової оцінки ризику і рівня РПБ є важливим завданням при сертифікації засобів АСУТП і може досягатися методами кількісної оцінки ймовірності відмов апаратної і програмної складових комплексів управління об'єктами критичної значущості.

Раціональними для оцінки ймовірності відмов апаратної частини є методи дерев відмов (FTA) для ініціюючих небезпечних подій і метод дерев подій (ETA) для відмов систем захисту і визначення сценаріїв наслідків таких відмов.

Розробка програмних комплексів, за допомогою яких може бути реалізована інформаційна технологія підтримки прийняття рішень при забезпеченні необхідного рівня SIL для керуючих комплексів об'єктів підвищеної небезпеки, актуальна і здійсненна при використанні пропонованих в статті методів і моделей.

СПИСОК ЛІТЕРАТУРИ

1. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью = Ч. 1. Общие требования: национальный стандарт Российской Федерации ГОСТ Р МЭК 61508-1-2007 / Федеральное агентство по техническому регулированию и метрологии. – М.: Стандартинформ, 2008. – V, 44 с.
2. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью = Ч. 2. Требования к системам: национальный стандарт Российской Федерации ГОСТ Р МЭК 61508-2-2007 / Федеральное агентство по техническому регулированию и метрологии. – М.: Стандартинформ, 2008. – V, 58 с.
3. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью = Ч. 3. Требования к программному обеспечению: национальный стандарт Российской Федерации ГОСТ Р МЭК 61508-3-2012 / Федеральное агентство по техническому регулированию и метрологии. – М.: Стандартинформ, 2014. – V, 97 с.
4. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью = Ч. 6. Руководство по применению ГОСТ Р МЭК 61508-2-2007 и ГОСТ Р МЭК 61508-3-2007 : национальный стандарт Российской Федерации ГОСТ Р МЭК 61508-6-2007 / Федеральное агентство по техническому регулированию и метрологии. - Москва : Стандартинформ, 2008. – V, 62 с.
5. Функциональная безопасность в непрерывных производствах. Руководство по безопасности процессов / национальный стандарт Российской Федерации ГОСТ Р МЭК 61511-1-2011 / Федеральное агентство по техническому регулированию и метрологии. – М.: Стандартинформ, 2013. – V, 66 с.
6. Руководство по функциональной безопасности для систем, связанных с безопасностью, и других применений с уровнем SIL2, SIL3 в соответствии со стандартами МЭК 61508 и МЭК 61511 / GM International Technology for safety / Via San Fiorano 70, 20058 Villasanta (MI) Italy, 2013. – D100, 77 p.
7. Dr. David J. Smith. Reliability, Maintainability and Risk. Practical methods for engineers. Butterworth-Heinemann. The Boulevard, Langford Lane, Kidlington, Oxford OX5 1GB, UK. 225 Wyman Street, Waltham, MA 02451, USA. Eighth edition 2011.
8. Безопасность программных средств: модели и методы (обзор) / Д. Б. Буй, В. Г. Скобелев // Радіоелектронні і комп'ютерні системи. - 2014. – № 1.
9. Липаев В. В. Обеспечение качества программных средств. Методы и стандарты. М.: СИНТЕГ, 2001. – 380 с.
10. Lyu M. R. Software Fault Tolerance. Published by John Wiley & Sons Ltd, 1996.
11. Ковалев И. В., Золотарёв В. В., Жуков В. Г., Жукова М. Н. Методика построения модели безопасности автоматизированных систем // Программные продукты и системы. 2012. № 2. С. 16.
12. Ландрини, Г. Критерии выбора компонентов с уровнем SIL 3 для РСУ и систем ПАЗ в соответствии со стандартами МЭК / Глизенте Ландрини // Современные технологии автоматизации. - 2009. – N 3. – С. 110-114.
13. Michael A. Mitchell. SIL – it is not difficult. Valve World Conference 2010. «Промышленная безопасность». – 2011. – № 5 (74).
14. Microsoft solutions framework. – URL: http://www.microsoft.com/Rus/Msdn/msf/Default.mspx.
15. Rational Unified Process. Методология и технология. Материалы компании Interface Ltd– URL: http://www.interface.ru/home.asp?artId=779.
16. Бек К. Экстремальное программирование / К.Бек. – СП-б: Питер, 2002. – 224 с.

17. IEEE 610.12-1990 Standard glossary of soft-ware engineering terminology, corrected edition [Текст]. – IEEE, 1991.
18. IEEE 1012-2004 Standard for verification and validation [Текст]. – IEEE, 2005.
19. ISO/IEC 12207 Systems and software engi-neering – software life cycle processes [Текст]. – ISO, 2008.
20. Галатенко В.А. Основы информационной безопасности [Текст] / В.А. Галатенко. – М.: ИНТУИТ, 2003. – 208 с.
21. Липаев В.В. Технологические процессы и стандарты обеспечения функциональной безопасности в жизненном цикле программных средств [Текст] / В.В. Липаев // Jet Info. – 2004. – № 3. – С. 2-19.
22. Липаев В.В. Функциональная безопасность программных средств [Текст] / В.В. Липаев // Jet Info. – 2004. – № 8. – С. 3-28.
23. Волобуев С.В. Философия безопасности социотехнических систем: информационные аспекты [Текст] / С.В. Волобуев. – М.: Вузовская книга, 2004. – 360 с.
24. Fagan M.E. Design and code inspections to reduce errors in program development [Текст] / M.E. Fagan // IBM Systems Journal. – 1976. – N 3. – P. 182-211.
25. Константайн Л. Разработка программного обеспечения [Текст] / Л. Константайн, Л. Ло-квуд. – СПб: Питер, 2004. – 592 с.
26. Anderson R. Security engineering: a guide to building dependable distributed systems [Текст] / R. Anderson. – NY: John Wiley & Sons, 2001. – 1040 p.
27. Dobrica L. A survey on software architecture analysis methods [Текст] / L. Dobrica, E. Niemela // IEEE Transactions on software engineering. – 2002. – № 7. – P. 638-653.
28. Лифарь В. А. Разработка метода оптимизации проведения ремонтно-восстановительных работ с учетом показателей риска / В. А. Лыфарь, С. А. Сафонова, В. Г. Иванов // Технологический аудит и резервы производства. – 2015. – № 2/2(22) – С. 11-17.
29. Лифар В.О. Моделі, методи та інформаційні технології оцінки техногенного ризику об'єктів підвищеної небезпеки: дис. ... д-ра техн. наук : 05.13.06 / Лифар В. О.; [Місце захисту: Чорноморський національний університет імені Петра Могили]. – Миколаїв, 2017. – 309 с.
30. Хенли Э. Дж., Кумамото Х. Надежность технических систем и оценка риска: Пер. с англ. В. С. Сыромятникова – М.: Машиностроение, 1984. – 528 с.
31. S. Nair, R. Jetley, A. Nair, "A Static Code Analysis Tool for Control System Software", SANER 2015, Montréal, Canada, pp. 459-463.
32. F. Narisco, A.-R. Bolivar, F. Hidrobo, O. Gonzalez, "A Syntactic Specification for the Programming Languages of the IEC 61131-3 Standard", Advances in Computational Intelligence, Man-Machine Systems and Cybernetics, pp. 171-176, 2010.
33. Müller and M. I. Schwartzbach, "Static Program Analysis", Department of Computer Science Aarhus University, Denmark, 113 p., 2018. http://users-cs.au.dk/amoeller/spa/spa.pdf.

REFERENCES

1. (2008) Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 1. General requirements: national standard of the Russian Federation GOST R IEC 61508-1-2007 / Federal Agency for Technical Regulation and Metrology. – Moskva.: Standartinform. – V, 44 s.
2. (2008) Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 2. Requirements for systems: national standard of the Russian Federation GOST R IEC 61508-2-2007 / Federal Agency for Technical Regulation and Metrology. – Moskva.: Standartinform. – V, 58 s.

3. (2014) Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 3. Software requirement: national standard of the Russian Federation GOST R IEC 61508-3-2012 / Federal Agency for Technical Regulation and Metrology. – Moskva: Standartinform. – V, 97 s.
4. (2008) Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 6. Guidelines on the application of GOST R IEC 61508-2-2007 and GOST R IEC 61508-3-2007 : national standard of the Russian Federation / Federal Agency for Technical Regulation and Metrology. - Moscow: Standartinform. – V, 62 s.
5. (2013) IEC 61511:2004 Functional Safety – Safety Instrumented Systems for the Process Industry Sector/ national standard of the Russian Federation / Federal Agency for Technical Regulation and Metrology. – M .: Standartinform. – V, 66 s.
6. (2013) Functional safety guidelines for safety related systems and other applications with SIL2, SIL3 level in accordance with IEC 61508 and IEC 61511 / GM International Technology for safety / Via San Fiorano 70, 20058 Villasanta (MI) Italy – D100, 77 p.
7. Dr. David J. Smith (2011). Reliability, Maintainability and Risk. Practical methods for engi-neers. Butterworth-Heinemann. The Boulevard, Langford Lane, Kidlington, Oxford OX5 1GB, UK. 225 Wyman Street, Waltham, MA 02451, USA. Eighth edition.
8. Software Security: Models and Methods (review) (2014). / D. B. Bui, V. G. Skobelev // Radio Electronics and Computer Systems. No. 1. (In Ukrainian).
9. Lipaev V.V. (2001). Software quality assurance. Methods and standards. Moskva: SINTEG, 380 s. (In Russian).
10. Lyu M. R. (1996). Software Fault Tolerance. Published by John Wiley & Sons Ltd.
11. Kovalev I.V., Zolotarev V.V., Zhukov V.G., Zhukova M.N. (2012). Methodology for constructing a security model for automated systems // Software Products and Systems. No. 2. P. 16. (In Russian).
12. Landrini, G. (2009). Criteria for choosing components with a SIL 3 level for DCS and PAZ systems in accordance with IEC / Glisente Landrini standards // Modern Automation Technologies. N 3. – s. 110-114
13. Michael A. Mitchell. (2011). SIL - it is not difficult. Valve World Conference 2010. "Industrial Safety". № 5 (74)
14. Microsoft solutions framework. URL: http://www.microsoft.com/Rus/Msdn/ msf/Default.mspx.
15. Rational Unified Process. Methodology and technology. Company Materials Interface Ltd URL: http://www.interface.ru/home.asp?artId=779.
16. Beck K. Extreme Programming. (2002) - SP-b: Peter, s. 224. (In Russian).
17. IEEE 610.12-1990 Standard glossary of soft-ware engineering terminology, corrected edition – IEEE, 1991.
18. IEEE 1012-2004 Standard for verification and validation IEEE, 2005.
19. ISO/IEC 12207 Systems and software engi-neering – software life cycle processes – ISO, 2008.
20. Galatenko V.A. (2003). The basics of information security. - Moskva.: INTUIT, s. 208. (In Russian).
21. Lipaev V.V. (2004). Technological processes and standards for ensuring functional safety in the software life cycle // Jet Info. No. 3. s. 2-19. (In Russian).
22. Lipaev V.V. (2004). Functional Security Software // Jet Info. No. 8. s. 3-28. (In Russian).
23. Volobuev S.V. (2004). The safety philosophy of socio-technical systems: informational aspects. Moskva: University Book, s. 360. (In Russian).
24. Fagan M.E. (1976). Design and code inspections to reduce errors in program development IBM Systems Journal. N 3. – P. 182-211.
25. Konstantin L. (2004). Software Development - St. Petersburg: Peter, s. 592. (In Russian).
26. Anderson R. (2001). Security engineering: a guide to building dependable distributed systems. NY: John Wiley & Sons, s. 1040.

27. Dobrica L. (2002). A survey on software architecture analysis methods IEEE Transactions on software engineering. № 7. s. 638-653.
28. Lifar V. A. Safonova S. A., V. G. Ivanov (2015). Development of a method for optimizing repair and restoration work taking into account indicators Technological audit and production reserves. – No. 2/2 (22) – s. 11-17. (In Ukrainian).
29. Lifar V.O. (2017). Models, Methods and Information Technologies for Evaluating Technogenic Risics of Public Prospects: Dis. ... Dr. tech. Sciences: 05.13.06; [I will clean it up: The Chornomorsk National University of the Name of Peter Mogili]. – Mikolaev, s. 309.
30. Henley E.J., Kumamoto H. (1984). Reliability of technical systems and risk assessment:, s. 528.
31. S. Nair, R. Jetley, A. Nair, (2015). "A Static Code Analysis Tool for Control System Software", SANER, Montréal, Canada, s. 459-463.
32. F. Narisco, A.-R. Bolivar, F. Hidrobo, O. Gonzalez (2010). "A Syntactic Specification for the Programming Languages of the IEC 61131-3 Standard", Advances in Computational Intelligence, Man-Machine Systems and Cybernetics. s. 171-176.
33. Müller and M. I. Schwartzbach. (2018). "Static Program Analysis" Department of Computer Science Aarhus University, Denmark, s. 113. http://users-cs.au.dk/amoeller/spa/spa.pdf.

Стаття надійшла до редакції 11.07.2019.

МАТЕМАТИЧНІ ТА ІНФОРМАЦІЙНІ МОДЕЛІ В ЕКОНОМІЦІ

УДК 532.5; 519.63

https://orcid.org/0000-0003-3368-8203
https://orcid.org/0000-0002-9871-2748

Г.Г. БУЛАНЧУК, О.М. БУЛАНЧУК, А.О. ОСТАПЕНКО, Р.В. ЧАБАНУ

ТЕКСТУРНА АДВЕКЦІЯ ПРИ МОДЕЛЮВАННІ В'ЯЗКИХ ТЕЧІЙ МЕТОДОМ ҐРАТКОВИХ РІВНЯНЬ БОЛЬЦМАНА

Анотація. *Візуалізація векторного поля швидкостей є невід'ємною частиною багатьох задач чисельного моделювання. Традиційним є представлення результатів у вигляді стрілочних діаграм поля швидкостей або колірних діаграм модуля швидкості. Але така інформація зрозуміла лише фахівцям з гідромеханіки і не дає вичерпну картину течії в цілому. В даній роботі досліджується метод текстурної адвекції при моделюванні течій в'язкої рідини, який за інформативністю максимально наближений до натурного експерименту і дає змогу отримати детальну картину течії. Розроблений метод базується на комбінації ідей методу плямистого шуму та адвекції Лагранжа – Ейлера. Поле швидкостей обчислюється методом ґраткових рівнянь Больцмана.*

Ключові слова: *лінії течії, текстурна адвекція, система частинок, поле швидкостей, метод ґраткових рівнянь Больцмана.*

DOI: 10.35350/2409-8876-2019-16-3-49-56

Вступ

Результатами чисельного моделювання в гідромеханіці зазвичай є великі масиви векторних або скалярних полів. Етап візуалізації результатів, отриманих під час обчислювального експерименту, повинен надати досліднику вичерпну інформацію про структуру течії, швидкості й інші характеристики. Успішний результат експерименту залежить від того, в якому вигляді будуть отримані ці дані дослідником і які висновки він зробить, ґрунтуючись на них.

Вектор швидкості при візуалізації за допомогою стрілочних діаграм відображається у вигляді стрілки, напрямок і величина якої відповідають значенням поля в точці. Недоліком стрілочних діаграм є низька роздільна здатність при відображенні векторного поля. При візуалізації вихрових структур має місце перетин векторних символів, що призводить до зашумлення зображення і неможливості його інтерпретації.

Серед сучасних методів візуалізації особливе місце займають методи текстурної візуалізації, які відображають картину течії неперервною текстурою. За своїм відображенням методи текстурної візуалізації подібні нанесенню суміші масла та фарби на поверхню рідини у натурному експерименті. Дані методи є досить перспективними і актуальними, оскільки дозволяють бачити картину течії в цілому і ефективно проводити дослідження.

Однією з перших робіт в напрямку текстурної візуалізації була робота Jack van Wijk [1], в якій він запропонував метод плямистого шуму. Цей алгоритм створює зображення течії за допомогою суперпозиції окремих еліптичних плям, що позначають частинки, поміщені в потік. Напрямок руху плями в текстурі відповідає напрямку поля швидкостей в розглянутій локальній області.

Подальші роботи в області текстурної візуалізації привели до створення алгоритмів сімейства лінійної інтегральної згортки (Line Integral Convolution) [2, 3]. Основна ідея цього методу полягає в побудові інтенсивності зображення векторного поля як результату згортки спеціально підібраної функції-фільтра і білого шуму вздовж лінії течії. Цей метод набув широкого поширення в зв'язку з високою якістю одержуваного зображення. Однак, для того, щоб розрахувати інтенсивність пікселя в цьому методі, необхідно провести інтегрування уздовж всієї лінії течії, що проходить через дану точку. Це призводить до високої обчислювальної вартості візуалізації. Була розроблена модифікація цих методів [4], що базується на використанні значень інтенсивностей точок, розташованих в околі даної точки.

Одним з найважливіших етапів розвитку галузі наукової візуалізації, що дали початок багатьом методикам, стали методи адвекції початкового зображення вздовж лінії течії. Термін “адвекція” означає перенесення скалярного значення у векторному полі, при якому це значення не змінюється. Одним із базових методів є текстурна адвекція Лагранжа – Ейлера (LEA-Largangian-Eulcrian Advection). Ідея цього алгоритму полягає в спільному використанні лагранжевої і ейлерової кінематики руху суцільного середовища. Перенесення текстурного значення відбувається разом із рухом частинки, потім колір у даній точці набуває значення кольору цієї частинки. Щоб початкове зображення з часом не було винесене за межі області, що візуалізується, на кожному кроці по часу застосовується підмішування до проадвектованого зображення шумової структури. Таким чином, відбувається накладання цих двох зображень: адвектованого і шумового. Обчислений результат бере участь у наступній ітерації.

Більш детальний огляд методів текстурної візуалізації векторних полів можна знайти в роботі [5].

1. Постановка завдання

У даній роботі досліджується застосування методів текстурної візуалізації до плоских течій в’язкої рідини при чисельному моделюванні методом ґраткових рівнянь Больцмана. Використовується методика, що комбінує основні ідеї методу плямистого шуму та адвекції Лагранжа – Ейлера. Метою роботи є програмна реалізація методів текстурної візуалізації двовимірних течій при чисельному моделюванні методом ґраткових рівнянь Больцмана (LBM).

Ідея методу LBM аналогічна ідеї методу крупних частинок, розробленого Білоцерковським та Давидовим у 1965 році. Обчислювальна область розбивається нерухомою ейлеровою сіткою, комірки якої трактуються як крупні частинки. Однак за методом LBM динаміка таких частинок описується не рівняннями Ейлера або Нав'є – Стокса, а кінетичним рівнянням Больцмана. Характеристики крупних частинок є осередненими характеристиками всієї сукупності мікроскопічних частинок у цій комірці і описуються статистично за допомогою функції розподілу частинок за координатами та швидкостями. Тож динаміка крупних мезоскопічних частинок моделюється таким чином, щоб на макроскопічному рівні виконувалися рівняння Нав'є – Стокса з точністю до малих першого порядку. Більш детальний опис даного методу можна знайти, наприклад, у роботах [6, 7].

Оскільки метод ґраткових рівнянь Больцмана поєднує в собі два підходи: переміщення частинок і розрахунок гідродинамічних характеристик для кожної комірки, зокрема поля швидкостей, що є осередненням по всіх частинках, то в даний алгоритм органічно вписується метод текстурної адвекції, оскільки візуалізація течії теж відбувається у два етапи: переміщення частинок певного кольору і суперпозиція зображень.

Слід відмітити, що ідея побудови ліній течії, як сліду руху частинок по заданому полю швидкостей у спрощеному варіанті була вже реалізована в роботі [8] за допомогою маркерів. Однак у попередньому алгоритмі необхідно було задавати початкове положення маркерів на деяких фіксованих відрізках, що є не дуже зручним, оскільки наперед не відомо, де краще розставити дані відрізки. Колір всіх маркерів при цьому задавався однаковим і не змінювався.

Метою роботи було створення програмного забезпечення для текстурної візуалізації двовимірного векторного поля, обчисленого методом ґраткових рівнянь Больцмана на основі комбінації відомих алгоритмів текстурної візуалізації. Дана візуалізація течій повинна відбуватись на основі завантажених каталогів дискретних полів швидкостей та дозволяти досліджувати картини ліній течії в динаміці. Також вона повинна бути придатною для візуалізації векторних полів, обчислених будь-яким іншим методом.

2. Алгоритм методу

При моделюванні методом ґраткових рівнянь Больцмана на виході ми маємо в кожен момент часу поле швидкостей, обчислене на рівномірній сітці, що покриває розрахункову область. Ідея методу візуалізації, що пропонується в даній роботі, полягає в наступному:

1. Завантажуємо поле швидкостей для деякого фіксованого моменту часу.
2. Генеруємо певну кількість рівномірно розподілених частинок у розрахунковій області незалежно від сітки. Кожна з цих частинок наділена яскравістю (для монохромного зображення) або кольором, що генерується випадковим чином. Яскравість або колір комірки відповідає кольору частинки, яка попала в дану комірку. Комірки, в які не попала частинка, зафарбовуються в чорний колір. Таким чином, на початковому етапі маємо зображення типу «білий шум».

3. Пересуваємо ці частинки по простору зі своїм кольором зі швидкістю, що відповідає полю швидкостей на один крок $\Delta\tau$. Отримуємо нове зображення. Якщо в комірку в результаті такого пересуву не зайшла ніяка частинка, то залишається колір, який був на попередньому кроці. Таких кроків робимо достатню кількість (чим більше, тим краще). Рух таких частинок, що мають певний колір, через певну кількість кроків по простору залишить за собою слід у вигляді ліній течії. Зауважимо, що крок $\Delta\tau$, з яким ми рухаємо частинки, не є тим кроком по часу, з яким проведені розрахунки. Це деякий умовний крок, з яким ми рухаємо частинки по полю швидкостей у фіксований момент часу t.
4. Підсумкове зображення формується як суперпозиція всіх попередніх зображень. Фактично, комірка зафарбовується в колір частинки, яка на останньому кроці зайшла в неї. Якщо не зайшла ніяка частинка – то в колір частинки, яка зайшла на попередньому кроці і т.д. У результаті ми будемо мати лінії течії в кожен момент часу.

Було розглянуто вплив параметрів методу на якість текстурного зображення та швидкість його отримання: кількості частинок, що генеруються, кількості зображень, що накладаються (фреймів), величини кроку $\Delta\tau$ та розміру комірок розрахункової сітки.

3. Результати моделювання

На рис. 1 зображено лінії течії в квадратній каверні з рухомою верхньою кришкою при числі Рейнольдса $\mathrm{Re} = 100$ із крупною сіткою 100×100 (10000 комірок). Картина побудована по полю швидкостей, яке було отримане методом ґраткових рівнянь Больцмана. Було згенеровано $n = 10000$ частинок.

Зроблено 1000 кроків при переміщенні частинок, таким чином фінальна картинка є суперпозицією $n_s = 1000$ зображень. Як бачимо, зображення не досить чітке і структура течії проглядається слабо.

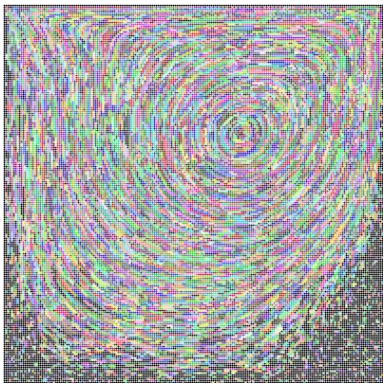

Рисунок 1 – Структура течії в квадратній каверні (число Рейнольдса Re = 100, крок зміщення по простору $\Delta\tau = 0.1$, сітка 100×100, кількість зображень для суперпозиції $n_s = 1000$)

Аналогічну картину ми бачимо при обтіканні циліндра в прямокутній області. На рис. 2 зображено картину течії при числі Рейнольдса Re = 500 і сітці 100×300, кількості зображень для суперпозиції n_s = 1000 і кількості згенерованих частинок n = 10000.

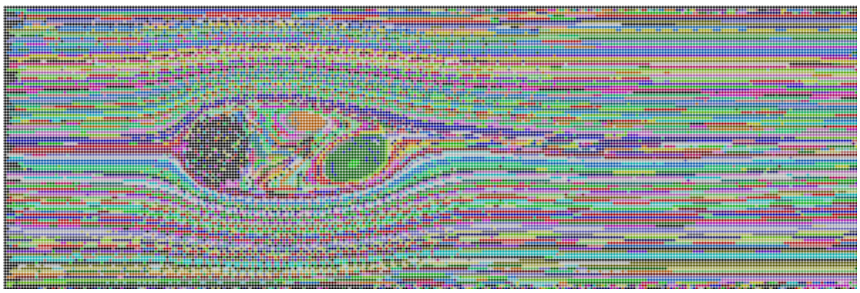

Рисунок 2 – Картина течії при обтіканні круглого циліндра (Re = 500, сітка 100×300**,** кількість зображень для суперпозиції n_s = 1000, крок зміщення по простору $\Delta\tau$ = 0.1)

Ситуація покращується при подрібненні сітки. На рис. 3 зображена картина ліній течії при обтіканні циліндра при числі Рейнольдса Re = 1000 і сітці 400×1200. Як бачимо, зернистість при таких параметрах ще зберігається, хоча структура течії вже достатньо чітка. Кількість зображень для суперпозиції n_s, крок зміщення $\Delta\tau$ = 0.1 і кількість згенерованих частинок n при цьому не змінились.

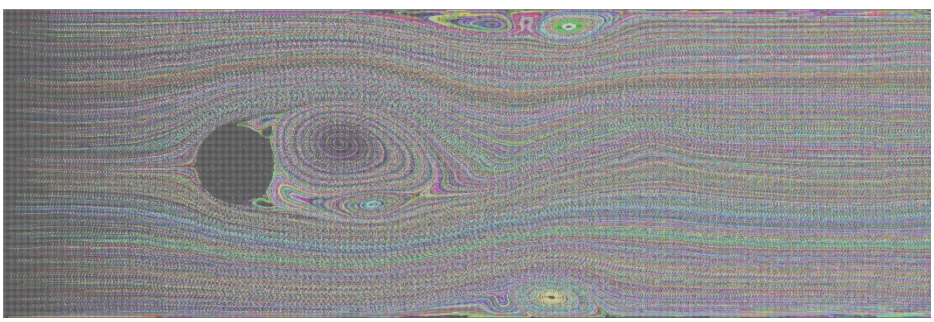

Рисунок 3 – Картина течії при обтіканні круглого циліндра з параметрами: Re = 1000, сітка 400×1200, кількість зображень для суперпозиції n_s = 1000, крок зміщення по простору $\Delta\tau$ = 0.1

Зі збільшенням кількості зображень, суперпозиція яких формує фінальне зображення, а також зі зменшенням кроку зміщення по простору, зображення стає більш чітким і гладким і зернистість практично зникає. На рис. 4 зображена картина течії за круглим циліндром у прямокутному каналі з параметрами Re = 1000, сітка 400×1200**,** кількість зображень для суперпозиції n_s = 4000, крок зміщення по простору $\Delta\tau$ = 0.01. Картина течії представлена для моменту часу t = 30. Час візуалізації для даного моменту часу при таких параметрах становить приблизно 2 хв.

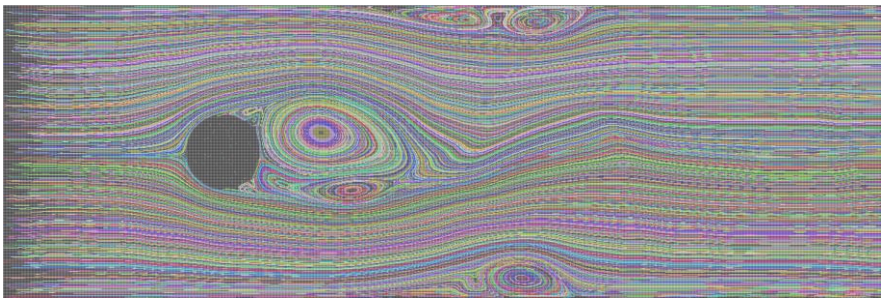

Рисунок 4 – Картина течії при обтіканні круглого циліндра з параметрами: Re = 1000, сітка 400×1200, кількість зображень для суперпозиції n_s = 1000, крок зміщення по простору $\Delta\tau$ = 0.01

Як показують дослідження, недоцільно генерувати велику кількість частинок при моделюванні з грубою сіткою. Верхнє зображення на рис. 5, виконане при генерації n = 600 частинок, краще передає структуру течії, ніж нижнє зображення, де згенеровано n = 1000 частинок.

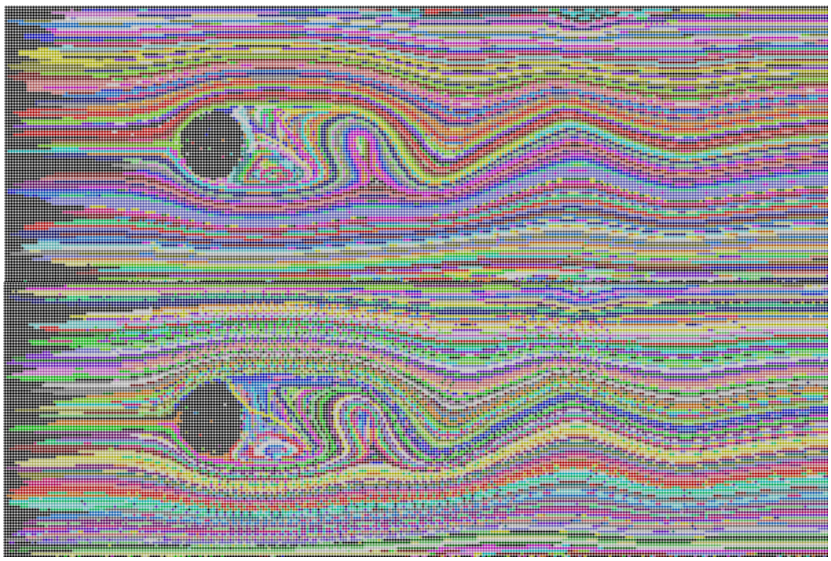

Рисунок 5 – Картина течії за циліндром з параметрами: Re = 500, сітка 100×300, кількість зображень для суперпозиції n_s = 1000, крок зміщення по простору $\Delta\tau$ = 0.01

Висновки

Дослідження вказують на те, що кількість частинок, які треба згенерувати, повинна бути тісно пов’язана з кількістю комірок розрахункової сітки. На грубій сітці кількість комірок не може бути досить великою, не більше ніж приблизно третина від кількості комірок. У той же час, при розрахунках з дрібною сіткою, кількість частинок не повинна бути занадто малою, принаймні не менше, ніж приблизно десята частина від кількості комірок.

Встановлено, що для отримання чіткого та якісного зображення необхідно збільшити кількість зображень для суперпозиції, зменшити крок $\Delta\tau$, з яким частинки рухаються по простору, а також збільшити кількість комірок розрахункової сітки. Слід враховувати, що все це призведе до збільшення часу отримання зображення. У подальшому планується провести розпаралелювання обчислень, щоб мати змогу отримати картину течії в реальному часі.

СПИСОК ЛІТЕРАТУРИ

1. Wijk J.J. Spot noise: Texture synthesis for data visualization // Computer Graphics 25 (4). – 1991. – P. 309-318.
2. Cabral B., Leedom L. C. Imaging vector fields using line integral convolution // In Proceeding of ACM SIGGRAPH 93, Computer Graphics Proceedings, Annual Conference.– 1993. – ACM., vol. 4. – P. 263-272.
3. D. Stalling LIC on Surfaces. In Texture synthesis with Line Integrak Convolution. ACM SIGGRAPH 97, International Conference on Computer Graphics and Interactive Techniques. – 1997. – P. 51-64.
4. D. Stalling, Hege H. C. Fast and Resolution independent line integral convolution. – 1995. – P. 249-256.
5. Потий О. А. Текстурная визуализация векторных полей с использованием возможностей графического оборудования: [Электронный ресурс]: Дис. канд. техн. наук:05.13.11. – Ростов н/Д: РГБ,2005.
6. Остапенко А. А. Исследование влияния переменной скорости звука в ячейке при моделировании течения в плоском канале и обтекания кругового цилиндра потоком вязкой жидкости при расчете методом решеточных уравнений Больцмана / А. А. Остапенко, О. Н. Буланчук, Г. Г. Буланчук // Вестник Черкасского университета. – 2016. – № 1. – С. 50-64.
7. Bulanchuk G. Investigation of the influence of the relaxation parameter on the viscous fluid flow over circular cylinder modeling process with the lattice Boltzmann method / G. Bulanchuk, A. Ostapenko // Bulletin of V. Karazin Kharkiv National University. Series «Mathematical Modeling. Information Technology. Automated Control Systems». – 2017. – Vol. 33. – P. 52-61.
8. Буланчук О. Н. Программа построения линий тока по дискретному полю скоростей / О. Н. Буланчук, Г. Г. Буланчук // Вестник Харьковского национального университета. Серия: Математическое моделирование. Информационные технологи. Автоматизированные системы управления. – 2013. – Т. 22. – С. 45-50.

REFERENCES

1. Wijk J.J. (1991) Spot noise: Texture synthesis for data visualization. Computer Graphics. 25 (4). 309-318.
2. Cabral B., Leedom L. C. (1993) Imaging vector fields using line integral convolution. In Proceeding of ACM SIGGRAPH 93, Computer Graphics Proceedings, Annual Conference. Vol. 4. 263-272.
3. Stalling D. (1997) LIC on Surfaces. In Texture synthesis with Line Integrak Convolution. ACM SIGGRAPH 97, International Conference on Computer Graphics and Interactive Techniques. 51-64.
4. Stalling D., Hege H. C. (1995) Fast and Resolution independent line integral convolution. 249-256.

5. Potii O. A. (2005) Teckstурnaya vizualizatcia vectornuh poley s ispolzovaniem vozmoshnostey graphicheskogo oborudovania [Textural visualization of vector fields using the capabilities of graphic equipment]. PhD Thesis. Rostov (in Rus)
6. Ostapenko A. A. (2016) Issledovaniye vliyaniya peremennoy skorosti zvuka v yacheyke pri modelirovanii techeniya v ploskom kanale i obtekaniya krugovogo tsilindra potokom vyazkoy zhidkosti pri raschete metodom reshetochnykh uravneniy Bol'tsmana [Investigation of the effect of variable velocity of sound in a cell in the simulation of a flow in a flat channel and the flow of a circular cylinder by a flow of viscous fluid when calculated by the method of lattice Boltzmann equations] Bulletin of Cherkasy University. No. 1. 50-64. (in Rus)
7. Bulanchuk G. (2017) Investigation of the influence of the relaxation parameter on the viscous fluid flow over circular cylinder modeling process with the lattice Boltzmann method. Bulletin of V. Karazin Kharkiv National University. Series «Mathematical Modeling. Information Technology. Automated Control Systems». Vol. 33. 52-61.
8. Bulanchuk O. N. (2013) Programma postroyeniya liniy toka po diskretnom polyu skorostey [The program of construction of streamlines on a discrete velocity field]. Vol. 22. 45-50. (in Rus)

Стаття надійшла до редакції 10.06.2019.

UDC 519.866

https://orcid.org/0000–0003–1031–7207
https://orcid.org/0000–0003–1674–9828
https://orcid.org/0000–0003–0402–6040
https://orcid.org/0000–0002–5156–2199

A. OLIYNYK, G. GRYGORCHUK, B. NEZAMAY, L. FESHANYCH

USAGE OF THE APPARATUS OF ORDINARY DIFFERENTIAL EQUATIONS IN MODELLING OF ECONOMIC AND ENVIRONMENTAL SYSTEMS

Abstract. *The ordinary differential equations techniques applying to investigate the economical and ecological systems has been considered in presented article. The interconnected economical complexes development for the countries with the different economical potential has been simulated. The population economical activity influence on the environment pollution and the state of region's flora has been investigated. The economical efficiency of the new technical diagnostics implementation has been studied. The methods of presented models realization has been presented and investigated, the results of tested calculations have been presented and one's analysis has been given. The directions of future investigations have been determined.*

Keywords: *differential equation, mathematical modeling method, modeling, diagnostics.*

DOI: 10.35350/2409-8876-2019-16-3-57-66

Introduction

The modeling of economic and environmental systems is performed with the use of linear and nonlinear systems of ordinary differential equations apparatus. As a basic, the development of which can be interpreted below, would be a model "predator – victim", created in 1925 by Alfred Lotka and Vito Volterra [2]. The basic equation system of this model is written as:

$$\begin{cases} \dfrac{dx}{dt} = k_1 x(t) - g_1 x(t) y(t) \\ \dfrac{dy}{dt} = -k_2 y(t) + g_2 x(t) y(t) \end{cases}. \qquad (1)$$

There $x(t)$ – the count of victim's population, $y(t)$ – the count of predator's population, $k_i, g_i, i = 1,2$ – the model's coefficients, detailed content of which is given in [2]. Models of economic systems of different nature are considered in [1, 4–9, 11–13]. The offered research touches a construction and research of three models of economic and economically – ecological systems, and also them practical realization and researching.

1. Model problems formulation

In predicting the development of interconnected economies, the question arises whether economies with relatively low levels of development may not suffer significant economic losses at a time when the world's leading economies are suffering losses as a result of the economic crisis. The methods of mathematical design are used for research of the indicated question with the use of the systems as a "predator – victim", that allows to build mathematical models and define their descriptions that would allow to answer theset questions. The task is reduced to solution ' Liabilities system of differential equations of the form:

$$\begin{cases} \frac{dx_1}{dt} = A_1 x_1 (A_2 - x_1) - A_3 x_1 x_2 + A_4 x_1 x_3 \\ \frac{dx_2}{dt} = A_5 x_2 (A_6 - x_2) - A_7 x_1 x_2 + A_8 x_1 x_3 \\ \frac{dx_3}{dt} = A_9 x_3 (A_{10} - x_3) + A_{11} x_1 x_3 + A_4 x_1 x_2 \end{cases}, \tag{2}$$

there x_1 and x_2 – economically strong countries, x_3 a country with a low level of economy with appropriate initial conditions $x_1(0) = x_{10}$; $x_2(0) = x_{20}$; $x_3(0) = x_{30}$. The coefficients A_i could be present as a time function $A_i = A_i(t)$.

Another model is related to a system described by three differential equations for functions: *x(t)* – population in the region; *y(t)* – the level of pollution and other non–harmful effects on the environment caused by the economic activity of the population; *z(t)* – the level of flora of the region (trees, agricultural products, forests, gardens, etc.), however, the equation system looks like:

$$\begin{cases} \frac{dx}{dt} = Ax - By + Cz \\ \frac{dy}{dt} = Dx - Ez \\ \frac{dz}{dt} = Hx - Gy + Fz \end{cases}. \tag{3}$$

Initial conditions must be specified for the correct formulation of the modeling task:

$$\begin{cases} X(0) = X_0 \\ Y(0) = Y_0 \\ Z(0) = Z_0 \end{cases}. \tag{4}$$

The third model describes a situation for which the functions *x(t)*, *y(t)*; *z(t)* are introduced with the following meaning: *x(t)* – costs for implementation of new technical diagnostics and control standards; *y(t)* – costs for elimination of emergencies consequences; *z(t)* is the efficiency of the studied industrial system's element. When a mathematical model is constructed, a differential equation system that describes how to modify the corresponding variables per unit of time in

assuming the nature of the relationship between the quantities is recorded. As a result, the following system of ordinary differential equations that binds the variables *x(t)*; *y(t)*; *z(t)* is obtained:

$$\begin{cases} \dfrac{dx}{dt} = K_1 x(A-x) - K_2 y + K_3 z \\ \dfrac{dy}{dt} = K_4 x(A-x) + K_5 y(B-y) + K_6 z \\ \dfrac{dz}{dt} = K_7 x - K_8 y \end{cases}, \qquad (5)$$

with appropriate initial conditions.

Systems of type (2) – (5) are a certain extension of the known predator–prey model. The algorithms for finding the coefficients of systems (2) and (3) by the method of expert estimation are proposed, and in the modeling of system (2) additional conditions for its coefficients in terms of obtaining asymptotically stable solutions are established.. Introducing nonlinear components into systems (2), (3), and (5) allows us to obtain solutions that more accurately reflect the essence of the phenomena and processes being modeled. In the implementation of the mentioned models, the following approach was used: in the first step, all the mentioned models were selected as linear, suitable calculations and analysis of the obtained results were carried out.. If there were doubts about the correspondence of these results to the characteristics of real systems, then new nonlinear terms describing the level of interaction of the relevant factors were introduced into the respective systems. If the qualitative behavior of the solutions satisfied the researcher, then methods of practical evaluation of the coefficients of the systems based on the results of their statistical studies, real data on the characteristics of their functioning were created. When model solutions, that meet certain economic requirements and environmental standards, are obtained, recommendations to optimize the systems under consideration by the necessary criteria, which are responsible for the stable operation of the respective systems with the fulfillment of their functions. All models are brought to numerical realization in the form of software complexes by Runge-Kutta methods [3], it allows to carry out a wide class of calculations in order to estimate the dynamics of the process development depending on the suitable coefficients of the model.

Special kind of models is the simulation of an advertising campaign for goods and services is an important element in ensuring that they hit the market. Often, advertising is carried out haphazardly or using certain empirical methods, which can have the opposite effect when product advertising begins to act as a counter–advertisement. At the same time, mathematical methods, in particular, the apparatus of ordinary differential equations, to build a model of an advertising campaign are promising for studying the features of the advertising process.

The advertising model is based on the following assumptions. It is believed that $\dfrac{dN(t)}{dt}$ – the rate of change in the number of consumers who know about the product and are ready to buy it ($N(t)$– the number of informed customers), function $\alpha_1(t)\cdot(N_0 - N(t))$ – characterizes the intensity of the advertising company, $\alpha_1(t) > 0$ characterizes the cost of advertising, N_0 – the total number of

potential buyers. It is also believed that people who know about the product, in one way or another, disseminate information about the product to customers who do not know about it (potential customers). This contribution is characterized by an addition $\alpha_2(t)\cdot N(t)\cdot(N_0 - N(t))$. The value $\alpha_2(t)$ characterizes the degree of communication of clients with potential clients.

Based on the made assumptions made, the equation [1] is obtained:

$$\frac{dN(t)}{dt} = [\alpha_1(t) + \alpha_2(t)N(t)](N_0 - N(t)) \tag{6}$$

with initial condition $N(0) = N_1$, $N_1 < N_0$. If $\alpha_1(t) >> \alpha_2(t)$, the next equation can be received (matches classic advertising campaigns):

$$\frac{dN(t)}{dt} = \alpha(t)N(t). \tag{7}$$

Otherwise, it is possible to receive the equation that describes the so-called "network marketing":

$$\begin{aligned} &\frac{dN(t)}{d\tau} = N(t)(N_0 - N(t)), \\ &d\tau = \alpha_2(t)dt. \end{aligned} \tag{8}$$

Obviously, equations (7) and (8) are squared:

$$N(t) = \frac{N_0 e^{N0t}}{1 + e^{N0t}}, \tag{9}$$

In this case, the number of informed consumers if $t \to \infty$ remains constant:

$$\lim_{t\to\infty} N = \lim_{t\to\infty} \frac{N_0 e^{N0t}}{1 + e^{N0t}} = N_0 \tag{10}$$

and is equal to the number of potential customers.

When the value $[\alpha_1(t) + \alpha_2(t)N(t)]$ becomes negative ($\alpha_2(t) < 0$ – negative evaluation of consumers of the quality of the goods) – manufacturers should further analyze and evaluate the possibilities of direct advertising in the promotion of products in the market.

Depending on the values $\alpha_1(t)$, $\alpha_2(t)$ and $N(t)$, product promotion activities can be aimed at improving the results of both direct advertising ($\alpha_1(t)$) and promoting indirect advertising ($\alpha_2(t)$).

If $N << N_0$ (a little-known product), and as a result, $\alpha_2(t)\cdot N << \alpha_1(t)$, then the equation (6) comes to view $\frac{dN(t)}{dt} = \alpha_1(t)N_0$ and has the solution

$$N = N_0 \int_0^t \alpha_1(t)dt\,. \tag{11}$$

As for (8), the solution (6) with conditions $\alpha_1(t) = \alpha_1$ і $\alpha_2(t) = \alpha_2$

$$N(t) = \frac{N_0 e^{(N_0\alpha_2+\alpha_1)} - N_0 \cdot \frac{\alpha_1}{\alpha_2}}{1+e^{(N_0\alpha_2+\alpha_1)}} \tag{12}$$

And, based on (10):

$$\lim_{t\to\infty} N = N_0\,. \tag{13}$$

Thus, the solution (1) is stable, which substantiates the correctness of the proposed models.

In the general case, integration (6) is performed using numerical methods [3] – for example, fourth-order Runge-Kutta methods. The order of precision of a method is made on the basis of solving model equations.

Based on the proposed model, the following tasks are solved:

– the task of estimating the profit of an advertising company,

– the dependence of the number of potential clients on the methods and intensity of the advertising campaign is investigated.

Methods for determining or selecting $\alpha_1(t)$, $\alpha_2(t)$ based on data on a planned (or ongoing) advertising campaign, have been developed to evaluate its effectiveness. The areas of further research may be related to the processing of statistics on various advertising campaigns, their effectiveness, duration over time in order to restore the analytical structure of the features introduced, and the possible correction of the model (1).

2. Analysis of the obtained results

In the implementation of model (2) the values of coefficients at which periodic crisis manifestations of countries with higher levels of economic development (series 1, 2 in Figure 1) do not affect the level of economy of a country with relatively weaker economic indicators (row 3) were established.

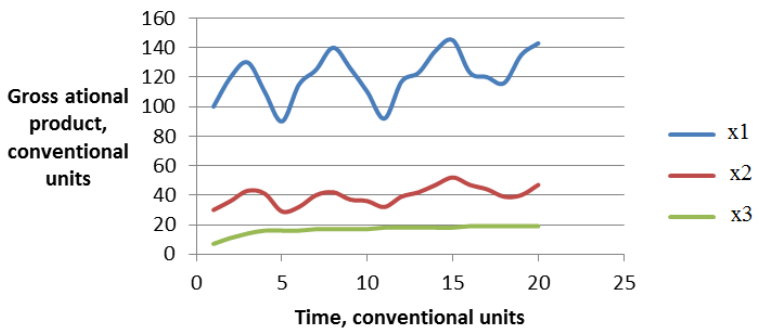

Figure 1 – Countries economics indicators dynamics

Implementation of the model (3), (4) allows you to set these coefficients, in which the stability of solutions with the desired asymptotic values (Figure 2) is provided.

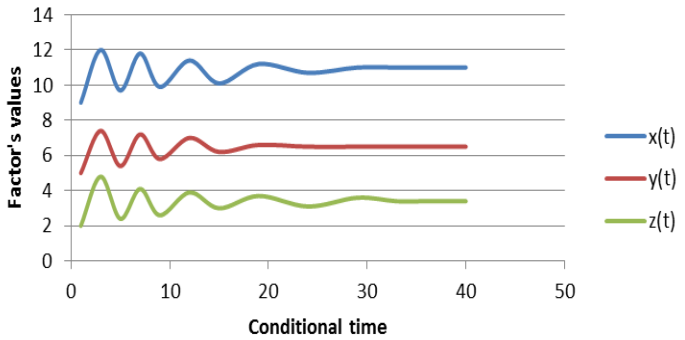

Figure 2 – The change of economic and ecological system indicators dynamics

The implementation of model (5) allows us to set the values of coefficients in which the stability of the solutions with the desired asymptotic values of the indicators and the dynamics of their change over time is ensured (figure 3):

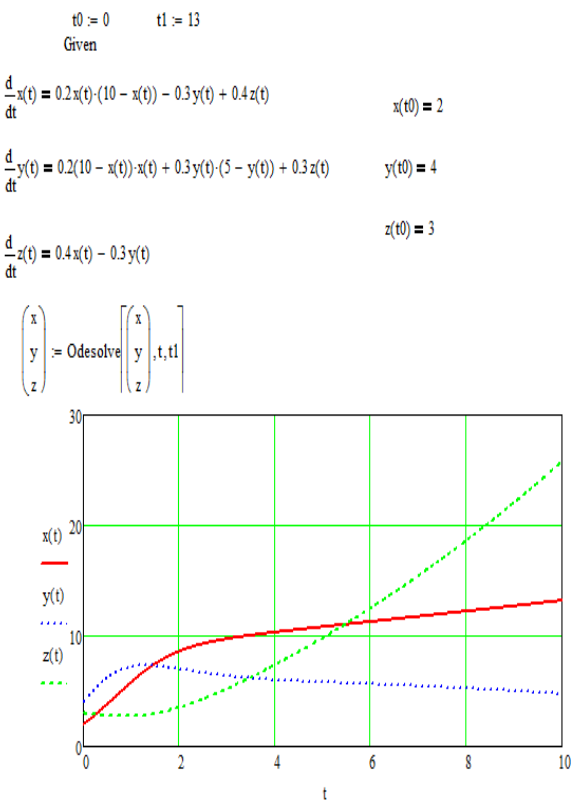

Figure 3 – The change of cost indicators for standards of technical diagnostics implementation, for elimination of emergencies consequences and efficiency of gas transmission system's work

The results of advertising campaign intensity model calculations are presented in Figure 4. The results of the calculations can determine the time at which the advertising campaign can be rolled – further investment has no proper effect.

Advertising campaign intesity

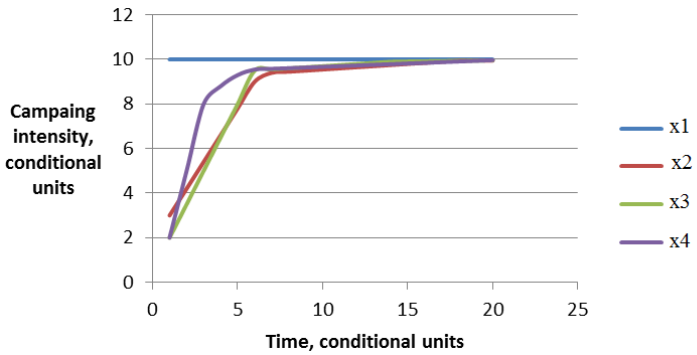

Figure 4 – The results of advertising campaign intensity model calculations

The conducted researches testify high efficiency of economic systems mathematical modeling method for their study, description and optimization. In fact, the modeling problem is divided into two stages – at the first, the relationships between its elements are studied in order to obtain qualitative indicators that adequately reflect its behavior, and the second, in fact, the inverse problem of selecting of the model coefficients that allow to determine the quantitative indices of the simulated systems is solved. The areas of further research are related to the adaptation of the developed models to real economic systems.

In particular, for the model of interconnected economies it is necessary to establish coefficients that quantitatively characterize the level of interconnection between each pair of economic complexes, and in the first stage of modeling these coefficients are normalized, their numerical values are chosen at the interval (0; 1) and are determined by the method of expert estimates, however in the analysis of real economic systems, it is necessary to switch to the dimensional values of these coefficients, which requires the interconnected efforts of specialists in the fields of economics and applied mathematics.

For the second model, which describes the functions $x(t)$ – population in the region; $y(t)$ – the level of pollution and other non–harmful effects on the environment caused by the economic activity of the population; $z(t)$ – the level of flora of the region (trees, agricultural products, forests, gardens, etc.) to determine the model coefficients it is necessary to take into account the peculiarities of each of the studied regions – it should be noted that the values of the coefficients will depend on the characteristics of the studied region – the coefficients for the industrial regions will differ from the coefficients determined for the Carpathian or Bukovina region. It is also advisable to use the method of expert estimation for model calculations, having in mind again the scaling of coefficients by the interval (0; 1).

To practical realization the third model with investigated functions $x(t)$ – costs for implementation of new technical diagnostics and control standards; $y(t)$ – costs for elimination of emergencies consequences; $z(t)$ is the efficiency of the studied

industrial system's element in determining the model values of the system coefficients by the method of expert assessments, an important point is the selection of experts who should be specialists in the operation and evaluation of the technical condition of the systems under study and on economic issues to find the best ways to distribute investments. At the same time, it is important to ensure the objectivity of expert assessments – the opinion of experts on only one issue should not prevail.

For the practical implementation of the proposed model of the advertising company it is necessary to take into account the fact that only in this model its coefficients are functions of time. This necessitates the need for a wide-ranging survey of advertising campaigns for different types of advertising items – although widely used consumer electronics campaigns, the number of such campaigns provides a great deal of material for determining the appropriate features – model equation coefficients, based on analysis of relevant statistics.

The peculiarity of each of the proposed models is the fact that they are most effective in predicting the behavior of the simulated systems, since the construction of sufficiently accurate forecasts allows you to solve the following problems:

– forecasting the development of interdependent economies based on the study of economic trends characteristic of previous periods;

– forecasting of economic and ecological characteristics of regions taking into account their peculiarities:

– predicting the technical and economic efficiency of implementing new diagnostic systems and the effectiveness of advertising campaigns.

Conclusions

1. The technique of ordinary differential equations can be successfully applied to the simulation of the interconnected economies development, to estimation the change of economic and ecological system indicators dynamics and the change of cost indicators for standards of technical diagnostics implementation, for elimination of emergencies consequences and efficiency of gas transmission system's work and to predictions the advertising campaign efficiency.

2. All this models can be realized using the simple linear and quadratic type relationships, which, however, allow to receive the numerical results that are sufficiently accurate in terms of practical needs.

3. Construction and implementation of models 1 – 3 is carried out in two stages – the first of them is a simulation of the desired behavior of the system (prediction) b and in the second – the model is corrected by developing a methodology for determining its coefficients (correction).

4. Model 4 uses only one differential equation, which in most cases can be solved analytically. The obtained solutions are stable, which is a confirmation of the correctness of the proposed models.

5. The above four models do not exhaust the entire class of problems of modeling environmental, economic and other types of systems – for the scope of this work, the results of the authors' work on modeling systems in medicine, as well as models of dimensions above three are presented. However, these models have been successfully used in the approaches presented in the presented work.

REFERENCES

1. Samarskiy, A. A., Mikhailov, A. P. (2005). Matematicheskoe modelirovanie [Mathematical modelling]. M.: Fizmatlit. 285–300. (In Russian).
2. Volterra, V. (1976). Matematicheskaya teoriya borby za suschestvovanie [Mathematical theory of fight for existence]. Moscow – Izhevsk: Institut kompyuternyih issledovaniy, 2004, 24–158. (In Russian).
3. Samarskiy, A. A., Gulin, A. V. (1982). Vvedenie v tsifrovyie metody [Introduction into digital methods]. M.: Nedra. 43–272. (In Russian).
4. Golovatyy, Yu. D., Kyrlych, V.M., Lavreniuk, S.P. (2011). Dyferentsialni rivnianni [Differential equations]. Lviv: LNU im.Ivana Franka. 140–198. (In Ukrainian).
5. Oborskyy, G. A., Dashchenko, A. F., Usov, A. V., Dmytryshyn, D. V. (2013). Modeliuvannia system [Systems modelling]. Odessa: Astroprynt. 280–368. (In Ukrainian).
6. Dubovoy V. M., R. N. Kcietnyy, O. I. Mykhalov, A. V. Usov. (2011). Modeliuvannia ta optymizatsiia system [Modelling and system optimization], Vinnytsia: PP «TD Edelveis». 804 s. (In Ukrainian).
7. Gonchar, N. S., Zhokhin, A. S., Kozinski, W. H. (2015). General Equilibrum and Recession Phenomenon. American Journal of Economics, Finance and Management. no 1. 559–73.
8. Makhort, A. P. (2016). About algorithms for determining the equilibrium states of an open economic system in the presence of monopolists. Systems Research and Information Technology. №4. 95–107.
9. Kompiuterne modeliuvannia system ta protsesiv. Metody obchyslen. (2012). [Computer simulation of systems and processes. Methods of calculation]. Pid red. Kvietnyy R. N. Vinnytsia, VNTU. Vol.1. 196 s. Vol.2. 230 s. (In Ukrainian).
10. Dudin, M. N., Lyasnikov, N. V. (2012). Foresight as a Tool to Provide Strategic Stability of Manufacturing, Business, European Research. Vol.26. №8. 1138–1141.
11. Fedotova, I. V. (2012). Determining the level of strategic stability for ATP functioning. Economics of a transport complex. Issue. 120. 90–102.
12. Makoni, S. V., Khodakovskyy, V. A. (2011). Osnovyi sistemnogo analiza. [System Analysis Basics] SPb: Peterb gos. Un-t putey soobscheniya. 143 s. (In Russian).
13. Busniuk, N. N., Cherniak, A. A. (2014). Matematicheskoe modelirovanie [Mathematical modelling]. Minsk: Belorussia, 214 s. (In Russian).

СПИСОК ЛІТЕРАТУРИ

1. Самарский А. А., Михайлов А. П. Математическое моделирование. М. Физматлит, 2005. 320 с.
2. Вольтерра В. Математическая теория борьбы за существование. Москва, Ижевск: Институт компьютерных исследований, 2004. 288 с.
3. Самарский А. А., Гулин А. В. Введение в численные методы. М.: Недра, 1982. 272 с.
4. Головатий Ю.Д., Кирлич В.М., Лавренюк С.П. Диференціальні рівняння. Львів: ЛНУ ім.Івана Франка, 2011. 470 с.
5. Оборський Г.А., Дащенко А.Ф., Усов А.В., Дмитришин Д.В. Моделювання систем: монографія. Одеса: Астропринт, 2013. 664 с.
6. Дубовой В.М., Квєтний Р.Н., Михальов О.І., Усов А.В. Моделювання та оптимізація систем. Вінниця: ПП «ТД Едельвейс», 2011. 804 с.
7. Gonchar N.S. Zhokhin A.S., Kozinski W.H. General Equilibrum and Recession Phenomenon. American Journal of Economics, Finance and Management, 2015. P. 559-573.
8. Махорт А.П. Про алгоритми визначення станів рівноваги відкритої економічної системи за наявності монополістів. Системні дослідження та інформаційні технології, 2016. №4. С. 95–107.

9. Комп’ютерне моделювання систем та процесів. Методи обчислень. Під ред. Квєтного Р.Н. Вінниця: ВНТУ, 2012. Ч.1. 196 с., Ч.2. 230 с.
10. Dudin M.N., Lyasnikov N.V. Foresight as a Tool to Provide Strategic Stability of Manufacturing, Business. European Research, 2012. Vol.26. №8. P. 1138–1141.
11. Федотова І.В. Визначення рівня стратегічної стійкості функціонування АТП. Економіка транспортного комплексу, 2012. №. 120, С. 90–102.
12. Макони С.В., Ходаковский В.А. Основы системного анализа. СПб: Петерб гос. Ун-т путей сообщения, 2011. 143 с.
13. Буснюк Н.Н., Черняк А.А. Математическое моделирование. Минск: Беларусь, 2014. 214 с.

Стаття надійшла до редакції 24.07.2019.

УДК 621.391 http://orcid.org/0000-0002-9993-2427

Б.В. ГОРЛИНСЬКИЙ

ОБЧИСЛЮВАЛЬНИЙ МЕТОД НЕЧІТКОГО ДЕКОДУВАННЯ БАГАТОКОМПОНЕНТНИХ ТУРБО КОДІВ В БЕЗПРОВОДОВИХ ЗАСОБАХ ПЕРЕДАЧІ ДАНИХ

Анотація. *Запропоновано обчислювальний метод нечіткого декодування багатокомпонентних турбо кодів в безпроводових засобах передачі даних для підвищення ефективності математичної моделі системи забезпечення достовірності інформації на основі адаптації кодових конструкцій.*

Ключові слова: *безпроводові засоби передачі даних, адаптивне кодування, турбо коди, алгоритми декодування.*

DOI: 10.35350/2409-8876-2019-16-3-67-81

Вступ

Аналіз принципів побудови безпроводових засобів передачі даних (БЗПД) свідчить про те, що в цих засобах радіозв'язку на фізичному рівні планується в якості модуляції сигналу застосовувати адаптивні спектрально-ефективні види модуляції, такі як ФМ-М та КАМ-М, адаптивні коригувальні коди – турбо коди (ТК), ортогонально-частотне розділення каналів OFDMA (Orthogonal Frequency-Division Multiple Access**)** та технології просторової обробки сигналів MIMO (Multiple-input multiple-output) [1-4].

Крім того, перспективні засоби радіозв'язку будуть створюватися з використанням програмно-апаратного принципу. Ці програмовані радіозасоби названі SDR (software defined radio) та розробляються по програмі JTRS (Joint Tactical Radio System). Одним з режимів роботи цих програмованих радіостанцій є режим протидії навмисним завадам. При цьому використовується розширення спектру методом псевдовипадкової перестройки робочої частоти (ППРЧ).

1. Сучасні методи забезпечення достовірності інформації в БЗПД

Відомо декілька підходів до забезпечення достовірності інформації в БЗПД з використанням турбо кодів (ТК).

Підходи [5-7] полягають в оптимізації перемежувача в структурі ТК. У цьому випадку енергетичний виграш відбувається при відношенні сигнал-завада в області "порога помилок" ТК.

Інший підхід [8] полягає в застосуванні додаткових бітів по завершенню кодування блоку даних з метою примусового переведення решітчастої діаграми рекурсивного систематичного згорточного коду (РСЗК) ТК у початковий стан. При цьому забезпечується енергетичний виграш в 0,1-0,3 дБ.

Відомий метод [9] враховує інформацію про стан каналу зв'язку при декодуванні ТК. Енергетичний виграш при цьому складає 0,1-0,2 дБ.

В роботі [9] запропонований підхід забезпечення достовірності інформації в засобах радіозв'язку (ЗРЗ), який заснований на тому, що інформаційні блоки після декодеру ТК, які мають помилки, можуть бути виявлені та відібрані. Енергетичний виграш складає при цьому від 0,25 дБ до 0,9 дБ для різних ймовірностей бітової помилки декодування при впливі різних навмисних завад.

В підході [10] для забезпечення достовірності інформації вирішено застосовувати адаптацію.

2. Загальна постановка задачі, об'єкт, предмет та мета досліджень

Забезпечити достовірність інформації в БЗПД можна шляхом використання багатокомпонентних ТК. В БЗПД з ТК принцип використання багатокомпонентних ТК досі не був розглянутий, тому що використання багатокомпонентних ТК вимагає затримки при обробці прийнятих інформаційних блоків, однак у зв'язку з останніми досягненнями в галузі мікропроцесорної техніки це стає досить реальним.

Таким чином, об'єктом досліджень є процеси формування і переробки кодованих даних у БЗПД, а предметом досліджень – методи забезпечення достовірності інформації у БЗПД. Мета досліджень – розробка обчислювального методу нечіткого декодування багатокомпонентних турбо кодів в безпроводових засобах передачі даних, з метою підвищення ефективності застосування математичної моделі системи забезпечення достовірності інформації в безпроводових засобах передачі даних на основі адаптації кодових конструкцій.

3. Методика і результати досліджень

Передбачається, що канал зв'язку гаусівський і має ідеальну імпульсну характеристику $h_c(t)=1$, внаслідок чого сигнал спотворюється тільки присутністю флуктуаційних шумів і навмисних завад.

Розглянемо принцип роботи кодера та декодера ТК.

Схема кодера турбо коду, представленого на рис. 1, використовує РСЗК зі швидкістю $1/n$ виду: $(1, g_1/g_0, \ldots, g_{n-1}/g_0)$,

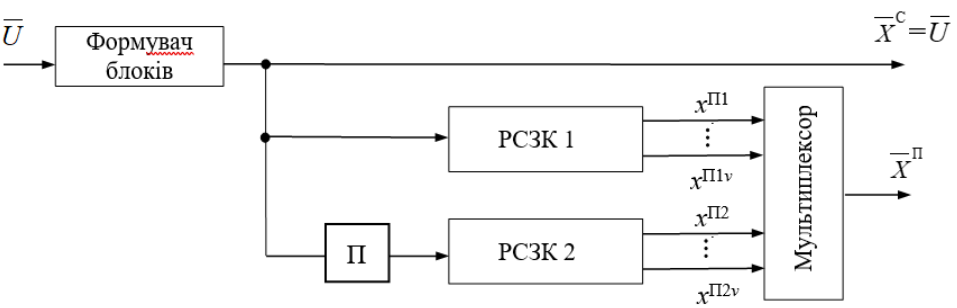

Рисунок 1 – Структурна схема двохкомпонентного кодера ТК

де g_0 – поліноміальний генератор зворотнього зв'язку, а $g_1, \ldots, g_{n-1}$ – поліноміальні генератори прямих зв'язків. Кожен РСЗК виконує кодування інформаційної послідовності по своїй діаграмі [11, 12].

Послідовність на виході кодера ТК має вигляд: $\overline{X} = (\overline{X}^{\text{С}}, \overline{X}^{\text{П}})$. Де $\overline{X}^{\text{С}} = \overline{U}$ – систематичний вихід кодера, а $\overline{X}^{\text{П}} = (\overline{X}^{\text{П1}}, \overline{X}^{\text{П2}})$ – перевірочний вихід кодера ТК. При цьому $\overline{X}^{\text{П1}} = (\overline{X}^{\text{П11}}, \ldots, \overline{X}^{\text{П1}v})$ – перевірочний вихід РСЗК 1, $\overline{X}^{\text{П2}} = (\overline{X}^{\text{П21}}, \ldots, \overline{X}^{\text{П2}v})$ – перевірочний вихід РСЗК 2, v – загальна кількість перевірочних символів кожного РСЗК кодера ТК.

Демодульована послідовність символів подається на декодери 1 і 2 (рис. 2):

$\overline{Y}^{1} = (L_c \overline{Y}^{\text{С1}}, L_c \overline{Y}^{\text{П1}})$ – для декодера 1, де $\overline{Y}^{\text{П1}} = (\overline{Y}^{\text{П11}}, \ldots, \overline{Y}^{\text{П1}v})$, L_c – параметр канальної "надійності". Відповідно $\overline{Y}^{2} = (L_c \overline{Y}^{\text{С2}}, L_c \overline{Y}^{\text{П2}})$ – для декодера 2, де $\overline{Y}^{\text{П2}} = (\overline{Y}^{\text{П21}}, \ldots, \overline{Y}^{\text{П2}v})$. $\overline{Y}^{\text{С1}} = \overline{Y}^{\text{С}}, \overline{Y}^{\text{С2}}$ – послідовності систематичних символів з урахуванням відповідної операції перемеження.

Розглядається такт роботи в момент часу *t*.

Так як ТК застосовується в каналах з підвищеним рівнем шуму, то на приймальній стороні приймаються рішення в умовах невизначеності.

Процес декодування розглядається як задача пошуку оптимального рішення в умовах невизначеності:

$$\begin{array}{c} \min Q\left(\vec{x}, \vec{z}, \overrightarrow{L_a}\right) \\ g_i\left(\vec{x}, \vec{z}, \overrightarrow{L_a}\right) = 0,\ i = \overline{1, N_i},\ N_i \le N_u \\ G_j\left(\vec{x}, \vec{z}, \overrightarrow{L_a}\right) \{\ge, \le\},\ j = \overline{1, N_j} \end{array}, \qquad (1)$$

де $Q(*)$ – показник оптимальності, $\vec{x}, \vec{z}, \overrightarrow{L_a}$ – відповідно послідовності переданих бітів, вибірки білого гаусовського шуму, апріорна інформація про передані біти.

В зв'язку з тим, що рішення на прийомній стороні приймаються за умов невизначеності, будемо розглядати нечітке описання функції $Q(*)$. При цьому задача (1) буде формулюватися наступним чином:

$$\begin{array}{l} Q(\vec{x}, \vec{z}, \overrightarrow{L_a}) \underset{\sim}{\le} q_0, \\ g\left(\vec{x}, \vec{z}, \overrightarrow{L_a}\right) \underset{\sim}{\le} 0, \end{array} \qquad (2)$$

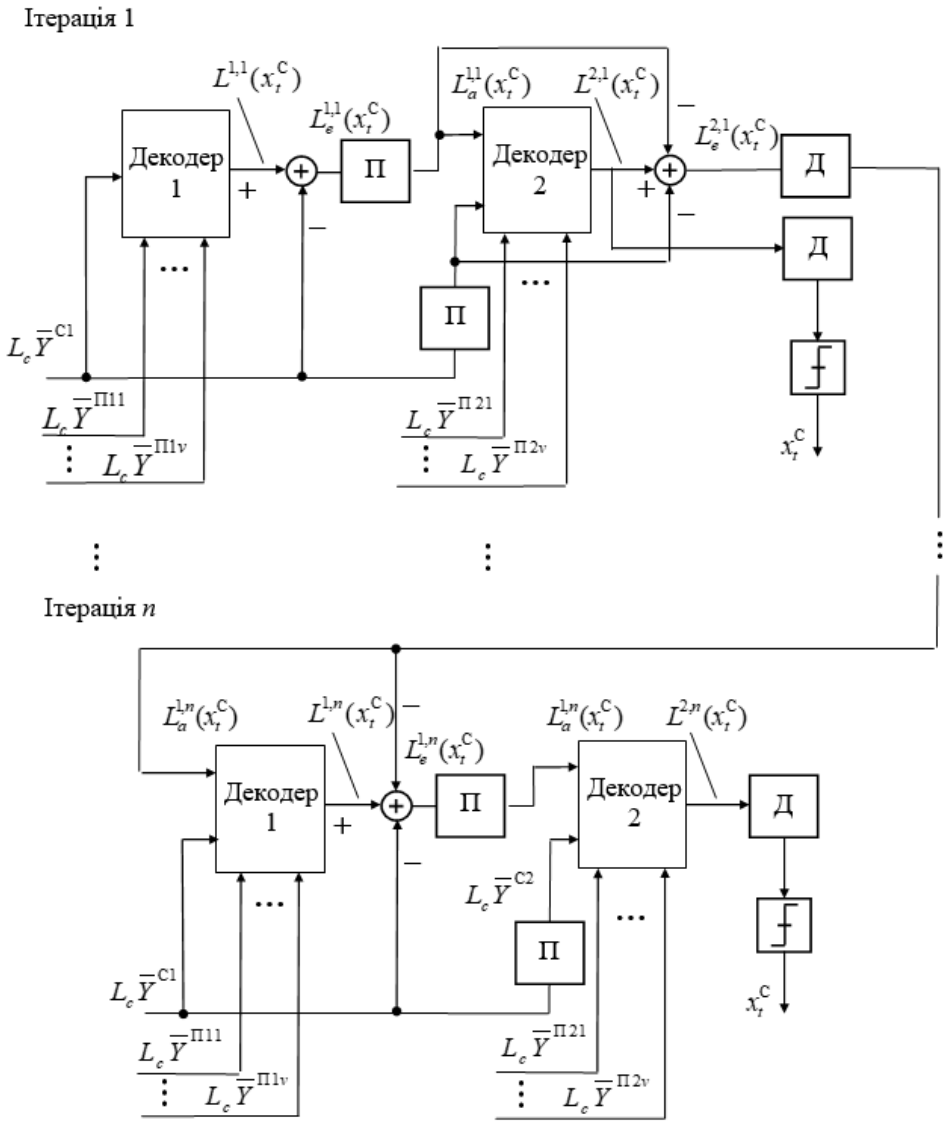

Рисунок 2 – Структурна схема двохкомпонентного декодера ТК

де хвиляста лінія в нерівностях свідчить про їх нечіткість, q_0 – задане значення функції мети $Q(*)$.

Функції приналежності нечіткої мети та обмежень записуються у вигляді:

$$\mu_M(\Gamma)=\begin{cases}0, \text{ якщо } Q(*)\le q_0-a,\\ \mu_1(\Gamma,a), \text{ якщо } q-a<Q(*)<q_0,\\ 1, \text{ якщо } Q(*)\ge q_0,\end{cases} \quad \mu_C(\Gamma)=\begin{cases}0, \text{ якщо } g(*)\ge b,\\ \mu_2(\Gamma,b), \text{ якщо } 0<g(*)<b,\\ 1, \text{ якщо } Q(*)\le q_0,\end{cases}$$

де $\mu_1, \mu_2 : \Gamma \to [0;1]$ – функції, які характеризують ступінь виконання відповідних нерівностей.

На першому етапі необхідно визначити показник оптимальності та ввести нечітку множину рішень.

Нехай $\Gamma = \{\gamma\}$ – задана множина альтернатив, тоді нечітка мета *M* буде ототожнюватися з фіксованою нечіткою множиною *M*, яка описується функцією приналежності $\mu_M : \Gamma \to [0;1]$. Дійсне представлення "м'якого" рішення або логарифмічне відношення функцій правдоподібності (ЛВФП) поза декодером визначається виразом [11, 12]:

$$L(x_t \mid y_t) = \ln \frac{P(y_t \mid x_t = +1)}{P(y_t \mid x_t = -1)} + \ln \frac{P(x_t = +1)}{P(x_t = -1)} = L_a(x_t) + L(y_t \mid x_t), \quad (3)$$

де $L(y_t \mid x_t)$ – ЛВФП y_t, яка одержується шляхом виміру y_t на виході каналу при чергуванні умов, що може бути переданий $x_t = +1$ або $x_t = -1$, а $L_a(x_t)$ – апріорне ЛВФП біта даних x_t. Для спрощення позначень рівняння (3) може бути переписане таким чином [10, 11]:

$$L'(x_t) = L_c(y_t) + L_a(x_t). \quad (4)$$

Тут $L_c(y_t)$ означає, що член ЛВФП визначається у результаті канальних вимірів, зроблених у приймачі.

Для систематичних кодів ЛВФП на виході декодера дорівнює [10, 11]:

$$L(x_t) = L'(x_t) + L_e(x_t). \quad (5)$$

У цьому виразі $L'(x_t)$ – ЛВФП поза демодулятором (на вході декодера), а $L_e(x_t)$ – "зовнішнє" ЛВФП, що представляє зовнішню інформацію, що випливає із процесу декодування. З рівнянь (4) і (5) вихідне ЛВФП декодера прийме вид:

$$L(x_t) = L_c(y_t) + L_a(x_t) + L_e(x_t). \quad (6)$$

Знак $L(x_t)$ є твердим рішенням про символ x_t, а модуль $|L(x_t)|$ – ступенем надійності (правдоподібності) цього рішення.

Декодер 1 у відповідності зі своїм алгоритмом виробляє "м'які" рішення про декодовані символи (вихідне ЛВФП), які складаються із трьох частин [11, 12]

$$L^1(x_t^{\mathrm{C}}) = L_c \cdot y_t^{\mathrm{C1}} + L_a^1(x_t^{\mathrm{C}}) + L_e^1(x_t^{\mathrm{C}}),$$

де x_t^{C} – систематичний символ кодера ТК.

При цьому “зовнішня” інформація декодера 1 про символ x_t^{C}, що є апріорною для декодера 2 (з урахуванням операції перемежіння), прийме вид [11, 12]

$$L_e^1(x_t^{\text{C}}) = L_a^2(x_t^{\text{C}}) = L^1(x_t^{\text{C}}) - L_a^1(x_t^{\text{C}}) - L_c \cdot y_t^{\text{C1}}.$$

Другий елементарний декодер, одержавши апріорні відомості про інформаційні символи, робить аналогічні обчислення, визначаючи свою “зовнішню” інформацію про символ x_t^{C} [12]

$$L_e^2(x_t^{\text{C}}) = L_a^1(x_t^{\text{C}}) = L^2(x_t^{\text{C}}) - L_a^2(x_t^{\text{C}}) - L_c \cdot y_t^{\text{C2}},$$

яка надходить на вхід декодера 1 наступної ітерації декодування.

Після виконання необхідної кількості ітерацій або у випадку примусової зупинки ітеративної процедури декодування, виносяться рішення про декодовані символи:

$$x_t^{\text{C}} = \begin{cases} 1, & \text{якщо } L(x_t^{\text{C}}) \geq 0 \\ 0, & \text{якщо } L(x_t^{\text{C}}) < 0 \end{cases}.$$

Структурна схема моделі кодера та декодера трьохкомпонентного ТК показана на рис. 3 та 4 відповідно.

Розглянемо особливості, якими буде володіти модель декодера трьохкомпонентного ТК, структурна схема якого зображена на рис. 4. Розглядається алгоритм *Max Log Map*.

Як і у випадку двохкомпонентного ТК, трьохкомпонентні декодери працюють послідовно. Особливістю декодування трьохкомпонентного ТК, на відміну від двохкомпонентного, є те, що апріорна інформація для трьохкомпонентного кодера формується як сума не двох (рис. 3), а трьох складових: канального відліку систематичного біта, а також значень ЛВФП, отриманих двома попередніми компонентними декодерами (якщо потрібно, то з попередньої ітерації).

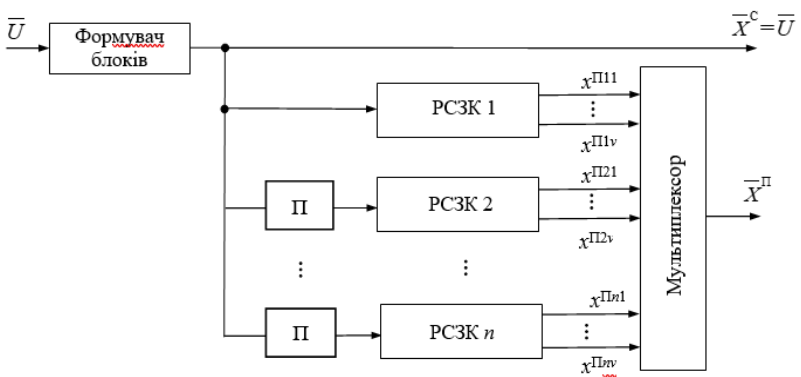

Рисунок 3 – Структурна схема багатокомпонентного кодера ТК

Основні рекурсії для першого, другого та третього декодера *n*-ї ітерації декодування будуть мати наступний вигляд:

$$\Gamma_t^{1,n}(s',s) \sim \frac{1}{2}\cdot\left(x_t^{\mathrm{C}}\cdot\left(L_a^{1,n}(x_t^{\mathrm{C}})+L_c\cdot y_t^{\mathrm{C}}\right)+L_c\cdot\sum_{i=1}^{v} y_t^{\Pi 2i}\cdot x_t^{\Pi 2i}\right);$$

$$\Gamma_t^{2,n}(s',s) \sim \frac{1}{2}\cdot\left(x_t^{\mathrm{C}}\cdot\left(L_a^{1,n}(x_t^{\mathrm{C}})+L_a^{2,n}(x_t^{\mathrm{C}})+L_c\cdot y_t^{\mathrm{C}}\right)+L_c\cdot\sum_{i=1}^{v} y_t^{\Pi 2i}\cdot x_t^{\Pi 2i}\right);$$

$$\Gamma_t^{3,n}(s',s) \sim \frac{1}{2}\cdot\left(x_t^{C}\cdot\left(L_a^{1,n}(x_t^{C})+L_a^{2,n}(x_t^{C})+L_a^{3,n}(x_t^{C})+L_c\cdot y_t^{C}\right)+L_c\cdot\sum_{i=1}^{v} y_t^{\Pi 2i}\cdot x_t^{\Pi 2i}\right);$$

$$\mathrm{A}_t^{1,n}(s) \approx \max_{s'}\left[\tilde{\mathrm{A}}_{t-1}^{1,n}(s')+\Gamma_t^{1,n}(s',s)\right];$$

$$\tilde{\mathrm{A}}_t^{1,n}(s) \approx \max_{s'}\left[\tilde{\mathrm{A}}_{t-1}^{1,n}(s')+\Gamma_t^{1,n}(s',s)\right]-\mathrm{A}_t^{1,n\ \max}(s);$$

$$\mathrm{A}_t^{2,n}(s) \approx \max_{s'}\left[\tilde{\mathrm{A}}_{t-1}^{2,n}(s')+\Gamma_t^{2,n}(s',s)\right];$$

$$\tilde{\mathrm{A}}_t^{2,n}(s) \approx \max_{s'}\left[\tilde{\mathrm{A}}_{t-1}^{2,n}(s')+\Gamma_t^{2,n}(s',s)\right]-\mathrm{A}_t^{2,n\ \max}(s);$$

$$\mathrm{A}_t^{3,n}(s) \approx \max_{s'}\left[\tilde{\mathrm{A}}_{t-1}^{3,n}(s')+\Gamma_t^{3,n}(s',s)\right];$$

$$\tilde{\mathrm{A}}_t^{3,n}(s) \approx \max_{s'}\left[\tilde{\mathrm{A}}_{t-1}^{3,n}(s')+\Gamma_t^{3,n}(s',s)\right]-\mathrm{A}_t^{3,n\ \max}(s);$$

$$\mathrm{B}_{t-1}^{1,n}(s') \approx \max_{s'}\left[\tilde{\mathrm{B}}_t^{1,n}(s)+\Gamma_t^{1,n}(s',s)\right];$$

$$\tilde{\mathrm{B}}_{t-1}^{1,n}(s') \approx \max_{s'}\left[\tilde{\mathrm{B}}_t^{1,n}(s)+\Gamma_t(s',s)\right]-\mathrm{A}_t^{1,n\max}(s);$$

$$\mathrm{B}_{t-1}^{2,n}(s') \approx \max_{s'}\left[\tilde{\mathrm{B}}_t^{2,n}(s)+\Gamma_t^{2,n}(s',s)\right];$$

$$\tilde{\mathrm{B}}_{t-1}^{2,n}(s') \approx \max_{s'}\left[\tilde{\mathrm{B}}_t^{2,n}(s)+\Gamma_t(s',s)\right]-\mathrm{A}_t^{2,n\max}(s);$$

$$\mathrm{B}_{t-1}^{3,n}(s') \approx \max_{s'}\left[\tilde{\mathrm{B}}_t^{3,n}(s)+\Gamma_t^{3,n}(s',s)\right];$$

$$\tilde{\mathrm{B}}_{t-1}^{3,n}(s') \approx \max_{s'}\left[\tilde{\mathrm{B}}_t^{3,n}(s)+\Gamma_t(s',s)\right]-\mathrm{A}_t^{3,n\max}(s).$$

Схема прийняття рішення щодо значень інформаційних бітів також змінюється. Рішення буде представляти суму рішень трьохкомпонентних декодерів.

Для першого, другого, третього декодера вихідне ЛВФП обчислюється за формулами відповідно:

$$L^{1,n}(x_t^{\mathrm{C}}) \approx \max_{\substack{(s',s)\\ u_{t-+1}}}\left[\tilde{\mathrm{A}}_{t-1}^{1,n}(s')+\Gamma_t^{1,n}(s',s)+\tilde{\mathrm{B}}_t^{1,n}(s)\right]-\max_{\substack{(s',s)\\ u_{t--1}}}\left[\tilde{\mathrm{A}}_{t-1}^{1,n}(s')+\Gamma_t^{1,n}(s',s)+\tilde{\mathrm{B}}_t^{1,n}(s)\right];$$

$$L^{2,n}(x_t^{\mathrm{C}}) \approx \max_{\substack{(s',s)\\ u_{t-+1}}}\left[\tilde{\mathrm{A}}_{t-1}^{2,n}(s')+\Gamma_t^{2,n}(s',s)+\tilde{\mathrm{B}}_t^{2,n}(s)\right]-\max_{\substack{(s',s)\\ u_{t--1}}}\left[\tilde{\mathrm{A}}_{t-1}^{2,n}(s')+\Gamma_t^{2,n}(s',s)+\tilde{\mathrm{B}}_t^{2,n}(s)\right];$$

$$L^{3,n}(x_t^{\mathrm{C}}) \approx \max_{\substack{(s',s)\\ u_{t-+1}}}\left[\tilde{\mathrm{A}}_{t-1}^{3,n}(s')+\Gamma_t^{3,n}(s',s)+\tilde{\mathrm{B}}_t^{3,n}(s)\right]-\max_{\substack{(s',s)\\ u_{t--1}}}\left[\tilde{\mathrm{A}}_{t-1}^{3,n}(s')+\Gamma_t^{3,n}(s',s)+\tilde{\mathrm{B}}_t^{3,n}(s)\right].$$

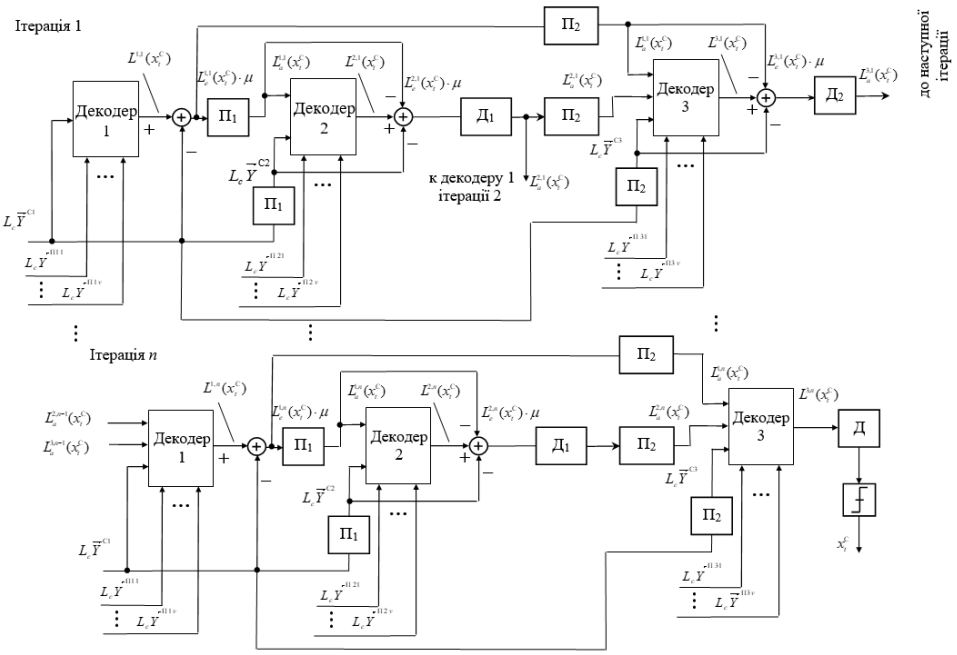

Рисунок 4 – Структурна схема модифікованого трьохкомпонентного декодера ТК

Перший декодер, використовуючи “вихідне” ЛВФП, апріорні ЛВФП з другого та третього декодера попередньої ітерації та інформацію з каналу, визначає “зовнішню” інформацію про символ x_t^{C}:

$$L_e^{1,n}(x_t^{\mathrm{C}}) = L^{1,n}(x_t^{\mathrm{C}}) - L_a^{2,n-1}(x_t^{\mathrm{C}}) - L_a^{3,n-1}(x_t^{\mathrm{C}}) - L_c \cdot y_t^{\mathrm{C2}}.$$

Другий декодер для визначення “зовнішньої” інформації про символ x_t^{C} використовує “вихідне” ЛВФП, апріорне ЛВФП з третього декодера попередньої ітерації та апріорне ЛВФП з першого декодера поточної ітерації, а також інформацію з каналу зв’язку:

$$L_e^{2,n}(x_t^{\mathrm{C}}) = L^{2,n}(x_t^{\mathrm{C}}) - L_a^{3,n-1}(x_t^{\mathrm{C}}) - L_a^{1,n}(x_t^{\mathrm{C}}) - L_c \cdot y_t^{\mathrm{C2}}.$$

Третій елементарний декодер, одержавши апріорні відомості про інформаційні символи з першого та другого декодера, а також використовуючи вихідне ЛВФП та інформацію, прийняту з каналу, визначає свою “зовнішню” інформацію про символ x_t^{C}:

$$L_e^{3,n}(x_t^{\mathrm{C}}) = L^{3,n}(x_t^{\mathrm{C}}) - L_a^{2,n}(x_t^{\mathrm{C}}) - L_a^{1,n}(x_t^{\mathrm{C}}) - L_c \cdot y_t^{\mathrm{C2}}.$$

Позначимо кількість змін знака при перетворенні величини L_a в L_e на послідовному декодері як cs (change of sign). Кількість змін знака на i-му послідовному декодері j-ї ітерації декодування – cs_{ij}. Значення величини буде

обчислюватись, як сумарна кількість змін знака при переходах $L_a \to L_e$ для всіх N інформаційних бітів, що обробляються i -м декодером j-ї ітерації ТК.

Якщо в процесі декодування кількість змін знаку $L_a^i(x_t^C) \to L_e^i(x_t^C)$ дорівнює нулю, то можна стверджувати, що прийнято жорстке рішення про декодований біт, і після кожного наступного декодеру значення ЛВФП про переданий біт буде приймати все менше (якщо був переданий біт «0») або все більше (якщо був переданий біт «1») значення. Може виникнути ситуація, внаслідок великого значення дисперсії шуму в каналі, що в процесі декодування кількість змін знаку $L_a^i(x_t^C) \to L_e^i(x_t^C)$ після виконання процедур ітеративного декодування всіма D декодерами не дорівнює нулю, внаслідок чого виникає невизначеність про значення переданого біту. Це призводить до виникнення помилки декодування з ймовірністю 0,5.

Таким чином, існують чотири події:

Подія 1 – A_1. Кількість змін знаку $L_a^i(x_t^C) \to L_e^i(x_t^C)$, $i \in \overline{1,D}$ в процесі ітеративного декодування після i-го декодеру дорівнює нулю. Прийняте жорстке рішення, що був переданий біт $x_t^C = 1$.

Подія 2 – A_2. Кількість змін знаку $L_a^i(x_t^C) \to L_e^i(x_t^C)$, $i \in \overline{1,D}$ в процесі ітеративного декодування після i-го декодеру дорівнює нулю. Прийняте жорстке рішення, що був переданий біт $x_t^C = 0$.

Подія 3 – A_3. Кількість змін знаку $L_a^i(x_t^C) \to L_e^i(x_t^C)$, $i \in \overline{1,D}$ в процесі ітеративного декодування не дорівнює нулю. З ймовірністю 0,5 приймається рішення, що був переданий біт $x_t^C = 1$.

Подія 4 – A_4. Кількість змін знаку $L_a^i(x_t^C) \to L_e^i(x_t^C)$, $i \in \overline{1,D}$ в процесі ітеративного декодування не дорівнює нулю. З ймовірністю 0,5 приймається рішення, що був переданий біт $x_t^C = 0$.

Враховуючи вищевикладене, отримаємо кількісну характеристику стану каналу, використовуючи оцінку невизначеності декодування.

Отримаємо кількісну оцінку невизначеності, використовуючи зміни знаку $L_a^i(x_t^C) \to L_e^i(x_t^C)$, $i \in \overline{1,D}$ в процесі ітеративного декодування: виконання циклу: якщо $L_a^i(x_t^C) L_e^i(x_t^C) < 1$, то $F = F + 1$, $i \in \overline{1,D}$, $t \in \overline{1,N}$ по всіх декодерах та для всіх бітів блоку N. Нормалізуємо величину F:

$$F^* = \frac{F}{NI},$$

де N – кількість бітів в блоці, I – кількість ітерацій декодування.

Принцип нечіткого ітеративного турбо декодування буде полягати в розрахунку математичного очікування показника оптимальності $M_{F^*} = \frac{1}{L}\sum_i^L F_i^*$ протягом вікна спостереження розміром L та змінення нечітких параметрів алгоритму декодування для досягнення нечіткої мети.

В якості показника оптимальності можна використовувати середньоквадратичну похибку *RMSE* (*Root Mean Square Error*):

$$RMSE = \sqrt{\frac{1}{M}\sum_{h=1}^{M}(F_h^* - F_н^*)^2},$$

де L – розмір вікна спостереження, $F_н^*$ – задане нормалізоване значення показника невизначеності.

Далі необхідно "зовнішнє" ЛВФП помножити на параметр μ, в результаті отримуємо:

$$L_e^{*1,n}(x_t^C) = L_e^{1,n}(x_t^C)\cdot\mu;$$
$$L_e^{*2,n}(x_t^C) = L_e^{2,n}(x_t^C)\cdot\mu;$$
$$L_e^{*3,n}(x_t^C) = L_e^{3,n}(x_t^C)\cdot\mu.$$

Перепишемо функції приналежності, які будемо використовувати в алгоритмі декодування *Max Log Map*:

$$\mu_A(RMSE) = \begin{cases} \varepsilon, \text{ якщ } RMSE \le \varepsilon \\ p + \dfrac{p\cdot RMSE}{3}, \text{ якщо } \varepsilon < RMSE \le 0{,}5, \\ p + \dfrac{p\cdot RMSE}{5}, \text{ якщо } 0{,}5 < RMSE \le 0{,}7, \\ p + \dfrac{p\cdot RMSE}{10}, \text{ якщо } 0{,}7 < RMSE \le 1, \end{cases}$$

$$\mu_B(RMSE) = \begin{cases} \varepsilon, \text{ якщ } RMSE \le \varepsilon, \\ p - \dfrac{p\cdot RMSE}{3}, \text{ якщ } \varepsilon < RMSE \le 0{,}5, \\ p - \dfrac{p\cdot RMSE}{5}, \text{ якщ } 0{,}5 < RMSE \le 0{,}7, \\ p - \dfrac{p\cdot RMSE}{10}, \text{ якщ } 0{,}7 < RMSE \le 1, \end{cases}$$

де ε – граничне значення середньоквадратичної помилки, p – деякий заздалегідь заданий коефіцієнт.

Алгоритм вибору значення функції приналежності наступний:

Крок 1. Одержуємо значення *RMSE* при поточному значенні коефіцієнта p.

Крок 2. За допомогою нечітких множин одержуємо значення функцій приналежності $\mu_A(RMSE)$ й $\mu_B(RMSE)$.

Крок 3. Знаходимо перетинання (узяття мінімуму) нечітких множин $\mu_A(RMSE)$ і $\mu_B(RMSE)$: $\mu_D^i(RMSE) = \min\{\mu_A^i(RMSE); \mu_B^i(RMSE)\}$.

Крок 4. Порівнюємо $\mu_D^i(RMSE)$ з попереднім значенням $\mu_D^{i-1}(RMSE)$.

Крок 5. Якщо $\mu_D^i(RMSE) < \mu_D^{i-1}(RMSE)$, то призначається нове значення коефіцієнта p, якщо $\mu_D^i(RMSE) > \mu_D^{i-1}(RMSE)$, то значення коефіцієнта p залишається без змін.

Функцію приналежності будемо використовувати при розрахунку перехідної рекурсії в алгоритмах декодування ТК:

$$\Gamma_t^{1,n}(s',s) \sim \frac{1}{2}\cdot\left(x_t^{\text{С}}\cdot\left(L_a^{1,n}(x_t^{\text{С}})\cdot\mu_M\left(RMSE\right)+L_c\cdot y_t^{\text{С}}\right)+L_c\cdot\sum_{i=1}^{v}y_t^{\text{П2}i}\cdot x_t^{\text{П2}i}\right);$$

$$\Gamma_t^{2,n}(s',s) \sim \frac{1}{2}\cdot\left(\begin{array}{l}x_t^{\text{С}}\cdot\left(L_a^{1,n}(x_t^{\text{С}})\cdot\mu_M\left(RMSE\right)+L_a^{2,n}(x_t^{\text{С}})\cdot\mu_M\left(RMSE\right)+L_c\cdot y_t^{\text{С}}\right)+\\ +L_c\cdot\sum_{i=1}^{v}y_t^{\text{П2}i}\cdot x_t^{\text{П2}i}\end{array}\right);$$

$$\Gamma_t^{3,n}(s',s) \sim \frac{1}{2}\cdot\left(\begin{array}{l}x_t^{\text{С}}\cdot\left(\begin{array}{l}L_a^{1,n}(x_t^{\text{С}})\cdot\mu_M\left(RMSE\right)+L_a^{2,n}(x_t^{\text{С}})\cdot\mu_M\left(RMSE\right)+\\ +L_a^{3,n}(x_t^{\text{С}})\cdot\mu_M\left(RMSE\right)+L_c\cdot y_t^{\text{С}}\end{array}\right)+\\ +L_c\cdot\sum_{i=1}^{v}y_t^{\text{П2}i}\cdot x_t^{\text{П2}i}\end{array}\right),$$

де $x_t^{\text{С}}, x_t^{\text{П2}i}, i\in(1,v)$ – відповідно систематичний символ кодера ТК і перевірочні символи РСЗК 2 до проходження каналу з флуктуаційним шумом і навмисними завадами; $y_t^{\text{С}}, y_t^{\text{П2}i}, i\in(1,v)$ – систематичний символ кодера ТК і перевірочні символи РСЗК 2 після проходження каналу з флуктуаційним шумом і навмисними завадами; $x_t^{\text{П3}i}, y_t^{\text{П3}i}, i\in(1,v)$ – перевірочні символи РСЗК 3 відповідно до проходження та після проходження каналу з флуктуаційним шумом і навмисними завадами; $L_a^2(x_t^{\text{С}})$ – апріорна інформація другого декодера; $L_a^3(x_t^{\text{С}})$ – апріорна інформація третього декодера; $\mu_M\left(RMSE\right)$ – функція приналежності, L_c – параметр канальної «надійності»; v – кількість перевірочних символів РСЗК, $v = q - 1$, де q – загальна кількість символів РСЗК (систематичний і перевірочні).

Оцінка ефективності запропонованого обчислювального методу була здійснена за допомогою імітаційної моделі.

Результати моделювання показані на рис. 5 та 6.

На рис. 5 показано графік залежності середньої ймовірності бітової помилки декодування $P_{B\,дек}$ від відношення сигнал-завада h_j^2 для різних значень параметрів $\mu_D^i\left(RMSE\right)$ при використанні модуляції ФМ-2, ТК з двохкомпонентними кодерами (декодерами), псевдовипадковим перемежувачем, $N=1000$, алгоритмом декодування *Max Log Map*, 8 ітераціями декодування, швидкістю кодування ТК R = 1/3 при впливі ШЗЧС ($\gamma=1$) і флуктуаційного шуму ($h_0^2=9{,}58$ дБ). Аналіз рисунку показує, що вплив параметра $\mu_D^{i+2}\left(RMSE\right)=0{,}8$ в алгоритмі декодування *Max Log Map* дозволяє підвищити ефективність запропонованої математичної моделі. Використання параметра $\mu_D^{i+2}\left(RMSE\right)=0{,}8$ підвищує ефективність запропонованої математичної моделі до 0,2 дБ в порівнянні з використанням параметра $\mu_D^{i+2}\left(RMSE\right)=1{,}0$.

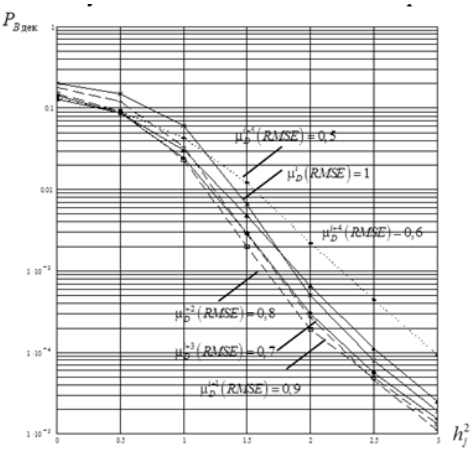

Рисунок 5 – Графік завадозахищеності для різних значень функцій приналежності та двохкомпонентного кодека

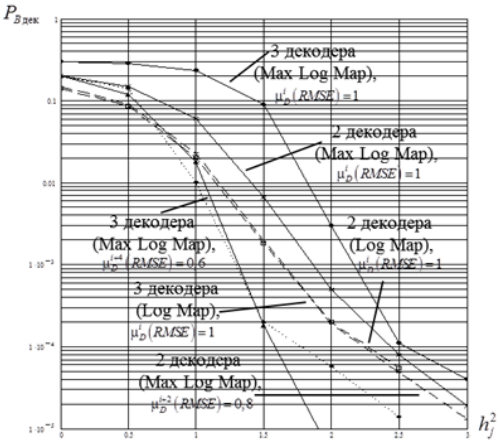

Рисунок 6 – Графік завадозахищеності для двох- та трьохкомпонентного кодеків при різних значеннях функцій приналежності

Графік залежності середньої ймовірності бітової помилки декодування $P_{B\,дек}$ від відношення сигнал-завада h_j^2 для параметрів $\mu_D^{i}(RMSE)=1,0$ та $\mu_D^{i+2}(RMSE)=\mu_{D\,\mathrm{opt}}^{i}$ при використанні модуляції ФМ-2, ТК з двох- та трьохкомпонентними кодерами (декодерами), псевдовипадковим перемежувачем, $N=1000$, алгоритмом декодування *Max Log Map, Log Map*, 8 ітерацій декодування, швидкістю кодування ТК R = 1/3 при впливі ШЗЧС ($\gamma=1$) і флуктуаційного шуму ($h_0^2=const$) показаний на рис. 6. Аналіз рисунку показує, що використовуючи трьохкомпонентний кодек з алгоритмом декодування *Max Log Map* та параметром $\mu_D^{i+4}(RMSE)=\mu_{D\,\mathrm{opt}}^{i}=0,6$, можна підвищити ефективність запропонованої математичної моделі в 1,2 раза (0,8 дБ) в порівнянні з використанням стандартного двохкомпонентного кодера з алгоритмом декодування *Max Log Map* та параметром $\mu_D^{i}(RMSE)=1,0$, та в 1,25 раза (1 дБ) в порівнянні з використанням трьохкомпонентного кодера з алгоритмом декодування *Max Log Map* та параметром $\mu_D^{i}(RMSE)=1,0$. Підвищення ефективності застосування запропонованої математичної моделі в 1,16 раза (0,65 дБ) можна отримати, використовуючи трьохкомпонентний кодек з алгоритмом декодування *Max Log Map* з $\mu_D^{i+4}(RMSE)=\mu_{D\,\mathrm{opt}}^{i}=0,6$ в порівнянні зі стандартним двохкомпонентним з алгоритмом *Max Log Map* з $\mu_D^{i+4}(RMSE)=\mu_{D\,\mathrm{opt}}^{i}=0,6$. Однак при цьому знижується швидкість цифрової обробки прийнятого інформаційного блоку.

Таким чином, у статті запропоновано обчислювальний метод нечіткого декодування багатокомпонентних турбо кодів в безпроводових засобах передачі даних, з метою підвищення ефективності застосування математичної моделі системи забезпечення достовірності інформації в безпроводових засобах передачі даних на основі адаптації кодових конструкцій. Сутність

методу полягає у використанні функцій приналежності та модифікованого логарифмічного відношення функції правдоподібності при моделюванні декодування двох- та трьохкомпонентних турбо кодів за допомогою алгоритму *Max Log Map*. Відмінність розробленого методу від існуючих, що визначає його новизну, полягає у застосуванні функцій приналежності при розрахунку перехідних рекурсій у алгоритмах декодування турбо кодів.

Ефект від впровадження полягає в тому, що розроблений метод дозволяє підвищити ефективність математичної моделі системи забезпечення достовірності інформації в безпроводових засобах передачі даних на основі адаптації кодових конструкцій. Наприклад, при впливі різних завад на БЗПД, використовуючи трьохкомпонентний кодек з алгоритмом декодування *Max Log Map* та параметром $\mu_D^{i+6}(RMSE)=0,6$, можна підвищити ефективність запропонованої математичної моделі в 1,2 раза (0,8 дБ) в порівнянні з використанням двохкомпонентного кодека з алгоритмом декодування *Max Log Map* та параметром $\mu_D^{i}(RMSE)=1,0$, та в 1,25 раза (1 дБ) в порівнянні з використанням трьохкомпонентного кодека з алгоритмом декодування *Max Log Map* та параметром $\mu_D^{i}(RMSE)=1,0$.

Висновки

1. На основі нових аналітичних залежностей для алгоритмів декодування багатокомпонентних турбо кодів розроблено обчислювальний метод нечіткого декодування багатокомпонентних турбо кодів в безпроводових засобах передачі даних для підвищення ефективності математичної моделі системи забезпечення достовірності інформації на основі адаптації кодових конструкцій.

2. Результати моделювання характеристик достовірності БЗПД з багатокомпонентними турбо кодами показали, що використання запропонованого методу дозволяє підвищити ефективність математичної моделі системи забезпечення достовірності інформації на основі адаптації кодових конструкцій.

3. Напрямком подальших розробок вважається дослідження характеристик достовірності багатокомпонентних турбо кодів з адаптацією в умовах впливу навмисних завад.

СПИСОК ЛІТЕРАТУРИ

1. Holma H. HSDPA/HSUPA for UMTS: High Speed Radio Access for Mobile Communications / H. Holma, A. Toskala. – John Wiley & Sons, 2006. – 268 p.
2. Peng F. Adaptive Modulation and Coding for IEEE 802.11n / F. Peng, J. Zhang, W. Ryan // Wireless Communications and Networking Conference, 11-15 March 2007. – 2007. – P. 656-661.
3. IEEE 802.16. Broadband Wireless Metropolitan Area Network (WirelessMAN) [Electronic resource] // Mode of access: http://standards.ieee.org/getieee802/802.16.html. – Title from the screen.
4. Ergen M. Mobile Broadband. Including WiMax and LTE / M. Ergen/ – Springer, 2009. – 513 p.

5. Zaitsev S. V. Adaptive selection of parameters of s-random interleaver in wireless data transmission systems with turbo coding / S. V. Zaitsev, V. V. Kazymyr, V. M. Vasilenko, A. V. Yarilovets // Radioelectronics and Communications Systems. – Allerton Press, Inc. – New York, 2018. – Vol. 61. – P. 13–21. DOI: 10.3103/S0735272715050039.
6. Пат. WO2008057906 A2, H03M13/27. Turbo interleaving for high data rates / Yongbin W., Jing S., Prasad M.; заявл. 01.11.06; опубл. 15.05.08, World Intellectual Property Organization.
7. Пат. KR20020031721, H03M13/29. Device for decoding turbo code using channel information and method thereof / Geun K., Seop L.; опубл. 03.05.02, World Intellectual Property Organization.
8. Пат. EP1906536 A2, H03M13/29. Tail-bitting turbo-code for arbitrary number of information bits / Zong S., Tak L.; заявл. 28.09.06; опубл. 02.04.08, European Patent Application, Bulletin 2008/14.
9. Пат. на корисну модель 43111, МПК H03M 13-37. Пристрій підвищення завадозахищеності систем з турбокодами при низьких значеннях відношення сигнал-шум в каналі / Зайцев С. В., Лівенцев С. П., Кувшинов О. В., Артюх О. І.; заявл. 05.08.08; опубл. 10.08.09, Бюл. № 15.
10. Zaitsev S. V. Structural adaptation of the turbo code coder and decoder for generating the transmission repeat request under conditions of uncertainty / S. V. Zaitsev, V. V. Kazymyr // Radioelectronics and Communications Systems. – Springer, 2017. – Vol. 60. – P. 18–27.
11. Особенности декодера турбокода в программируемых радиостанциях при воздействии помех / С. П. Ливенцев, С. В. Зайцев, С. В. Кныр [и др.] // Зв'язок. – 2007. – № 2. – С. 31-35.
12. Woodard J. Comparative Study of Turbo Decoding Techniques: An Overview / J. Woodard, L. Hanzo // IEEE Transactions on Vehicular Technology. – 2000. – Vol. 49, No. 6. – P. 2208–2232.

REFERENCES

1. Holma H. HSDPA/HSUPA for UMTS: High Speed Radio Access for Mobile Communications / H. Holma, A. Toskala. – John Wiley & Sons, 2006. – 268 p.
2. Peng F. Adaptive Modulation and Coding for IEEE 802.11n / F. Peng, J. Zhang, W. Ryan // Wireless Communications and Networking Conference, 11-15 March 2007. – 2007. – P. 656-661.
3. IEEE 802.16. Broadband Wireless Metropolitan Area Network (WirelessMAN) [Electronic resource] // Mode of access: http://standards.ieee.org/getieee802/802.16.html. – Title from the screen.
4. Ergen M. Mobile Broadband. Including WiMax and LTE / M. Ergen/ – Springer, 2009. – 513 p.
5. Zaitsev S. V. Adaptive selection of parameters of s-random interleaver in wireless data transmission systems with turbo coding / S. V. Zaitsev, V. V. Kazymyr, V. M. Vasilenko, A. V. Yarilovets // Radioelectronics and Communications Systems. – Allerton Press, Inc. – New York, 2018. – Vol. 61. – P. 13–21. DOI: 10.3103/S0735272715050039.
6. Patent WO2008057906 A2, H03M13/27. Turbo interleaving for high data rates / Yongbin W., Jing S., Prasad M.; declared 01.11.06; published 15.05.08, World Intellectual Property Organization.
7. Patent KR20020031721, H03M13/29. Device for decoding turbo code using channel information and method thereof / Geun K., Seop L.; published 03.05.02, World Intellectual Property Organization.
8. Patent EP1906536 A2, H03M13/29. Tail-bitting turbo-code for arbitrary number of information bits / Zong S., Tak L; declared 28.09.06; published 02.04.08, European Patent Application, Bulletin 2008/14.

9. Utility model patent 43111, МПК H03M 13-37. Device for enhancing noise immunity of systems with turbo codes at low signal-to-noise ratio in the channel / Zaitsev S. V., Liventsev S. P., Kuvshinov O. V., Artyukh O. I.; declared 05.08.08; published 10.08.09, Bulletin № 15.
10. Zaitsev S. V. Structural adaptation of the turbo code coder and decoder for generating the transmission repeat request under conditions of uncertainty / S. V. Zaitsev, V. V. Kazymyr // Radioelectronics and Communications Systems. – Springer, 2017. – Vol. 60. – P. 18–27.
11. Features of the turbo code decoder in programmable radio stations under interference / S. P. Liventsev, S. V. Zaitsev, S. V. Knir // Зв'язок. – 2007. – № 2. – P. 31-35.
12. Woodard J. Comparative Study of Turbo Decoding Techniques: An Overview / J. Woodard, L. Hanzo // IEEE Transactions on Vehicular Technology. – 2000. – Vol. 49, No. 6. – P. 2208–2232.

Стаття надійшла до редакції 22.06.2019.

АНАЛІЗ, ОЦІНКА ТА ПРОГНОЗУВАННЯ В ЕКОНОМІЦІ

УДК 004.942 ; 626/627 ; 504.05

https://orcid.org/0000-0002-7620-1613

Д.В. СТЕФАНИШИН

ЛОГІКО-ІМОВІРНІСНЕ МОДЕЛЮВАННЯ І ПРОГНОЗУВАННЯ АВАРІЙ НА НАПІРНИХ ГІДРОСПОРУДАХ ДНІСТРОВСЬКОГО ГІДРОВУЗЛА (ЧАСТИНА 2. РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ)

Анотація. *Стаття є другою частиною комплексної роботи, присвяченої моделюванню і прогнозуванню гіпотетичних аварій, з оцінюванням ймовірностей їх виникнення, на гідроспорудах, що формують напірний фронт Дністровського гідровузла. В першій частині було обґрунтовано актуальність проблеми, розглянуто загальну постановку задачі досліджень, викладено методологію досліджень та сформульовано їх мету, окреслено прийняті гіпотези і припущення, дано коротку характеристику моделей, методів і підходів, що використовувалися при вирішенні поставленої задачі. В цій статті наведено результати досліджень. Розв'язання поставленої задачі здійснювалося за допомогою графоаналітичного, логіко-імовірнісного методу дерев відмов і несправностей. В результаті проведених досліджень було отримано верхні граничні оцінки ймовірностей виникнення аварій на окремих гідроспорудах і узагальнену оцінку ймовірності аварії на гідровузлі в цілому. Було встановлено, що ці ймовірності не перевищують допустимого значення ймовірності аварії на напірних гідроспорудах відповідного класу відповідальності за наслідками. На основі цього було зроблено висновок про достатню надійність і безпеку Дністровського гідровузла як об'єкта національної критичної інфраструктури і потенційно небезпечного об'єкта.*

Ключові слова*: аварія, безпека, випадкова подія, дерево відмов і несправностей, Дністровський гідровузол, імовірність аварії, моделювання, надійність, напірні гідроспоруди, об'єкт критичної інфраструктури, подія-припущення, прогнозування, сценарій, форма аварії.*

DOI: 10.35350/2409-8876-2019-16-3-82-98

Вступ

Ця стаття є другою частиною комплексної роботи, присвяченої моделюванню та прогнозуванню гіпотетичних аварій, з оцінюванням ймовірностей їх виникнення, на напірних гідроспорудах Дністровського гідровузла як об'єкта

національної критичної інфраструктури. Вона є продовженням статті [1], в якій було дано загальну характеристику гідровузла та гідроспорудам, що формують напірний фронт; обґрунтовано актуальність проблеми, розглянуто загальну постановку задачі досліджень, викладено методологію досліджень та сформульовано їх мету; окреслено прийняті гіпотези та припущення; дано коротку характеристику моделей, методів та підходів, що використовувалися при вирішенні поставленої задачі.

Основну увагу в цій статті приділено розв'язанню задачі досліджень та аналізу отриманих результатів. В якості основного методу для розв'язання поставленої задачі використано графоаналітичний, логіко-імовірнісний метод дерев відмов і несправностей. Основні його положення наведено в [1-7].

1. Загальні зауваження

При моделюванні та прогнозуванні гіпотетичних аварій на напірних гідроспорудах Дністровського гідровузла розглядалися наступні п'ять гіпотетичних аварійних подій (модельних сценаріїв аварії): A_1 – аварія внаслідок переповнення Дністровського водосховища; A_2 – аварія на правобережній кам'яно-земляній греблі; A_3 – аварія в межах напірної секції монтажної площадки; A_4 – аварія в межах водозливної будівлі ГЕС; A_5 – аварія на лівобережній кам'яно-земляній греблі.

При побудові дерева відмов і несправностей, згідно з рекомендаціями Дж. Фусселя [4], використовувалися наступні евристичні прийоми аналізу (декомпозиції) аварійних подій, що гіпотетично можуть відбуватися на гідроспорудах гідровузла:

1) заміна більш загальної події на більш конкретну подію;

2) «поділ» більш складної події на більш прості несумісні події;

3) встановлення можливих причин настання складної події, щоб використати їх в якості більш простих і конкретних подій;

4) заміна однієї події двома, одна з яких трактується як «заборона» («блокування», «невиконання захисних дій» тощо);

5) виявлення спільної дії (перетину) кількох більш простих, конкретних причин, які спільно спричинюють настання результуючої події;

6) уточнення події за рахунок використання умов її оцінювання тощо.

В процесі аналізу все, що стосується можливої аварії на гідроспоруді, уявно розчленовувалося на окремі складові елементи – менш складні події і стани, що формують різного роду причинно-наслідкові відношення, до встановлення базових подій і станів, ймовірності виникнення яких відомі або можуть бути встановлені тим чи іншим методом. Для зручності перевірки правильності побудови й розрахунку діаграми дерева відмов і несправностей будувалися окремі фрагменти діаграми, що охоплювали частину проблемної ситуації (окремий модельний сценарій аварії). Для уникнення надмірної складності моделювання причинно-наслідкових відношень використовувався також системно-інтегруючий підхід (агрегування). Найбільш прості аварійні події й стани, якщо це було можливо, цілеспрямовано інтегрувалися у більш загальні події й стани, що надалі вже вважалися базовими. При цьому використовувався принцип найменшої взаємодії в системі, згідно з яким базові аварійні події відбиралися серед стохастично незалежних подій.

2. Розв'язання задачі та отримані результати

Діаграма дерева відмов і несправностей, що використовувалось при прогнозуванні аварій на напірних гідроспорудах Дністровського гідровузла та оцінюванні їх ймовірностей, представлена окремими фрагментами на рис. 1-5. На рис. 1 наведено її вершинні події, з деталізацією аварії в межах напірної секції монтажної площадки (аварійна подія A_3), де скорочення РВБ – рівень верхнього б'єфу, ФПР – форсований підпірний рівень, МРЗ – максимальний розрахунковий землетрус.

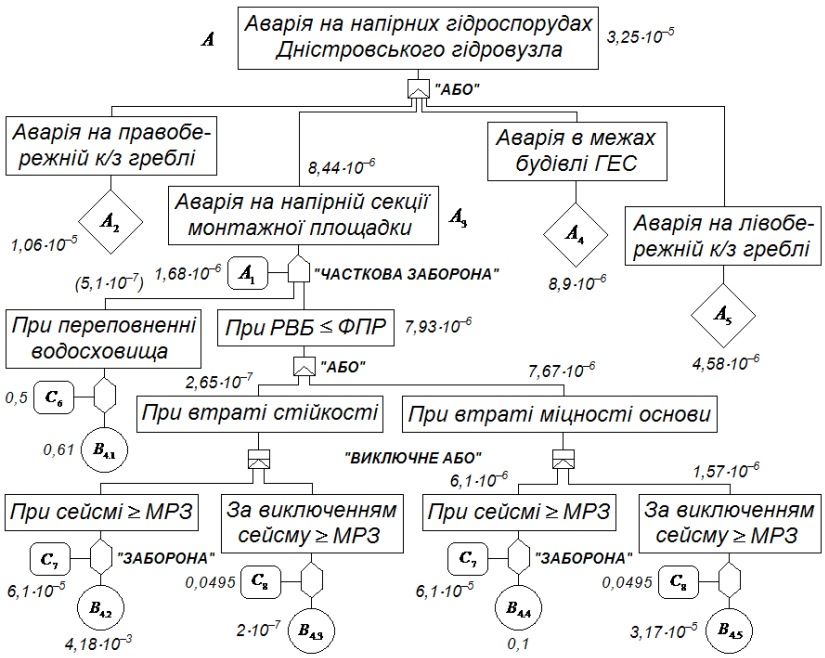

Рисунок 1 – Дерево відмов і несправностей для оцінювання ймовірності аварії на напірних гідроспорудах Дністровського гідровузла (вершинні події, продовження діаграми див. на рис. 2-5)

2.1. Оцінювання ймовірності переповнення Дністровського водосховища

Фрагмент діаграми дерева відмов і несправностей, що стосується оцінювання ймовірності переповнення Дністровського водосховища (події A_1) при різних гіпотетичних аварійних ситуаціях, наведено нижче на рис. 2.

В табл. 1 описано відповідні аварійні ситуації, за яких прогнозувалося переповнення Дністровського водосховища, та представлено їх розрахункові ймовірності. Максимальні витрати води р. Дністер у створі Дністровського гідровузла при відповідних ситуаціях та ймовірності їх перевищення наведено в табл. 2. Базові аварійні події на водопропускних спорудах, при яких прогнозувалося переповнення Дністровського водосховища, та їх розрахункові ймовірності наведено в табл. 3, де ймовірність перебування механічного обладнання (МО) на суміщеній з водозливом будівлі ГЕС в несправному стані оцінювалася за формулою [2, 6]:

$$P(t+t_r)=1-\exp\{-\lambda\cdot t\cdot\exp(-\mu\cdot t_r)\}, \quad (1)$$

де λ – інтенсивність відмов об'єкта до першої відмови; μ – інтенсивність відновлення його працездатності; t_r – додатковий час, що відпускається на відновлення працездатності об'єкта.

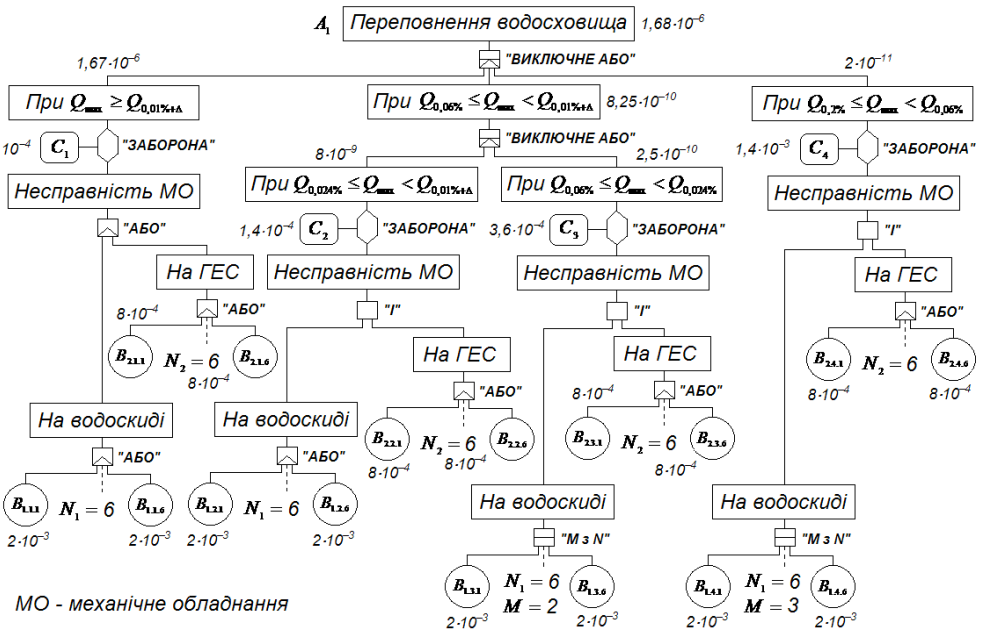

Рисунок 2 – Фрагмент діаграми дерева відмов і несправностей для оцінювання ймовірності переповнення водосховища Дністровського гідровузла

Таблиця 1 – Ситуації, за яких прогнозувалося переповнення Дністровського водосховища, та їх розрахункові ймовірності

Ситуація	Опис ситуації	Ймовірність, рік$^{-1}$
C_1	Максимальні витрати води р. Дністер перевищують 13260 м^3/с, $Q_{\max} \geq Q_{0,01\%+\Delta}$	10^{-4}
C_2	Максимальні витрати води р. Дністер перевищують 11000 м^3/с, але не досягають 13260 м^3/с, $Q_{0,024\%} \leq Q_{\max} < Q_{0,01\%+\Delta}$	$1{,}4\cdot10^{-4}$
C_3	Максимальні витрати води р. Дністер перевищують 9130 м^3/с, але не досягають 11000 м^3/с, $Q_{0,06\%} \leq Q_{\max} < Q_{0,024\%}$	$3{,}6\cdot10^{-4}$
C_4	Максимальні витрати води р. Дністер перевищують 7260 м^3/с, але не досягають 9130 м^3/с, $Q_{0,2\%} \leq Q_{\max} < Q_{0,06\%}$	$1{,}4\cdot10^{-3}$

Таблиця 2 – Розрахункові максимальні витрати $Q_{\max}$ води р. Дністер при ймовірності перевищення P

P, %	0,01	0,024	0,06	0,1	0,2	0,5	1	5	10	25
$Q_{\max}$, м^3/с	13260	11000	9130	8320	7260	6000	5140	3400	2750	1950

Таблиця 3 – Базові аварійні події, при яких прогнозувалося переповнення Дністровського водосховища, та їх ймовірності

Подія	Опис події	Ймовірність, рік$^{-1}$
$B_{1.1.1}$, …, $B_{1.1.6}$	Несправність механічного обладнання водоскиду, що призводить до неможливості підйому робочих затворів, при ситуації C_1	$2{\cdot}10^{-3}$
$B_{1.2.1}$, …, $B_{1.2.6}$	Несправність механічного обладнання водоскиду, що призводить до неможливості підйому робочих затворів, при ситуації C_2	$2{\cdot}10^{-3}$
$B_{1.3.1}$, …, $B_{1.3.6}$	Несправність механічного обладнання водоскиду, що призводить до неможливості підйому робочих затворів, при ситуації C_3	$2{\cdot}10^{-3}$
$B_{1.4.1}$, …, $B_{1.4.6}$	Несправність механічного обладнання водоскиду, що призводить до неможливості підйому робочих затворів, при ситуації C_4	$2{\cdot}10^{-3}$
$B_{2.1.1}$, …, $B_{2.1.6}$	Несправність механічного обладнання ГЕС, що призводить до неможливості підйому ремонтних затворів, при ситуації C_1	$8{\cdot}10^{-4}$
$B_{2.2.1}$, …, $B_{2.2.6}$	Несправність механічного обладнання ГЕС, що призводить до неможливості підйому ремонтних затворів, при ситуації C_2	$8{\cdot}10^{-4}$
$B_{2.3.1}$, …, $B_{2.3.6}$	Несправність механічного обладнання ГЕС, що призводить до неможливості підйому ремонтних затворів, при ситуації C_3	$8{\cdot}10^{-4}$
$B_{2.4.1}$, …, $B_{2.4.6}$	Несправність механічного обладнання ГЕС, що призводить до неможливості підйому ремонтних затворів, при ситуації C_4	$8{\cdot}10^{-4}$

Інтенсивність відмов системи «затвор-підйомний механізм» λ приймалася за статистичними даними (див., наприклад, [2]): для системи «робочий затвор-козловий кран» на водозливі $\lambda = 2{\cdot}10^{-3}$, рік$^{-1}$; для системи «ремонтний затвор-мостовий кран» на ГЕС $\lambda = 10^{-3}$, рік$^{-1}$. З запасом ризику для всіх випадків пропуску паводків на гідровузлі додатковий час, що

відпускається на відновлення працездатності систем «затвор-підйомний механізм», приймався рівним t_r = 0. Час служби механічного обладнання, протягом якого очікується хоча б одна робоча операція, для водоскидних споруд приймався рівним 1 року, t = 1 рік; для ГЕС t = 0,7945 рік.

2.2. Врахування живучості гідроспоруд при аварійних ситуаціях

При моделюванні аварійних ситуацій на напірних гідроспорудах гідровузла, зокрема при переповненні водосховища, враховувалася їх живучість при аварійних перевантаженнях (див. коефіцієнти живучості в [8] в залежності від типу гідроспоруд). При цьому умовні ймовірності розвитку аварійних подій на напірних гідроспорудах оцінювалися як доповнення коефіцієнта живучості κ_v до одиниці.

Для кам'яно-земляних гребель κ_v = 0,77 і, відповідно, умовна ймовірність розвитку аварії буде 0,23. Для бетонних гідроспоруд (монтажна площадка, будівля ГЕС суміщена з водозливом) коефіцієнт живучості κ_v = 0,39. Умовна ймовірність розвитку аварії відповідно буде 0,61.

Серед подій-умов, за яких можуть втратити живучість напірні гідроспоруди Дністровського гідровузла, також розглядалися (див. табл. 4): для кам'яно-земляних гребель – дія вітрових хвиль 50% ймовірності перевищення (подія-умова C_5); для бетонних гідроспоруд – дія навантаження від льоду 50% ймовірності перевищення (подія-умова C_6).

Таблиця 4 – Ситуації, за яких прогнозувалася втрата живучості напірних гідроспоруд Дністровського гідровузла, та їх ймовірності

Ситуація	Опис ситуації	Ймовірність, рік$^{-1}$
C_5	Дія вітрових хвиль 50% ймовірності перевищення	0,5
C_6	Дія навантаження від льоду 50% ймовірності перевищення	0,5

2.3. Врахування сейсмічного фактору

Згідно з новими картами сейсмічного районування (карти ЗСР-2004 [9]) територія розміщення напірних гідроспоруд Дністровського гідровузла віднесена до зони, де можливе виникнення землетрусів: з інтенсивністю сейсмічних струшувань 6 балів за шкалою MSK-64 для середніх ґрунтів з періодом повторюваності 1 раз в 500 років (карта ЗСР-2004-А) або щорічною ймовірністю перевищення відповідної сейсмічної події $2\cdot10^{-3}$, рік$^{-1}$; з інтенсивністю сейсмічних струшувань 7 балів за шкалою MSK-64 для середніх ґрунтів з періодом повторюваності 1 раз в 5000 років (карта ЗСР-2004-С) або щорічною ймовірністю перевищення відповідної сейсмічної події $2\cdot10^{-4}$, рік$^{-1}$. Розрахункове сейсмічне прискорення (для напірних гідроспоруд гідровузла – землетрусу інтенсивністю 7 балів) приймалось рівним $0{,}1\cdot g$, де g = 9,8 м/с^2 – прискорення вільного падіння.

Забезпеченість (ймовірність перевищення) цього прискорення при максимальному розрахунковому землетрусі (МРЗ) інтенсивністю 7 балів (див., наприклад, [10]) складає 80%, а забезпеченість цього ж прискорення при землетрусі інтенсивністю 6 балів оцінюється в 25%.

Для землетрусів інтенсивністю 7 балів за шкалою MSK-64 ймовірність $P(I_7)$ приймалась рівною ймовірності перевищення відповідної сейсмічної події з інтенсивністю сейсмічних струшувань 7 балів: $P(I_7) = 2\cdot10^{-4}$, рік$^{-1}$. Відповідно, для землетрусів інтенсивністю 6 балів, з врахуванням умови формування повної групи подій, $P(I_6) = 1{,}8\cdot10^{-3}$, рік$^{-1}$. Тоді, повна ймовірність перевищення сейсмічного прискорення величиною $0{,}1\cdot g$ максимального розрахункового землетрусу (МРЗ) з врахуванням сейсмічних подій інтенсивністю сейсмічних струшувань в 6 і 7 балів на площадці розміщення гідроспоруд Дністровського гідровузла буде:

$$P(a_{\max} \geq 0{,}1g) = \sum_{k=6,7} P(a_{\max} \geq 0{,}1g \mid I_k) \cdot P(I_k), \qquad (2)$$

де $P(a_{\max} \geq 0{,}1g \mid I_k)$ – ймовірність перевищення сейсмічного прискорення $a_{\max} = 0{,}1\cdot g$ при землетрусі інтенсивністю k балів; $P(I_k)$ – щорічна ймовірність сейсмічної події інтенсивністю сейсмічних струшувань в k балів. Маємо $P(a_{\max} \geq 0{,}1g) = 6{,}1\cdot10^{-4}$, рік$^{-1}$.

Верхню граничну (sup) оцінку ймовірності настання граничного стану першої групи, пов'язаного з порушенням загальної міцності або стійкості гідроспоруди при МРЗ, з врахуванням коефіцієнта сполучення навантажень $\gamma_{lc} = 0{,}9$ [11], приймемо (з запасом ризику) рівною 0,1.

Результати оцінювання ймовірностей реалізації подій-умов (ситуацій) C_7, C_8, пов'язаних з врахуванням сейсмічного фактору, наведено в табл. 5.

Розрахунки гідроспоруд на сейсміку зазвичай проводяться при рівнях води у верхньому б'єфі близьких до нормального підпірного рівня (НПР). Оскільки перевищення НПР для гідроспоруд класу СС-3 протягом призначеного строку служби в 100 років очікується не більше ніж один раз в 10 років (при розрахунковому паводку щорічною ймовірністю перевищення 0,1%), то повна ймовірність аварійного сполучення навантажень при сейсмічних впливах (події-умови C_7) буде: $P(C_7) = 6{,}1\cdot10^{-5}$, рік$^{-1}$.

Таблиця 5 – Ситуації, пов'язані з врахуванням сейсмічного фактору, при яких прогнозувалися аварії на напірних гідроспорудах Дністровського гідровузла, та їх ймовірності (ФПР – форсований підпірний рівень)

Ситуація	Опис ситуації	Ймовірність, рік$^{-1}$
C_7	Навантаження при РВБ ≤ ФПР і землетрусі інтенсивністю ≥ МРЗ	$6{,}1\cdot10^{-5}$
C_8	Навантаження при РВБ ≤ ФПР та за виключенням землетрусу інтенсивністю ≥ МРЗ	0,0495

Для визначення щорічної ймовірності реалізації події-умови (ситуації) C_8 формувалася повна група у складі події C_8 та подій A_1 і C_7. Покладалося, що протягом призначеного строку служби гідроспоруди T_p = 100 років (встановленого для гідроспоруд класу СС-3 згідно з чинними нормами [2]) повна ймовірність реалізації однієї з подій A_1, C_7 буде:

$$P(A_1, C_7, T_p) = 1 - \left[1 - P(A_1) - P(C_7)\right]^{T_p}. \quad (3)$$

Повна ймовірність реалізації події-умови C_8 в розрізі T_p = 100 років:

$$P(C_8, T_p) = 1 - P(C_1, T_p). \quad (4)$$

Щорічна ймовірність події-умови C_8, що доповнює події A_1 і C_7:

$$P(C_8) = 1 - \left[1 - P(C_8, T_p)\right]^{\frac{1}{T_p}}. \quad (5)$$

2.4. Прогнозування аварій на напірних гідроспорудах гідровузла

Базові події, за яких прогнозувалася аварія в межах монтажної площадки (подія A_3, див. рис. 1), та їх розрахункові ймовірності, наведено в табл. 6.

Таблиця 6 – Базові аварійні події, за яких прогнозувалася аварія в межах монтажної площадки, та їх ймовірності

Подія	Опис події	Ймовірність, рік$^{-1}$
$B_{4.1}$	Втрата живучості конструкції напірної секції монтажної площадки при переповненні водосховища	0,61
$B_{4.2}$	Втрата стійкості напірної секції монтажної площадки при РВБ ≤ ФПР і сейсміці інтенсивністю ≥ МРЗ	$4{,}18 \cdot 10^{-3}$
$B_{4.3}$	Втрата стійкості напірної секції монтажної площадки при РВБ ≤ ФПР та за виключенням сейсміки ≥ МРЗ	$2 \cdot 10^{-7}$
$B_{4.4}$	Втрата міцності напірної секції монтажної площадки при РВБ ≤ ФПР і сейсміці інтенсивністю ≥ МРЗ	0,1
$B_{4.5}$	Втрата міцності напірної секції монтажної площадки при РВБ ≤ ФПР та за виключенням сейсміки ≥ МРЗ	$3{,}17 \cdot 10^{-5}$

При оцінці ймовірності порушення міцності бетонної споруди на скельній основі, приймалося, що така подія можлива на контакті з боку верхової грані внаслідок напружень розтягу. З запасом ризику допустиме

значення напруження приймалося рівним нулю. Встановлювався критерій порушення міцності основи на контакті у вигляді $\sigma_1 \le 0$, і, в залежності від ситуації C, оцінювалася умовна ймовірність порушення міцності основи на контакті в припущенні нормального закону розподілу напружень σ_1:

$$P(\sigma_1 \le 0 \mid C) = \Phi\langle \sigma_1 = 0, m(\sigma_1), s(\sigma_1) \rangle, \tag{6}$$

де $\Phi\langle \sigma_1 = 0, m(\sigma_1), s(\sigma_1) \rangle$ – інтегральна функція імовірності нормального закону розподілу при $\sigma_1 = 0$, математичному сподіванні $m(\sigma_1)$ та середньому квадратичному відхиленні $s(\sigma_1)$ напруження σ_1, визначених за умови C.

В табл. 7 наведено базові події, за яких прогнозувалася аварія на правобережній кам'яно-земляній греблі (аварійна подія A_2), та їх ймовірності. Фрагмент діаграми дерева відмов і несправностей для оцінювання ймовірності виникнення аварій на цій греблі показано на рис. 3.

Таблиця 7 – Базові аварійні події, за яких прогнозувалася аварія на правобережній кам'яно-земляній греблі, та їх ймовірності

Подія	Опис події	Ймовірність, рік$^{-1}$
$B_{3.1}$	Втрата живучості конструкції правобережної кам'яно-земляної греблі при переповненні водосховища	0,23
$B_{3.2}$	Зсув верхового укосу греблі при РВБ ≤ ФПР і сейсмічних впливах інтенсивністю ≥ МРЗ	$2{,}1 \cdot 10^{-2}$
$B_{3.3}$	Зсув низового укосу греблі при РВБ ≤ ФПР і сейсмічних впливах інтенсивністю ≥ МРЗ	$1{,}2 \cdot 10^{-2}$
$B_{3.4}$	Зсув верхового укосу греблі при РВБ ≤ ФПР та за виключенням сейсмічних впливів ≥ МРЗ	$1{,}5 \cdot 10^{-4}$
$B_{3.5}$	Зсув низового укосу греблі при РВБ ≤ ФПР та за виключенням сейсмічних впливів ≥ МРЗ	$5{,}4 \cdot 10^{-6}$
$B_{3.6}$	Руйнування греблі внаслідок суфозії в ядрі при РВБ ≤ ФПР і сейсмічних впливах ≥ МРЗ	10^{-2}
$B_{3.7}$	Руйнування греблі внаслідок суфозії в основі при РВБ ≤ ФПР і сейсмічних впливах ≥ МРЗ	$3{,}5 \cdot 10^{-3}$
$B_{3.8}$	Руйнування греблі внаслідок суфозії в ядрі при РВБ ≤ ФПР та за виключенням сейсміки інтенсивністю ≥ МРЗ	$2 \cdot 10^{-6}$
$B_{3.9}$	Руйнування греблі внаслідок суфозії в основі при РВБ ≤ ФПР і за виключенням сейсміки інтенсивністю ≥ МРЗ	10^{-7}

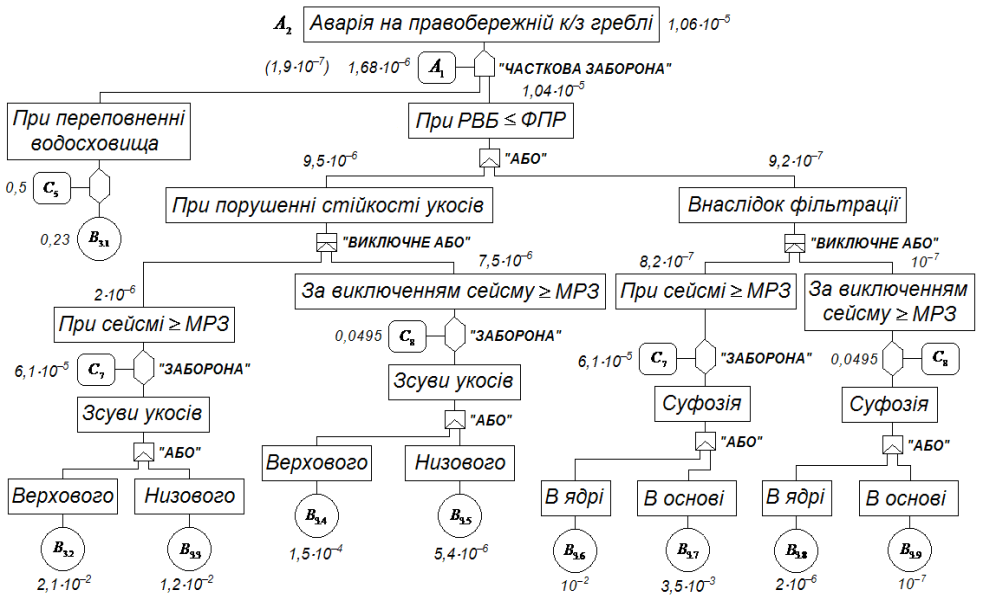

Рисунок 3 – Фрагмент дерева відмов і несправностей для оцінювання ймовірності аварії на правобережній кам'яно-земляній греблі

В табл. 8 наведено базові події, за яких прогнозувалася аварія в межах суміщеної з водозливом будівлі ГЕС (аварійна подія A_4), та їх ймовірності. В табл. 9 описано ситуації, при яких прогнозувалися аварії, пов'язані з порушенням загальної стійкості і міцності будівлі ГЕС при РВБ ≤ ФПР і за виключенням сейсміки ≥ МРЗ, та представлено їх розрахункові ймовірності.

Таблиця 8 – Базові аварійні події, за яких прогнозувалася аварія в межах суміщеної з водозливом будівлі ГЕС, та їх ймовірності

Подія	Опис події	Ймовірність, рік$^{-1}$
1	2	3
$B_{5.1}$	Втрата живучості споруди при переповненні б'єфу	0,61
$B_{5.2}$	Втрата стійкості секції будівлі ГЕС при РВБ ≤ ФПР і сейсмічних впливах інтенсивністю ≥ МРЗ	$6{,}28\cdot10^{-3}$
$B_{5.3}$	Втрата стійкості секції будівлі ГЕС при РВБ ≤ ФПР та за виключенням сейсмічних впливів інтенсивністю ≥ МРЗ при аварійному розрахунковому випадку	$3{,}3\cdot10^{-6}$
$B_{5.4}$	Втрата стійкості секції будівлі ГЕС при РВБ ≤ ФПР та за виключенням сейсміки ≥ МРЗ при основному розрахунковому випадку (РВБ = 123,0 м; РНБ = 74,2 м)	$4{,}7\cdot10^{-6}$
$B_{5.5}$	Втрата стійкості секції будівлі ГЕС при РВБ ≤ ФПР та за виключенням сейсміки ≥ МРЗ при основному розрахунковому випадку (РВБ = 121,0 м; РНБ = 68,0 м)	$6{,}4\cdot10^{-7}$
$B_{5.6}$	Втрата стійкості секції будівлі ГЕС при РВБ ≤ ФПР та за виключенням сейсмічних впливів інтенсивністю ≥ МРЗ при ремонтному розрахунковому випадку	$1{,}1\cdot10^{-5}$

Продовження таблиці 8

1	2	3
$B_{5.7}$	Втрата міцності секції будівлі ГЕС при РВБ ≤ ФПР і сейсмічних впливах інтенсивністю ≥ МРЗ	0,1
$B_{5.8}$	Втрата міцності секції будівлі ГЕС при РВБ ≤ ФПР та за виключенням сейсмічних впливів інтенсивністю ≥ МРЗ при аварійному розрахунковому випадку	$3{,}17\cdot10^{-5}$
$B_{5.9}$	Втрата міцності секції будівлі ГЕС при РВБ ≤ ФПР та за виключенням сейсмічних впливів ≥ МРЗ при основному розрахунковому випадку (РВБ = 123,0 м; РНБ = 74,2 м)	$4{,}29\cdot10^{-4}$
$B_{5.10}$	Втрата міцності секції будівлі ГЕС при РВБ ≤ ФПР та за виключенням сейсмічних впливів ≥ МРЗ при основному розрахунковому випадку (РВБ = 121,0 м; РНБ = 68,0 м)	$3{,}17\cdot10^{-5}$
$B_{5.11}$	Втрата стійкості секції будівлі ГЕС при РВБ ≤ ФПР та за виключенням сейсмічних впливів інтенсивністю ≥ МРЗ при ремонтному розрахунковому випадку	$2{,}74\cdot10^{-6}$

Таблиця 9 – Ситуації, при яких прогнозувалися аварії, пов'язані з порушенням загальної стійкості і міцності будівлі ГЕС, та їх ймовірності

Ситуація	Опис ситуації	Ймовірність, рік$^{-1}$
C_9	Розрахунковий паводок 0,1% забезпеченості	10^{-3}
C_{10}	Ремонт гідроагрегату	0,015
C_{11}	РВБ = 123,0 м; рівень нижнього б'єфу (РНБ) = 68,0 м	$1{,}4\cdot10^{-3}$
C_{12}	РВБ = 121,0 м; РНБ = 68,0 м	0,0321

Ймовірність виникнення ситуації C_9 приймалася рівною ймовірності перевищення розрахункового паводку 0,1% забезпеченості. При цьому приймалася до уваги можливість виходу з ладу частини механічного обладнання на водоскиді і ГЕС і необхідність форсування РВБ до ФПР.

Ймовірність виникнення ситуації C_{10} встановлювалася за даними статистики відмов гідроагрегатів, що потребують ремонту з осушенням проточного тракту [12]. З запасом ризику ймовірність $P(C_{10}) = 0{,}015$, рік$^{-1}$.

Ймовірність виникнення ситуації C_{11} приймалася рівною ймовірності ситуації C_4, при якій максимальні витрати води р. Дністер можуть перевищити 7260 м^3/с, але не перевищують 9130 м^3/с: $P(C_{11}) = 1{,}4\cdot10^{-3}$, рік$^{-1}$. При цьому приймалася до уваги можливість виходу з ладу частини механічного обладнання на водоскиді і ГЕС і необхідність форсування РВБ до РВБ = 123,0 м. Нарешті, ймовірність виникнення ситуації C_{12} встановлювалася з врахуванням того, що ситуації C_9, C_{10}, C_{11} і C_{12}, разом, в повній групі подій, складають ситуацію C_8. Тоді $P(C_{12}) = 1{,}4\cdot10^{-3}$, рік$^{-1}$.

Фрагмент діаграми дерева відмов і несправностей для оцінювання ймовірності виникнення аварій в межах будівлі ГЕС показано на рис. 4.

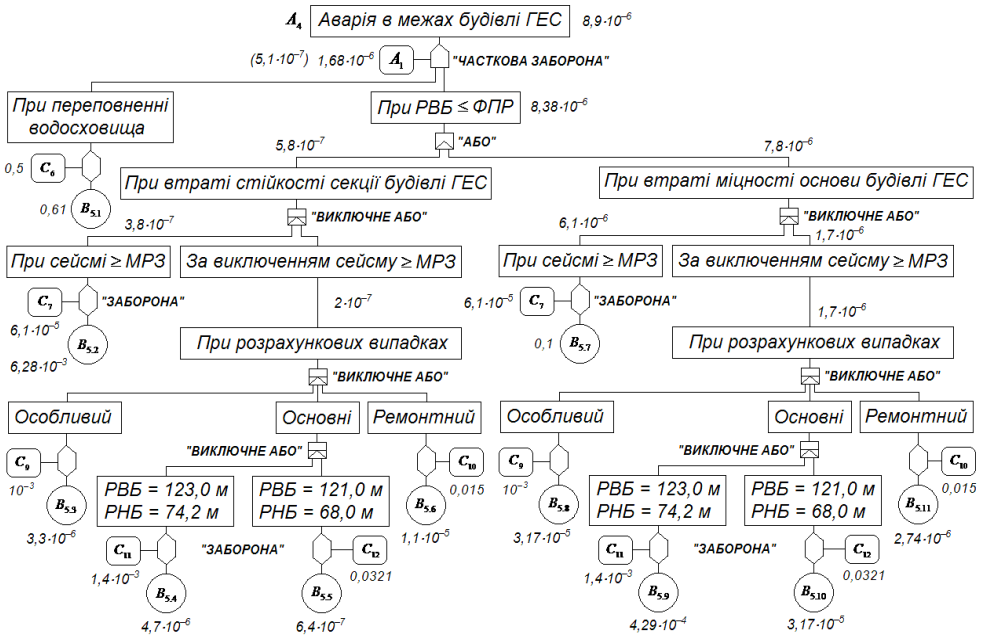

Рисунок 4 – Фрагмент дерева відмов і несправностей для оцінювання ймовірності аварії в межах суміщеної з водозливом будівлі ГЕС

В табл. 10 наведено базові події, за яких прогнозувалася аварія на лівобережній кам'яно-земляній греблі (аварійна подія A_5), та їх ймовірності. Фрагмент діаграми дерева відмов і несправностей для оцінювання ймовірності виникнення аварій на цій греблі показано на рис. 5.

Таблиця 10 – Базові аварійні події, за яких прогнозувалася аварія на правобережній кам'яно-земляній греблі, та їх ймовірності

Подія	Опис події	Ймовірність, рік$^{-1}$
1	2	3
$B_{6.1}$	Втрата живучості конструкції лівобережної кам'яно-земляної греблі при переповненні водосховища	0,23
$B_{6.2}$	Зсув верхового укосу греблі при РВБ ≤ ФПР і сейсмічних впливах інтенсивністю ≥ МРЗ	$1{,}75\cdot10^{-2}$
$B_{6.3}$	Зсув низового укосу греблі при РВБ ≤ ФПР і сейсмічних впливах інтенсивністю ≥ МРЗ	$1{,}2\cdot10^{-2}$
$B_{6.4}$	Зсув верхового укосу греблі при РВБ ≤ ФПР та за виключенням сейсмічних впливів ≥ МРЗ	$1{,}5\cdot10^{-4}$
$B_{6.5}$	Зсув низового укосу греблі при РВБ ≤ ФПР та за виключенням сейсмічних впливів ≥ МРЗ	$5{,}4\cdot10^{-6}$
$B_{6.6}$	Руйнування греблі внаслідок суфозії в ядрі при РВБ ≤ ФПР і сейсмічних впливах ≥ МРЗ	10^{-2}

Продовження таблиці 10

1	2	3
$B_{6.7}$	Руйнування греблі внаслідок суфозії в основі при РВБ ≤ ФПР і сейсмічних впливах ≥ МРЗ	$5\cdot10^{-3}$
$B_{6.8}$	Руйнування греблі внаслідок суфозії в ядрі при РВБ≤ ФПР та за виключенням сейсміки інтенсивністю ≥ МРЗ	10^{-5}
$B_{6.9}$	Руйнування греблі внаслідок суфозії в основі при РВБ ≤ ФПР та за виключенням сейсміки ≥ МРЗ	10^{-7}

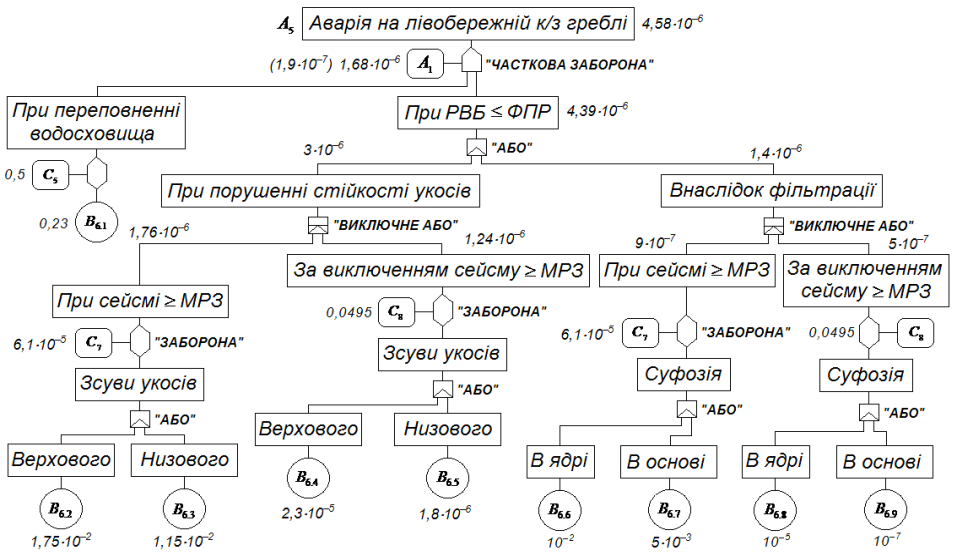

Рисунок 5 – Фрагмент дерева відмов і несправностей для оцінювання ймовірності аварії на лівобережній кам’яно-земляній греблі

3. Аналіз отриманих результатів

Результати моделювання і прогнозування аварій на напірних гідроспорудах Дністровського гідровузла з оцінюванням їх ймовірностей представлено на діаграмах дерева відмов і несправностей (див. рис. 1-5) та зведено в табл. 11.

Таблиця 11 – Результати оцінювання ймовірностей аварій на напірних гідроспорудах Дністровського гідровузла

Гідроспоруда	$P(A)$, рік$^{-1}$	$[P(A)]$, рік$^{-1}$	Висновок про надійність
Правобережна кам’яно-земляна гребля	$1{,}06\cdot10^{-5}$	$5\cdot10^{-5}$	надійна
Напірна секція монтажної площадки	$8{,}44\cdot10^{-6}$	$5\cdot10^{-5}$	надійна
Суміщена з водозливом будівля ГЕС	$8{,}9\cdot10^{-6}$	$5\cdot10^{-5}$	надійна
Лівобережна кам’яно-земляна гребля	$4{,}58\cdot10^{-6}$	$5\cdot10^{-5}$	надійна
Гідровузол в цілому	$3{,}25\cdot10^{-5}$	$5\cdot10^{-5}$	надійний

Згідно з отриманими результатами верхня гранична (sup) оцінка ймовірності аварії на напірних гідроспорудах гідровузла, узагальнена за різними її формами, сценаріями та спорудами, склала $3{,}25 \cdot 10^{-5}$, рік$^{-1}$.

В табл. 11 виконано порівняння розрахункових значень ймовірностей аварій на напірних гідроспорудах гідровузла з допустимими значеннями щорічної ймовірності виникнення аварій на напірних гідроспорудах (див. ДБН В.2.4-3:2010 [11]). Як можна бачити, узагальнені за різними подіями ймовірності аварій на кожній з напірних гідроспоруд Дністровського гідровузла, що формують його напірний фронт, а також і узагальнена за різними гідроспорудами ймовірність аварії на гідровузлі в цілому, не перевищують допустимих значень для класу за наслідками СС-3.

Отримані оцінки ймовірностей аварій на напірних гідроспорудах Дністровського гідровузла є максимальними граничними оцінками (sup), перевищення яких за прийнятих режимів експлуатації гідроспоруд натепер не очікується. Ймовірність аварії в залежності від гідроспоруди гідровузла змінюється в межах від $4{,}58 \cdot 10^{-6}$, рік$^{-1}$, на лівобережній кам'яно-земляній греблі, до $1{,}06 \cdot 10^{-5}$, рік$^{-1}$, на правобережній кам'яно-земляній греблі.

При подальших дослідженнях можливе уточнення отриманих оцінок ймовірностей аварій на напірних гідроспорудах Дністровського гідровузла в сторону їх зменшення. Особливо це стосується правобережної кам'яно-земляної греблі. Більш високе значення ймовірності виникнення аварії на цій греблі в порівнянні з іншими напірними гідроспорудами гідровузла, зокрема, з імовірністю аварії на лівобережній кам'яно-земляній греблі, пояснюється дефіцитом інформації про реальний стан гідроспоруди і, як наслідок, більш обережними оцінками ймовірностей базових аварійних подій. З тієї ж причини дещо завищеними є також значення ймовірностей виникнення аварій в межах монтажної площадки та суміщеної з водозливом будівлі ГЕС, що також пояснюється більш високим рівнем невизначеності інформації про їх реальний стан в порівнянні з лівобережною кам'яно-земляною греблею.

Висновки

1. Виконано прогнозування аварій на напірних гідроспорудах Дністровського гідровузла на основі імовірнісного підходу. Встановлено, що узагальнені за різними аварійними подіями ймовірності аварій на кожній з напірних гідроспоруд гідровузла, що формують його напірний фронт, а також узагальнена оцінка ймовірності аварії на гідровузлі в цілому, не перевищують допустимих значень, що регламентуються чинними нормами.

2. Показано, що прогнозування аварії на гідровузлі є складною, «слабо структурованою» системною задачею, обтяженою невизначеністю різної природи – стохастичною і гносеологічною, структурною і параметричною тощо. З метою структуризації задачі досліджень і подолання невизначеності інформації використано метод дерев відмов і несправностей – логіко-імовірнісний метод прогнозування аварій, який дозволяє врахувати системний характер виникнення гіпотетичних аварій на гідровузлі, вплив різних природних і техногенних факторів на аварійність споруд, в тому числі і взаємодію різних гідроспоруд, обладнання та устаткування на рівні системи.

3. Прогнозування аварій на гідровузлі в межах імовірнісного підходу відкриває нові можливості щодо раціонального обґрунтування додаткових

досліджень та зусиль, які можуть спрямовані на підвищення рівня знань про гідроспоруди, що формують напірний фронт гідровузла, і, відповідно, рівня їх надійності та безпеки. Зокрема, в межах таких досліджень можлива реалізація на практиці концепції практично досяжного мінімального ризику, згідно з якою зусилля на зменшення ймовірності аварії на гідровузлі й підвищення таким чином його надійності і безпеки можуть узгоджуватися з економічними та технологічними можливостями.

4. Результати моделювання та прогнозування аварій на напірних гідроспорудах Дністровського гідровузла було використано при оцінюванні його надійності і безпеки за імовірнісним критерієм, а також можуть бути використані при аналізі та оцінюванні ризику аварій на гідровузлі з врахуванням як ймовірностей відповідних аварійних подій, так і їх наслідків. Це сприятиме кращому розумінню проблем забезпечення належної надійності і безпеки Дністровського гідровузла як об'єкта національної критичної інфраструктури та потенційно небезпечного об'єкта.

СПИСОК ЛІТЕРАТУРИ

1. Стефанишин Д.В. Логіко-імовірнісне моделювання і прогнозування аварій на напірних гідроспорудах Дністровського гідровузла (Частина 1. Методологія, гіпотези та припущення). Математичне моделювання в економіці. 2019. № 2 (15). С. 69-85.
2. Векслер А.Б., Ивашинцов Д.А., Стефанишин Д.В. Надежность, социальная и экологическая безопасность гидротехнических объектов: оценка риска и принятие решений. С.-Петербург : ВНИИГ им. Б.Е. Веденеева. 2002. 591 с.
3. Стефанишин Д.В. Прогнозування аварій на греблях в задачах оцінки й забезпечення їх надійності та безпеки. Гідроенергетика України. № 3-4. 2011. С. 52-60.
4. Kumamoto H., Henley E.J. Probabilistic risk assessment and management for engineers and scientists. N.Y.: IEEE Press, 1996. 597 p.
5. The use of risk analysis to support dam safety decisions and management. Trans. of the 20-th Int. Congress on Large Dams. Vol.1. Q.76. Beijing-China, 2000. 896 p.
6. Беллендир Е.Н., Ивашинцов Д.А., Стефанишин Д.В. и др. Вероятностные методы оценки надежности грунтовых гидротехнических сооружений. СПб.: В 2-х томах. Изд-во ОАО «ВНИИГ им. Б. Е. Веденеева», 2003. 553 с. 524 с.
7. Рябинин И.А. Надёжность и безопасность структурно-сложных систем. СПб.: Издательство СПбГУ, 2007. 276 с.
8. Стефанишин Д.В. Статистичні оцінки живучості гребель. Екологічна безпека та природокористування. Зб. наук. праць. Вип. 11. Київ: КНУБА, ІТГІП НАНУ, 2012. С. 53-61.
9. ДБН В.1.1-12:2006. Захист від небезпечних геологічних процесів, шкідливих експлуатаційних впливів, від пожежі. Будівництво в сейсмічних районах України. Мінбудівництва, архітектури та житлово-комунального господарства України. Київ: 2006. 83 с.
10. Світовий центр даних з геоінформатики та сталого розвитку. Сейсмічна небезпека. URL : http://wdc.org.ua/uk/node/178.
11. ДБН В.2.4-3:2010. Гідротехнічні, енергетичні та меліоративні системи і споруди, підземні гірничі виробки. Гідротехнічні споруди. Основні положення. Київ : Міністерство регіонального розвитку та будівництва України, 2010. 37 с.
12. Стефанишин Д.В., Романчук К.Г. Логіко-імовірнісна оцінка ризику збитків від аварійного виливу води з басейну добового регулювання Зарамагської ГЕС-1. Системні дослідження та інформаційні технології. 2013. №3. С. 130-141.

REFERENCE

1. Stefanyshyn, D.V. (2019). Lohiko-imovirnisne modeliuvannia i prohnozuvannia avarii na napirnykh hidrosporudakh Dnistrovskoho hidrovuzla (Chastyna 1. Metodolohiia, hipotezy ta prypushchennia). [Logic-probabilistic modeling and forecasting of accidents on water retaining hydraulic structures of the Dnistrovsky waterworks (Part 1. Methodology, hypotheses and assumptions)]. Matematychne modeliuvannia v ekonomitsi, № 2, 69-85. (In Ukrainian).
2. Veksler, A.B., Yvashyntsov, D.A., Stefanyshyn, D.V. (2002). Nadezhnost, sotsyalnaia y эkolohycheskaia bezopasnost hydrotekhnycheskykh obъektov: otsenka ryska y pryniatye reshenyi. [Reliability, social and environmental safety of hydraulic facilities: risk assessment and decision making]. S.-Peterburh, VNYYH ym. B.E. Vedeneeva. 591 s. (In Russian).
3. Stefanyshyn, D.V. (2011). Prohnozuvannia avarii na hrebliakh v zadachakh otsinky y zabezpechennia yikh nadiinosti ta bezpeky. [Forecasting accidents on the dam in the tasks of assessment and ensuring their reliability and safety]. Hidroenerhetyka Ukrainy, № 3-4, 52-60. (In Ukrainian).
4. Kumamoto, H., Henley, E.J. (1996). Probabilistic risk assessment and management for engineers and scientists. N.Y., IEEE Press, 597 p.
5. The use of risk analysis to support dam safety decisions and management. (2000). Trans. of the 20-th Int. Congress on Large Dams, Vol. 1, Q. 76, Beijing-China, 2000, 896 p.
6. Bellendyr, E.N., Yvashyntsov, D.A., Stefanyshyn, D.V. y dr. (2003). Veroiatnostnыe metodы otsenky nadezhnosty hruntovыkh hydrotekhnycheskykh sooruzhenyi. [Probabilistic methods for assessing the reliability of earth hydrotechnacal structures]. S.-Peterburh, V 2-kh tomakh, VNYYH ym. B. E. Vedeneeva, 553 s. 524 s. (In Russian).
7. Riabynyn, Y.A. (2007). Nadëzhnost y bezopasnost strukturno-slozhnыkh system. [Reliability and safety of structurally complex systems]. S.-Peterburh, Yzdatelstvo SPbHU, 276 s. (In Russian).
8. Stefanyshyn, D.V. (2012). Statystychni otsinky zhyvuchosti hrebel. [Statistical estimates of the survivability of dams]. Ekolohichna bezpeka ta pryrodokorystuvannia, Vyp. 11, Kyiv, KNUBA, ITHIP NANU, 53-61. (In Ukrainian).
9. DBN V.1.1-12:2006. (2006). Zakhyst vid nebezpechnykh heolohichnykh protsesiv, shkidlyvykh ekspluatatsiinykh vplyviv, vid pozhezhi. Budivnytstvo v seismichnykh raionakh Ukrainy. [DBN V.1.1-12: 2006. Protection from dangerous geological processes, harmful operational influences, from fire. Construction in seismic areas of Ukraine]. Minbudivnytstva, arkhitektury ta zhytlovo-komunalnoho hospodarstva Ukrainy, Kyiv, 83 s. (In Ukrainian).
10. Svitovyi tsentr danykh z heoinformatyky ta staloho rozvytku. Seismichna nebezpeka. [World Data Center for Geoinformatics and Sustainable Development. Seismic danger]. Retrieved from http://wdc.org.ua/uk/node/178. (In Ukrainian).
11. DBN V.2.4-3:2010. (2010). Hidrotekhnichni, enerhetychni ta melioratyvni systemy i sporudy, pidzemni hirnychi vyrobky. Hidrotekhnichni sporudy. Osnovni polozhennia. [DBN V.2.4-3: 2010. Hydrotechnical, energy and reclamation systems and structures, underground mining. Waterworks. Substantive provisions]. Kyiv, Ministerstvo rehionalnoho rozvytku ta budivnytstva Ukrainy, 37 s. (In Ukrainian).
12. Stefanyshyn, D.V., Romanchuk, K.H. (2013). Lohiko-imovirnisna otsinka ryzyku zbytkiv vid avariinoho vylyvu vody z baseinu dobovoho rehuliuvannia Zaramahskoi HES-1. [Logical-probabilistic assessment of risk of damages due to fail water pouring out the daily regulation basin of the Zaramagskaya HPP-1]. Systemni doslidzhennia ta informatsiini tekhnolohii, №3, 130-141.

Стаття надійшла до редакції 07.07.2019

УДК 330.101.541-336.7

https://orcid.org/0000-0003-2925-0276
https://orcid.org/0000-0002-9339-4242

Б.Б. ДУНАЕВ, А.А. ЛЮБИЧ

ДЕПРЕССИЮ ЭКОНОМИКИ ВЫЗЫВАЕТ И СОХРАНЯЕТ ДЕНЕЖНАЯ ДЕФЛЯЦИЯ

Аннотация. *Экономики высокоразвитых стран после начавшегося в 2008 г. кредитного кризиса, переросшего в глобальный финансовый кризис, находятся в состоянии депрессии, сохраняемой денежной дефляцией. Центральными банками проводится политика выхода из депрессии через наращивание денежных баз, снижение до нуля процентных ставок, ежемесячный многомиллиардный выкуп токсичных активов банков и таргетирование инфляции не более двух процентов. Эта политика привела к резкому росту спекулятивного финансового сектора, углублению кредитного кризиса, сохранению денежной дефляции в реальном секторе экономики и не позволяет расти потребительскому спросу. Сдерживание роста инфляции для обеспечения имеющегося курса валюты и повышения стоимости денег сохраняет денежную дефляцию и поддерживает депрессию экономики. Без увеличения инфляции невозможно выйти из депрессии.*

Ключевые слова: *экономика, равновесие, спрос, предложение, кризис, рынок, конъюнктура, труд, капитал, деньги, амортизация, инвестиции, инфляция, дефляция.*

DOI: 10.35350/2409-8876-2019-16-3-99-119

Введение

Главной проблемой мировой экономики после начавшегося в 2008 г. кредитного кризиса, который перерос в глобальный финансово-экономический кризис, является состояние депрессии из-за отсутствия роста потребительского спроса на рынке благ. Превышение спроса над предложением вызывает увеличение цен, инфляцию, обеспечивает рыночное равновесие и выход из кризиса. Рынок уравновешивает спрос и предложение также при отрицательной инфляции, т.е. при дефляции, когда нет равновесия экономики и углубляется кризис, а при выходе из дефляции неизбежна экономическая катастрофа [1–3]. Выход из депрессии возможен через инфляцию или через дефляцию.

Для ускорения выхода из депрессии центральные банки ведущих высокоразвитых стран: США – Федеральная резервная Система (ФРС), стран Евросоюза – Центральный Банк Европы (ЕЦБ), Японии – Банк Японии, Англии – Банк Англии, – стремятся обеспечить уровень инфляции не более двух процентов, выкупают активы с балансов банков и снизили процентные ставки до нуля. Они проводят резкую накачку денег в экономику своих стран. Денежные базы центральных банков США, Англии, Европейского Союза, Японии увеличились в течение трех лет в 3-5 раз. В результате возобновился рост активов в мировом финансовом секторе вне банковского регулирования. Объем деривативов вырос за последние три года на одну треть и достиг квадриллиона долларов. Глобальный теневой банковский сектор вырос в 2012 г. на 5 трлн $ (+ 7%) до 71 трлн $ и составил 117% валового внутреннего

продукта (ВВП). Об этом говорится в ноябрьском 2013 г. докладе Совета по финансовой стабильности (FSB) при G20 "Глобальный мониторинг теневого банкинга – 2013" [4]. Экономики развитых стран продолжают балансировать на грани дефляции. Если в 1998–2007 гг. в развитых странах инфляция составляла 2,0%, то в 2015 г. – только 0,3% и в США она сравнялась с 0% [5]. Дефляционное давление на экономику стран Европейского союза (ЕС) нарастало в 2012–2018 гг. Для обеспечения стабильности цен с декабря 2011 г. Европейский центральный банк (ЕЦБ) начал снижать процентные ставки. В настоящее время они составляют: по основным операциям рефинансирования – 0%, по маржевой схеме кредитования – 0,25% и по депозитам – 0,4% [6]. Но этого оказалось недостаточно и в январе 2015 г. ЕЦБ, по примеру Федеральной Резервной Системы США, принял, а в марте того же года запустил масштабную программу количественного смягчения в размере 1,1 трлн евро и объемом ежемесячного выкупа активов на сумму 60 млрд евро [7]. В марте 2016 г. размер количественного смягчения был увеличен до 80 млрд евро ежемесячно, а в декабре 2016 г. Совет управляющих ЕЦБ оставил на нулевых уровнях процентные ставки и подтвердил продолжение программы выкупа активов в 2017 г. [8]. Предложение дешевых денег не ограничивается, но банки не направляют экстремально дешевый кредит в сферу производства, а накапливают деньги в виде резервов, чтобы избежать банкротства и роста инфляции. Они присоединились к общему спекулятивному инвестиционному процессу финансового сектора, где функционируют венчурные паевые, инвестиционные и хеджевые фонды. Проводимая банками и инвесторами спекулятивная политика привела к тому, что прибыль производства перераспределилась в финансовый сектор в пользу владельцев финансового капитала и в ущерб сфере производства. Будут ли дальше экономики развитых стран испытывать инфляцию или дефляцию, остается темой дебатов [9, 10]. Если в США рост реального ВВП составил в 2018 г. 3,1% после принятых президентом Дональдом Трампом мер по восстановлению обрабатывающих отраслей промышленности и увеличению на один миллион количества рабочих мест, то в ЕС и Японии практически нет роста ВВП.

Необходимо определить причины погружения экономик высокоразвитых стран в состояние депрессии и возможность выхода из состояния депрессии на стабильный рост реального ВВП.

1. Регулирование равновесия на рынке денег

Процесс создания денег двухуровневой банковской системой в общем виде определяется активами Центрального банка, т.е. денежной базой H; а также минимальными резервами $M_{\text{р}}$, избыточными (необязательными) резервами $И_{\text{р}}$, кредитами Ξ и депозитами D банков и наличными деньгами $M0$. Депозиты банков состоят из депозитов до востребования D_1, срочных депозитов D_2 и долгосрочных более четырех лет депозитов D_3:

$$D = D_1 + D_2 + D_3 . \qquad (1)$$

В имеющейся в течение года на рынке денег страны денежной массе выделяются кроме наличных денег $M0$ три денежных агрегата: $M1 = M0 + D_1$ – сумма наличности и депозитов до востребования; $M2 = M1 + D_2$; $M3 = M2 + D_3$. Процесс создания денег банковской системой при выданных банками кредитах Ξ и балансе ε банковской системы выражается системой уравнений:

$$\begin{cases} H = M0 + M_{\text{р}} + И_{\text{р}}; \\ \varepsilon = M3 - H - \Xi; \\ M1 = M0 + D_1; M2 = M0 + D_1 + D_2; \\ M3 = M0 + D_1 + D_2 + D_3. \end{cases} \tag{2}$$

Денежная база H увеличивается через рост наличности $M0$ и рост резервов $M_{\text{р}} + И_{\text{р}}$. Если ввести коэффициенты: $(M_{\text{р}} + И_{\text{р}}) / D_1 = \alpha$ – установленный норматив банковских резервов; $M0 / D_1 = \beta$ – отношение наличности к депозитам до востребования, – то процесс создания денег банковской системой можно представить двумя уравнениями:

$$\begin{cases} H = (\alpha + \beta) D_1; \\ \Xi = M3 - H - \varepsilon. \end{cases} \tag{3}$$

Определим $M1 = M0(1+\beta)/\beta$ и $H = (\alpha+\beta)(M1 - M0) = M1(\alpha+\beta)/(1+\beta)$. Отсюда произведение денежной базы H и денежного мультипликатора $m = (1+\beta)/(\alpha+\beta)$ тождественно сумме наличности и депозитов до востребования $M1$ [1–3]:

$$M1 \equiv mH \ . \tag{4}$$

Изменение денежной базы Центрального банка H через изменение резервов банков $M_{\text{р}} + И_{\text{р}}$ согласно (2) не влияет на сумму наличности и депозитов до востребования $M1 = M0 + D_1$. Сумма наличности и депозитов до востребования не зависит от банковских резервов и от выданных кредитов.

Равновесие на рынке денег обеспечивается при спросе на деньги M^D, равном предложению денег M^S. Экономические субъекты нуждаются в деньгах для оплаты приобретаемых ими благ между моментами получения дохода, т.е. для совершения сделок купли – продажи. За рассматриваемый период, обычно год, производители могут получить за проданные блага такую сумму денег, которой располагают потребители, т.е. которая определяет денежный спрос, равный номинальному ВВП ω,

$$\omega = P_{\text{дн}} \bar{\Omega} \ , \tag{5}$$

где $P_{\text{дн}}$ – денежный дефлятор; $\bar{\Omega}$ – реальный потребительский спрос [1, с. 41].

Сколько раз в среднем за год предприниматели получат доход $M1$, равный сумме наличности и депозитов до востребования, такова будет скорость обращения денег μ в денежном кругообороте, $\mu = \omega / M1$. Спрос экономических субъектов на деньги M^D для сделок купли – продажи в течение года при скорости обращения денег μ определяется согласно (5) суммой наличности и депозитов до востребования:

$$M^D = M1 = P_{\text{дн}}\bar{\Omega} / \mu \ . \qquad (6)$$

Спрос на деньги M^D экономических субъектов для сделок купли – продажи с учетом альтернативных издержек упущенного дохода от хранения денег в банке определяется моделью Баумоля – Тобина как спрос на реальные денежные остатки [11, 12]. Издержки хранения денег определяются суммой издержек на банковские услуги по получению экономическими субъектами денег в банке для оплаты потребляемых благ и альтернативных издержек упущенного процентного дохода по депозитам до востребования D_1. Между двумя начислениями дохода с изымаемой из банка суммы X общая сумма издержек за год при потребительском спросе $\omega = P_{\text{дн}}\bar{\Omega}$ составит $З = P_{\text{дн}} b(P_{\text{дн}}\bar{\Omega} / X) + iX / 2$, где b – реальная стоимость снятия денег со счета в банке. Из условия равенства нулю производной, $З = P_{\text{дн}} b(P_{\text{дн}}\bar{\Omega} / X) + iX / 2$, определяется оптимальная сумма изымаемых из банка денег X, при которой максимален процентный доход от хранения денег в банке, $X = P_{\text{дн}}\sqrt{2b\bar{\Omega} / i}$. Отсюда определяется оптимальный спрос экономических субъектов на деньги для сделок купли – продажи $M^D = M1 = X / 2$ от нормы процента i:

$$M^D = M1 = X / 2 = P_{\text{дн}}\sqrt{0{,}5b\bar{\Omega} / i} \ . \qquad (7)$$

Имеется спекулятивный спрос на деньги финансового сектора за счет выданных банками кредитов под ценные бумаги заемщиков. Долгосрочные кредиты банков Ξ при наличии годового финансового резерва банковской системы страны, $\varepsilon > 0$, не будут согласно (1 – 3) больше кредитной базы $\bar{\Xi}$, $\Xi \le \bar{\Xi} = D - M_{\text{р}} - И_{\text{р}}$ при $\varepsilon > 0$. Равновесие банковской системы страны, определяемое наличием денежного резерва, $\varepsilon > 0$, возможно согласно (3) при кредитах банков Ξ, не больших разности денежной массы и денежной базы,

$$\Xi \le M3 - H \ . \qquad (8)$$

Увеличивая денежную базу через избыточные резервы банков, центральный банк сужает кредитную базу. Если коммерческими банками выданы кредиты Ξ больше имеющихся депозитов D, балансом банковской системы $\varepsilon = \bar{\Xi} - \Xi$ согласно (2) и (8) является денежный дефицит, $\varepsilon < 0$ при $\Xi > D$,

наступает кредитный кризис – вкладчикам не могут быть возвращены их депозиты, банки перестают кредитовать друг друга, единственным кредитором остается Центральный банк [13]. При выданных коммерческими банками кредитах Ξ получим сумму наличности и депозитов до востребования $M1^*$, минимально необходимую для сделок купли-продажи и возврата полученных кредитов, $M1^* + D_2 + D_3 \geq \Xi + H$. Подставив значение Ξ согласно (2), имеем $M1^* \geq M3 - \varepsilon - D_2 - D_3 = M1 - \varepsilon$. Отсюда согласно (4) определим сумму наличности и депозитов до востребования $M1^*$, минимально необходимую для сделок купли-продажи и возврата экономическими субъектами полученных кредитов Ξ [13]:

$$M1^* \geq mH - \varepsilon . \qquad (9)$$

При наличии резерва, $\varepsilon \geq 0$, спекулятивный спрос на деньги финансового сектора, функционирующего за счет выданных кредитов, не оказывает никакого влияния на необходимую согласно (4) сумму наличности и депозитов до востребования $M1^*$ для сделок купли - продажи, так как $M1 \equiv mH$ при $\varepsilon \geq 0$. Спрос на деньги при наличии денежного резерва банковской системы определяется только спросом на деньги для сделок купли – продажи на рынке благ и не зависит от выданных кредитов и от финансового сектора. Выход из кредитного кризиса возможен только за счет увеличения количества наличных денег в необходимом для возврата кредитов размере, т.е. только за счет инфляции.

Денежное равновесие обеспечивается равенством количества денег в годовом кругообороте $M1\mu$ денежному спросу (5) $P_{\text{дн}}\bar{\Omega}$ при денежном дефляторе не меньше единицы [1, 2, 13]:

$$M1\mu = P_{\text{дн}}\bar{\Omega} \text{ при } P_{\text{дн}} \geq 1 . \qquad (10)$$

При денежном дефляторе, меньшем единицы, не может быть удовлетворен реальный потребительский спрос без повышения стоимости денег, поэтому будет нарушено равновесие на рынке денег. Денежный дефлятор $P_{\text{дн}}$ измеряет стоимость денег в годовом кругообороте $M1\mu$ относительно реального совокупного спроса на блага $\bar{\Omega}$. Согласно (6) и (10) денежный дефлятор $P_{\text{дн}}$, изменяя пропорционально сумму наличности и депозитов до востребования, $M1$, не влияет на скорость обращения денег μ. Реальная стоимость денег тождественна отношению суммы наличности и депозитов до востребования к денежному дефлятору:

$$M^* \equiv M1 / P_{\text{дн}} . \qquad (11)$$

Согласно (10) и (11) скорость обращения денег при реальном совокупном спросе на блага $\bar{\Omega}$ определяется только реальной стоимостью

денег M^* и не зависит от суммы наличности и депозитов до востребования $M1$, $\mu \equiv \bar{\Omega} / M^*$.

Модель Боумоля – Тобина может быть использована в качестве теории равновесной нормы процента i при спросе согласно (6) на деньги $M^D = M1 = P_{\text{дн}} \bar{\Omega} / \mu$ в (7):

$$i = 0{,}5\mu^2 b / \bar{\Omega}. \tag{12}$$

Равновесная норма процента определяется скоростью обращения денег [1, 13]. Центральный банк, регулируя сумму наличности и депозитов до востребования $M1 = M0 + D_1$ и скорость обращения денег μ через норму процента i, обеспечивает необходимое согласно (5), (10) и (12) количество денег в обращении $M1\mu$. Установленные ЦБ норма процента i и нормированная стоимость снятия денег со счета в банке $\bar{b} = b / \bar{\Omega}$ определяют скорость обращения денег:

$$\mu = \sqrt{2i / \bar{b}}. \tag{13}$$

Депозиты до востребования D_1 являются величиной фиксированной, и изменить сумму $M1$ можно за счет эмитируемой ЦБ наличности $M0$, которая определяется инфляционной наличностью из-за таргетирования ЦБ инфляции и наличностью из-за действий на внутреннем валютном рынке. При поступлении валюты ЦБ эмитирует наличные деньги под предложение иностранной валюты. Валютная наличность $M0_{\text{вл}}$ определяется предложением и спросом на валюту в банковской системе: экспортом E, импортом Z, интервенциями ЦБ $E_{\text{цб}}$, прямыми иностранными инвестициями и трансфертами из-за границы $E_{\text{ит}}$, – и курсом λ (грн/долл) валюты на рынке, т.е.

$$M0_{\text{вл}} = \lambda(E - Z + E_{\text{цб}} + E_{\text{ит}}). \tag{14}$$

Инфляционная наличность $M0_{\text{и}}$ равна разности эмитируемой ЦБ наличности $M0$ и валютной наличности $M0_{\text{вл}}$:

$$M0_{\text{и}} = M0 - M0_{\text{вл}}. \tag{15}$$

2. Условия равновесия экономики

В рассматриваемом году t на рынке благ отношение ВВП номинального ω_t к ВВП реальному Ω_t определяет дефлятор ВВП, т.е. индекс изменения уровня цен,

$$P_t = \omega_t / \Omega_t. \tag{16}$$

Изменение в году t уровня цен, измеряемого дефлятором ВВП, относительно уровня цен предыдущего года t - 1, принимаемого за единицу, называют инфляцией [1, 2, 13, 14],

$$p = P - 1. \tag{17}$$

Количество денег в годовом кругообороте $M1\mu$ согласно (5), (10) и (14) определяет и ограничивает денежный потребительский спрос на рынке благ, т.е. номинальный ВВП, и определяет равновесие равенством спроса и предложения:

$$\omega = P_{\text{дн}}\bar{\Omega} = P\Omega = M1\mu \ . \tag{18}$$

Отсюда согласно тождеству рынка денег (11) выразится тождество $\bar{\Omega} \equiv P\Omega M^* / M1$, и согласно (12) получим тождество количественной теории денег $\mu \equiv P\Omega / M1$ [13, 14].

На рынке труда страны взаимодействием спроса на труд N^D и предложения труда N^S определяется количество N^S работающих в экономике. Реальное предложение благ в рассматриваемом году, т.е. реальный ВВП, можно аппроксимировать функцией загруженных в сфере производства капитала стоимостью K и количества работающих в производстве $\Pi = N\xi$ при коэффициенте ξ от занятого населения в экономике:

$$\Omega = \sigma Q = \sigma (N\xi)^{1/\ln k_0} K^{1-1/\ln k_0}, \tag{19}$$

где Q – реальный совокупный общественный продукт, σ – коэффициент материалоемкости производства, $k_0 = K / \Pi_0$ – равновесная капиталоемкость труда, Π_0 – количество работающих в сфере производства при полной занятости населения в экономике, $1/\ln k_0$ – коэффициент технологии производства при постоянстве отдачи от масштаба [1, 2, 13, 15].

При равенстве количества работающих в экономике количеству N_0 полной занятости, $N = N_0$, обеспечивается равновесие на рынке труда с равновесной ставкой реальной зарплаты $w_0 = k_0 / (e \ln k_0)$, где e – основание натурального логарифма. Реальный потребительский спрос измеряется реальным ВВП при полной занятости населения в экономике, $N = N_0$, т.е. согласно (19) получим [1, 2, 13, 15]:

$$\bar{\Omega} = \Omega(N_0) = \sigma K e^{-1}. \tag{20}$$

Подставив в уравнение (10) равновесия на рынке денег величину $\bar{\Omega}$, получим уравнение равновесия на рынке денег $M1\mu = P_{\text{дн}}\sigma K e^{-1}$. Отсюда

согласно (11) скорость обращения денег при их реальной стоимости $M^* \equiv M1/P_{\text{дн}}$ пропорциональна стоимости загруженного в производстве капитала,

$$\mu = \sigma K / (M^* e). \tag{21}$$

Скорость обращения денег пропорциональна произведению стоимости загруженного в производстве капитала и коэффициента материалоемкости производства и не зависит от количества денег в обращении и от денежного дефлятора.

Отношением реального ВВП Ω_t года t к номинальному ВВП ω_{t-1} предыдущего года t–1 измеряется согласно (16) изменение δ_t реального ВВП в ценах предыдущего года:

$$\delta_t = \Omega_t / (P_{t\text{-}1}\Omega_{t-1}) - 1. \tag{22}$$

В процессе народнохозяйственного кругооборота равновесие на рынке благ обеспечивается равенством стоимости проданных предпринимателями благ $P\Omega$ и стоимости купленных благ ω всеми экономическими субъектами: сектором домашних хозяйств C; предпринимателями $R_{\text{пр}}$; государством $J_{\text{г}}$ и заграницей $E - Z$,

$$\omega = P\Omega = C + R_{\text{рг}} + J_{\text{s}} + E - Z \text{ , при } P \geq 1. \tag{23}$$

Условием равновесия на рынке благ является наличие инфляции (17) [1, 2, 13–16]. Инвестиционный спрос сферы производства на капитал определяется амортизацией A загруженного капитала и чистыми инвестициями $J_{\text{ч}}$, $R_{\text{пр}} = A + J_{\text{ч}}$. Чистые инвестиции являются частью чистой прибыли Ч производства с загруженного капитала, другая часть $\text{И}_{\text{дх}}$ является доходом домашних хозяйств с капитала, $\text{Ч} = J_{\text{ч}} + \text{И}_{\text{дх}}$. Чистая прибыль, по определению, $\text{Ч} = Y - \text{Н}_{\text{пр}} - W_{\text{пр}}$, где $Y = \omega - A$– доход производства, $\text{Н}_{\text{пр}}$ – налог с дохода производства, $W_{\text{пр}} = W\text{П}$ – зарплата в сфере производства, W – номинальная ставка зарплаты. Основным источником инвестиций в экономике являются амортизационные отчисления $A = P\theta K$ с загруженного в производстве капитала при норме амортизации θ. Инвестиции, бóльшие амортизации, обеспечиваются чистыми инвестициями. Источником роста реального ВВП, увеличения производственного капитала и роста потребительского спроса является получаемая производством прибыль π с капитала. Часть получаемой производством прибыли изымается государством в виде налога $\text{Н}_{\text{пр}}$ с дохода производства, $\pi = \text{Ч} + \text{Н}_{\text{пр}}$, и расходуется на содержание непроизводственной сферы, на пенсионное обеспечение и на выплаты по обслуживанию долгов. За счет получаемой в сфере производства прибыли, с одной стороны, проводятся инвестиции $J_{\text{ч}}$,

а с другой стороны, растут потребительский спрос домашних хозяйств C и потребительский спрос государства $J_{\text{г}}$, вызывающие необходимость увеличения прибыли для обеспечения инвестиций и в будущем. Обязательным условием проведения инвестиций является рост потребительского спроса. Реальная чистая прибыль производства определяется функцией:

$$\text{ч} = \text{Ч} / P = (1-\chi)(\Omega - \theta K) - w\Pi, \tag{24}$$

где $w = W / P$ – ставка реальной зарплаты. Отсюда при выплаченной в сфере производства реальной зарплате $w = W / P$ всегда существует норма амортизации простого воспроизводства капитала $\bar{\theta} = [\Omega - w\Pi(1-\chi)] / K$, при которой чистая прибыль равна нулю. Выразив $w\Pi$, получим согласно (22) закон реальной чистой прибыли [1, 2, 16]:

$$\text{ч} = K(1-\chi)(\bar{\theta} - \theta) \ . \tag{25}$$

Существует оптимальная ставка налога на доход производства χ_{opt}, при которой остающаяся в производстве прибыль Ч^* после выплаты налогов равна выплаченным налогам $\text{Н}^*_{\text{пр}}$, т.е. $\text{Н}^*_{\text{пр}} = \chi_{opt} Y = \text{Ч}^*$, и обеспечивается стабильный от года к году рост производства и дохода государственного бюджета [17]. Согласно полученным в [17] результатам, в Украине $\chi_{opt} \approx 1/3$. При выплаченной зарплате, равной третьей части дохода, определяется практическое правило оптимального налогообложения производства, $\text{Н}^*_{\text{пр}} = \text{Ч}^* = Y/3$ при $W\Pi = Y/3$.

При норме амортизации простого воспроизводства, $\theta = \bar{\theta}$, и инвестициях, меньших амортизации, $R_{\text{пр}} < A$, возможно только суженное воспроизводство капитала, т.е. происходит проедание капитала. Границей нормы амортизации является норма выбытия капитала из эксплуатации $\theta_{\text{выб}}$, определяемая его физическим износом и моральным старением. В пределах $\theta_{\text{выб}} < \theta < \bar{\theta}$ осуществляется ускоренная амортизация капитала. Норма амортизации, меньшая нормы выбытия капитала, $\theta < \theta_{\text{выб}}$, уменьшает имеющийся капитал на величину недоамортизации, $\Delta = (\theta_{\text{выб}} - \theta)KP$, поэтому получим функцию стоимости имеющегося в производстве капитала:

$$K_{\text{пр}t} = P_{t-1} K_{\text{пр}t-1} + J_{\text{ч}t-1} - \Delta_{t-1}. \tag{26}$$

Чистые инвестиции должны регулироваться государством нормой ψ с чистой прибыли (23) через поощрительное налогообложение, $J_{\text{ч}} = \psi K P(1-\chi)(\bar{\theta} - \theta)$, а доход домашних хозяйств с капитала определится функцией $\text{И}_{\text{дх}} = (1-\psi)KP(1-\chi)(\bar{\theta} - \theta)$.

В реальной экономике имеющийся в сфере производства капитал загружается не полностью, а в зависимости от рыночной конъюнктуры потребительского спроса пропорционально коэффициенту загрузки υ, $K = \upsilon K_{\text{пр}}$ [1–3, 14, 16–18]. Рост загруженного в производстве капитала вызывает согласно (21) увеличение количества денег в годовом кругообороте. Предприниматели регулируют объемы производства в году t по объему продаж в предыдущие годы изменением количества работающих Π_t относительно количества работавших в предыдущем году Π_{t-1} по рыночной конъюнктуре $\Re_t$, $\Pi_t = \Re_t \Pi_{t-1}$. При свободной конкуренции и наличии незагруженного капитала функция рыночной конъюнктуры определена в [1–3, 13, 15–17]:

$$\Re_t = \begin{cases} 1 + \delta_{t-1} - \delta_{t-2}, \\ P_{t-1} \quad \text{при } P_{t-1} < 0. \end{cases} \tag{27}$$

Конъюнктурное изменение предпринимателями количества работающих приводит к пропорциональному изменению загрузки капитала, $\upsilon_t = \upsilon_{t-1} \Re_t$.

Функционирование экономики обеспечивают рынки денег, благ и труда. При равновесии на всех трех рынках существует общее рыночное равновесие. Имеется рыночное равновесие при равновесии на рынках денег и благ и при наличии безработицы на рынке труда [1–3].

Фактическая безработица равна разности количества работающих при полной занятости населения и фактического количества работающих,

$$f_{\text{ф}} = N_0 - N \ . \tag{28}$$

Отсюда уровень безработицы определяется отношением фактической безработицы к количеству работающих N_0 при полной занятости населения в экономике,

$$\varphi = f_{\text{ф}} / N_0 = (N_0 - N) / N_0 \ . \tag{29}$$

Равновесие экономики определяется ростом реального ВВП, $\delta_t > 0$, спад реального ВВП, т.е. $\delta_t < 0$, означает нарушение равновесия экономики, экономический кризис. Рост реального ВВП, $\delta_t > 0$, обеспечивается согласно (19) и (26) ростом загруженного в производстве капитала $K = \upsilon K_{\text{пр}}$. Рост загруженного в производстве капитала возможен при сохранении или улучшении рыночной конъюнктуры согласно (25), $\Re_t > 1$ и $\upsilon_t \geq \upsilon_{t-1} \Re_t$; расширенном воспроизводстве имеющегося в сфере производства капитала согласно (26). Отсюда, необходимыми условиями равновесия экономики являются расширенное воспроизводство загруженного в сфере производства капитала, $K_t > P_{t-1} K_{t-1}$, и равновесие согласно (23) на рынке благ, $P \geq 1$.

3. Модель регулирования равновесия экономики

При расширенном воспроизводстве загруженного в сфере производства капитала, $K_t > P_{t-1}K_{t-1}$, и наличии безработицы системой уравнений (10), (18) и (26) описывается саморегулирование равновесия экономики [19, 20]:

$$M1\mu = P_{\text{дн}}\bar{\Omega}\ ;\ P\Omega = P_{\text{дн}}\bar{\Omega}\ ;\ f_{\text{ф}} = N_0 - N\ ;\ \text{при}\ K_t > P_{t-1}K_{t-1}\ ,\ P \geq 1. \qquad (30)$$

Равновесие экономики, саморегулирующееся на рынке благ по величине дефлятора ВВП, не меньшей единицы, является устойчивым, т.е. стабильным. Необходимыми условиями стабильного равновесия экономики являются дефлятор ВВП, не меньший единицы, $P \geq 1$, и наличие безработицы, $f_{\text{ф}} > 0$. Таким состоянием характеризуются экономики высокоразвитых стран после начавшегося в 2008 г. мирового кризиса. При отсутствии безработицы, $N > N_0$, занятость населения в экономике является избыточной, поэтому согласно (28) и (29) безработица и уровень безработицы отрицательны, $f_{\text{ф}} < 0$, $\varphi < 0$ при $N > N_0$. Избыточная занятость населения в экономике приводит согласно (19) к реальному предложению благ, бóльшему реального потребительского спроса (20), $\Omega > \bar{\Omega}$ при $N > N_0$, поэтому может быть нарушено равновесие экономики из-за перепроизводства благ. Для обеспечения равновесия на рынке благ и равновесия экономики при $N > N_0$, необходимо Центральному банку предложить количество денег в обороте $M1\mu$, бóльшее реального предложения благ Ω, с обесцениванием денег пропорционально дефлятору ВВП P, $M1\mu = P\Omega$ при $P > 1$. Уравновешенное Центральным банком нестабильное равновесие экономики описывается системой уравнений:

$$M1\mu = P\Omega\ ;\ P\Omega = P_{\text{дн}}\bar{\Omega}\ ;\ f_{\text{ф}} = N_0 - N\ ;\ \text{при}\ K_t > P_{t-1}K_{t-1}\ ,\ P \geq 1. \qquad (31)$$

Таким состоянием характеризовались экономики высокоразвитых стран и, в первую очередь, экономика США до начавшегося в 2008 г. мирового кризиса.

Из условия (18) неизбежного равенства стоимости купленных благ всеми экономическими субъектами и стоимости проданных предпринимателями благ, $P\Omega = P_{\text{дн}}\bar{\Omega}$, выражается производственный дефлятор отношением реального потребительского спроса $\bar{\Omega}$ к реальному предложению благ Ω, откуда согласно (19) получим:

$$P_{\text{пр}} = \bar{\Omega} / \Omega = \left(N_0 / N\right)^{1/\ln k_0} = (1-\varphi)^{-1/\ln k_0}. \qquad (32)$$

Производственный дефлятор $P_{\text{пр}}$ является инструментом ограничения предложения благ предпринимателями для увеличения прибыли с капитала через сокращение количества работающих и одной из причин роста уровня цен (инфляции). Величина производственного дефлятора однозначно

определяет фактическую безработицу $f_{\text{ф}}$ и уровень фактической безработицы φ как результат конъюнктурного регулирования в экономике количества работающих,

$$f_{\text{ф}} = N_0(1 - P_{\text{пр}}^{-\ln k_0}); \varphi = 1 - P_{\text{пр}}^{-\ln k_0} \ . \tag{33}$$

Инфляционным саморегулированием равновесия на рынке благ определяется согласно (18) равенство дефлятора ВВП P произведению дефляторов денежного $P_{\text{дн}}$ и производственного $P_{\text{пр}}$,

$$P = P_{\text{дн}} P_{\text{пр}} . \tag{34}$$

Дефлятор ВВП, или согласно (17) инфляция $p = P–1$, как результат инфляционного саморегулирования равновесия на рынке благ и регулирования Центральным банком количества денег в обращении, является функцией денежного дефлятора и уровня безработицы:

$$P = P_{\text{дн}}(1 - \varphi)^{-1/\ln k_0} . \tag{35}$$

Производственный дефлятор, при наличии безработицы, всегда согласно (32) больше единицы. Поэтому при денежном дефляторе, меньшем единицы, т.е. денежной дефляции из-за нарушения равновесия на рынке денег (10), и наличии безработицы согласно (28) возможно стабильное равновесие экономики (30), $P = P_{\text{дн}} P_{\text{пр}} \geq 1$, с незначительной инфляцией. Стабильное равновесие экономики (30) с нулевой инфляцией, $P = 1$, возможно согласно (34) и (35) при предельном денежном дефляторе, являющемся обратной величиной производственного дефлятора [20, 21],

$$\overline{P}_{\text{дн}} = (1 - \varphi)^{1/\ln k_0} . \tag{36}$$

При расширенном воспроизводстве загруженного в сфере производства капитала и нарушенном равновесии на рынке денег величиной денежного дефлятора, меньшей единицы и большей предельного значения, $1 > P_{\text{дн}} \geq (1 - \varphi)^{1/\ln k_0}$, обеспечивается сколь угодно долго саморегулирующееся равновесие экономики (30) с незначительным ростом потребительского спроса и реального ВВП, называемое депрессией [20, 21]. Для выхода из депрессии на стабильный рост потребительского спроса и реального ВВП необходимо количество денег в обороте с денежным дефлятором, бóльшим единицы. При денежном дефляторе, меньшем предельного $P_{\text{дн}} < (1 - \varphi)^{1/\ln k_0}$, происходит дефляция и углубление кризиса со спадом реального ВВП, на грани которых балансируют экономики высокоразвитых стран после начала в 2008 г. кризиса. При нестабильном равновесии экономики (31) производственный дефлятор согласно (32) всегда меньше единицы, а денежный дефлятор согласно (34) всегда больше единицы. Нестабильное равновесие экономики (31) с нулевой инфляцией, $P = 1$, возможно при

предельном денежном дефляторе, являющемся обратной величиной дефлятора производственного согласно (36). При избыточной занятости населения в экономике, расширенном воспроизводстве загруженного в сфере производства капитала и денежном дефляторе, бóльшем предельного, $P_{\text{дн}} > (1-\varphi)^{1/\ln k_0}$, обеспечивается сколь угодно долго рост реального ВВП. А при денежном дефляторе, меньшем предельного $P_{\text{дн}} < (1-\varphi)^{1/\ln k_0}$, дефлятор ВВП становится меньше единицы, происходит дефляция со спадом реального ВВП, наступает кризис перепроизводства.

Графики зависимости от уровня безработицы φ (в процентах) предельных значений денежной инфляции $\overline{p}_{\text{дн}} = \overline{P}_{\text{дн}} - 1 = (1-\varphi)^{1/\ln k_0} - 1$ (в процентах) показаны на рис. 1 при коэффициентах технологии производства $1/\ln k_0 =$ 0,1; 0,075; 0,0666 – определяемых соответственно равновесными ставками реальной зарплаты в высокоразвитых странах $w_0 = k_0 / (e \ln k_0) =$ 810; 19877; 8017 условных единиц (у.е.). Графики показывают, что при уровне безработицы 8%-10% значение денежной дефляции не меньше 1% и при уровне безработицы 5% денежная дефляция не меньше 0,5%. Инфляция 0,25% в ЕС и Японии при безработице больше 6% определяет наличие денежной дефляции больше 0,2%.

Изменение дефлятора ВВП можно выразить в зависимости от ставки зарплаты W. Номинальная ставка зарплаты W_t текущего года t может быть определена только системой национального счетоводства в результате бухгалтерского учета по итогам года через дефлятор ВВП P_t и ставку реальной зарплаты w_t, т.е. $W_t = P_t w_t$. При коэффициенте изменения тарифной ставки зарплаты на начало текущего года t по сравнению с предыдущим, $w_{\text{д}\,t} = z_t w_{\text{д}\,t-1}$, определяется реальная ставка зарплаты $w_t = z_t W_{t-1}$ [1, 22]. Отсюда выражена в [22] согласно (33) существующая в экономике зависимость темпа изменения ставки зарплаты $\breve{W}_t = (W_t - W_{t-1}) / W_{t-1}$ от уровня безработицы $\breve{W} = zP_{\text{дн}}(1-\varphi)^{-1/\ln k_0} - 1$. При предельных значениях денежного дефлятора и равном единице тарифном коэффициенте темп изменения ставки зарплаты равен нулю, т.е. при безинфляционном потребительском спросе ставка зарплаты постоянна. При z=1 и $P_{\text{дн}}$ =1 существует зависимость темпа изменения ставки зарплаты $\breve{W}$ от уровня безработицы $\breve{W} = (1-\varphi)^{-1/\ln k_0} - 1$, график которой при равновесной ставке зарплаты $w_0 = 19877$ у.е. показан на рис. 1. Из графика видно, что темп роста ставки зарплаты всегда увеличивается с ростом уровня безработицы.

В экономической теории до сих пор используется для измерения макроэкономических показателей ошибочная зависимость темпа роста ставки зарплаты от уровня безработицы, описываемая эмпирической кривой Филлипса $\breve{W}_{Fl} = -0,9 + 9,638\varphi^{-1,394}$ [22, 23]. График кривой Филлипса на рис. 1 показывает ошибочность утверждений кейнсианской теории о снижении ставки зарплаты предпринимателями с ростом уровня безработицы [1, 13, 21]. Ошибочность утверждений о снижении ставки зарплаты с ростом уровня безработицы создала ошибочное представление о снижении инфляции

с ростом уровня безработицы, так как $\breve{W} = p$ при z = 1 [21, с. 141] и $p_{Fl} = \breve{W}_{Fl} = -0,9 + 9,638\varphi^{-1,394}$ при z = 1.

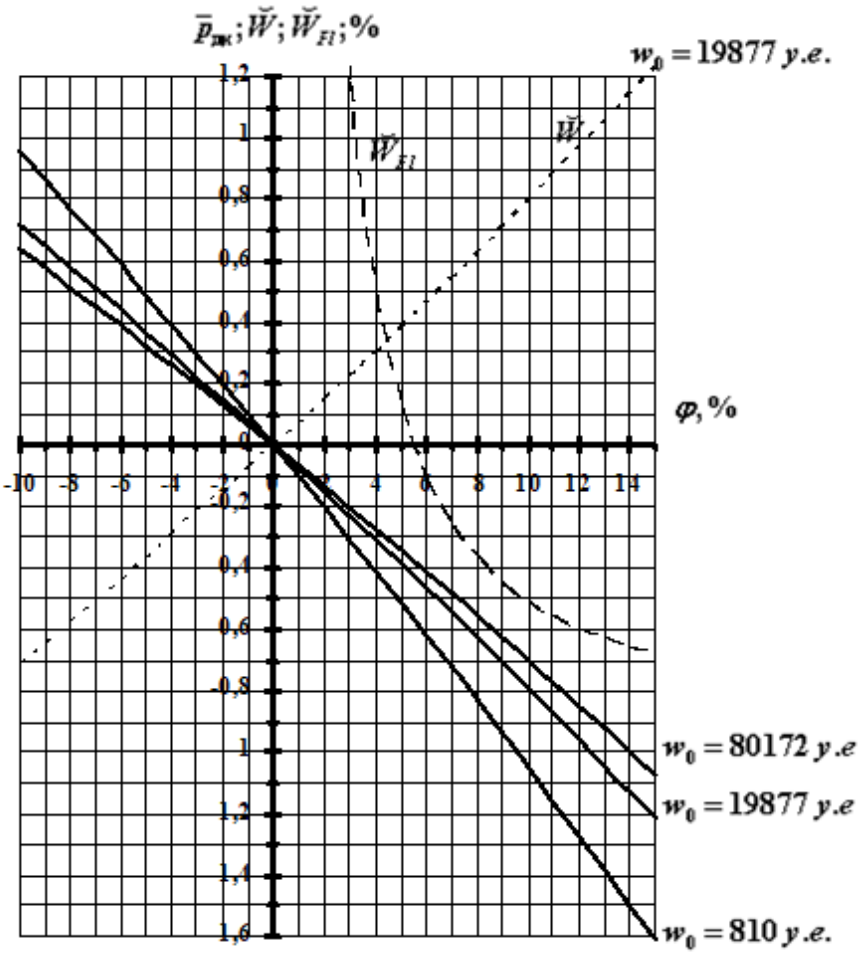

Рисунок 1 – Зависимость предельных значений денежной инфляции и темпа роста ставки зарплаты от уровня безработицы

Однако центральные банки высокоразвитых стран применяют прогнозные модели макроэкономики, используя ошибочную кривую Филлипса в поисках несуществующего «оптимального сочетания» инфляции и безработицы [24, 25]. Рост безработицы всегда вызывает согласно (35) рост инфляции. Ошибочные прогнозные модели центральных банков высокоразвитых стран не позволяют около десяти лет достичь в их экономиках уровня инфляции в два процента без увеличения наличности в обороте. Эти модели не позволяют правильно определить необходимый размер наличности для обеспечения инфляции в два процента. Кроме того, при ставке процента меньше одного процента ее регулирующая функция скорости обращения денег исчезает. Стоимость снятия денег со счетов в банках $\bar{b} = b / \bar{\Omega} = 0,01$ и норма процента $i = 0,01$ определяют скорость

обращения денег $\mu = \sqrt{2}$. Согласно (13) при ставке процента $i = 0{,}005$ и нормированной стоимости снятия денег со счетов в банках $b / \bar{\Omega} = 0{,}01$ скорость обращения денег равна единице и регулирование количества денег в обращении ставкой процента невозможно.

4. Модель таргетирования Центральным банком инфляции

Дискретная динамическая детерминированная модель функционирования открытой экономики [17–20, 26], описываемая системой уравнений (10), (13 – 20), (22), (26) – (28), (30), (32), (34), (35):

$$\left\{\begin{array}{l} M1\mu = P_{\text{дн}}\bar{\Omega};\ P\Omega = P_{\text{дн}}\bar{\Omega};\ f = N_0 - N;\ P_{\text{дн}} = P / P_{\text{пр}}; \\ K_{\text{пр}t} = P_{t-1}K_{\text{пр}t-1} + J_{\text{ч}t-1} - \Delta_{t-1};\ K = \upsilon K_{\text{пр}}; \\ \Omega = \sigma (N\xi)^{1/\ln k_0} K^{1-1/\ln k_0};\ \bar{\Omega} = \sigma K e^{-1};\ P_{\text{пр}} = \bar{\Omega} / \Omega; \\ \mu = \sqrt{2i / \bar{b}};\ M1 = \omega / \mu;\ M0 = M1\beta / (1+\beta); \\ M0_{\text{вл}} = \lambda(E - Z + E_{\text{цб}} + E_{\text{ит}});\ M0_{\text{и}} = M0 - M0_{\text{вл}}; \\ \delta_t = \Omega_t / \omega_{t-1} - 1;\ \Re_t = \delta_{t-1} - \delta_{t-2} + 1;\ \Pi_t = \Re_t \Pi_{t-1};\ \upsilon_t = \Re_t \upsilon_{t-1} \end{array}\right\}, \qquad (37)$$

позволяет определить макроэкономические показатели страны в среднесрочной перспективе. В этой модели осуществляется рыночное саморегулирование инфляции; государство регулирует воспроизводство имеющегося в производстве капитала, налоги и бюджет; Центральный банк регулирует количество обращающихся денег по ставке процента и сумме наличности и депозитов до востребования через таргетируемую инфляцию и обеспечивает превышение на внутреннем валютном рынке при имеющемся курсе валюты предложения валюты над спросом на валюту. Моделирование макроэкономических показателей возможно при прогнозируемых: численности населения T; экспорте E, импорте Z, трансфертах $E_{\text{ит}}$, курсе валюты λ, – по заданным ЦБ: инфляции $p = P - 1$, нормированной стоимости $\bar{b}$ снятия денег со счетов в банках, ставке процента i, отношению β наличности к депозитам до востребования, – при известных: материалоемкости производства σ, коэффициенте работающих в производстве ξ, амортизации A, чистых инвестициях $J_{\text{ч}}$ и недоамортизации Δ капитала. При моделировании могут быть определены в рассматриваемом t периоде при известных в предыдущем $t-1$ периоде: стоимость имеющегося в производстве капитала $K_{\text{пр}}$ согласно (26), рыночная конъюнктура $\Re$ согласно (27), количество работающих в сфере производства $\Pi_t = \Re_t \Pi_{t-1}$, коэффициент загрузки капитала в сфере производства $\upsilon_t = \upsilon_{t-1}\Re_t$, стоимость загруженного в сфере производства капитала $K = \upsilon K_{\text{пр}}$, реальный потребительский спрос $\bar{\Omega} = \sigma K e^{-1}$ согласно (20), количество работающих в экономике $N = \Pi / \xi$, равновесное количество работающих в экономике $N_0 = 0{,}46T$ и в производстве $\Pi_0 = \xi N_0$,

уровень безработицы φ согласно (29), коэффициент технологии производства $1/\ln k_0 = \ln(K/\Pi_0)^{-1}$, реальный ВВП Ω согласно (19), изменение δ реального ВВП согласно (22), номинальный ВВП ω согласно (16), денежный дефлятор $P_{\text{дн}} = P/P_{\text{пр}}$ согласно (34) и (32), скорость обращения денег μ согласно (13), сумма наличности и депозитов до востребования $M1$ согласно (18), количество наличных денег $M0 = M1\beta/(1+\beta)$ согласно (4), валютная наличность $M0_{\text{вл}}$ согласно (14), инфляционная наличность $M0_{\text{и}}$ согласно (15), регулируемые государством чистые инвестиции $J_{\text{ч}}$ и недоамортизация капитала Δ.

В таблице 1 определены возможные макроэкономические показатели Украины в 2019–2025 гг. по статистическим сведениям 2017 и 2018 годов согласно [27–31]. При моделировании приняты сложившиеся в предыдущие годы: коэффициент работающих в производстве $\xi = 0,75$, нормированная стоимость снятия денег со счета в банке $\bar{b} = 0,01$, амортизация $A = 0,02K$, чистые инвестиции по годам $J_{\text{ч}} = 0,2; 0,24; 0,27; 0,3(\omega - 0,1K)$, недоамортизация капитала $\Delta = 0,005K$, коэффициент материалоемкости производства $\sigma = 0,45$.

Таргетирование Национальным банком инфляции в 2020 году через дефлятор ВВП $P = 1,03$ и снижение ставки процента до 11,5% потребовало увеличить инфляционную наличность с $M0_{\text{и}} = 58,94$ млрд грн в 2019 году до $M0_{\text{и}} = 213,4$ млрд грн, а при дефляторе ВВП $P = 1,02$ и снижение ставки процента до 9% в 2021 году – до $M0_{\text{и}} = 381,59$ млрд грн. Снижение ставки процента сокращает скорость обращения денег и для сохранения их количества в обороте требует в разы увеличить наличность, которая позволяет еще и снизить инфляцию. В рассмотренном примере при существующем уровне безработицы возможна денежная дефляция 0,99 в 2022 году и 0,996 в 2023 году при инфляции $p = P - 1$ соответственно 0,01 и 0,015. По результатам в таблице видно, что при инфляции в два процента, $P = 1,02$, нет денежной дефляции, и причиной инфляции в экономиках ЕС и Японии, меньшей двух процентов, является неправильное определение необходимой инфляционной наличности $M0_{\text{и}}$ по применяемым центральными банками моделям прогнозирования.

При расширенном воспроизводстве загруженного в сфере производства капитала и наличии безработицы равновесие экономики, саморегулирующееся на рынке благ по дефлятору ВВП, т.е. по инфляции, является стабильным по росту реального ВВП. Дефлятор ВВП определяется произведением денежного и производственного дефляторов. При наличии безработицы производственный дефлятор всегда больше единицы.

Таблица 1 – Моделирование макропоказателей экономики Украины в 2019–2025 годы

Годы	2017	2018	2019	2020	2021	2022	2023	2024	2025
Показатели	Исходные сведения по годам								
Населения T, млн	42,3	42,1	41,9	41,7	41,5	41,3	41,1	40,9	40,7
Дефлятор ВВП P	1,191	1,123	1,094	1,03	1,02	1,01	1,015	1,02	1,02
Экспорт E, млрд \$	50,9	54,42	60,79	60,00	58,0	57,00	58,00	59,00	60,00
Импорт Z, млрд \$	59,02	61,81	66,18	68,00	65,0	65,00	64.00	63,00	63,00
$E_{\text{ит}}$, млрд \$	17,00	17,00	16,00	16,50	16,0	17,00	18,00	17,00	17,00
Ставка процента i, %	15	13,7	14	11,5	9,0	7,0	5,0	5,0	5,0
β	1,3	1,222	1,25	1,2	1,22	1,23	1,25	1,26	1,25
$E_{\text{цб}}$, млрд \$	1,45	1,37	1,72	1,88	1,5	1,55	1,5	1,4	1,2
λ, грн/\$	26,8	27	26,5	30,0	31,0	32,0	33,0	34,0	33,0
Показатели	Результаты моделирования по годам								
$K_{\text{пр}}$, млрд грн	19155	22344	25386	28058	29 250	30 315	30 950	31756	32756
Конъюнктура $\Re_{\text{р}}$	1,02	1,011	0,997	0,992	0,98	0,987	0,992	1,021	1,03
П, млн. чел.	11,23	11,35	11,32	11,23	11,0	10,87	10,78	11,00	11,33
Загрузки υ	0,81	0,82	0,818	0,812	0,8	0,77	0,764	0,78	0,8
K, млрд грн	15 515	18 322	20 766	22 783	23 276	23 343	23 646	24 763	26318
N, млн чел.	14,97	15,14	15,03	14,98	14,68	14,49	14, 37	14,67	15,11
N_0, млн чел.	19,47	19,37	19,27	19,18	19,1	19,00	18,906	18,81	18,77
φ, %	23,05	21,8	22,00	23,45	23,1	23,72	24,19	22,03	19,29
$1/\ln k_0$	0,0721	0,0712	0,0705	0,07	0,0699	0,0699	0,0698	0,0696	0,0692
Ω, млрд грн	2 519	2 940	3 380	3 710	3784,4	3791,	3840,2	4026,	4295
$\bar{\Omega}$, млрд грн	2 568	2 993	3 438	3 772	3853,2	3954,3	3914,51	4099,4	4356,8
Скорость денег μ	5,48	5,2	5,29	3,39	3,0	2,65	2,236	2,236	2,236
δ, %	3,5	3,16	2,39	0,3	- 0,95	- 1,78	0,29	3,3	4,59
$P_{\text{пр}}$	1,0196	1,018	1,017	1,0167	1,0182	1,0193	1,0193	1,0182	1,0144
$P_{\text{дн}}$	1,168	1,103	1,076	1,061	1,002	0,99	0,996	1,0018	1,0055
ϖ, млрд грн	3 000	3 302	3 699	3 821	3860	3829	3897,6	4106,6	4381
$J_{\text{ч}}$, млрд грн	259, 7	323,3	389,45	464,6	467,46	448,5	459,6	489,2	524,7
Δ, млрд грн	77,576	91,610	103,83	113,9	116,4	116,7	118,2	123,8	131,6
$M1$, млрд грн	545,52	634,95	694,22	1127,1	1286,7	1444,9	1743,1	1836	1959
$M0$, млрд грн	308,34	349,19	385,68	614,8	707,09	797	968,4	1024	1089
$M0_{\text{вл}}$, млрд грн	276,84	296,46	326,75	401,4	325,5	337,6	445,5	489,6	501,6
$M0_{\text{и}}$, млрд грн	23,16	52,73	58,94	213,4	381,59	459,4	522,9	534,4	587,4

При денежном дефляторе, меньшем единицы, и наличии безработицы возможно сколь угодно долго стабильное равновесие экономики с незначительной инфляцией и низким ростом реального ВВП, называемое депрессией.

Безынфляционное равновесие экономики возможно при денежном дефляторе, равном обратной величине производственного дефлятора.

Наличие денежной дефляции не позволяет расти потребительскому спросу и реальному ВВП, т.е. не позволяет выйти из депрессии. Центральные банки высокоразвитых стран, обеспечивая имеющийся курс валюты и стремясь к его снижению, т.е. к повышению стоимости денег, вынуждены сохранять денежную дефляцию, сдерживая рост инфляции, и поддерживают депрессию своих экономик. Без увеличения инфляции невозможно выйти из депрессии.

Заключение

Проводимая в течение 2009–2018 годов центральными банками высокоразвитых стран политика выхода из кредитного кризиса через выкуп токсичних активов с балансов банков, резкое наращивание денежных баз и снижение до нуля процентных ставок при сохранении денежной дефляции привела к резкому росту спекулятивного финансового сектора и к депрессии реального сектора экономики. Наращивая денежную базу через избыточные резервы банков, защищающие их от банкротства, центральные банки сужают кредитную базу, т.е. углубляют кредитный кризис. При ставке процента меньше одного процента ее регулирующая функция скорости обращения денег исчезает.

Центральные банки высокоразвитых стран пользуются прогнозными моделями макроэкономики, основанными на ошибочной кривой Филлипса, в поисках несуществующего «оптимального сочетания» инфляции и безработицы. Ошибочные прогнозные модели центральных банков высокоразвитых стран не позволяют около десяти лет достичь в их экономиках уровня инфляции в два процента. Эти модели не позволяют правильно определить необходимый размер инфляционной наличности для обеспечения инфляции в два процента. Моделирование показало, что нет денежной дефляции при правильном определении необходимой наличности в обороте, обеспечивающей инфляцию в два процента.

Сдерживание инфляции центральными банками высокоразвитых стран, не большей двух процентов, при использовании существующих прогнозных моделей определения необходимой наличности в обороте затянет выход из депрессии еще на многие годы. Необходимо согласиться с инфляцией в три-пять процентов, исключающей денежную дефляцию, и ускорить выход из депрессии к стабильному росту реального ВВП.

ЛИТЕРАТУРА

1. Дунаев Б.Б. Благосостояние – труд, капитал и деньги: Основы теории воспроизводства. – 2-е издание дополненное. – Киев: Интердрук, 2013. – 231 с.
2. Дунаев Б.Б. Макроэкономическое государственное регулирование и саморегулирование рыночного равновесия // Кибернетика и системный анализ. – 2006. – № 5. – С. 55–68.
3. Дунаев Б.Б., Кириленко Л.В. Дефляционное регулирование рыночного равновесия // Кибернетика и системный анализ. 2018. № 2. С. 95–108.
4. "Global monitoring of shadow bankinga – 2013". http://www.group-global.org/ru/lecture/view/7207
5. World Economic Outlook: Too Slow for Too Long (2016). Washington, DC: IMF. April 2016. p. 168-177.

6. Monetary policy decisions (2017). ECB. Press Release. 19 January 2017. URL: http://www.ecb.europa.eu/press/pr/date/2017/html/pr170119.en.html.
7. ECB announces expanded asset purchase programme (2015). ECB. Press Release. 22 January 2015. URL: https://www.ecb.europa.eu/press/pr/date/2015/html/ pr150122_1.en.html.
8. Draghi M. (2017). Introductory statement to the press conference (with Q&A). 19 January 2017. URL: http://www.ecb.europa.eu/press/pressconf/2017 /html/is170119.en.html#qa
9. The great debate: Inflation, deflation and the implications for financial management. Article Carl Steidtmann, Dan Latimore, Elisabeth Denison. January 01. 2011. https://dupress.deloitte.com/.../the-great-debate-inflation-defl
10. Borio C., Erdem M., Filardo A., Hofmann B. (2015). The costs of deflations: a historical perspective. BIS Quarterly Review, March 2015. pp. 31-54.
11. Baumol W.J. The Transaction Demand for Cash: An Inventory Theoretic Approach // Quarterly Journal of Economics. 66 : 545-566, November 1952.
12. Баумоль У. Экономическая теория и исследование операций. М., 1965.
13. Дунаев Б.Б. Монетарное регулирование равновесия экономики // Кибернетика и системный анализ. – 2012. – № 2. – С. 55–68.
14. Сакс Д., Ларрен Ф. Макроэкономика. Глобальный подход: Пер. с англ.– М.: ДЕЛО, 1999. – 848 с.
15. Дунаев Б.Б. Модель расчета валового внутреннего продукта как функции труда и капитала // Кибернетика и системный анализ. – 2004. – № 1. – С. 104–116.
16. Миллер Р.Л., Ван Хуз Д.Д. Современные деньги и банковское дело / Пер. с англ. – М.: ИНФРА – М, 2000. – 856 с.
17. Дунаев Б.Б. Оптимизация ставки налога на доход производства // Кибернетика и системный анализ. – 2019. – № 3. – С. 99–111.
18. Дунаев Б.Б. Динамика экономических циклов // Кибернетика и системный анализ. 2017. Т. 53, № 2. С. 146–162.
19. Дунаев Б.Б., Варнавский В.Г., Кириленко Л.В. Циклы экономики России. Научные исследования и разработки. Экономика. «Научно-издательский центр ИНФРА-М». 2018. Т. 6. № 4, С. 21–30.
20. Дунаев Б.Б. Безынфляционный потребительский спрос // Кибернетика и системный анализ. – 2016. – № 4. – С. 103–117.
21. Дунаев Б.Б. Функция темпа роста ставки зарплаты от уровня безработицы // Кибернетика и системный анализ. – 2011. – № 5. – С. 140–149.
22. Горидько Н.П. Моделирование краткосрочной кривой Филлипса для США // Бізнес Інформ. – 2012. – № 4. – С. 49–52. http://nbuv.gov.ua/j-pdf/binf_2012_4_16.pdf.
23. Овчаров А.О. Актуальные проблемы современных научных исследований: методология, экономика, статистика. Сб. ст. – М.: Директ-Медиа, 2013. – 143 с.
24. Gosselin, M.-A. and Lalonde, R. “MUSE: The Bank of Canada’s New Projection Model of the U.S. Economy” Bank of Canada Technical Report, 2005, No. 96
25. http://www.cbr.ru/dkp/ccbshb29r.pdf Практика инфляционного таргетирования – 2012. Джил Хеммонд. Банк Англии.
26. Дунаєв Б.Б., Любіч О.О. Моделювання макроекономічних процесів // Математичне моделювання в економіці. – 2018. – № 1. – С. 109–125.
27. http://www.bank.gov.ua Грошово-кредитна та фінансова статистика.
28. https://www.google.com/search?client=firefox-b-ab ig=валютные+интервенции+цб +2017.
29. http://www.ukrstat.gov.ua Зведені національні рахунки за 2017 рік.
30. https://www.google.com/search?client=firefox-b-ab ig=валютные+интервенции+ цб+2018.
31. http://www.me.gov.ua/Tags/ DocumentsByTag? lang=uk-UA&tag=Ekonomichna SituatsiiaTaMakroekonomichnePrognozuvannia Макроекономічний аналіз та прогнозування.

REFERENCES

1. Dunaev B.B. Well-Being: Labor, Capital, and Money. Fundamentals of the of Reproduction Theory [in Russian], Kyiv. (2013).
2. Dunaev B.B. “Macroeconomic governmental regulation and self-regulation of market equilibrium", Cybern. Syst. Analysis, Vol. 42, No. 5, Springer. 702–713 (2006).
3. Dunaev B.B., Kirilenko L.V. “Deflationary Regulation of Market Equilibrium", Cybern. Syst. Analysis, Vol. 54, No. 2, Springer. pp. 258 – 270 (2018).
4. "Global monitoring of shadow bankinga – 2013". http://www.group-global.org/ru/lecture/view/7207
5. World Economic Outlook: Too Slow for Too Long (2016). Washington, DC: IMF. April 2016. p. 168-177.
6. Monetary policy decisions (2017). ECB. Press Release. 19 January 2017. URL: http://www.ecb.europa.eu/press/pr/date/2017/html/pr170119.en.html.
7. ECB announces expanded asset purchase programme (2015). ECB. Press Release. 22 January 2015. URL: https://www.ecb.europa.eu/press/pr/date/2015/html/ pr150122_1.en.html.
8. Draghi M. (2017). Introductory statement to the press conference (with Q&A). 19 January 2017. URL: http://www.ecb.europa.eu/press/pressconf/2017/html/ is170119.en.html#qa
9. The great debate: Inflation, deflation and the implications for financial management. Article Carl Steidtmann, Dan Latimore, Elisabeth Denison. January 01. 2011. https://dupress.deloitte.com/.../the-great-debate-inflation-defl
10. Borio C., Erdem M., Filardo A., Hofmann B. (2015). The costs of deflations: a historical perspective. BIS Quarterly Review, March 2015. pp. 31-54.
11. Baumol W.J. The Transaction Demand for Cash: An Inventory Theoretic Approach // Quarterly Journal of Economics. 66 : 545-566, November 1952.
12. Baumol W. Economic Theory and Operations Research. M., 1965.
13. Dunaev B.B. “Monetary control of economic equilibrium", Cybern. Syst. Analysis, Vol. 48, No. 2, Springer. 702–713 (2012).
14. J.D. Sachs D and F. Larrain, Macroeconomics in the Global Economy. Prentice Hall (1993).
15. Dunaev B.B. “Calculating gross domestic product as a function of labor and capita"l. Cybern. Syst. Analysis, Vol. 40, No. 1, Springer. 104 – 116 (2004).
16. D.D. Miller and R.L. Van Hoose, Money, Banking and Financial Markets. South-Western Cengage Learning, Mason. (2007).
17. Dunaev B.B. “Optimization of production income tax rate", Cybern. Syst. Analysis, Vol. 55, No. 2, Springer. 430 – 440 (2019).
18. Dunaev B.B. “Dynamics of Economic Cycles", Cybern. Syst. Analysis, Vol. 53, No. 3, Springer. 293 – 307 (2017).
19. Dunaev B.B., Varnavsky V.G., Kirilenko L.V. Cycles of the Russian economy. Scientific Research and development. Economy. "Scientific and Publishing Center INFRA-M". 2018. V. 6. No. 4, 21 – 30.
20. Dunaev B.B. “Non-inflationary consumer demand", Cybern. Syst. Analysis, Vol. 52, No. 4, Springer. 588–599 (2016). // Кибернетика и системный анализ. 2016. № 4. С. 103 – 117.
21. Dunaev B.B. The rate of growth of wage rate as a function of unemployment rate. Cybern. Syst. Analysis, Vol. 47, No. 5, 791–799 (2011).
22. Goridko NP Simulation of the short-term Phillips curve for the United States // BISNESSInform. – 2012. – No. 4. – P. 49 – 52. http://nbuv.gov.ua/j-pdf/binf_2012_4_16.pdf.
23. Ovcharov A.O. Actual problems of modern scientific research: methodology, economics, statistics. Sat. Art. – M .: Direct-Media, 2013. – 143 p.
24. Gosselin, M.-A. and Lalonde, R. “MUSE: The Bank of Canada’s New Projection Model of the U.S. Economy” Bank of Canada Technical Report, 2005, No. 96.
25. http://www.cbr.ru/dkp/ccbshb29r.pdf The practice of inflation targeting is 2012. Jill Hammond. Bank of England.

26. Dunaev B.B., Lyubich O.O. Model of macroeconomic processes // Mathematical model of economical. – 2018. – No. 1. – S. 109 – 125.
27. http://www.bank.gov.ua Groshovo-credit and financial statistics.
28. https://www.google.com/search?client=firefox-b-ab ig = currency + interventions + cb + 2017.
29. http://www.ukrstat.gov.ua Established national rakhunki for 2017 rik.
30. https://www.google.com/search?client=firefox-b-ab ig = currency + interventions + cb + 2018.
31. http://www.me.gov.ua/Tags/ DocumentsByTag? lang = uk-UA & tag = EkonomichnaSituatsiia TaMakroekonomichnePrognozuvannia Macroeconomic analysis and forecasting.

Стаття надійшла до редакції 18.08.2019.

РЕФЕРАТИ / ABSTRACTS

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ
INFORMATION TECHNOLOGY IN ECONOMY

УДК 004.056.53:303.732.4

Інформаційний і кібернетичний простори як джерело сучасних загроз / Качинський А.Б., Стьопочкіна І.В. // Математичне моделювання в економіці. – 2019. – №3 – С. 5–17.

Виділено найбільш небезпечні тенденції розвитку сучасних загроз, проаналізовано історію вживання термінів “інформаційний простір”, “кібернетичний простір” науковим суспільством на основі онлайнових баз публікацій із використанням математичного апарату, зокрема вперше обчислено статистичні характеристики, які дозволяють зробити висновки про взаємозалежність категорій при існуванні водночас суттєвих відмінностей. Для цього здійснено підрахунок кількості наукових публікацій за джерелами JSTOR, ScienceDirect, GoogleScholar, в яких вживаються або цитуються категорії «інформаційний простір», «кіберпростір» (за період 1950-2018 рр.), побудовано відповідні залежності, що ілюструють динаміку змін. Відмічено наявність трьох часових періодів в характері розвитку вживання категорій інформаційного та кібернетичного просторів, які тісно пов’язані із усвідомленням суспільством відповідних класів загроз.

UDC 004.056.53:303.732.4

Information space and cyber space as a source of modern threats / Kachynskyy A.B., Styopochkina I.V. // Mathematical modeling in economy. – 2019. – № 3. – P. 5–17.

The most dangerous tendencies of evolution of modern threats have been identified, the history of the use of the terms "information space", "cybernetic space" by the scientific society have been analyzed on the basis of online databases with the use of mathematical means, in particular the statistical characteristics which allow to make conclusions about the interdependence of categories and existing differences have been calculated. To do this, the number of scientific publications by sources JSTOR, ScienceDirect, GoogleScholar, in which the categories "information space", "cyberspace" (for the period 1950-2018) are used or cited, have been obtained. The corresponding dependencies illustrating the dynamics of change have been constructed,. Three time periods in the development of the use of categories of information and cyberspace, which are closely related to the public awareness of the relevant classes of threats, have been pointed out.

УДК 519.1, 514.128

Про нові потокові алгоритми створення чутливих дайджестів електронних документів / Пустовіт О.С., Устименко В.О. // Математичне моделювання в економіці. – 2019. – №3 – С. 18–35.

Для прийняття обґрунтованих планових рішень у суспільно-економічній сфері, спеціалісти повинні користуватися перевіреними документами. До засобів перевірки документів належать криптографічно стабільні алгоритми компресії великого файлу

в дайджест визначеного розміру, чутливий до будь-якої зміни символів на вході. Пропонуються нові швидкі алгоритми компресії, криптографічна стабільність яких пов'язується зі складними алгебраїчними проблемами, такими як дослідження систем алгебраїчних рівнянь великої степені та задача розкладу нелінійного відображення простору за твірними. Запропоновані алгоритми створення чутливих до змін дайджестів документів будуть використані для виявлення кібератак та аудиту усіх файлів системи після зареєстрованого втручання.

UDC 519.1, 514.128
A new stream algorithms generating sensitive digests of digital documents / Pustovit O.S., Ustimenko V.O. // Mathematical modeling in economy. – 2019. – № 3. – P. 18–35.
Specialists must use well checked documents to elaborate well founded,decisions and plans in the socio-economic field. Check tools include cryptographically stable algorithms for compressing a large file into a digest of a specified size, sensitive to any change in the characters on the input. New fast compression algorithms are proposed, whose cryptographic stability is associated with complex algebraic problems, such as the study of systems of algebraic equations of large power and the problem of the expansion of nonlinear mapping of space by generators. The proposed algorithms for creation of change-sensitive digests will be used to detect cyberattacks and audit all system files after a registered intervention.

УДК 004.942: 052:056
Теоретико-методичні аспекти концепції забезпечення необхідного рівня повноти безпеки автоматизованих систем управління об'єктами підвищеної небезпеки / Іванов В.Г., Лифар В.О., Лифар О.К. // Математичне моделювання в економіці. – 2019. – №3 – С. 36–48.
Представлені аспекти сучасних підходів до вирішення науково-технічної проблеми щодо забезпечення необхідного рівня повноти безпеки технічних засобів АСУТП об'єктами підвищеної небезпеки. Сформульовано завдання досліджень і теоретико-методична концепція визначення показників надійності і безпеки апаратних і програмних засобів АСУТП. Розглянуто існуючі та запропоновано оригінальні методи визначення нормуючих показників надійності при проведенні SIL-аналізу. Розглянуто проблеми підготовки фахівців до забезпечення необхідного рівня SIL при розробці АСУТП.

UDC 004.942: 052:056
Theoretical and methodological aspects of the concept of ensuring the necessary safety of the security system of automated systems for managing the objects of public awareness / Ivanov V.G., Lifar V.O., Lifar O.K. // Mathematical modeling in economy. – – 2019. – № 3. – P. 36–48.
Aspects of modern approaches to solving a scientific and technical problem to ensure the necessary level of safety integrity of automatic systems for managing hazardous facilities are presented. Research objectives and a theoretical and methodological concept for determining the reliability and safety indicators of hardware and software for process control systems are formulated. Existing methods are considered and original methods for determining the standardizing reliability indicators during the SIL analysis are proposed. The problems of training specialists to ensure the necessary level of SIL in the development of process control systems are considered.

МАТЕМАТИЧНІ ТА ІНФОРМАЦІЙНІ МОДЕЛІ В ЕКОНОМІЦІ
MATHEMATICAL AND INFORMATIONAL MODELS IN ECONOMY

УДК 532.5; 519.63

Текстурна адвекція при моделюванні в'язких течій методом ґраткових рівнянь Больцмана / Буланчук Г.Г., Буланчук О.М., Остапенко А.О., Чабану Р.В. // Математичне моделювання в економіці. – 2019. – № 3. – С. 49–56.

Візуалізація векторного поля швидкостей є невід'ємною частиною багатьох задач чисельного моделювання. Традиційним є представлення результатів у вигляді стрілочних діаграм поля швидкостей або колірних діаграм модуля швидкості. Але така інформація зрозуміла лише фахівцям з гідромеханіки і не дає вичерпну картину течії в цілому. В даній роботі досліджується метод текстурної адвекції при моделюванні течій в'язкої рідини, який за інформативністю максимально наближений до натурного експерименту і дає змогу отримати детальну картину течії. Розроблений метод базується на комбінації ідей методу плямистого шуму та адвекції Лагранжа – Ейлера. Поле швидкостей обчислюється методом ґраткових рівнянь Больцмана.

UDC 532.5; 519.63

Texture advection in the viscous fluid flow modeling with the lattice Boltzmann method / Bulanchuk G.G., Bulanchuk O.N., Ostapenko A.A., Chabanu R.V. // Mathematical modeling in economy. – 2019. – № 3. – P. 49–56.

Visualization of the vector velocity field is an essential part of many problems of numerical simulation. It is traditional to present the results in the form of arrow diagrams of the velocity field or color diagrams of the velocity module. But such information is easily understandable only for hydromechanics specialists and does not give a full picture of the flow as a whole. In this paper, we study the method of texture advection in modeling viscous fluid flows, which is as informative as possible close to a full-scale experiment and allows us to obtain a detailed picture of the flow. The developed method is based on a combination of the ideas of the spotted noise method and Lagrangian - Euler advection. We calculated the velocity field by the method of lattice Boltzmann equations.

УДК 519.866

Використання апарату звичайних диференціальних рівнянь при моделюванні економічних та екологічних систем / Олійник А.П., Григорчук Г.В., Незамай Б.С., Фешанич Л.І. // Математичне моделювання в економіці. – 2019. – № 3. – С. 57–66.

У статті представлені звичайні методи диференціальних рівнянь, що застосовуються для дослідження економічної та екологічної систем. Проведено моделювання взаємозв'язку розвитку економічних комплексів для країн з різним економічним потенціалом. Досліджено вплив економічної активності населення на забруднення навколишнього середовища та стан флори регіону. Вивчено економічну ефективність впровадження нової технічної діагностики. Представлені та досліджені методи реалізації представлених моделей, представлені результати перевірених розрахунків та дано аналіз. Визначено напрямки майбутніх досліджень.

UDC 519.866

Usage of the apparatus of ordinary differential equations in modelling of economic and environmental systems / Oliynyk A.P., Grygorchuk G.V, Nezamay B.S., Feshanych L.I. // Mathematical modeling in economy. – 2019. – № 3. – P. 57–66.

The ordinary differential equations techniques applying to investigate the economical and ecological systems has been considered in presented article. The interconnected economical complexes development for the countries with the different economical potential has been simulated. The population economical activity influence on the environment pollution and the state of region's flora has been investigated. The economical efficiency of the new technical diagnostics implementation has been studied. The methods of presented models realization has been presented and investigated, the results of tested calculations have been presented and one's analysis has been given. The directions of future investigations have been determined.

УДК 621.391

Обчислювальний метод нечіткого декодування багатокомпонентних турбо кодів в безпроводових засобах передачі даних / Горлинський Б.В. // Математичне моделювання в економіці. – 2019. – № 3. – С. 67–81.

Запропоновано обчислювальний метод нечіткого декодування багатокомпонентних турбо кодів в безпроводових засобах передачі даних для підвищення ефективності математичної моделі системи забезпечення достовірності інформації на основі адаптації кодових конструкцій.

UDC 621.391

Computational method of fuzzy decoding of multicomponent turbo codes in wireless data communication / Horlynskyi B.V. // Mathematical modeling in economy. – 2019. – № 3. – P. 67–81.

A computational method of fuzzy decoding of multicomponent turbo codes in wireless data transmission systems is proposed to improve the efficiency of a mathematical model of a system of ensuring information reliability based on the adaptation of code structures.

АНАЛІЗ, ОЦІНКА ТА ПРОГНОЗУВАННЯ В ЕКОНОМІЦІ
ANALYSIS, EVALUATION AND FORECASTING IN ECONOMY

УДК 004.942 ; 626/627 ; 504.05

Логіко-імовірнісне моделювання і прогнозування аварій на напірних гідроспорудах Дністровського гідровузла (Частина 2. Результати досліджень) / Стефанишин Д.В. // Математичне моделювання в економіці. – 2019. – № 3. – С. 82–97.

Стаття є другою частиною комплексної роботи, присвяченої моделюванню і прогнозуванню гіпотетичних аварій, з оцінюванням ймовірностей їх виникнення, на гідроспорудах, що формують напірний фронт Дністровського гідровузла. В попередній статті було обґрунтовано актуальність проблеми, розглянуто загальну постановку задачі досліджень, викладено методологію досліджень та сформульовано їх мету, окреслено прийняті гіпотези і припущення, дано коротку характеристику моделей, методів і підходів, що використовувалися при вирішенні поставленої задачі. В цій статті наведено результати досліджень. Розв'язання поставленої задачі здійснювалося за допомогою графоаналітичного, логіко-імовірнісного методу дерев відмов і несправностей. В результаті проведених досліджень було отримано верхні граничні оцінки ймовірностей виникнення аварій на окремих гідроспорудах і узагальнену оцінку ймовірності аварії на гідровузлі в цілому. Було встановлено, що ці ймовірності не перевищують допустимого значення ймовірності аварії на напірних гідроспорудах відповідного класу відповідальності за наслідками. На основі цього було зроблено висновок про достатню надійність і безпеку Дністровського гідровузла як об'єкта національної критичної інфраструктури і потенційно небезпечного об'єкта.

UDC 004.942 ; 626/627 ; 504.05

Logic-probabilistic modelling and forecasting of accidents on water retaining hydraulic structures of the Dnistrovsky waterworks (Part 2. Research results) / Stefanyshyn D.V. // Mathematical modeling in economy. – 2019. – № 3. – P. 82–97.

The article is the second part of the complex work devoted to modelling and predicting hypothetical accidents, with the estimation of their probability of occurrence, on water retaining hydraulic structures forming the pressure front of the Dniester waterworks. In the previous article, the urgency of the problem was substantiated, the general statement of the research issue was considered, the research methodology was presented and the purpose of the research was formulated, hypotheses and assumptions were outlined, and the brief description of the models, methods and approaches used in solving the problem was given. This article presents results of the research. The solution of the task was carried out with the aid of a graph-analytic, logical-probabilistic method of tree of failures and faults. As a result of the conducted studies, the upper boundary estimates of the probability of occurrence of accidents on individual hydraulic structures and the generalized estimation of the probability of an accident on the waterworks as a whole were obtained. It was found that these probabilities do not exceed the permissible value of the probability of an accident on the water retaining hydraulic structures of the corresponding class of responsibility for the consequences. On the basis of this, the conclusion on sufficient reliability and safety of the Dniester waterworks as an object of national critical infrastructure and a potentially dangerous object was made.

УДК 330.101.541-336.7

Депресію економіки викликає і зберігає грошова дефляція / Дунаєв Б.Б., Любіч О.О. // Математичне моделювання в економіці. – 2019. – № 3. – С. 98–118.

Економіки високорозвинених країн після розпочатої в 2008 р кредитної кризи, яка переросла в глобальну фінансову кризу, знаходяться в стані депресії, що зберігається грошовою дефляцією. Центральними банками проводиться політика виходу з депресії через нарощування грошових баз, зниження до нуля процентних ставок, щомісячний багатомільярдний викуп токсичних активів банків і таргетування інфляції не більше двох відсотків. Ця політика призвела до різкого зростання спекулятивного фінансового сектора, поглиблення кредитної кризи, збереження грошової дефляції в реальному секторі економіки і не дозволяє рости споживчому попиту. Стримування зростання інфляції для забезпечення наявного курсу валюти і підвищення вартості грошей зберігає грошову дефляцію і підтримує депресію економіки. Без збільшення інфляції неможливо вийти з депресії.

UDC 330.101.541-336.7

Depression of economy is caused and saved by money deflation / Dunaev B.B., Lyubich A.A. // Mathematical modeling in economy. – 2019. – № 3. – P. 98–118.

The economies of highly developed countries after the credit crisis that began in 2008, which grew into a global financial crisis, are in a state of depression, maintained by monetary deflation. Central banks pursue a policy of overcoming depression by increasing monetary bases, lowering interest rates to zero, monthly multi-billion dollar repurchase of toxic assets banks and inflation targeting of no more than two percent. This policy has led to a sharp increase in the speculative financial sector, the deepening credit crisis, the preservation of monetary deflation in the real sector of the economy and does not allow consumer demand to grow. Holding back inflation to maintain the current exchange rate and increase the value of money keeps monetary deflation and supports a depressed economy. Without increasing inflation, it is impossible to get out of depression.

ІНФОРМАЦІЯ ПРО АВТОРІВ
INFORMATION ABOUT THE AUTHORS

Буланчук Галина Григорівна – кандидат фізико-математичних наук, доцент, доцент кафедри вищої та прикладної математики ДВНЗ “Приазовський державний технічний університет” (Україна, м. Маріуполь).

Буланчук Олег Миколайович – кандидат фізико-математичних наук, доцент, методист національного центру «Мала академія наук України» (Україна, м. Маріуполь).

Горлинський Борис Вікторович – начальник управління Департаменту захисту інформації Адміністрації Державної служби спеціального зв’язку та захисту інформації України (Україна, м. Київ).

Григорчук Галина Василівна – аспірант, асистент кафедри прикладної математики Івано-Франківського національного технічного університету нафти і газу (ІФНТУНГ) (Україна, м. Івано-Франківськ).

Дунаєв Борис Борисович – кандидат технічних наук, старший науковий співробітник ДННУ «Академія фінансового управлення» (Україна, м. Київ).

Іванов Віталій Геннадійович – кандидат технічних наук, доцент кафедри програмування та математики Східноукраїнського національного університету ім. Володимира Даля (СНУ ім. В. Даля) (Україна, м. Сєвєродонецьк).

Качинський Анатолій Броніславович – доктор технічних наук, професор, професор кафедри інформаційної безпеки Фізико-технічного інституту Національного технічного університету України “Київський політехнічний інститут імені Ігоря Сікорського” (НТУУ “КПІ” ім. Ігоря Сікорського) (Україна, м. Київ).

Bulanchuk Galina – PhD, Associate Professor at Department of High and Applied Mathematics of Pryazovskyi State Technical University (Ukraine, Mariupol).

Bulanchuk Oleg – PhD, Associate Professor, Methodist of the National Center "Small Academy of Sciences of Ukraine" (Ukraine, Mariupol).

Horlynskyi Borys – Head of Office of Department of Information Protection of Administration of State Service of Special Communication and Information Protection of Ukraine (Ukraine, Kyiv).

Grygorchuk Galyna – post-graduate student, assistant of the Department of Applied Mathematics, Ivano-Frankivsk National Technical University of Oil and Gas (Ukraine, Ivano-Frankivsk).

Dunaev Boris – PhD, senior researcher at the State educational, SESE «Academy of Financial Management» (Ukraine, Kyiv).

Ivanov Vitaliy – PhD in Technical Science, Associate Professor of the Department of Mathematics and Program Engineering, Volodymyr Dahl East Ukrainian National University (Ukraine, Severodonetsk).

Kachynskyy Anatoliy – Doctor of sciences (Eng.), Professor, Professor of Information security chair, The Institute of Physics and Technology of the National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic University” (Ukraine, Kyiv).

Лифар Володимир Олексійович – доктор технічних наук, зав. кафедри програмування та математики Східноукраїнського національного університету ім. Володимира Даля (СНУ ім. В. Даля) (Україна, м. Сєвєродонецьк).

Лифар Олена Костянтинівна – старший викладач кафедри комп'ютерних наук та інженерії Східноукраїнського національного університету ім. Володимира Даля (СНУ ім. В. Даля) (Україна, м. Сєвєродонецьк).

Любіч Олександр Олексійович – доктор економічних наук, професор, заслужений економіст України, віце-президент ДННУ «Академія фінансового управлення» (Україна, м. Київ).

Незамай Борис Сергійович – кандидат технічних наук, доцент кафедри прикладної математики Івано-Франківського національного технічного університету нафти і газу (ІФНТУНГ) (Україна, м. Івано-Франківськ).

Олійник Андрій Петрович – доктор технічних наук, професор, завідувач кафедри прикладної математики Івано-Франківського національного технічного університету нафти і газу (ІФНТУНГ) (Україна, м. Івано-Франківськ).

Остапенко Артем Олексійович – асистент кафедри вищої та прикладної математики ДВНЗ "Приазовський державний технічний університет" (Україна, м. Маріуполь).

Пустовіт Олександр Сергійович – молодший науковий співробітник відділу онтологічних систем та прикладної алгебраїчної комбінаторики Інституту телекомунікацій та глобального інформаційного простору Національної академії наук України (ІТГІП НАН України) (Україна, м. Київ).

Стефанишин Дмитро Володимирович – доктор технічних наук, провідний науковий співробітник Інституту телекомунікацій і глобального інформаційного простору (ІТГІП) НАН України, професор кафедри гідротехнічного будівництва та гідравліки Національного університету водного господарства та природокористування (НУВГП) (Україна, м. Рівне).

Lifar Volodimir – Doctor of Technical Sciences, Head of the Department of Programming and Mathematics Schedule, Volodymyr Dahl East Ukrainian National University (Ukraine, Severodonetsk).

Lifar Olena – senior lecturer of the Department of Computer Science and Engineering, Volodymyr Dahl East Ukrainian National (Ukraine, Severodonetsk).

Lyubich Oleksander – Doctor of Economics, Professor, Honored economist of Ukraine, vice-president, SESE «Academy of Financial Management» (Ukraine, Kyiv).

Nezamay Borys – Candidate of technical science, docent of the Department of Applied Mathematics, Ivano-Frankivsk National Technical University of Oil and Gas (Ukraine, Ivano-Frankivsk).

Oliynyk Andriy – Doctor of sciences, professor, Head of the Department of Applied Mathematics, Ivano-Frankivsk National Technical University of Oil and Gas (Ukraine, Ivano-Frankivsk).

Ostapenko Artem – assistant of the Department of High and Applied Mathematics of Pryazovskyi State Technical University (Ukraine, Mariupol).

Pustovit Olexandr – junior researcher in the department of ontological systems and applied algebraic combinatorics at the Institute of Telecommunications and the Global Information Space of the National Academy of Sciences of Ukraine (ITGIP NAS of Ukraine) (Ukraine, Kyiv).

Stefanyshyn Dmytro – Doctor of sciences (Eng.), Department of natural resources, Lead researcher, The Institute of Telecommunications and Global Information Space of the NAS of Ukraine, associate professor, professor, Department of hydro construction and hydraulics, The National University of Water and Environmental Engineering (Ukraine, Rivne).

Стьопочкіна Ірина Валеріївна – кандидат технічних наук, доцент кафедри інформаційної безпеки Фізико-технічного інституту Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського" (НТУУ "КПІ" ім. Ігоря Сікорського) (Україна, м. Київ).

Устименко Василь Олександрович – доктор фізико-математичних наук, професор, завідувач відділу онтологічних систем та прикладної алгебраїчної комбінаторики Інституту телекомунікацій та глобального інформаційного простору Національної академії наук України (ІТГІП НАН України) (Україна, м. Київ), завідувач кафедри алгебри та дискретної математики, Інститут математики, відділення математики, фізики та інформатики, університет Марі Кюрі-Склодовської у м. Любліні (Польща).

Фешанич Лідія Ігорівна – кандидат технічних наук, доцент кафедри автоматизації та комп'ютерно інтегрованих технологій Івано-Франківського національного технічного університету нафти і газу (ІФНТУНГ) (Україна, м. Івано-Франківськ).

Чабану Родіон Володимирович – магістр кафедри вищої та прикладної математики ДВНЗ "Приазовський державний технічний університет" (Україна, м. Маріуполь).

Styopochkina Iryna – PhD in Technical Science, Associate Professor, Information security chair, the Institute of Physics and Technology of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic University" (Ukraine, Kyiv).

Ustimenko Vasyl – Doctor of Sciences (Physics and Mathematics), Professor, Head of the department of ontological systems and applied algebraic combinatorics of the Institute of Telecommunications and the Global Information Space of the National Academy of Sciences of Ukraine (ITGIP NAS) (Ukraine, Kyiv), Head of the department of algebra and discrete mathematics, Institute of Mathematics, Department of Mathematics, Physics and Informatics, University of Marie Curie-Sklodowska in Lublin (Poland).

Feshanych Lidiia – PhD in Technical Science, Associate Professor, Department of automation and computer integrated technologies, Ivano-Frankivsk National Technical University of Oil and Gas (Ukraine, Ivano-Frankivsk).

Chabanu Radion – master of the Department of High and Applied Mathematics of Pryazovskyi State Technical University (Ukraine, Mariupol).

ДО УВАГИ АВТОРІВ ЖУРНАЛУ

Зміст матеріалів, що направляються до редакції, повинен відповідати профілю та науково-технічному рівню журналу. Тематика журналу стосується математичного моделювання у всіх сферах господарської діяльності, тобто, економіки в її широкому розумінні. До друку приймаються статті українською, англійською та російською мовами.

Кожна наукова стаття повинна мати вступ, розділи основної частини та висновки, а також анотацію і ключові слова двома мовами (українською та англійською). Також двома мовами подаються реферати до статті, які будуть розміщені в електронному варіанті журналу «Математичне моделювання в економіці» на сайті журналу. Вимоги до оформлення наведені на сайті журналу.

Усі представлені в редакцію рукописи проходять ретельне багатоланкове рецензування відповідними фахівцями за профілем статті. Якщо сумарна оцінка рецензентів менша за встановлений поріг, рукописи відхиляються. Автору надсилається відповідне повідомлення. Матеріали, отримані від автора, редакцією не повертаються. Після доопрацювання автор може подати матеріал повторно, з виконанням усіх процедур подачі матеріалу.

Статті, що були представлені в редакцію і прийняті після рецензування, але не попали в поточний номер журналу, будуть надруковані в наступних номерах журналу.

Зміст статті та якість написання або перекладу (українською або англійською мовами) переглядаються коректорами журналу, проте відповідальність за зміст та якість статті несуть автори матеріалу. До статті можуть бути внесені зміни редакційного характеру без згоди автора.

Розділ журналу, до якого буде віднесена стаття, визначається редакцією, узгоджується – головним редактором або його заступником.

Остаточний висновок щодо публікації матеріалів схвалює редакційна колегія журналу.

Електронна версія журналу, правила оформлення та вимоги до статей, зміни і доповнення до тематичних розділів будуть оперативно подаватися в Інтернеті на сайті журналу «Математичне моделювання в економіці» www.mmejournal.in.ua

Журнал також представлений на сайті Інституту телекомунікацій і глобального інформаційного простору НАН України http://itgip.org/ у розділі «Видавнича діяльність».

АДРЕСА РЕДАКЦІЇ

03186, м. Київ, Чоколівський бульв., 13,
Інститут телекомунікацій і глобального інформаційного простору НАН України
Телефони: (044) 245-87-97
(044) 524-22-62
e-mail: economconsult@gmail.com
journal.mme@gmail.com

Електронна версія журналу в Інтернеті www.mmejournal.in.ua українською та англійською мовами

ISSN (print) **2409-8876**
ISSN (on-line) **2663-9068**

Коректор – **Берчун В. П**.

Надруковано:

Видавничий дім «Юстон»
01034, м. Київ, вул. О. Гончара, 36.
Тел.: (044) 360-22-66
Реєстраційне свідоцтво НБ № 153324 від 05.11.2012 р.

Підписано і здано до друку 26.09.2019. Формат 70Х108/16. Папір офсетний. Офсетний друк. Умовн. друк. арк. 11.8
Обл.-вид. арк. 12.3 Тираж 300 примірників Замовлення № ___

КИЇВ 2019