Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки

БАКАЛАВРСЬКА КВАЛІФІКАЦІЙНА РОБОТА
на тему:
Комп'ютеризована система моніторингу захищеності об'єкту

ПОЯСНЮВАЛЬНА ЗАПИСКА

Виконала студентка 4 курсу, групи 1КІ-18б
спеціальності123 — Комп'ютерна інженерія
Артоуз А. О.

Керівник к.т.н., доц. каф. ОТ
Колесник І. С.

Опонент к.т.н., доц. каф. ЗІ
Куперштейн Л. М.

Допущено до захисту
д.т.н., проф. Азаров О.Д.

" " 2022 р.

ВНТУ 2022

ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки
Освітній рівень — бакалавр
Спеціальність — 123 Комп'ютерна інженерія

ЗАТВЕРДЖУЮ

Завідувач кафедри обчислювальної техніки

О.Д. Азаров
"9" лютого 2022 р.

З А В Д А Н Н Я

НА БАКАЛАВРСЬКУ ДИПЛОМНУ РОБОТУ СТУДЕНТУ

студентці Артоуз Анастасії Олександрівні

1 Тема роботи «Комп'ютеризована система моніторингу захищеності об'єкту», керівник Колесник Ірина Сергіївна к. т. н., доцент кафедри ОТ, затверджено наказом вищого навчального закладу від «24» березня 2022 року №66

2 Строк подання студентом роботи 13 червня 2022.

3 Вихідні дані до роботи пакет Mathcad.

4 Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): вступ, загрози безпеці інформації, безпека обєкта, оцінка рівня безпеки підприємства, висновки, література, додатки.

5 Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень): технічне завдання, організація комплексної безпеки об'єктів інформаційної діяльності, графік оцінки розкиду функціонування системи захисту, розкид оптимального функціонування елементів системи захисту графіки функціонування елементів системи.

6 Дата видачі завдання 10.02.2022.

7 Календарний план виконання БДР приведений в таблиці 2.

Таблиця 2 — Календарний план

№ з/п	Назва етапів БДР	Строк виконання	Підпис
1	Інформаційний пошук та огляд літературних джерел	28.03.2022 р.	ВИК
2	Дослідження підходів та розробка системи	18.04.2022 р.	ВИК
3	Підготовка матеріалів пояснювальної записки	22.04.2022 р.	ВИК
4	Перевірка якості оформлення БДР	1.05.2022 р.	ВИК
5	Оформлення пояснювальної записки і презентації	12.05.2022 р.	ВИК
6	Перевірка «антиплагіат»	16.05.2022 р	ВИК
9	Попередній захист	18.05.2022 р.	ВИК

Студент Артоуз А. О

Керівник к.т.н., доц. Колесник І. С

АНОТАЦІЯ

Пояснювальна записка містить 84 сторінки, 11 рисунків, 10 формул та 30 посилань.

У бакалаврській дипломній роботі досліджується комп'ютеризована система моніторингу захищеності об'єкту.

Головною метою створення комп'ютеризованої системи моніторингу захищеності об'єкту є досягнення максимальної ефективності захисту за рахунок одночасного використання всіх необхідних ресурсів, методів і засобів, що виключають несанкціонований доступ до інформації

Ключові слова: система захисту атак, інтенсивність атак, бар'єр захисту, інформаційний простір, види мережевих атак, firewall

ANNOTATION

The explanatory note contains 99 pages, 99 figures, 99 tables, 99 formulas and 99 references.

The bachelor's thesis investigates a computerized system for monitoring the security of the object.

The main purpose of creating a computerized system for monitoring the security of the object is to achieve maximum effectiveness of protection through the simultaneous use of all necessary resources, methods and tools that exclude unauthorized access to information

Keywords: attack protection system, attack intensity, protection barrier, information space, types of network attacks, firewall

ЗМІСТ

					8-23 БДР.001.00.000 ПЗ		
Змн.	Лист	№ докум.	Підпис	Дата			
Розроб.		Артоуз А. О.			Комп'ютеризована система моніторингу захищеності об'єкту. Пояснювальна записка	Літ.	Арк. 6 / Акрушів 82
Перевір.		Колесник І.С.					
Реценз.		Куперштейн Л.				ВНТУ, 1КІ-18б	
Н. Контр.		Швець С. І					
Затверд.		Азаров О. Д.					

ВСТУП

Проблеми та кількість різноманітних загроз інформаційній безпеці збільшуються з кожним днем. У той же час збільшується кількість систем, призначених для захисту бізнесу від даних загроз. Більшість великих компаній мають брандмауер, антивірусне рішення та систему виявлення атак – це мінімум на сьогодні. Крім того, мережа має власну базу даних, операційну систему і програмні засоби для проектування. Усі ці підсистеми формують різноманітні звіти та події. Якщо компанія має кілька філіалів або аутсорсингових офісів, потік даних з інформаційної підсистеми збільшується вдесятеро!

В результаті адміністратори щодня отримують значну (≈100 тис.) кількість запитів від різних підсистем. Робота кожної окремої підсистеми важлива для всього бізнесу, тому спеціалісти вимушені аналізувати увесь потік інформації. Ізолювати важливі повідомлення стало все важче, тому вартість одного рішення безпеки зводиться до нуля, а час відновлення інформаційних систем після збою різко зріс.

Ефективне використання даних, отриманих від датчиків (серверів), для виявлення атак і атак брандмауера (до атак, які вони демонструють) дозволяє використовувати системи моніторингу інформаційної безпеки. Системи моніторингу дозволяють об’єднувати всі події та інциденти в одній консолі, забезпечують інтелектуальний аналіз атак та їх наслідків, а також допомагають адміністраторам вживати контрзаходи. Крім того, система моніторингу фіксує та підтримує всі інциденти інформаційної безпеки, що дозволяє використовувати вилучені матеріали як докази під час розслідування інцидентів та судових розглядів.

Мета і завдання дослідження. Метою роботи є підвищення ефективності управління сучасними комп’ютерними системами для моніторингу захищеності об’єкту.

Для досягнення поставленої мети потрібно розв’язати такі задач:

– провести аналіз стану розробки моделей систем моніторингу захищеності об’єкту;

– виконати аналіз типових ресурсних структур об’єктів – послідовних, паралельних з ресурсними і часовими зв’язками між підсистемами;

– розробити узагальнену модель оптимального управління процесами функціонування систем обслуговування;

– проаналізувати альтернативи оптимального агрегування систем обслуговування з урахуванням зв’язків в часі;

– виконати моделювання тестової структури комп’ютерної системи.

Об’єкт дослідження – процеси функціонування тестової системи проектів моніторингу захищеності об’єкту.

Предмет дослідження – методи оптимального агрегування комп’ютерних систем моніторингу захищеності об’єкту.

Методи дослідження: методи прикладного системного аналізу в побудові моделей проектів і методи оптимального агрегування в моделюванні систем моніторингу захищеності об’єкту.

Апробація результатів. Основні положення та результати виконані в бакалаврській роботі досліджень доповідались та обговорювались на конференції «LI Науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії, Вінниця, 2022 року».

1 ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ

Щоб дослідити категорію «загрози» в інформаційній безпеці, потрібно мати уявлення про чотири ключові терміни:

— інформаційний простір;
— інформаційна безпека;
— інформаційна загроза;
— інформаційний ризик.

1.1 Інформаційний простір

Існує кілька визначень інформаційного простору. Зокрема, інформаційний простір можна розглядати як сукупність сховищ даних, технологій, які їх обробляють, і телекомунікаційних інформаційних систем, що забезпечують інформаційні відносини між організаціями та громадянами.

По-перше, інформаційний простір слід розглядати не як територіальний, фізичний, а як соціальний простір без нормальних кордонів і територій. Його структура визначається інформацією та знаннями та людьми, які перебувають у стані інформаційної співпраці.

По-друге, відповідно до Українського словника інформаційної безпеки, інформаційний простір — це інформаційне середовище, в якому інформаційні відносини та процеси пов’язані зі створенням, збиранням, реєстрацією, відображенням, збиранням, зберіганням, захистом та поширенням інформації, інформаційних продуктів та ресурсів повинні бути застосовним.

Інформаційний простір — це набір об’єктів, які є частиною інформаційної співпраці, та технологій, які підтримують цю співпрацю. Складається з інформаційних ресурсів, засобів інформаційної співпраці та інформаційної інфраструктури. Інформаційні простори зосереджені на суб’єктах, які створюють, засвоюють, збирають і передають інформацію в ході свого виконання. Цими

суб’єктами можуть бути окремі особи, соціальні групи, компанії, державні установи — усі, хто користується можливостями нинішніх інформаційних технологій, але в будь-якому випадку інформаційний простір невіддільний від людської діяльності.

Інформаційний простір – це динамічне середовище, де фізичні об’єкти зазвичай мають чіткі фізичні межі, тимчасову інформацію можна використовувати, а простір структурований [1].

На думку американського дослідника Д. Елема, інформаційний простір складається з набору об’єктів, що спілкуються між собою, і технології цієї співпраці.

Інформаційний простір — це вид інформаційного дизайну, при якому зображення інформаційних об’єктів розміщуються в основному просторі. По суті, розташування та напрям дають змогу зображати й орієнтуватися [2].

Власне, термін «інформаційний простір» є одним із первинних понять і не має однозначного визначення. Його часто розуміють як логічне протиставлення об’єктивному світу (об’єктивному, фізичному, матеріальному).

1.2 Інформаційна безпека

Інформаційну безпеку слід розуміти як захист інтересів основного органу інформаційних відносин. Загалом, перш ніж вивчати термін «інформаційна безпека», важливо визначити термін «інформація». Це поняття дуже широко використовується сьогодні в багатьох аспектах. У літературі інформацію визначають як відомості про людей, об’єкти, факти, випадки, явища і процеси не зважаючи на форму їх вираження. Інформація має такі характеристики: цілісність, конфіденційність та доступність. З огляду на це, перш за все, «інформаційна безпека — це збереження секретності, нероздільності та доступності інформації; Також, можна розглядати інші характеристики, такі як автентичність, відстежуваність, неспростовність і надійність» [3].

Інформаційна безпека — стан безпеки систем обробки та зберігання даних, що забезпечує конфіденційність, доступність та цілісність інформації або являє собою

комплекс заходів, скерований на захист інформації від несанкціонованого доступу, застосування, розголошення, знищення, внесення змін, інформування, перевірки, фіксації чи видалення (у цьому контексті частіше використовується термін «захист даних») [4].

Враховуючи різноманітність інформації, термін «інформаційна безпека» може мати різне значення в різних контекстах. Інформаційна безпека — це захист інформації та інформаційно-забезпечуючої інфраструктури від навмисних або випадкових дій, які можуть завдати неприйнятної шкоди суб'єктам інформаційних відносин.

Термін «інформаційна безпека» зазвичай означає обмеження або доступ до інформації, свободу вираження поглядів, свободу обміну. За його словами, держава може обмежити цей процес [5]. В Україні обмеження можливі лише на підставі закону, тобто Верховна Рада регулює підстави та порядок втручання держави у реалізацію права на свободу вираження поглядів.

Правда, увага до механізмів безпеки та автентифікації забезпечує обмежений погляд на інформаційну безпеку, а вузьке бачення є небезпечним. Метою безпечної системи є запобігання будь-якому несанкціонованому використанню інформації, негативний тип вимоги [6].

Щоб краще зрозуміти термін «інформаційна безпека», було б корисно шукати визначення з різних джерел.

Інформаційна безпека — це захист інформації, що мінімізує ризик розголошення інформації неавторизованих особам [7].

Інформаційна безпека — це обґрунтована впевненість в тому, що інформаційні ризики врівноважені відповідними заходами контролю і управління [8].

Інформаційна безпека — це захист інформації та знижує ризик її розкриття третім особам [9] .

Проблеми інформаційної безпеки можна розділити на два класи:

— інформаційний захист (попередження загроз інформації);

— захист від інформації (попередження інформаційних загроз).

З іншого боку, інформаційна безпека розглядається в кількох сферах, включаючи безпеку:

— окремі особи, громади та держави страждають від низької якості інформації;

— інформація та інформаційні ресурси від несанкціонованого впливу третіх осіб;

— інформаційні права і свободи громадян [10].

З юридичної точки зору «інформаційна безпека — це стан захисту життєво важливих інтересів особи, суспільства та держави, який захищається від шкоди шляхом:

— використання неповної, невчасної та недостовірної інформації;

— негативний вплив інформації;

— негативні наслідки використання інформаційних технологій;

— несанкціоноване розкриття, використання та недотримання цілісності, приватності та доступу до інформації» [11].

У військові сфері інформаційна безпека визначається як захищеність об’єкта від інформаційних загроз або негативних інформаційних впливів.

Суб'єктами інформаційної безпеки є відповідні державні органи, що забезпечують регулярний доступ до інформації для прийняття стратегічних рішень та захисту інформаційних ресурсів країни. Важливими умовами інформаційної безпеки є захист інформаційних ресурсів країни та доступність інформації для прийняття стратегічних рішень.

1.3 Інформаційні загрози

Загроза інформаційній безпеці — це сукупність факторів та умов, що загрожують життєво необхідним інтересам особи, громади та держави в інформаційному просторі.

Загроза інтересам учасників інформаційних відносин — це потенційна подія, процес чи явище, які, впливаючи на інформацію чи інші елементи інформаційної системи, можуть прямо чи опосередковано завдати шкоди інтересам цих учасників.

Загрози інформаційній безпеці частіше виникають із появою та реалізацією загроз в економічній та політичній сферах, у сфері державних функцій, і шкоді в інформаційній галузі є насамперед засобом досягнення інших цілей.

Тому, відповідно до концепції загроз інформаційній безпеці держави, її доцільно визначити як «сукупність умов і факторів, які загрожують життєвим інтересам суспільства та особистості через ймовірність негативну інформаційну дію на свідомість та поводження громадян, а ще інформаційні ресурси та інформаційно-технічну інфраструктуру» [12]. До важливих ознак загроз інформаційній безпеці держави належать вибіркові, прогнозні та шкідливі [13].

Згідно з визначенням Національного інформаційного словника, інформаційна загроза — це будь-яка ситуація або подія, яка може негативно вплинути на інформаційну систему через несанкціонований доступ, знищення, розкриття, зміну інформації та/або відмову в обслуговуванні.

Інформаційна загроза - інструмент, який може негативно вплинути на здатність або намір загрозливого агента щодо автоматизованої системи, об'єкта або операції [14].

Усі загрози інформаційної безпеки діляться на такі основні групи:

— загроза згубного впливу належної інформації (недостовірної, шкідливої, неправдивої інформації) на інтереси особи, суспільства та держави;

— загроза несанкціонованого або протиправного впливу третіх осіб на інформацію та інформаційні ресурси місцевого самоврядування, фізичних і юридичних осіб, а також органів державної влади;

— загрози обмеження інформаційних прав особи та механізми їх реалізації.

1.4 Інформаційна небезпека

З точки зору інформаційної безпеки розглядається ризик втрати продукту через порушення конфіденційності, цілісності, достовірності та доступності інформації чи інформаційних ресурсів.

«Інформаційний ризик — це ризик, пов’язаний із використанням інформаційних систем, які підтримують бізнес-цілі організації» [15].

У банківській діяльності «інформаційний ризик – це ймовірність втрати чи додаткового збитку, втрати очікуваного доходу в результаті внутрішніх і зовнішніх подій, пов’язаних з банківськими інформаційними системами та іншими інформаційними ресурсами, які використовуються для досягнення цілей банку, відсутність внутрішнього контролю або недостатня процесів або є внутрішньою помилкою. банк у сфері інформаційно-комунікаційних технологій. Інформаційний ризик є частиною операційного ризику» [16].

1.5 Види мережевих атак на інформаційні системи

Розглянемо деякі з найнебезпечніших типів мережевих атак. Одним з найпоширеніших типів атак є переповнення буфера. Даний тип атак часто є частиною різних видів шкідливих атак. Атаки «Переповнення», у свою чергу, мають багато типів: стекові атаки, атаки форматування рядків. Завдання атак на стек полягає в тому, щоб заповнити його буфер записом даних (набір символів зі стека та будь-які інструкції для програми переповнюються) більше, ніж задають спеціалісти. В результаті програма може виконувати інструкції, записані в стеку після заповнення буфера. Атака форматування рядків також впливає на стек, але включає підміну з однієї адреси на іншу, яка містить шкідливі команди.

Атаки «пасивних» сніферів особливо небезпечні, оскільки їх важко виявити і здійснюються з локальної мережі. «Пасивні» атаки допомагають зловмисникам отримати пряму інформацію з мережі: інформацію про мережу, трафік SSL або TLS, TCP та UDP, отримання IP або MAC-адрес, номерів використаних портів, імена користувача, паролів.

1.6 Методи захисту інформації

Створення системи інформаційної безпеки передбачає виявлення джерел інформаційних загроз. Є чотири дії, пов’язані з інформацією, які можуть становити небезпеку:

— збір;
— модифікація (спотворення);
— витік;
— знищення інформації.

Ці дії є базовими для розгляду класифікації джерел інформаційних небезпек і загроз.

Повна класифікація загроз надана у вигляді діаграми на рисунку 1.1.

Рисунок 1.1 —Класифікація інформаційних загроз

Рівень захисту сучасних інформаційних систем є недостатнім, що обумовлює актуальність роботи. Є декілька широко відомих злочинів такого роду.

Перший випадок, Stuxnet і ядерна програма Ірану [17] 2010 рік. Комп'ютерний черв'як Stuxnet успішно атакував ядерну систему Ірану і частково вивів її з ладу. За даними іранських джерел, восени вірус заблокував роботу однієї п'ятої частини іранських центрифуг, водночас скопіював запис систем відеоспостереження та прокрутив її під час операції, щоб служба безпеки нічого не запідозрила. Оскільки атака була успішною, було припущено, що це розробка ізраїльських спецслужб, яким допомагали США.

У другому випадку команда Валдіра Паулу де Алмейди, найвідомішого спамера, надсилала 3 мільйони фішингових листів на день під час його арешту бразильською владою. За даними багатьох джерел, йому вдалося вкрасти з банківських рахунків до 37 мільйонів доларів за допомогою «трояна», який проникав на пристрої користувачів онлайн-банкінгу через шкідливі електронні листи. Група 18 чоловік.

В іншому випадку, у лютому 2004 року Microsoft повідомила про крадіжку вихідного коду Windows 2000 [19]. Викрадено 600 МБ даних або 31 000 файлів або 13,5 мільйонів рядків коду. Витік інформації також торкнувся Windows NT4. Спочатку компанія заявила, що код був вкрадений партнером Microsoft, але пізніше виявили, що інформація була вкрадена безпосередньо з мережі Microsoft. Викрадені дані опублікували в мережі Інтернет.

Нинішній захист інформації здійснюється за допомогою трьох способів [20]:

а) апаратний;
- генератори кодів;
- пристрої "прозорого" шифрування;
- біометричні пристрої;

б) програмний;
- криптографічні засоби;
- засоби ідентифікації користувачів;
- антивірусне ПЗ;

— засоби аудиту;

в) організаційний;

— розробляти організаційно-розпорядчі документи, що регулюють весь процес отримання, обробки, зберігання, передачі та захисту персональних даних;

— створити відділ корпоративної інформаційної безпеки, відповідальний за інформаційну безпеку.

Апаратно-програмні заходи захисту ґрунтуються на використанні електронного обладнання та спеціальних програм, що входять до складу автоматизованої системи і виконують функції безпеки (як окремо, так і в поєднанні з іншими засобами).

Організаційні заходи необхідні для забезпечення ефективного впровадження та застосування інших заходів і засобів правового захисту у регулюванні діяльності людини. У той же час організаційні заходи повинні підтримуватися потужними апаратними та програмними заходами.

Очевидно, що найбільш вигідним є впровадження програмних засобів захисту, оскільки вони не вимагають розробки, закупівлі обладнання та додаткового навчання персоналу. З них найбільш перспективним є використання шифрування для захисту даних, через те що він сприяє безпеці, цілісності та полегшує контроль доступу.

Аналіз отриманої інформації є дуже важливою особливістю будь-якої системи виявлення атак. Існує два основних методи виявлення зловмисної діяльності: виявлення аномалій і виявлення зловживань.

Метод виявлення аномалій використовує моделі очікуваної поведінки користувачів і програм, трактуючи відхилення від «нормальної» поведінки як потенційне порушення захисту. Методи виявлення аномалій базуються на тому, що дії атак різняться від нормальної поведінки системи. Коли виявлено аномалії,

створюються профілі, які описують нормальну роботу користувачів, хостів або мережевих підключень, які можна точно змоделювати.

Скажімо, певний користувач виконує звичайні щоденні операції (входить у певний час, перевіряє електронну пошту, виконує транзакції з базою даних, неактивний під час обіду та після роботи, робить декілька помилок при доступі до файлів тощо). Ці профілі створюються на основі інформації історії під час нормальної роботи системи. Потім, якщо система помічає, що користувач виконує дії, які не відповідають записаному профілі (вхід вночі, за допомогою засобів компіляції та редагування, при зверненні до файлів виникає велика кількість помилок) і визначає такі дії як підозрілі. Шкода , методи виявлення аномалій засновані на системі виявлення атак генерують багато помилкових тривог, оскільки закономірності, що описують «нормальну» поведінку користувача та системи, не мають чітких меж. Не дивлячись на цей недолік, імовірно, що аномальні системи виявлять нові форми атак. Крім того, конфігурація таких систем ускладнена в середовищі, де відбуваються значні зміни.

Методи виявлення зловживань припускають, що під час аналізу системних подій багато з них перевіряються на відповідність заздалегідь визначеним шаблонам, які описують відомі атаки. Якщо порівнюваний шаблон відповідає відомій атаці, то такий збіг називається сигнатурою. Використання методів виявлення зловживань дуже ефективно для виявлення атак без створення великої кількості помилкових тривог.

Коли виявлено зловживання, інструмент або технологію атаки, вона швидко діагностується, що дозволяє адміністратору вчасно вжити заходів безпеки. Вони дозволяють системним адміністраторам аналізувати інцидент, незалежно від рівня їх навичок безпеки. Недоліком такого підходу є постійний моніторинг оновлень бази даних з новими сигнатурами, оскільки детектори можуть аналізувати лише раніше відомі сигнатури.

1.7 Дії системи після виявлення вторгнень

Після отримання та аналізу інформації про події система створює відповідні звіти, які побудовані в стандартному форматі, або автоматизовані дії, такі як закриття порту. Існують також більш активні відповіді, які робляться при виявленні конкретних типів низькорівневих атак, наприклад, надсилання повідомлення на телефон, звуковий сигнал.

Активні дії можуть включати налаштування маршрутизатора для блокування адреси зловмисника або організацію атаки. Такі заходи дуже небезпечні, оскільки можуть бути спрямовані проти невинної людини, оскільки зловмисники часто використовують підроблені адреси. Наприклад, у разі атаки з підробленим трафіком з фальшивою IP-адресою система може попередити адміністратора про атаку.

1.8 Firewall, як вид захисту від атак

Firewall — це розподілене локальне або функціональне програмне забезпечення, яке контролює інформацію, що надходить або виходить з інформаційної системи.

Він служить брандмауером між локальною та зовнішньою мережею та запобігає будь-яким загрозам. Він призначений для управління вхідним і вихідним трафіком на вашому комп'ютері або локальній мережі, дозволяє блокувати практично всі види мережевих атак, не відправляє інформацію про ваш комп'ютер на інші «чужі» сервери, непотрібні програми — трояни та інструменти управління дозволяє віддалено .

Робота брандмауера полягає в аналізі структури та вмісту інформаційних пакетів, що надходять із зовнішньої мережі, і залежно від результатів аналізу пакети передаються у внутрішню мережу або повністю фільтруються. Існує два типи стін: апаратні та програмні.

Апаратне забезпечення — це пристрій, який фізично підключений до мережі. Цей пристрій відстежує всі аспекти вхідного та вихідного зв'язку, а також адреси та призначення кожного обробленого повідомлення, що забезпечує безпеку, запобігаючи небажаному вторгненню в мережу чи комп'ютер.

Програмне забезпечення виконує ті ж функції, але є не зовнішнім пристроєм, а програмним продуктом, який працює на комп'ютері або призначеному шлюзі. Найпоширеніший тип програмного забезпечення від стіни до стіни.

Брандмауери можуть працювати на різних рівнях протоколів OSI. На рівні мережі вхідні та вихідні пакети фільтруються за IP-адресою. На транспортному рівні фільтрація також здійснюється через номери портів TCP і прапори, що містяться в пакетах. На прикладному рівні аналізуються програмні протоколи та відстежується вміст процесу даних.

1.9 Лог–файли, як спосіб контролю за станом системи

Ведення обліку подій у системі означає знати все, що відбувається в системі, контролювати її роботу та стан.

Файл журналу — це спеціальний файл, який збирає службову та статистичну інформацію про системні (програмні) події. Операційні системи (особливо серверні операційні системи) і серверне програмне забезпечення зазвичай мають розширену систему реєстрації. Їх можна використовувати, щоб змусити систему (програму) записувати практично будь-які події у файли журналів. Відповідно, різні типи подій, різна інформація можуть зберігатися в їхніх спеціальних звітах. Файли записів — це вихідні дані, які необхідно обробити. Визначає якість обробки та якість статистичних даних.

Вони мають всю необхідну інформацію, щоб знати все про користувачів і клієнтів інформаційної системи.

Слід мати на увазі, що повністю «реальну» статистику отримати практично неможливо з ряду технічних причин. Точних способів оцінки відхилення

«реальності» від виміряних значень немає, але за оцінками, це відхилення в середньому не перевищує 5-10%.

1.10 Проблема збору даних

Для своєчасного аналізу та виявлення шкідливих дій необхідна детальна інформація про роботу системи. Більшість операційних систем виконують різні типи аудиту, створюючи журнали транзакцій для різних користувачів. Журнали можна налаштувати лише для подій, пов’язаних із безпекою, або для надання повного звіту про всі системні виклики, ініційовані системою.

Брандмауери та маршрутизатори також записують події в журнали, які містять інформацію про мережу або записи кожного переданого пакету.

Збір та зберігання інформації для подальшого аналізу є залежністю між вартістю та ефективністю системи виявлення конфіденційності. У разі конфігурації системи, в якій усі події детально записуються у файли журналів, вам знадобиться висока обчислювальна потужність і великий обсяг дискового простору, що призведе до збільшення витрат.

Збір і зберігання точної інформації надзвичайно важливий, хоча й дорогий. Залишається питання про те, яку інформацію слід фіксувати і де вона збирається.

1.11 Модель кількісної оцінки рівня уразливості системи

Зручним є використання математичної моделі для визначення рівня безпеки інформаційної системи.

Одна з цих дуже універсальних моделей враховує вплив множини випадкових факторів. Самі по собі їхній вплив не призводить до несанкціонованого доступу до інформації, а скоріше до появи каналів несанкціонованого отримання інформації, які можуть бути використані зловмисником.

Імовірність несанкціонованого отримання інформації порушником k-ї категорії на і-му каналі несанкціонованого отримання інформації в зоні I і-го структурного компонента системи визначається залежністю, наведеною у формулі 1.1.

$$P_{ijkI} = P_{kiI}^{(a)} P_{ijI}^{(c)} P_{ijkI}^{(v)} P_{ijI}^{(i)} \quad (1.1)$$

де $P_{kiI}^{(a)}$ — ймовірність того, що порушник класу k потрапить в і-ю область і-го компонента системи;

$P_{ijI}^{(c)}$ — ймовірність j-го KNOI в і-ій області і-го компонента системи;

$P_{ijkI}^{(v)}$ — ймовірність того, що порушник k-ї категорії потрапить до j-го KNOI в і-й зоні і-го компонента за умови входу порушника в зону;

$P_{ijI}^{(i)}$ — імовірність інформації в j-му KNOI в і-ій області і-го компонента при відвідуванні порушника.

Ймовірність того, що клас зловмисників отримає інформацію в певному компоненті системи без авторизації на KNOI, називають основним показником інформаційної вразливості [4], а її вигляд показано у формулі 1.2.

$$P_{ijk}^{(B)} = 1 - \prod_{i=1}^{N} [1 - P_{kiI}^{(a)} P_{ijI}^{(c)} P_{ijkI}^{(v)} P_{ijI}^{(i)}] \quad (1.2)$$

де N – загальна кількість компонентів системи.

Після виконання згортки основного показника ризику за компонентами системи і, в Отримавши канал інформації j і категорію зловмисника k, ми отримуємо загальну вразливість системи [4], як показано у формулі 1.3.

$$P = 1 - \prod_i [1 - P_{ijk}^{(B)}] \prod_j [1 - P_{ijk}^{(B)}] \prod_k [1 - P_{ijk}^{(B)}] \quad (1.3)$$

2 РОЗРОБКА МАТЕМАТИЧНИХ МОДЕЛЕЙ І ПРОГРАМ ОПТИМАЛЬНОГО УПРАВЛІННЯ СИСТЕМ МОНІТОРИНГУ ЗАХИЩЕНОСТІ ОБ'ЄКТУ

В цьому виконуємо аналіз і розробку моделей і методі оцінки ризиків в системах моніторингу захищеності об'єкту, по можливості – управління ризиками на базі імітаційних моделей. Моделі повинні давати рішення системних задач вибору базового виробника: - між власною системою торгівлі (рітейлу) і оптовими системами; - між власною системою оптових поставок рітейлерам і незалежними системами обслуговування. Надійне рішення можна отримати тільки на базі імітаційних моделей та оптимального агрегування.

2.1 Аналіз особливостей прогнозування на базі моделей

В певних умовах прогноз ризиків майбутнього для певної системи моніторингу захищеності об'єкту може змінювати результати розвитку системи в майбутньому. Така концепція активного прогнозування набула широкого розповсюдження, зокрема у формі так званого «що буде якщо аналізу».

Прогнозування розвитку систем моніторингу захищеності об'єкту принципово відрізняється від прогнозів еволюції сонячної системи тим, що можемо, свідомо, чи не свідомо, змінювати майбутнє своїми діями. Тобто сам прогноз створює варіанти дійсності (прогнозування виборів створює результат виборів). Це не раз відзначалось в історії людства, особливо сьогодні. Вплив прогнозів і певних дій дослідив в теорії і практиці відомий фінансист і філантроп Дж. Сорос. Теж саме стверджував засновник індустріальної динаміки Д. Форрестер. Академік Н.Н. Моісеєв писав, що сьогодні майбутнє не прогнозується, а конструюється, і вкрай незадовільно [18].

"Що буде якщо" аналіз може бути активним прогнозуванням - моделюємо на комп'ютері різні варіанти майбутнього, відбираємо сприятливі для нас варіанти

майбутнього і дивимось, що треба зробити сьогодні, щоб настало бажане завтра. Іноді для цього достатньо найменшого поштовху.

Відомо, що моделі складних систем ніколи не бувають абсолютно ідентичними і остаточними, тому стратегічна ціль даного проекту — на прикладі розробки моделі системи виробників продукції певного класу і проведення досліджень дати можливість користувачу освоїти технологію розробки і використання моделей для прийняття рішень [6].

Виробничі системи(ВС) являють собою ієрархічні структури великої розмірності. Імітаційні моделі ВС повинні задовільно відображати структуру і функції елементів і системи в цілому. Для подальшого розгляду важливо відзначити, що поняття «елемент ВС» ситуативно і динамічно: технологічний процес виробництва деякого продукту — автомобіля, мікропроцесора, хліба опарного з метою оптимізації може розбиватися на субпроцеси і відповідні підсистеми, або, навпаки субпроцеси і підсистеми можуть агрегуватися.

Природно, що і система моделей ВС повинна бути гнучкою для відображення цієї структурної динамічності. Елемент ВС також розглядаємо як технологічний перетворювач ресурсів у продукт. Для цілей даної роботи важливо, щоб моделі елементів і системи в цілому належали до одного класу об'єктів, для яких можна створити алгебру. Аналогом такої алгебри може бути алгебра для лінійних динамічних систем. Довільні структури із елементів динамічних систем заданих передавальними функціями і з'єднаних паралельно, послідовно і зворотними зв'язками можуть бути перетворені в еквівалентний по входу-виходу елемент. У даній роботі використовується аналогічна (ізоморфна) алгебра виробничих систем з доповненням – вбудованою оптимізацією .

На рисунку 2.2 представлені моделі виробничого елемента і базових структур з'єднань елементів.

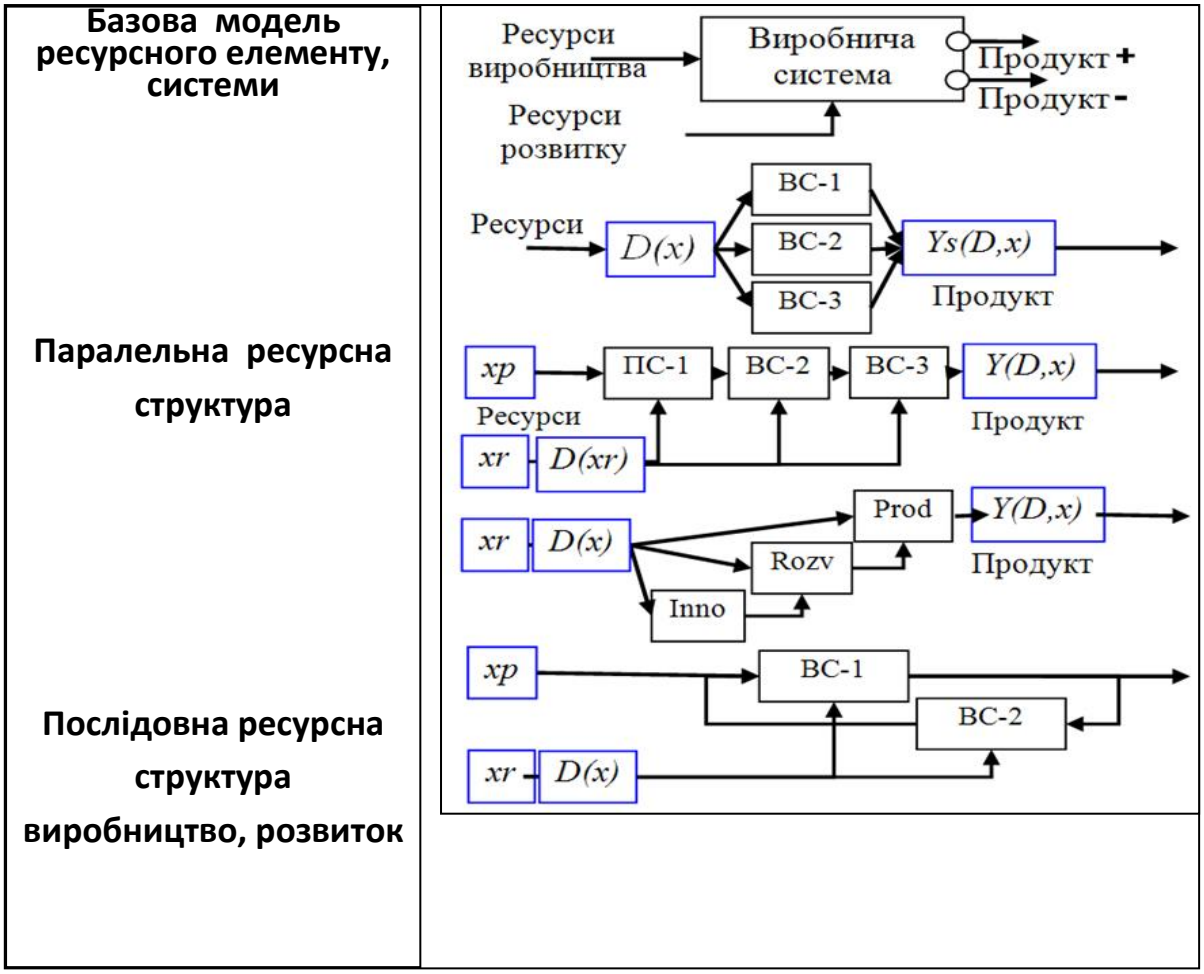


Рисунок 2.2 — Базові ресурсні структури виробничих систем

Формально моделі статики і динаміки систем виробничих рівня «підприємство» мають високу розмірність. Високу розмірність мають і оптимізаційні задачі. Проте урахування властивостей структур і функцій виробничих систем дозволяє зменшувати розмірність оптимізаційних задач. У практиці і теорії широко використовується агрегування у виробничих системах для випадку паралельно працюючих елементів.

Типовий приклад — агрегування до рівня сумарного виробництва держави. Математичним моделям виробництва більше 200 років. Були розроблені статистичні методи агрегування на базі простого підсумовування. Потім під можливості арифмометрів розробили лінійне програмування, яке досі є здоровою,

безвідмовної базою автоматизованих систем. Головні недоліки таких моделей – апроксимація статистичних даних неадекватними моделями — статичними, логарифмічними функціями; агрегування для стихійно сформованих розподілів ресурсів або навантаження виробничих потужностей [3].

Методологія та конкретні методи оптимального агрегування не вирішують проблеми «прокляття розмірності», негладких функцій, гіперболічних розподілів ймовірностей і пошуках в локальних екстремумах [4].

Принципова відмінність методу оптимального агрегування від аналогів в тому, що воно виконується виходячи з умови максимізації сумарного випуску (для базової задачі) випуску. Змінна управління - вектор розподілу ресурса. Можна сказати, що для кожного значення ресурсу системи шукаємо максимум, її можливість - вбудовуємо задачу оптимізації в завдання еквівалентного перетворення виробничої системи.

Принципова відмінність від класики нелінійного програмування в тому, що при оптимізації шукається не точкове рішення (оптимальний розподіл обмеженого ресурсу і сумарний випуск), а функції від величини обмеження по ресурсах.

Принципова відмінність алгебри виробничих елементів від алгебр чисел, розподілів ймовірностей, передаточних функцій лінійних систем — збереження «пам'яті» попередніх операцій.

Головний практичний висновок за результатами розглянутої методології оптимального агрегування - можливість звести досить широкий клас виробничих систем у еквівалентні оптимальні одновимірні, не втрачаючи інформації про характеристики елементів і зв'язки між ними. Це виправдовує використання на перших етапах аналізу і синтезу одновимірних - агрегованих моделей динаміки ВС [5]. На рисунку 2.3 представлено оптимальне агрегування типових структур виробничих систем.

У даній роботі аналіз ризиків базується не тільки на статистичному аналізі, але і на ефективних моделях динаміки виробничих систем. Уточнимо розхожий термін

«ефективний»: мається на увазі модель, що відтворює реальні суттєві для задач дослідження внутрішні і зовнішні причинно-наслідкові зв'язки системи, що допускає оптимізацію без обмежень на класи залежностей типів: тільки лінійні, тільки квадратичні, «опуклі», не перервні і т.д. Особливо виділимо радикальну особливість методу оптимального агрегування» усунення проблем розмірності оптимізаційної задачі.

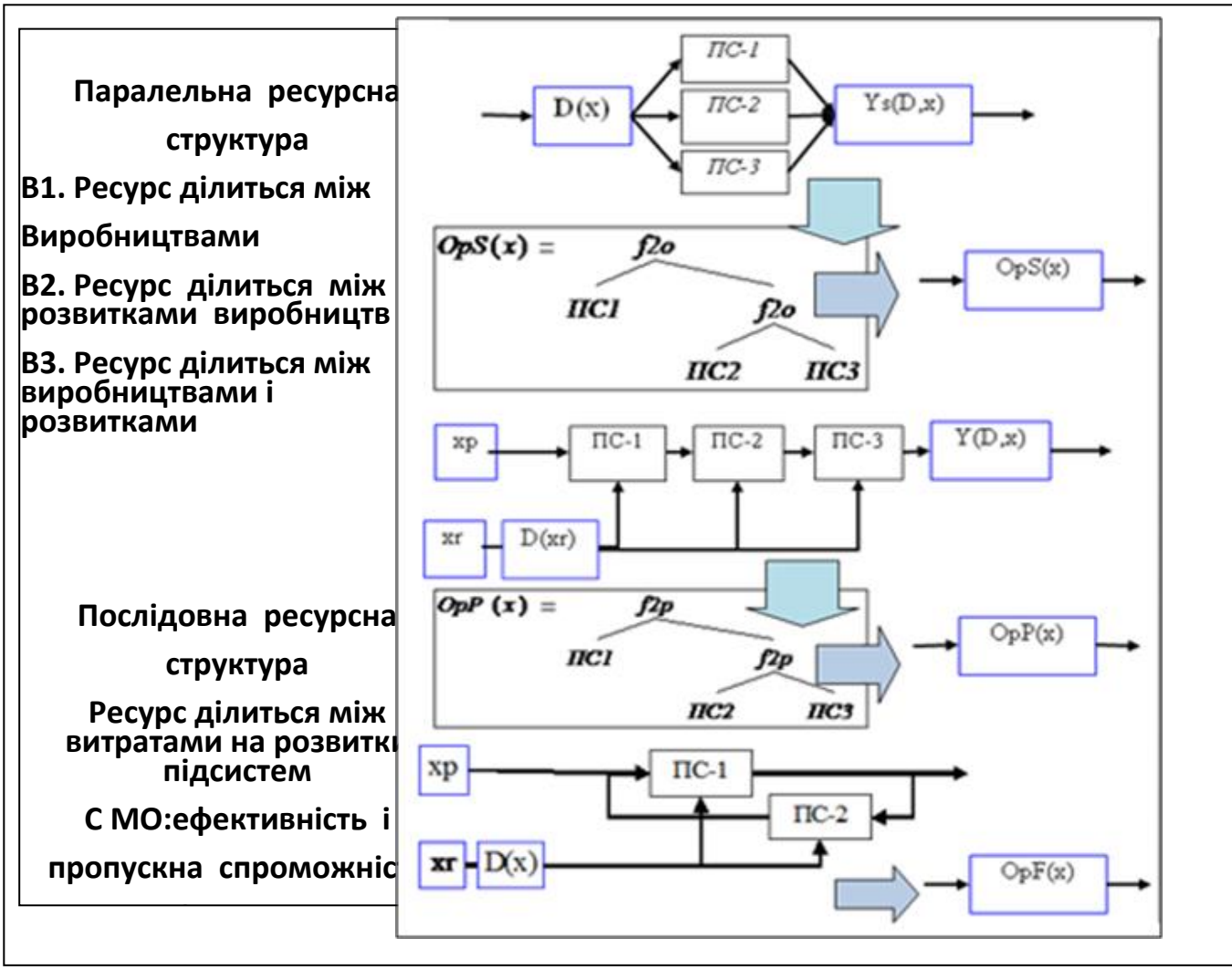


Рисунок 2.3 — Оптимальне агрегування типових структур ВС

Проблему розмірності Р. Беллман називав «прокляттям розмірності». Щоб знайти методом перебору екстремум функції однієї змінної з точністю 0.01 треба обчислити її 100 разів, а для функції від 10 змінних — вже 10010 разів. Від проблеми

можна позбавитись або вирішивши її, або усунувши. В методі оптимального агрегування ця проблема саме усувається: задачу оптимізації функції 10 змінних ми розкладаємо в 10 одновимірних задач.

2.2 Детерміновані моделі статики і динаміки ВС

Виконаємо короткий огляд відібраних концептуальних основ для формування моделей, орієнтованих на аналіз ризиків [6]. Інтелектуальні системи не є замінниками логіки і математиками в області побудови оптимальних і живучих комп'ютерних систем. Всі процедури там пошукові, а в сучасних компютерно інтегрованих системах всі обчислення прив'язуються до реального часу — «минулого», «поточного», «майбутнього». Проблеми узгодження процесів обслуговування, управління конвеєрами, аеропортами суттєво актуальні, рішення цих проблем відомі, але методи оптимального агрегування виконують узгодження процесів в часі не тільки з гарантованою точністю і надійністю, але і оптимально за ресурсними критеріями мінімізації витрат і втрат. Розглянемо базові моделі функціонування і розвитку ВС. Спочатку, визначимо використані терміни: — функціонування: випуск продукції при незмінних ФВ; — розвиток: зміна ФВ: підвищення ефективності, виробничих потужностей, за рахунок витрат на нове обладнання, модернізацію та ін.

Динамічні системи можна представити різними способами, в тому числі, як модулі над кільцями, але це надлишково-відносні цілі роботи. Безперервні динамічні системи можна представити звичайними нелінійними диференціальними рівняннями. Відразу будемо прив'язувати загальні моделі до конкретних задач моделювання процесів функціонування та розвитку ВС. Запишемо разом диференційні рівняння для одновимірної і багатовимірної систем:

$$\frac{d}{dt}x(t) = fin(y(t), i) \text{ — одновимірна,} \qquad (2.1)$$

$\frac{d}{dt}X(t) = Fin(Y(t), i)$ — багатовимірна система, (2.2)

де $x(t)$, $y(t)$ — поточні значення стану і управління;

$X(t)$, $Y(t)$ — поточні стану векторів стану і управління;

$fin(y(t), i)$, $Fin(Y(t), i)$ — праві частини диференційних рівнянь — функція і вектор-функція від змінних стану та управління.

Прив'язуємо модель до задачі розвитку: $fin(y(t), i)$ — функція розвитку (інша назва - функція віддачі інвестицій); $y(t)$ - обсяг ресурсів за одиницю часу — крок моделювання, планування, виділених на розвиток [7]. Далі використовуються складніші структури даних, функцій і операторів . Щоб отримати конкретне рішення диференційного рівняння, слід задати граничні умови, Рішення лінійного диференційного рівняння може бути представлено у вигляді інтеграла згортки двох функцій. На рисунку 2.4 представлені базові моделі функціонування та розвитку ВС.

Модель "задача розподілу" (Р.Беллман)

Модель об'єкта: $\frac{d}{dt}x_i(t) = Gi[x_i(t), y_i(t)]$;

вихід: $X(t) = \sum_i x_i(t)$;

управління: $Y(t) = \sum_i y_i(t)$

Критерій $J(Y(t)) = \int_0^T F(X(t), Y(t))\,dt$ (першого роду - не квадратичний)

Управління: $(y_1, y_2, .., y_i, .., y_N)$; $i = 1..N$; $0 \le Y(t) \le X(t)$;

де $X(t)$- сумарний темп виробництва;
$y(t)$- сумарний темп витрат на розвиток.

Обмеження моделі: модель "виробництва" - лінійна, проблеми розмірності.

Базова агрегована модель розвитку

Модель об'єкта $\frac{d}{dt}x_i(t) = fin[x_i(t) \cdot u_i(t)]$; $i = 1..N$

Агрегування $\frac{d}{dt}X(t) = Fop(X(t) \cdot U(t))$; $Fop(y) = Opagr(Fin(y), f2o, N)$

де $Opagr$ - оператор оптимального агрегування виробничої системи;
$Fin(y)$ - вектор-функція з ФР елементів;
$f2o$ - бінарний оператор оптимального агрегування.

Критерій $J(u(t)) = \int_0^T Fop\,[X(t) \cdot (1 - U(t))]\,dt$ - накопичення.

Управління - $0 \le U(t) \le 1$ частка ресурсу в розвиток виробництва.

Дезагрегування управління - вбудоване в бінарний оператор $f2o(f1, f2)$.

Рисунок 2.4 — Базові моделі функціонування та розвитку ВС

Дискретизовані моделі динаміки виробничих систем. Існують дискретні моделі реальних дискретних систем (наприклад, кулемет або курка-несучка) та еквівалентні дискретні моделі безперервних систем [8-9].

Запишемо різницеві рівняння для одновимірної і багатовимірної системи:

$x_{k+1} = fp(x_k, y_k, \Delta T)$ — одновимірна; (2.3)

$X_{k+1} = Fp(X_k, Y_k, \Delta T)$ — багатовимірна система, (2.4)

де ΔT — крок квантування процесу;

x_k, y_k, X_k, Y_k — поточні значення стану і управління на k-му кроці процесу;

$fp(x_k, y_k, \Delta T)$, $Fp(X_k, Y_k, \Delta T)$ — оператори переходу між сусідніми станами.

У разі багатовимірних систем оператори та стани можуть бути більш складними, ніж матриці і вектори, взаємоузгодженими структурами, наприклад куб з матриць, матриця, елемента якої – вектори і матриці.

Наведемо приклад такої структури для системи масового обслуговування з паралельними каналами. Не використовуємо те, що напрацьовано в галузі інтегральних рівнянь, зокрема інтегральні згортки. У теоретичному плані в якості побічного результату уникаємо проблеми перевірки та докази адекватності моделей функціонування та розвитку виробничих систем: якщо для техпроцесів достовірно виявлені породжуючі механізми (типу законів механіки, електро- і термодинаміки, біології, екології та психології). Сучасні моделі і методи адекватності базуються на апроксимації, статистикою і квадратичному інтегральному критерії [10].

У середовищі пакетів для моделювання завжди можна отримати робочі моделі - аналоги інтегралів згортки (перехідної функції динамічної системи і вхідного сигналу).

$$X_{k+1} = Fp\left(X_k, \Delta T\right) \tag{2.5}$$

$$KMd\left(N, X0, \Delta T\right) = \left| \begin{array}{l} Xx_1 \leftarrow X0 \\ for\ \ k \in 2..N \\ \quad Xx_k \leftarrow Fp\left(X_{k-1}, \Delta T\right) \\ Xx^T \end{array} \right. \tag{2.6}$$

Результат роботи наведеної програми — масив чисел: матриця з N стовпців-векторів стану системи для кожного кроку дискретизованого процесу. Для отримання конкретного процесу необхідно задати параметри системи. Це гарантовано властивостями динамічних систем і алгоритмічними методами обчислення [11].

Зауваження. Використання вбудованих методів програмних середовищ, комплексів для рішення типових задач управління обмежене спрощеними моделями і методами, закритими текстами та ін. На жаль, важкі і витратні задачі управління не можуть бути розподілені на зразок аутсорсингу: процес розробки моделей і програм повинен бути локалізованим в руках малої групи виконавців. [6]

Сучасні можливості програмування дозволяють отримувати рішення числовими методами в параметризованій формі. Результат отримується у вигляді функції користувача від змінних і параметрів. Фактично отримуємо повноцінний замінник аналітичних рішень в алгебраїчній формі.

2.3 Аналіз і розробка модулів нелінійних перетворень випадкових процесів

2.3.1 Моделі невизначеностей зовнішнього середовища

Сучасні комп’ютерні системи працюють в умовах різноманітних невизначеностей і збурень зовнішнього і внутрішнього середовищ. Ці невизначеності мають різні джерела і різний характер. Саме невизначеності диктують методологію і технологію побудови математичних моделей обчислювальних систем, а ефективність процесів функціонування і розвитку комп’ютерних систем суттєво буде залежати ефективності імітаційних моделей, що використовуються як інструменти тактичного і стратегічного управління комп’ютерною системою. В даній роботі використовуються інформаційні технології побудови імітаційних моделей в середовищах відповідних пакетів.

Постановка задачі. На базі проведеного в розділі 1 аналізу сучасних комп’ютерних систем виділяємо їх суттєві особливості. На цій основі робимо абстрактну модель комп’ютерної системи. Реалізуємо абстрактну модель у зручному середовищі моделювання — робочу модель комп’ютерної системи. Відлагоджуємо субмоделі невизначеностей та управління КС. В обчислювальних експериментах оцінюємо адекватність моделі на системному рівні — відтворення якісних характеристик процесів функціонування комп’ютерних систем згідно методології Д. Форрестера [11]. Після проведення етапу верифікації можна перейти до етапу розробки інтерпретацій моделі обчислювальної системи з урахуванням впливу невизначеностей. На цьому етапі потрібна повна і достовірна інформація відносно комп’ютерної системи певного класу.

Аналіз невизначеностей. Для аналізу і синтезу моделей комп’ютерних систем використовуються такі концепції: виробничі системи; системи масового обслуговування. Компьтерні системи мають безліч застосувань, а розробка в даному проекті повинна забезпечувати настроювання на весь їх спектр. На рис 2.4 подано класифікацію комп’ютерних систем для більш частих застосувань.

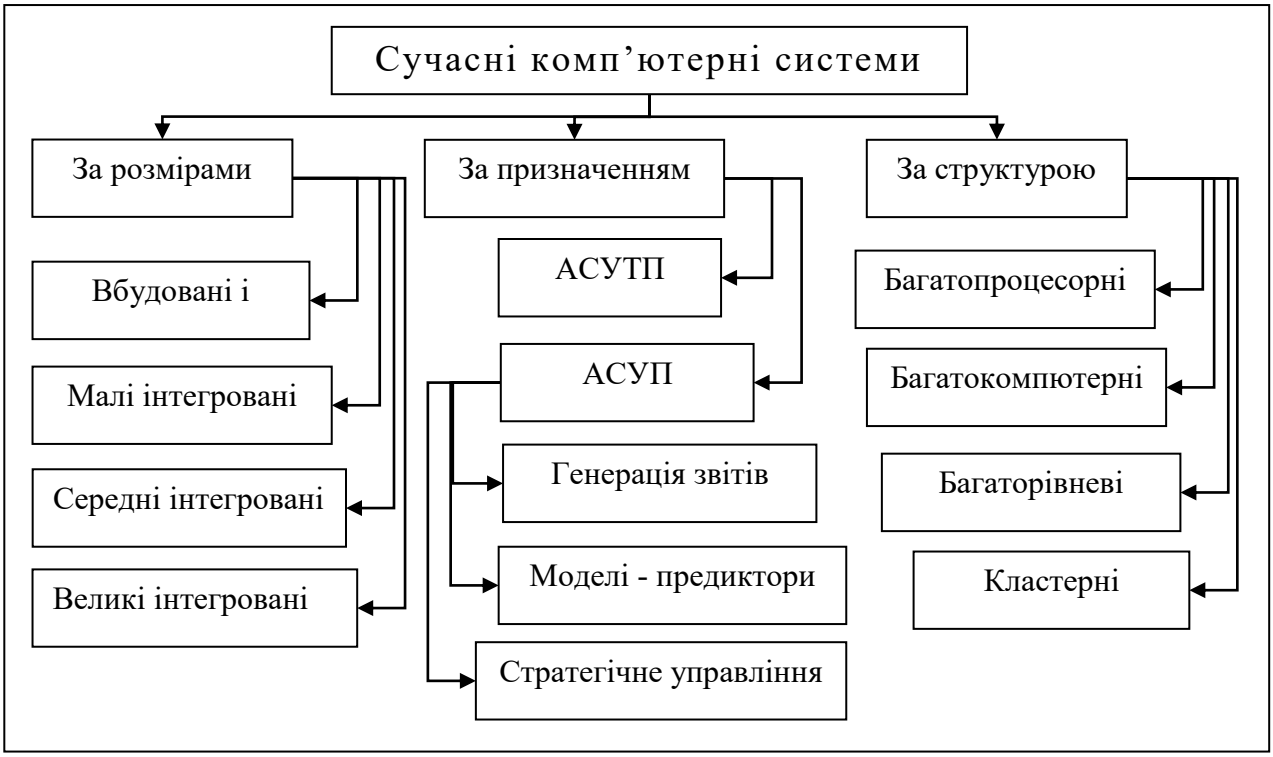


Рисунок 2.4 — Класифікація комп'ютерних систем

В даній роботі розглядати комп'ютерну систему як виробництво «багатопродуктову розподілену систему» у випадку досить стабільного потоку задач, і «багатофазну, розподілену багатоканальну систему масового обслуговування» для суттєво імовірнісного потоку задач. Робимо орієнтовану на цілі роботи класифікації комп'ютерних систем — за розмірами, призначенням і структурою Особливість такого типу класифікації в тому, що між рівнями класифікацій існує узгодженість — для КС кожного призначення існують оптимальні масштаби і структура.

Класифікацію невизначеностей виконаємо в термінах виробничих систем: «ресурс», «продукт», функції «виробництва», «розвитку», «освоєння», «попиту». Існують інші альтернатива побудови класифікації. Розглядаємо: - невизначеність виробництва; — невизначеність ринку; — невизначеність прийняття рішень (управління).

В детермінованій моделі ресурси елементу КС виділені на розвиток виробництв ділились згідно певному критерію очікуваної ефективності. В імовірнісній моделі даного розділу ресурси діляться між елементами теж пропорційно очікуваній ефективності, але імовірнісно. На рис. 2.5 подана орієнтована на побудову системи імітаційних моделей КС класифікація невизначеностей.

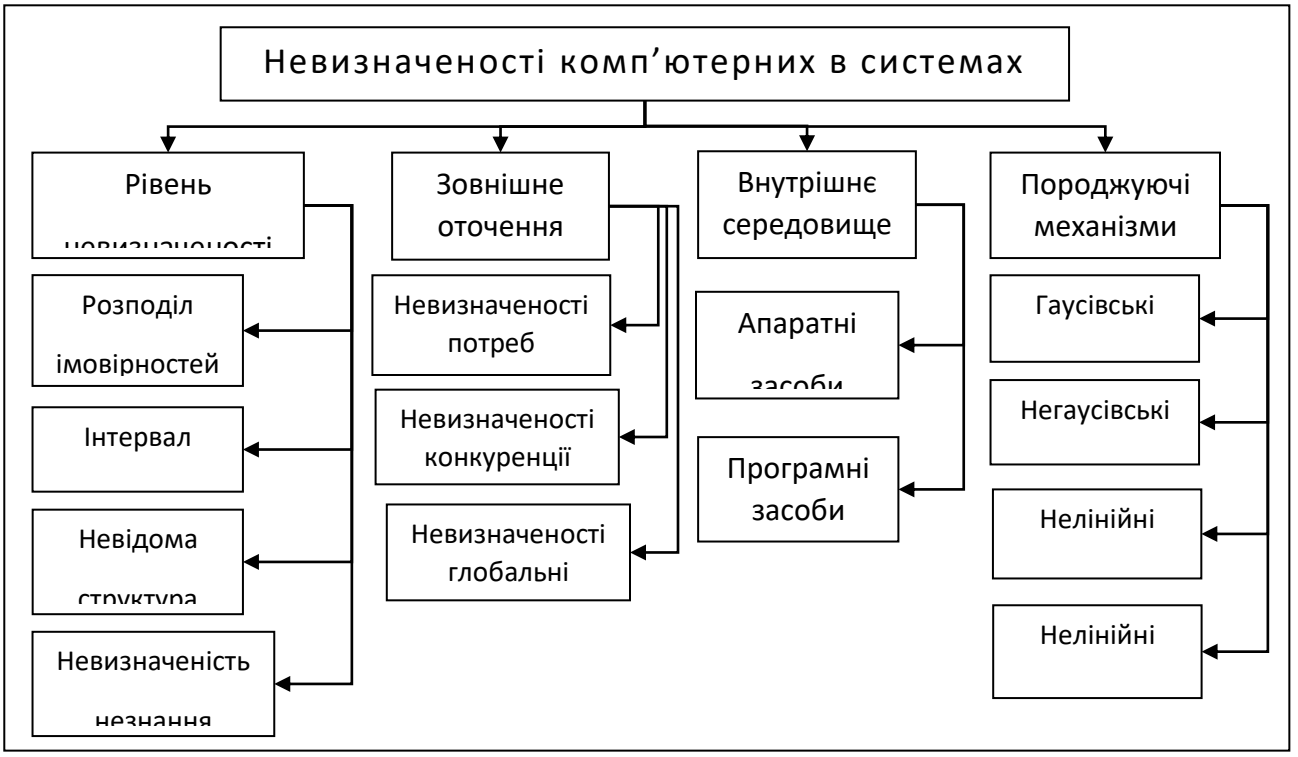


Рисунок 2.5— Класи невизначеностей в комп'ютерних системах

Невизначеність в прийнятті рішень може трактуватися як результат невизначеності вхідних даних для прийняття рішень, неадекватності математичних моделей процесів. Сьогодні багато наукових робіт присвячено проблемі суб'єктивності менеджерів в прийнятті рішень, зокрема такому ефекту як намагання "відіграти ся" у разі програшу — у виробництві. на ринку.

Природно оцінити вплив такої випадковості, коли менеджер в середньому діє раціонально, але з певними випадковими відхиленнями. Невизначеність є одним з методів "боротьби" з невизначеністю зовнішнього оточення. Суть такого підходу в

тому, щоб в умовах невизначеності робити випадкові проби, експерименти, а потім по результатам проб - коректувати імовірності певних рішень. Це відповідає природним механізмам навчання, на цьому базується метод випадкового пошуку. Існують більш глибокі причини корисності невизначеності і ризиків у великих системах отримання інформації про динаміку об'єкта і характеристики випадкових збурень. . На рис. 2.6 подана структура типових перетворень.

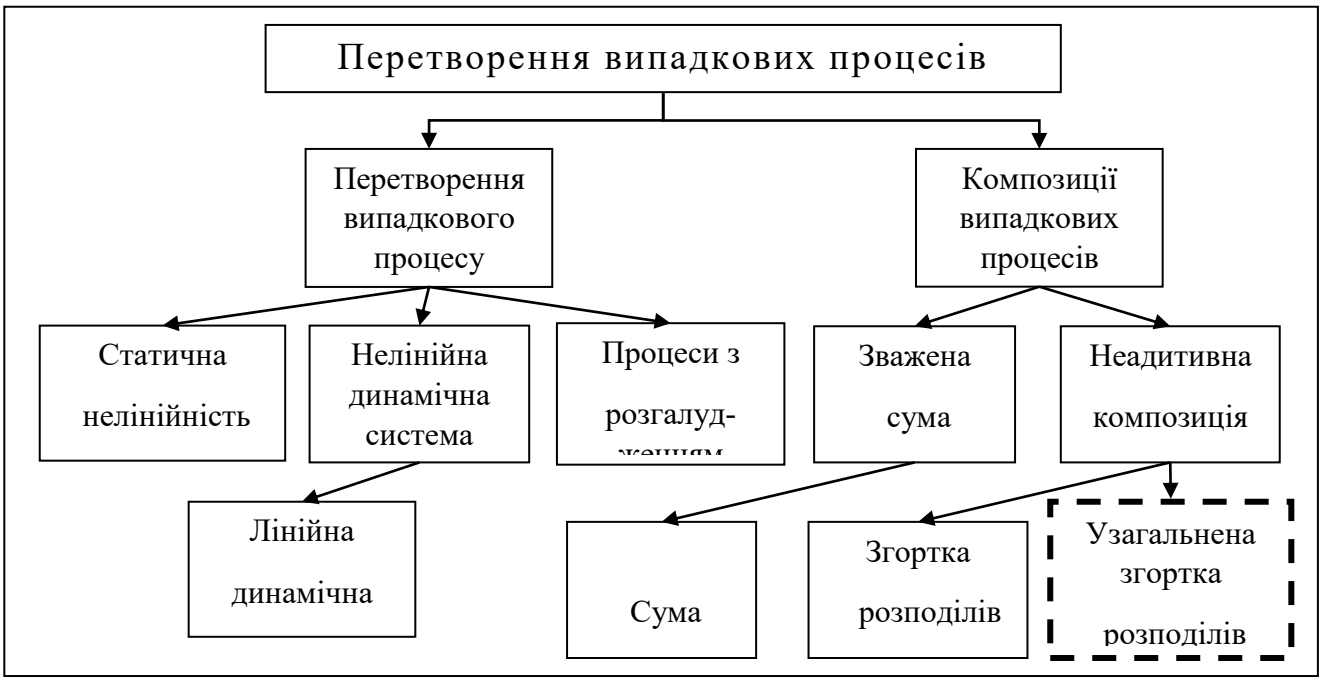


Рисунок 2.6 — Операції перетворень випадкових процесів

Кінцевий етап дослідження — виявлення та кількісна оцінка ризиків. Будуємо орієнтовану на цілі дослідження класифікацію ризиків (рис. 2.7). Природно при оцінці втрат при певних порушеннях роботи КС проаналізувати порушення в роботі об'єкта управління чи обслуговування для даної. КС.

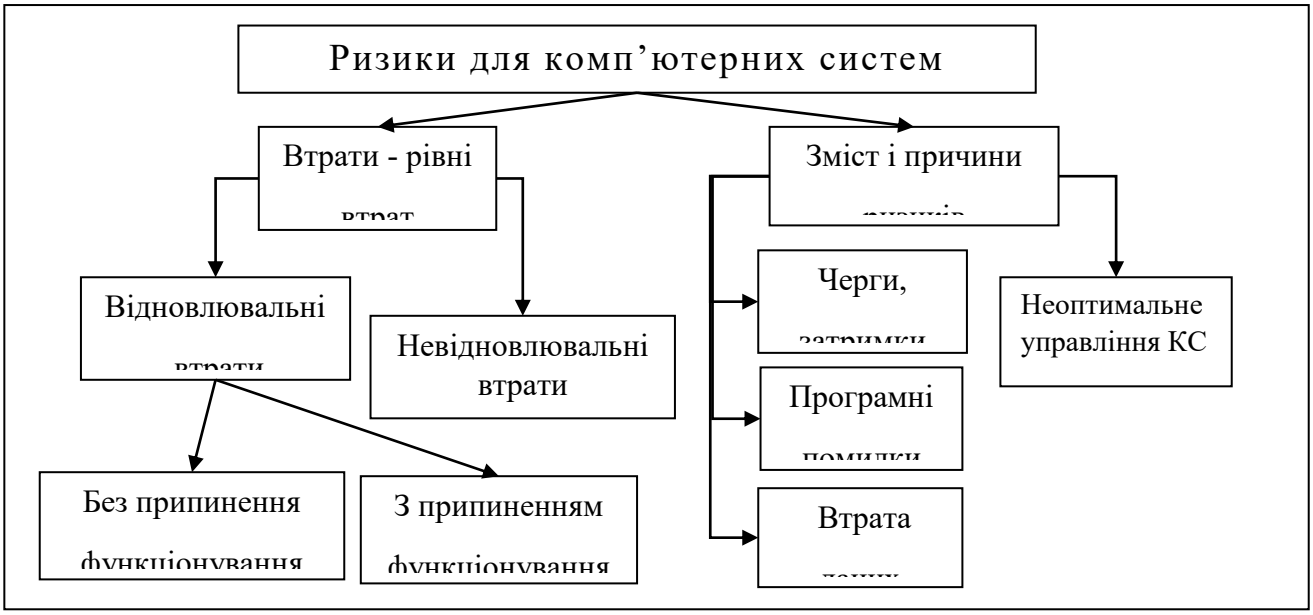


Рисунок 2.7 — Об'єкти і наслідки втрат в комп'ютерних системах

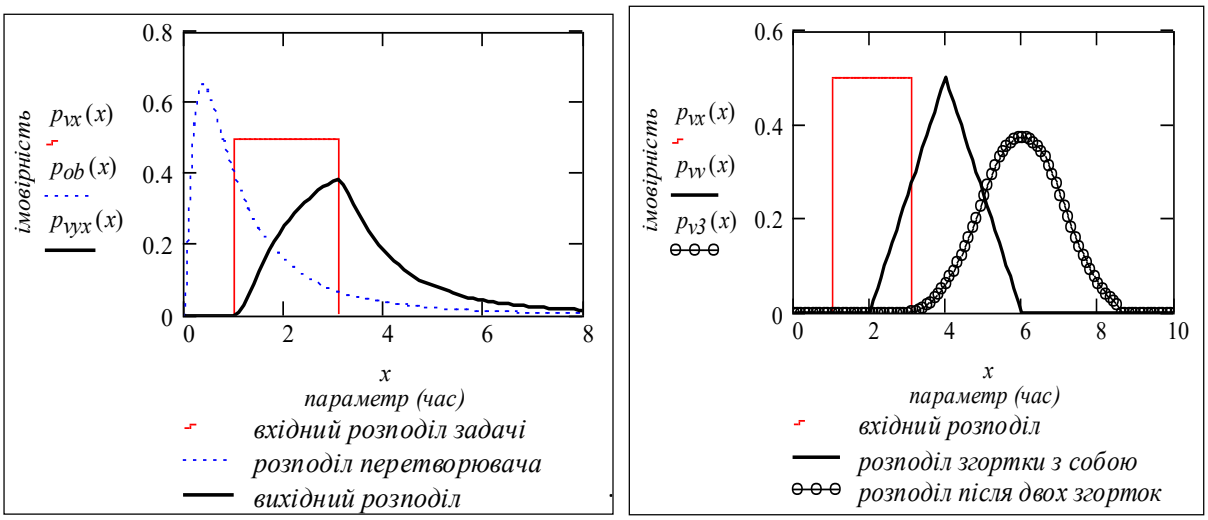
Головна задача дослідженні не стільки оцінка ризикових втрат, скільки розробка моделей і методів зменшення і усунення втрат. Як було сформульовано в розділі 1, було вибрано доповнення і розширення від статистики на базі реальних об'єктів, статистику базовану на імітаційних моделях об'єктів вибрано.

2.3.2 Породжуючі механізми для типових розподілів ймовірностей

Наука і практика оперує переважно з гаусівською статистикою, основні властивості якої: згортки довільних розподілів з кінцевою дисперсією, в тому числі багаторазова згортка довільного розподілу з собою, сходяться до Гаусівського (нормального) розподілу. Центр уваги в обробці даних – обчислення критеріїв перевірки статистичних гіпотез. В даній роботі вибрано підхід на базі «породжуючих механізмів» [J. Forrester]. Відповідь на питання, чому такий підхід не використовувався раніше? — раніше ще не було ефективних комп'ютерних систем та ІВС.

На рис.2.7 подано приклади згорток: ліворуч — логнормального і рівномірного розподілів, праворуч — рівномірного розподілу з собою: один раз —

трикутне, два рази — подібнтй до нормального розподіл. Неважко прийти до висновку, що результатом повторення згортки з собою буде нормальний розподіл



Рискнок 2.7 — Приклади згорток розподілів ймовірностей

Існує поняття «стійкий розподіл ймовірностей». Теорія ймовірності розділяється на дві частини:

— розподіли з обмеженою дисперсією – гаусівські, нормальні;

— розподіли з нескінченою дисперсією – негаусівські , гіперболічні.

Ці розподіли є зовнішніми проявами різних породжуючих механізмів:

Гіперболічні розподіли породжуються процесами зростання в біології, техніці, економіці і екології — в активних системах.

Гаусівські розподіли породжуються процесами в пасивних системах — в економіці — в рівноважних, в геології — утворення рельєфів, русел та ін.

Гаусівський розподіл має кінцеву дисперсію. Перевіряємо це експериментально, записуємо формулу для дисперсії (середньоквадратичного відхилення від середнього), підставляємо вбудовану функцію пакету нормального розподілу з дисперсією 2. Обчислюємо вираз для двох інтервалів інтегрування.

$$disp = \int_{-DX}^{DX} (mu - dnorm(x, mu, sigm))^2 \, dx \qquad DX1 := 10 \qquad DX2 := 1000$$

$$\frac{1}{DX1} \cdot \int_{-DX1}^{DX1} (1 - dnorm(x, 1, 2))^2 \, dx = 1.814 \qquad \frac{1}{DX2} \cdot \int_{-DX2}^{DX2} (1 - dnorm(x, 1, 2))^2 \, dx = 1.998$$

Гаусівські розподіли імовірностей. Існує два підходи до ідентифікації емпіричних частотних розподілів — формальний: приймається «гіпотеза про теоретичний розподіл» і за певними критеріями приймається чи не приймається ця гіпотеза; аналізуються причини, механізми породження випадкового процесу, будується модель, шукаються параметри породжуючого механізму, що генерують процес близький, за певним критерієм до реального процесу. Тобто ідентифікація проводиться не на рівні розподілів а на рівні породжуючих процесів.

Таким чином, перше що нам потрібно — мати певну базу знань про типові частотні розподіли імовірностей. За кожним розподілом ймовірностей стоїть певний породжуючий механізм. Тобто сам по собі розподіл для нас — індикатор діючих у виробничій, сервісній в обчислювальній системах механізмів. Знаючи цей механізм, ми зможемо ефективно прогнозувати стан системи, а головне ми можемо ефективно управляти системою, зокрема, змінити сам породжуючий механізм, наприклад, «механізми взаємодії виробника і користувачами.

Аналіз породжуючих механізмів теоретичних розподілів. Між емпіричними розподілами відносних частот — «гістограмами» і «теоретичними» розподілами ймовірностей має місце тісний зв'язок. Часто їх не розрізняють, але це може привести до помилок. Розподіл ймовірностей - гранична форма розподілів відносних частот при необмеженому збільшенні кількості спостережень чи експериментів. Такий розподіл прийнято називати істинним розподілом ймовірностей для генеральної сукупності даного типу експерименту. Розподіли імовірностей можуть бути дискретними і неперервними. Вивчення розподілів

почнемо з неперервних розподілів імовірностей. Будуємо модуль імітації механізму породження нормального розподілу:

$$pn(x,\mu,\sigma) := \frac{1}{\sigma\cdot\sqrt{2\cdot\pi}}\cdot\exp\left[\frac{-1}{2\cdot\sigma^2}\cdot(x-\mu)^2\right] \qquad (2.7)$$

Нормальний розподіл. Перевіримо, що розподіл для випадкового числа, що є сумою незалежних випадкових чисел сходиться до нормального розподілу.

Задаємо: обсяг вибірки $Nv := 100000$; $i := 1..Nv$; кількість інтервалів гістограми $kin := Nv \div 1000$ Формуємо вибірки: одне вч $Vd1_i := 10\,rnd(1) - 5$

два випадкових числа $Vd2_i := \left(\frac{10}{2}\right)\cdot(rnd(1) + rnd(1)) - 5$

чотири випадкових числа $Vd4_i := \left(\frac{10}{4}\right)\cdot(rnd(1) + rnd(1) + rnd(1) + rnd(1)) - 5$.

Будуємо гістограми $Hi1 := histogram(kin, Vd1)$; $Hi2 := histogram(kin, Vd2)$

$Hi4 := histogram(kin, Vd4)$

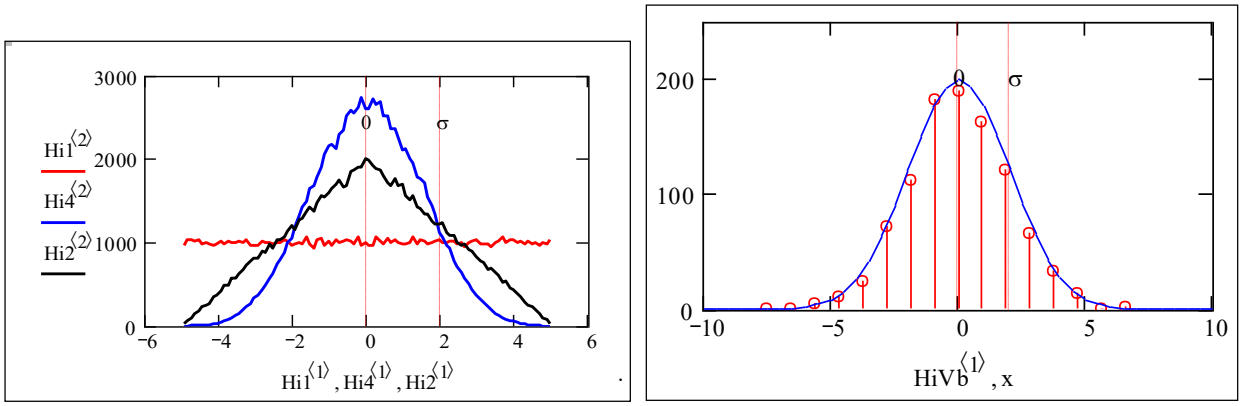


Рисунок 2.9 — Модуль генерації нормального розподілу

В сучасних пакетах для статистичного моделювання зроблено вбудовані функції, що видають задану кількість випадкових чисел с заданим частотним розподілом. Використовуємо в побудові моделей цю функцію так (рис.2.7, 2) :

скільки:= 1000 ; кількість інтервалів ki := 16 середнє := μ станд_відхил := σ .

Реалізація: Vbn := rnorm(скільки, середнє, станд_відхил) HiVb := histogram(ki , Vbn)

Пуасонівський розподіл. Рівняння для розподілу щільності імовірностей (= "частотного розподілу")

$$pp(k,\lambda) := \frac{e^{-\lambda}\cdot\lambda^{k}}{k!} \quad ; \qquad (2.8)$$

Будуємо графіки розподілу (2.8). Задаємо параметри розподілу (тільки один): $\lambda := 15$ - середнє , змінна розподілу $k := 1..40$.

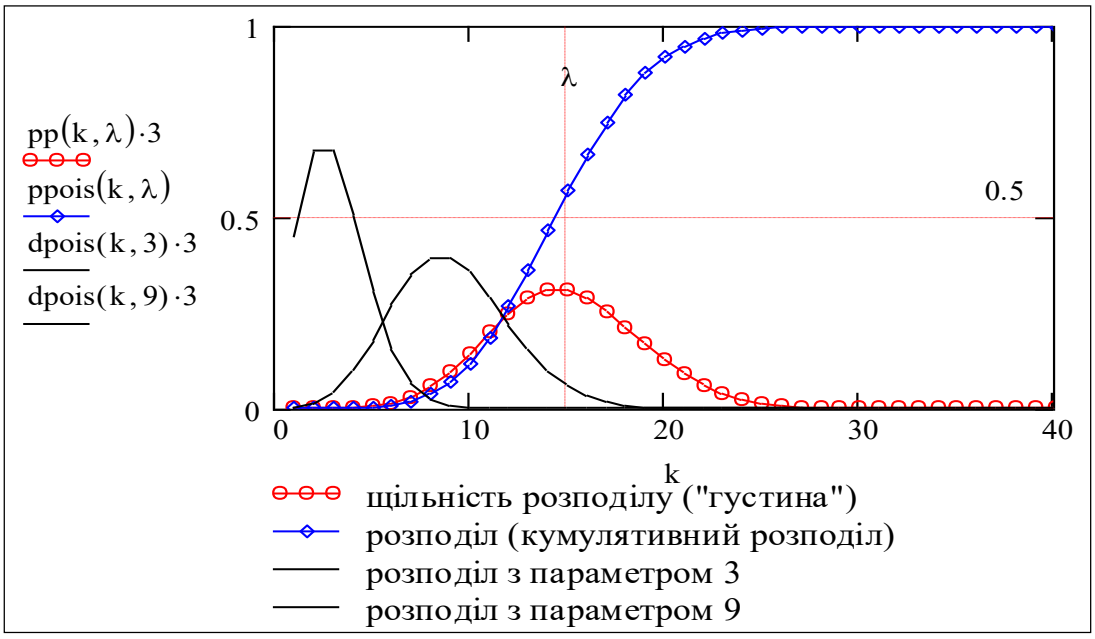


Рисунок 2.10 — Модуль генерації Пуассонівського розподілу

Механізм породження Пуассонівського розподілу: маємо незалежні події (так —1 , ні —0), що відбуваються незалежно (некорельовано) у випадкові моменти часу. Параметр характеризує середню кількість подій в одиницю часу. Розподіл — залежність імовірності випадкової величини "кількість подій за одиницю часу" від значення кількості подій. Моделювання механізму породження Пуассонівського розподілу. Робимо імітаційну модель породження випадкового процесу

Пуассонівським розподілом. Робимо базову відкриту імітаційну модель для урахування цих відхилень. Задаємо вхідні дані $lmd := 10$; Задаємо: кількість незалежних джерел подій $Nob := 100$; $k := 1..Nob$; обсяг вибірки ("кількість заявок в одиницю часу") $Nvyb := 1000$; $i := 1..Nvyb$

$$Impup(lm) := \left| \begin{array}{l} par \leftarrow \frac{lm}{Nob} \\ sumpo \leftarrow 0 \\ \text{for } q \in 1..Nob \\ \quad sob_q \leftarrow rnd(1) \le par \\ \quad sumpo \leftarrow sumpo + sob_q \\ sumpo \end{array} \right.$$

$Vyb_i := Impup(lmd)$

$Vyb =$

	1
1	7
2	13
3	9
4	4
5	9

(2.9)

Функція генерації чисел з заданим розподілом – основа імітації вхідних потоків задач. Технологія її застосування: $скільки := 1000$; кількість інтервалів $ki := 20$; $середнє := lmd$; Власне генератор: $Vbn := rpois(скільки, середнє)$ $HiVb := histogram(ki, Vbn)$. Дивимось на цей графік і робимо висновок:

а) поданий вище програмний модуль імітує випадкову подію в СМО "кількість замовлень протягом однієї хвилини"; емпіричний розподіл досить добре збігається з теоретичним, параметри якого ми задали в програмі імітації. Оце і є ідентифікація, а перевірка гіпотези "чи даний емпіричний розподіл є відображенням даного теоретичного" за критеріями Пірсона, Колмогорова є поліруванням висновку.

Дослідження породжуючих механізмів невизначеностей. Негаусівський розподіл процесу з розгалуженнями. В комп'ютерних системах мають місце процеси, де наступна випадкова подія залежить від попередніх. Існують декілька

альтернативних математичних моделей для опису функціонування активних систем. Процеси з розгалуженням при певних умовах породжують негаусівські розподіли ймовірностей.

Будуємо базовий модуль «процес з розглудженням» (отримані 2 свідоцтва на програми) . В такому процесі, деякі елементи можуть ймовірнісно рости, «розмножуватись», «зникати». Механізм процесів з розгалуженням описати досить легко, але отримати аналітичні розв'язання навіть для простих задач дуже важко. Для реалістичних задач майже єдиний шлях досліджень — використання імітаційної моделі процесу з розгалуженням.

Побудова робочої математичної моделі процесу з розгалуженням. Словесна формула базової моделі процесу породження задач обробки даних, випуску чергової моделі мікропроцесора та ін:

— імовірність появи нової задачі від певного джерела (підсистеми виробництва) за час Dt, при умові появи вже X задач, вважаємо пропорційною цій кількості, тобто:

$$p1(x->x+1) = \lambda*x*Dt = Функція\_росту(\lambda x,t) \quad (2.10)$$

— імовірність припинення появи нових задач на інтервалі Dt вважаємо постійною

$$p2(process->stop) = \mu*Dt = Функція\_зупинки(\mu x,t) \quad (2.11)$$

Запишемо у загальному вигляді математичну модель - систему рівнянь процесу.

$$\begin{pmatrix} S_{q,t+1} \\ Y_{q,t+1} \end{pmatrix} = \begin{pmatrix} ФункціяЗупинки(\mu, t, Y_{q,t}) \cdot S_{q,t} \\ Y_{q,t} + ФункціяРосту(\lambda, Y_{j,t-1}) \cdot S_{q,t} \end{pmatrix} \quad (2.12)$$

де $S_{q,t}$ — змінна-індикатор: “чи припилась поява нових задач з q-го джерела задач на t-ому кроці”;

$Y_{q,t}$ —змінна “кількість задач від q-ого елемента на t-ому кроці процесу”.

Задаємо параметри процесів росту $\lambda a = 0.09$ та зупинки $\mu ю = 0.17$, початкові умови $Y_{q,1} := 1$; $S_{q,1} := 1$. Записуємо тепер робочі рівняння згідно з прийнятими моделями росту і зупинки:

$$\begin{pmatrix} S_{q,t+1} \\ Y_{q,t+1} \end{pmatrix} := \begin{bmatrix} if\left(rnd(1) > \mu ю, 1, 0\right) \cdot S_{q,t} \\ Y_{q,t} + if\left[rnd(1) > \left(1 - \lambda a \cdot Y_{q,t}\right), 1, 0\right] \cdot S_{q,t} \end{bmatrix} \qquad (2.13)$$

Будуємо графіки частотних і рангових розподілів обчислених для двох наборів параметрів (рис.2.12). Бачимо схожість з теорією. Період моделювання $Tmodel \equiv 30$ Число елементів $Me \equiv 1000$ Ймовірності: успіху $\lambda a \equiv .09$ зупинки: $\mu ю \equiv .17$. Ймовірності: успіху $\lambda 3 \equiv .5$, зупинки: $\mu 3 \equiv .15$

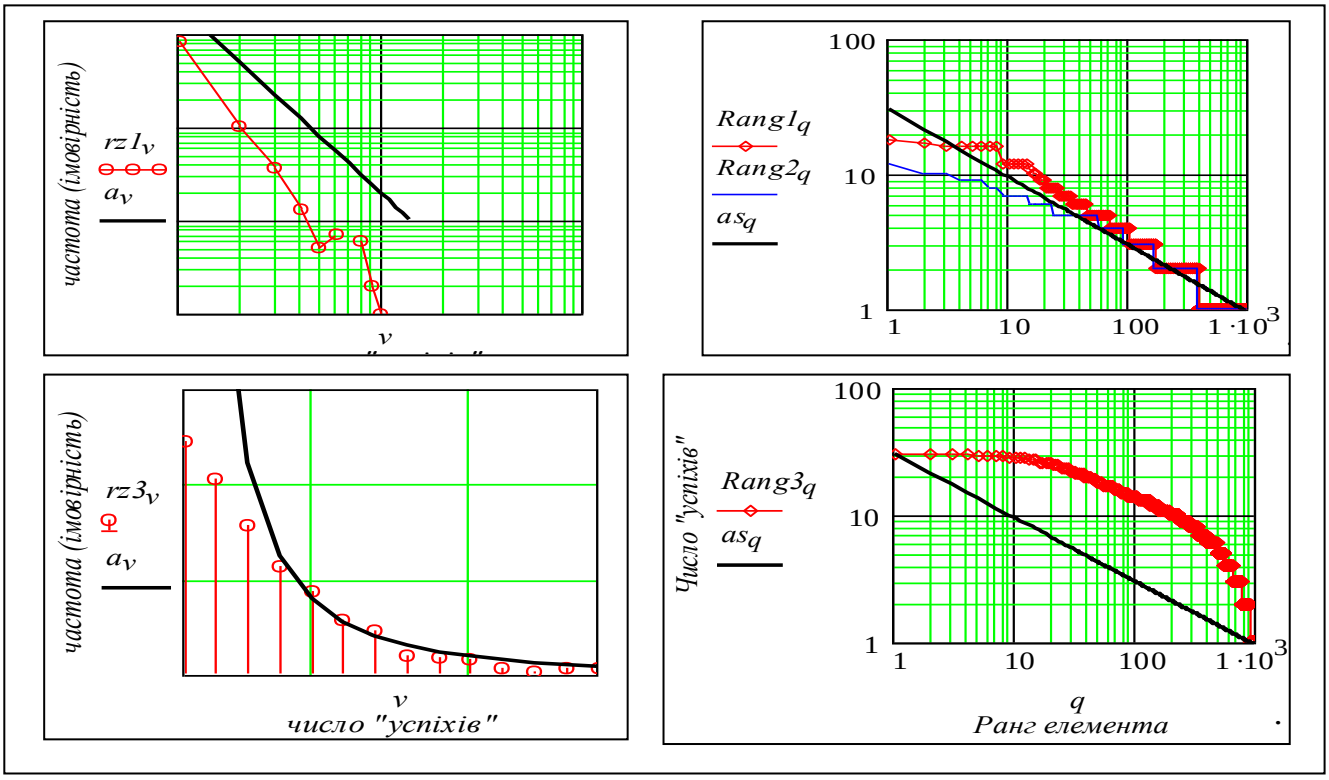


Рисунок 2.12 — Результати моделювання процесу з гіперболічною статистикою

Розробка моделей і програмних модулів отримання перетворень розподілу для стохастичного процесу при нелінійному перетворенні. Інтерпретація: відома монотонно зростаюча нелінійна залежність між витратами ресурсів комп'ютерної системи і темпом обробки задачі. Маємо формалізовану задачу: перетворення розподілу ймовірностей випадкового процесу при проходженні через статичну нелінійність. В комп'ютерних системах можуть виникати складні нелінійні перетворення вхідних потоків. Зауважимо, що існують два стійких гіперболічних розподіли з нахилами асимптот (в подвійних логарифмічних масштабах a1 = -1, a2 = - 2). Це важливі для аналізу виробничої системи індикатори.

В даному розділі подано розробку робочих моделей (таких, що програмно реалізовані) для — створення бібліотеки моделей породжуючих механізмів для розподілів імовірності в комп'ютерних системах. Розглянемо приклади розподілів ймовірності для елемента деякої КС, отриманих на імітаційних моделях розподілених систем [3, 4]. На рис.2.13 подані розподіли ймовірності для рівня завантаження елементу: .1 - без урахування нелінійних обмежень в розподілі навантаження між елементами системи обслуговування. На графіках 2.13-2, 2.13-3, 2.13-.4 — подані розподіли ймовірності для кращого елементу в системі з трьох елементів і трьох класів задач обслуговування при варіації параметра ефективності цього елементу. Ці розподіли — багатомодові, для даного прикладу моди мають чітко виражені моди. При зміні параметрів системи деякі моди можуть бути слабо вираженими і взагалі бути відсутніми.

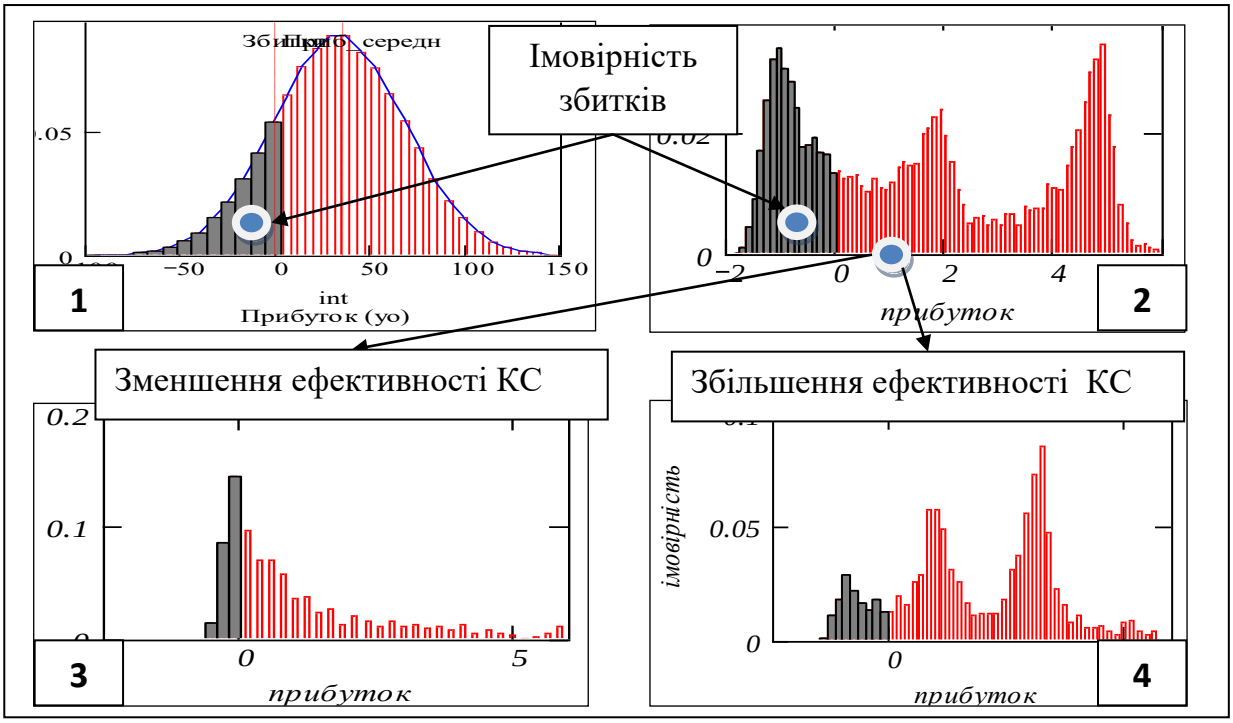


Рисунок 2.13 Розподіли ймовірності для елементу розподіленої комп'ютерної системи

Ми виділили для моделювання такі механізми перетворення випадкових потоків: - проходження через статичну нелінійність; Обмежимося дослідженням впливу статичних нелінійностей. На рис.2.14 подана схема перетворення. Це результати моделювання за розробленою моделлю, та інформаційні технології візуалізації.

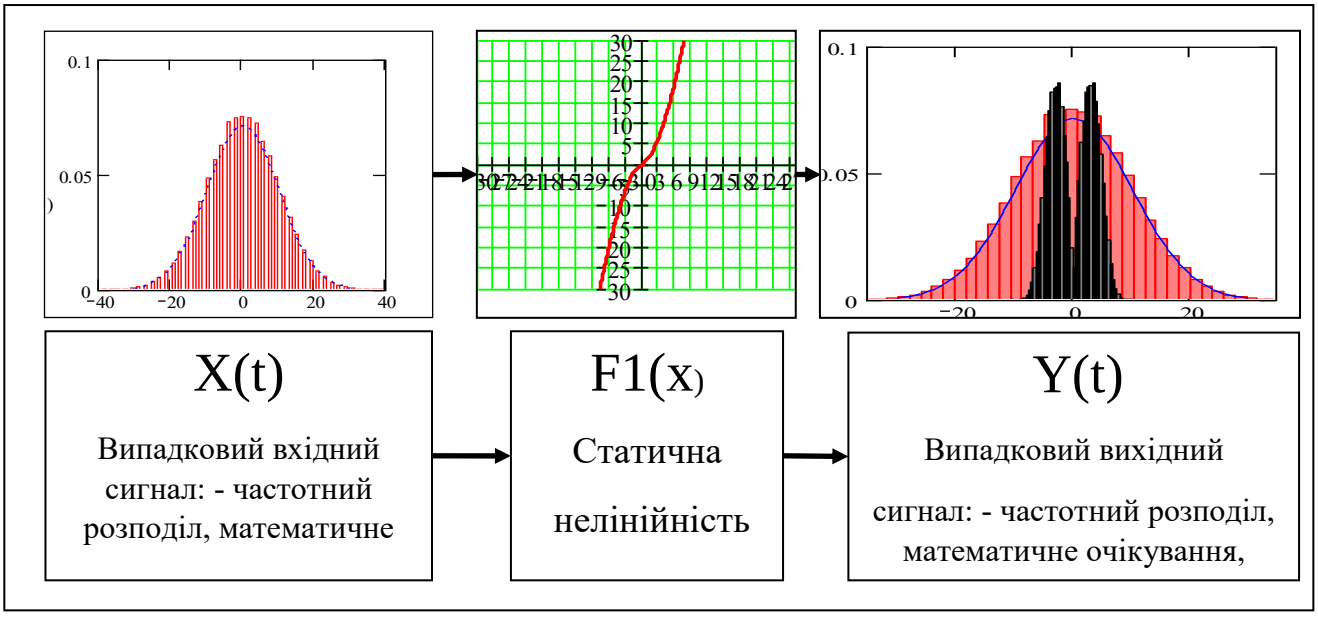


Рисунок 2.14 — Схема задач "проходження випадкового сигналу через нелінійність"

Запишемо робочу модель задач максимально використовуючи вбудовані функції пакету. Задаємо: число кроків процесу (об'єм вибірки) $Tm := 120000$; $t := 1 .. Tm$. Генеруємо вибірку «випадковий сигнал з нормальним розподілом». Параметри вхідного сигналу: амплітуда $Ax := 10$; середнє $mu := 0$; розкид $sig := 1$. Вхідний сигнал.

$$X := Ax \cdot rnorm(Tm, mu, sig) \tag{2.14}$$

Генеруємо також вибірку «випадковий сигнал з рівномірним розподілом». Параметри вхідного сигналу (межі) $x1 := -12$; $x2 := 12$.

$$X1 := Ax \cdot runif(Tm, x1, x2) \tag{2.15}$$

Записуємо вирази для теоретичних розподілів, нормальний розподіл: $rvte(x) := dnorm(x, mu, sig)$; рівномірний розподіл: $rvte1(x) := dunif(x, x1, x2)$.

Отримуємо гістограми для вхідного сигналу з нормальним розподілом $kin := 50$; $rvemX := histogram(kin, X)$ і для вхідного сигналу з рівномірним розподілом $kin1 := 50$; $rvemX1 := histogram(kin1, X1)$. Обчислюємо характеристики випадкового вхідного сигналу з нормальним розподілом: максимум $maxm := max(X)$; середнє

$muem := \frac{1}{Ax} \cdot mean(X)$; мінімум $miem := min(X)$; стандартне відхилення $stdem := \frac{1}{Ax} \cdot stdev(X)$ ..

Виконаємо такі ж обчислення для вхідного сигналу з рівномірним розподілом: Будуємо графіки емпіричних частотних розподілів (гістограми) для двох випадків разом з теоретичними розподілами (рис. 2.15)

$$rvte(xx) := dnorm(xx, mu, Ax \cdot sig) \; ; \quad rvte1(xx) := dunif(xx, x1, x2)$$

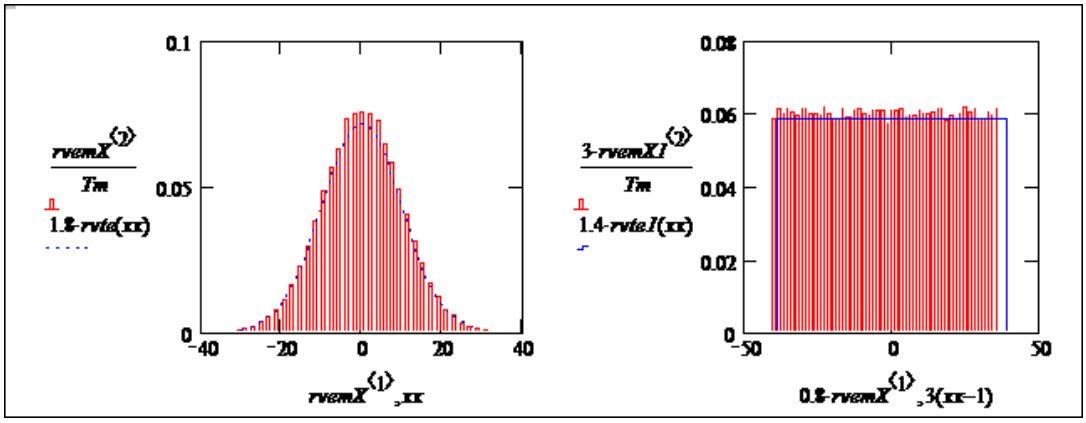


Рисунок 2.15 — Частотні розподіли вхідних сигналів

Дані рутинні обчислення приведені як простий приклад технології конструювання робочих моделей — контроль всіх кроків розробки: бачимо що гістограми вибірок дійсно сходяться до закладених в ці процеси теоретичних розподілів.

Обчислення розподілів імовірностей вихідного сигналу. Розподіли вірогідності на виході нелінійності знаходимо «безвідмовним» методом імітаційного моделювання. Можливі інші альтернативи, але наша модель — тільки перший крок до вирішення складніших завдань проходження випадкового процесу через нелінійні динамічні елементи. Для прикладу візьмемо дві типові нелінійні функції

«узагальнена нелінійна статична залежність»:

$$F(x, aa) := 1.0 \cdot sign(x) \cdot \left| x^{aa} \right| \; ;$$

«узагальнена увігнуто-випукла»:

$$F2(x, ss) := \left[9.4 \cdot \left| \left(1 - e^{-0.5 \cdot |x|}\right)^{ss} \right| \cdot sign(x) \right] + 0.1 \cdot x \,.$$

Будуємо графіки цих нелінійностей (рис.2.14):

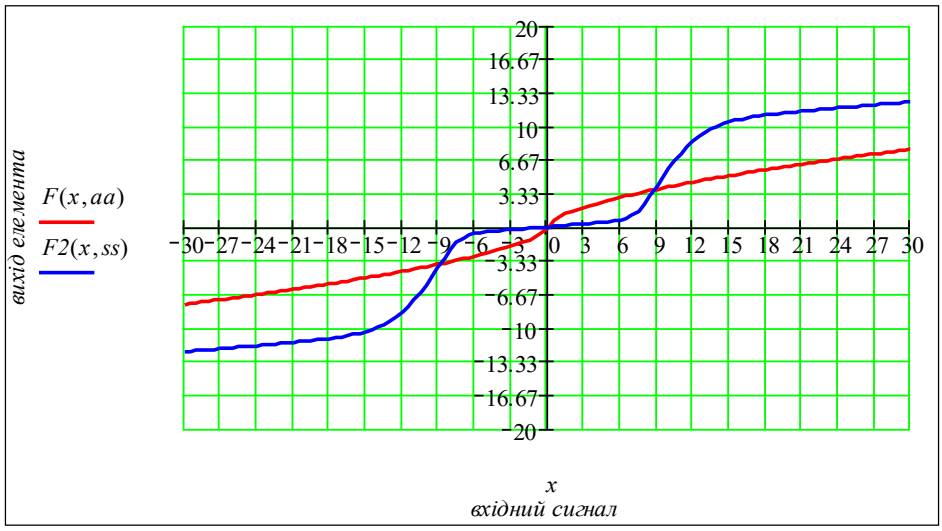


Рисунок 2.14 — Приклади нелінійних характеристик

Над кожним значенням вхідної змінної xt виконується нелінійне перетворення

$$y_t = F\left(x_t, aa\right),$$

де t — дискретний час,

aa – вектор параметрів функції.

Рівняння (2.16) відображає масив (вибірку) вхідних даних X в масив вихідних даних Y. Використовуємо оператора векторизації, який інтерпретується так: виконати перетворення F(X,aa) над кожним елементом масива X, з однаковим параметром aa.

Використання векторизації дає ряд переваг, серед яких підвищення швидкості обчислень в 4 — 8 разів, — на останньому місці. Головна перевага розширення меж класичної математики, наприклад, в [11] запропоновано радикальне рішення задачі нелінійного програмування про оптимальний розподіл обмеженого ресурсу. Головний елемент рішення оператор оптимальної агрегації побудований з

використанням векторизації [12]. Ще один приклад — векторизований оператор «вибір – навчання», який обробляє вибір і зміну переваг безлічі споживачів на безлічі продуктів певного класу [12]. Запишемо вирази для вихідних масивів для випадку опуклої нелінійності і входів з нормальним і рівномірним розподілами. ;

$$Yv := \overrightarrow{F(X, aa)} \; ; \quad Yv1 := \overrightarrow{F(X1, aa)} \tag{2.16}$$

Також запишемо виразу для випадків вігнутоопуклої нелінійності з нормальним і рівномірним розподілами.

$$Ynv := \overrightarrow{F2(X1, aa)} \; ; \; Ynv := \overrightarrow{F2(X, aa)} \tag{2.17}$$

Побудова гістограми. Визначаємо розподіли виходу для входів з нормальним і рівномірним розподілами

$$rvemY := histogram(kin, Yv) \; ; \; rvenY := 1 \cdot histogram(kin, Ynv) \tag{2.18}$$

Записуємо частотний розподіл вихідних даних з нормальним розподілом і не випуклою нелінійністю $rvemY1 := 1 \cdot histogram(kin, Yv1)$; $rvemnY1 := 1 \cdot histogram(kin, Ynv1)$.

Виконаємо візуальний аналіз частотних розподілів. На рис. 2.15 поданий графік з трьома залежностями: вхідний розподіл, теоретичний емпіричний і вихідний розподіл. Під цим графіком представлена "причина" — характеристика нелінійного елементу (повернену, так, щоб сумістити вихід нелінійного елементу і шкалу "величина виходу" на графіку частотних розподілів).

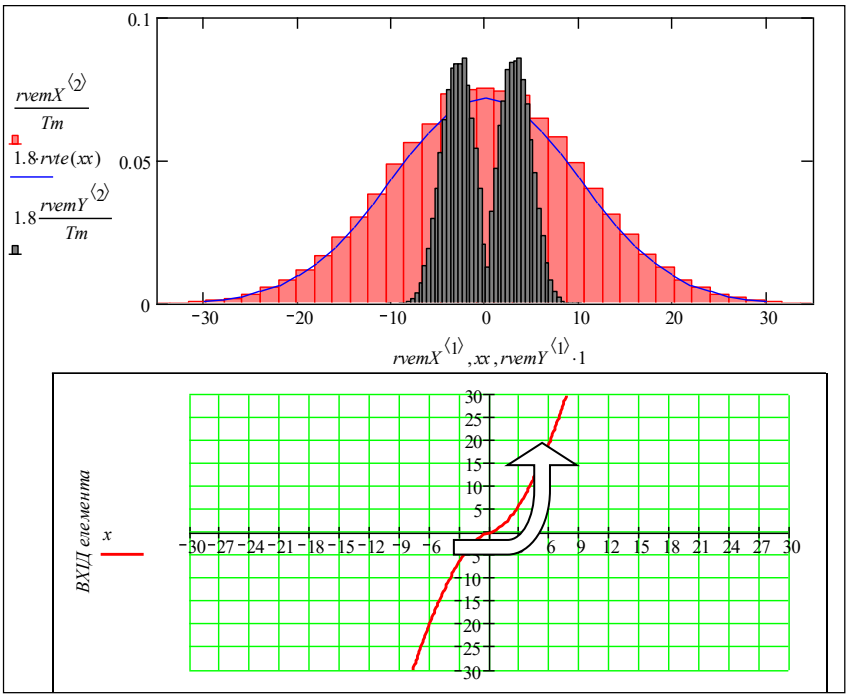


Рисунок 2.15 — Перетворення нормального розподілу випуклою нелінійністю

Черговий елемент технології конструювання робочих моделей: перевірка коректності результатів. Нормуємо отримані дискретні розподіли, перевіряємо умову «повнота множини подій»: $\frac{mean\left(rvemX^{\langle 2\rangle}\right)\cdot kin}{Tm} = 1$ $\frac{mean\left(rvemY^{\langle 2\rangle}\right)\cdot kin}{Tm} = 1$.

На рис.2.16 подано результат моделювання для випадків відповідних нелінійності увігнутої нелінійності. Вихідний розподіл - одномодовий, не гаусівський.

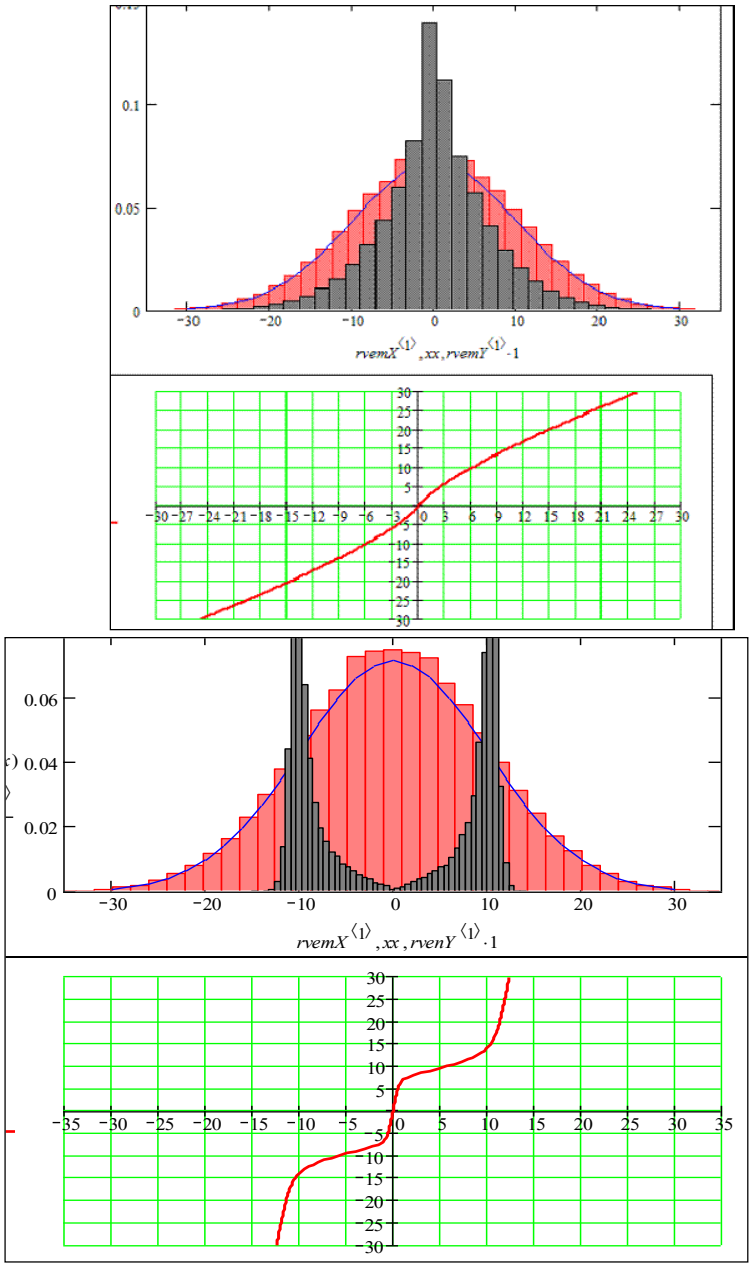


Рисунок 2.17 — Перетворення нормального розподілу сигналу увігнутою нелінійністю

Уявіть собі , що ви маєте тільки результати нелінійного перетворення, не знаєте «породжуючі механізми» перетворення і шукаєте їх за допомогою нейронечітких методів. На рис. 2.16 представлені результати обчислень для випадків увігнутої і випуклої функцій. Бачимо очевидні закономірності:

— увігнута нелінійність "концентрує" розподіл навколо середнього;

— випукла нелінійність "розсуває" розподіл в дві моди щодо середнього.

Зробимо теж саме, але вже для рівномірного розподілу (рис. 2.17). Бачимо — результати перетворення топологічно подібні попереднім. Тобто інформація отримана на моделях використовуватись для «навчання» - підвищення ефективності підсистеми прогнозування і планування

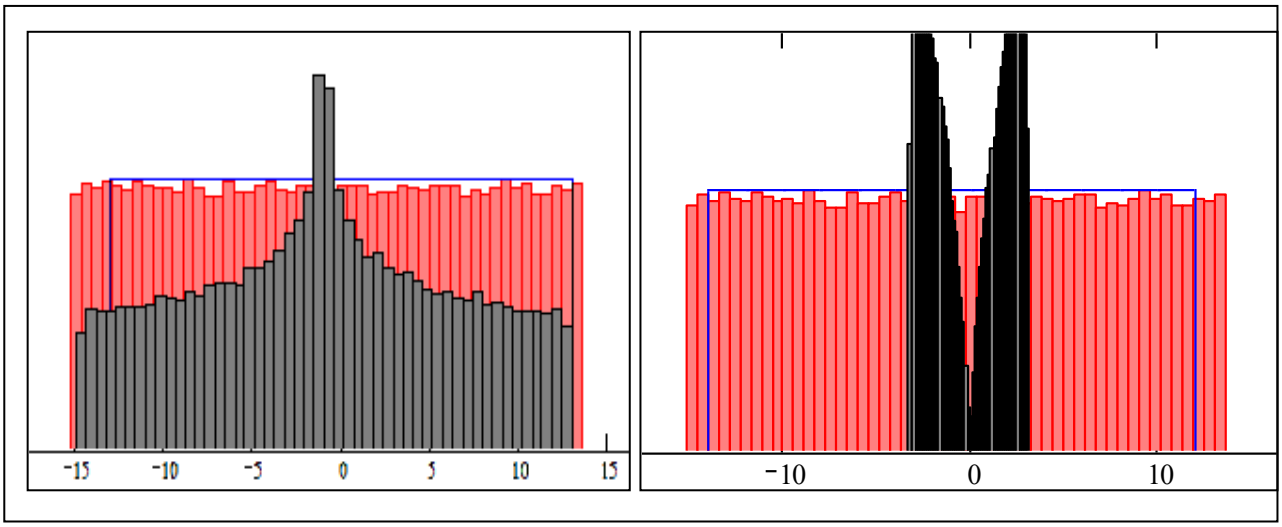


Рисунок 2.17 — Аналіз перетворення сигналу з рівномірним розподілом, що проходить через випуклу і увігнуту нелінійність

На рис. 2.18 представлена альтернативна форма інформації для задач на рис. 2.16 і 2.17 на двох альтернативних рівнях: процесів і частотних розподілів.

Представлено два приклади — перетворення увігнутою нелінійністю випадкових величин з нормальним і рівномірним розподілами. На графіках ліворуч подано «натуральні» випадкові процеси, праворуч — частотні розподіли. Для спеціалістів така альтернатива —дає «стереоскопічне» бачення проблеми, підвищення ефективності в інноваційних розробках. Якими займаються спеціалісти всього світу із змінним успіхом. Нагадаємо — нелінійні графіки функцій нелінійних перетворювачів подано на рис. 2.16.

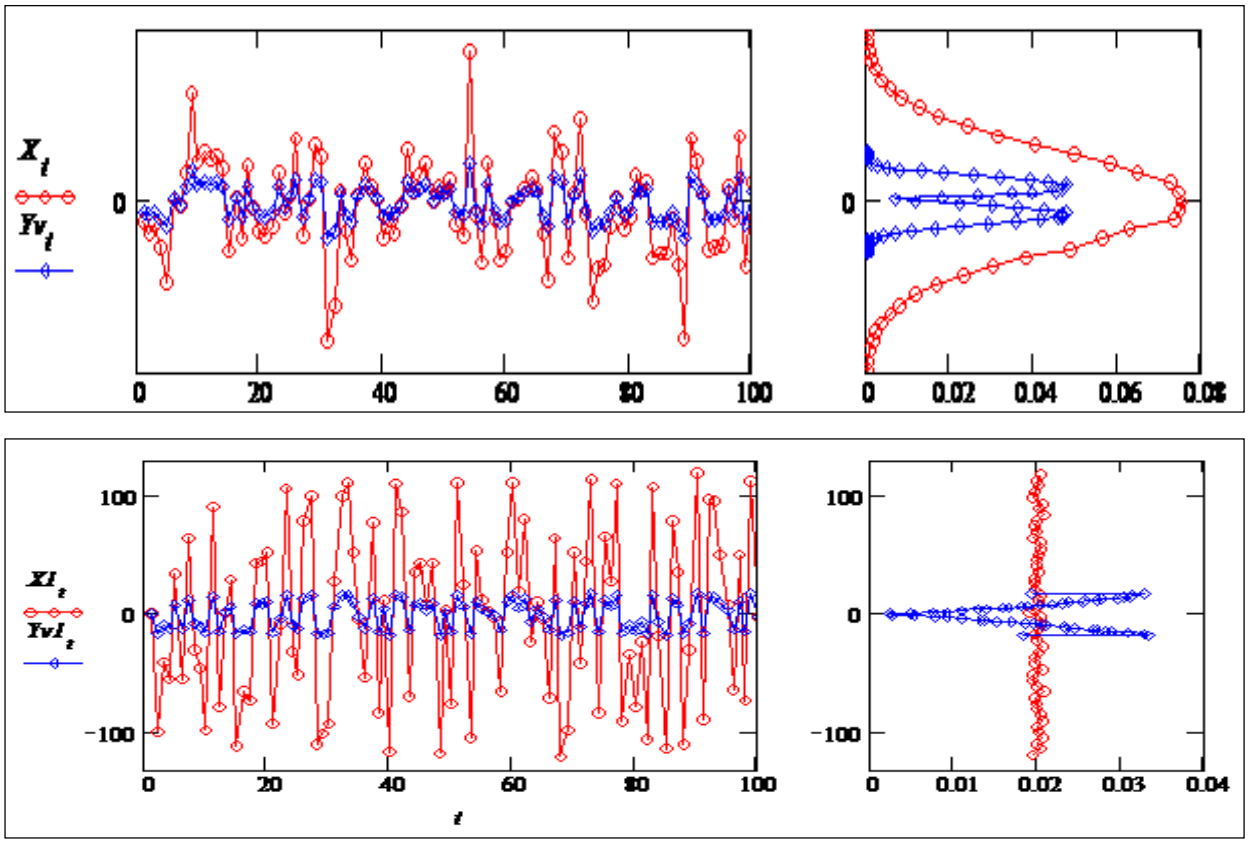


Рисунок 2.18 — Випадкові процеси і нелінійні перетворення. Приклад

Поставлено задач аналізу і прогнозування показників функціонування комп'ютерних систем на статистичних даних - частотних розподілів. На відміну від робіт-прототипів, аналіз орієнтується на ідентифікацію системних механізмів класу «рівень завантаження — витрати ресурсів. Для вирішення задач використана інформаційна технологія конструювання робочих моделей. Розроблена імітаційна модель для процесу проходження випадкової величини через статичну нелінійність. Проаналізували тимчасові і частотні характеристики процесу. Це дозволяє поставити задачу конструктивного, на рівні породжуючих механізмів, порівняльного аналізу реальних і синтезованих віртуальних розподілів імовірності для змінних входів і змінних стану КС.

3 РОЗРОБКА І ТЕСТУВАННЯ ПРОГРАМ КОМПЛЕКСНОГО АНАЛІЗУ НЕВИЗНАЧЕНОСТЕЙ І ЗБУРЕНЬ СИСТЕМИ ОБСЛУГОВУВАННЯ

Дослідження стану проблеми невизначеностей виконане в розділі 1, аналіз і розробка окремих моделей і програмних дозволили виділити нові, актуальні і складні проблеми, що можуть бути вирішені ефективними методами імітаційного моделювання і оптимального агрегування.

3.1 Постановка задачі оптимального агрегування стохастичних систем

Базова характеристика будь-якого засобу виробництва чи обслуговування це функція класу «витрати, випуск». Випуск продуктів споживання, технічних систем і засобів, продуктів промислового призначення все це оцінюється, продається відповідно показників витри виробництва, використанні і випуску продукції з певною ціною і цінністю. Все це має ризики конкуренції, надійності і якості та інших численних показників. Тому потрібні ефективні моделі і методи оцінювання надійності іефективності елементів виробничих системах етапах життєвого цикл. Задано номінальні функції виробництва ФВ усіх виробничих елементів виробничої системи - не строго монотонні і позитивні обмежені функції обмеженого аргументу «ресурси».

$$f(i, x_i, Vf_i)\ ,\ i = 1..N \tag{3.1}$$

де i — індекс елемента в системі, визначає параметричний клас ФВ;

x_i — обсяг ресурсу для і-го елемента;

Vf_i — вектор параметрів і-го елемента.

Задані для кожного елемента функції розподілу ймовірностей:

$$d(i, x_i, Vd(x_i)) \tag{3.2}$$

де $d(\blacksquare)$ — функція розподілу ймовірностей для кожного (на сітці значень) значення ресурсу x_i;

$Vd(x_i)$ — вектор параметрів розподілу.

Маємо систему розподілів ймовірностей, прив'язану до значень аргументу x – обсяг ресурсу. Візьмемо таку інтерпретацію формальної моделі. Окремий випадок: спрощена модель, що має постійний розподіл ймовірностей - $d(i, x_i, Vd)$.

Схема процесу отримання розподілу ймовірностей для оптимальної еквівалентної ФВ виробничої системи. Маємо набір елементів, кожен з яких видає випадкове число з детермінованим середнім та випадковим - центрованою випадковою величиною з розподілом і параметрами, залежними від входу - обсягу ресурсу x_i.

$$y_i = f(i, x_i, Vf_i) + rd(i, x_i, Vd(x_i)) \quad xop = OpsN \tag{3.3}$$

де $rd(\blacksquare)$ — функція, що видає випадкове число з заданим розподілом ймовірностей;

$OpsN$ — функція користувача, оператор оптимального агрегування, що повертає еквівалентну оптимальну ФВ системи: вектор значень xop_1 - та вектор-функцію оптимального розподілу ресурсу, матрицю значень xop_2 - вектор значень для кожного значення сумарного ресурсу: $X_k = \Delta X \cdot k$, $k:=1..Kt$; $\Delta X = zn$.

Оптимальні частки ресурсу для кожного елемента визначаються:

$$x_{i,k} = (xop_2)_{i,k} \cdot X_k \tag{3.4}$$

Оператор оптимального агрегування повертає нормовані значення розподілу ресурсів. В даному випадку маємо дві альтернативи до аналізу впливу невизначеностей:

— пасивний: вважаємо випадкові відхилення значень ФВ елементів такі, що не вимірюються і не прогнозуються, а оптимальний розподіл визначаємо для номінальних значень ФВ (Функції Виробництва);

— активний: вважаємо випадкові відхилення значень ФВ елементів вимірюються і прогнозуються, і оптимальний розподіл ресурсу визначаємо для цих значень ФВ;

Знаходимо сумарне виробництво:

$$Yops_k = \sum_{i=1}^{N} y_{i,k} \tag{3.5}$$

Повторюємо цей процес для утворення потрібної вибірки. В результаті для заданих ФВ та їх розподілів ймовірності отримуємо розподіл ймовірностей для розподілу ймовірностей сумарного виробництва.

Збираємо всі операції в параметризований модуль і отримуємо оператор, що будує для адитивної функції від незалежних випадкових величин, заданими розподілами ймовірностей систему розподілів ймовірностей сумарного виробництва за умови оптимального розподілу ресурсу. Аналог отриманого результату - розподіл суми випадкових величин з довільними розподілами. Відомо, що при виконанні умови обмеженості дисперсій такий розподіл швидко сходиться до нормального. Дана розробка — нова область: отримуємо функцію користувача з вбудованою оптимізацією і нелінійними перетвореннями випадкових величин.

Для отримання робочих програм спочатку будуємо і досліджуємо робочі моделі модулів для детермінованої задачі. Після цього реалізуємо в робочих моделях розглянуту вище схему аналізу впливу невизначеностей для оптимізованої системи з паралельно працюючими елементами (багатоканальну СМО).

3.2 Розробка модуля оптимального агрегування

Розширення задачі. Введемо вектор-функцію оптимального розподілу ресурсу $Dop(R)$, $0 \le R \le Rmax$, де $Rmax$ — максимальне значення обмеження. Це вектор—функція, компоненти якої задають оптимальний по критерію сумарного виробництва розподіл заданої кількості ресурсу [8] .

Функція $Dop(R)$ для припустимих виробничих функцій має такі властивості:

$\sum_{i=1}^{N} Dop(R)_i = R$ - баланс ресурсу; $Dop(R)_i \ge 0$; $i \in$1,...N.

Введемо оптимальну еквівалентну функцію виробництва системи:

$$Yop(R) = \sum_{i=1}^{N} fi\left(Dop(R)_i\right) \qquad (3.6)$$

Функція $Yop(R)$ для кожного значення обмеження по ресурсу R задає максимальну продуктивність перетворення ресурсу в продукт. Наприклад, максимум обслуговування заявок при даному обмежені ресурсів, Подаємо формулювання узагальненої оптимізаційної задачі. Задано N виробничих підсистем з відповідними ФВ, адитивне обмеження по ресурсу і адитивний критерій — сумарне виробництво; треба знайти оптимальну виробничу функцію системи $Yop(R)$ і вектор-функцію оптимального розподілу ресурсу $Dop(R)$. Створюємо "бібліотеку" математичних моделей для типових технологічних залежностей «витрати-випуск» виробничих функцій.

Ступенева: $F1(x, A, w, s) \equiv 1A \cdot x^{10w}$; (3.7)

Логарифмічна: $F2(x, A, w, s) \equiv 1.5A \cdot ln(x + 1)$ (3.8)

Експоненційна: $F3(x, A, w, s) \equiv 10 \cdot A \cdot \left(1 - e^{-w \cdot x}\right)$ (3.9)

Увігнуто-випукла (S-функція):

$$F4(x, A, w, s) \equiv 10 \cdot A \cdot \left(1 - e^{-w \cdot x}\right)^{s} \quad (3.10)$$

Лінійна з обмеженням і порогом витрат функції

$$F5(x, A, w, s) := \begin{cases} 10w \cdot x & \text{if } 10w \cdot x < 10A \\ 10A & \text{otherwise} \end{cases} ; \quad (3.11)$$

Лінійна з обмеженням

де x — обсяг ресурсу;

a, w, s — параметри функцій (3.12)

$$F6(x, A, w, s) := \begin{cases} 0 & \text{if } 0 \le x < 2s \\ 10A\,w \cdot (x - 2s) & \text{if } 0 \le x - 2s < 1 \div w \\ 10A & \text{otherwise} \end{cases}$$

Ступінчаста (дискретні вироби):

$$F7(x, A, es, ls) := 10 \min(trunc(x \div ls) \cdot es \cdot ls, A) \quad (3.13)$$

Параметри ступінчастої функції: A — максимальне значення; es — ефективність інвестиції; ls — величина "кванта інвестування" (вартість "верстата").

Звернемо увагу на визначення ФВ — ступінчасті, кусочно-лінійні: методи оптимального агрегування більше, ніж тільки метод нелінійного програмування. Переваги нової методології: відсутність пошукових процедур оптимізації: багатовимірна задача оптимізації замінюється системою одновимірних, кожна з яких обчислюється в режимі векторизації. Результат — обчислювальні витрати з ростом розмірності задачі оптимізації зростають не більше ніж лінійно [8]. Природне питання — чому спеціалісти і корпорації не переходять на інноваційний метод. Відповідь: гарантовано стануть непотрібні існуючі програмні продукти, В США для багатьох продуктів виробництва крім ціни продажу додається сертифікат цінності продукту для споживача. Тобто не витрати, а цінність визначає ціну продажу, а собівартість —справа технологів і конструкторів.

Виробничі функції — технологічна категорія, а їх вимірювання подвоєння в грошових одиницях - ситуативна умовність. Дійсно, порівняємо дві ситуації:

Використаємо метод оптимального агрегування [12]. Введемо множину функцій:

$$f\alpha(f1, f2, \alpha, x) := f1(\alpha \cdot x) + f2[(1 - \alpha) \cdot x]. \quad (3.14)$$

Оптимальна виробнича функція системи з двох елементів є огинаючою системи функцій $f\alpha(f1, f2, \alpha, x)$, $0 \le \alpha \le 1$, тобто результатом застосування операції $max(..)$, яка є асоціативною і комутативною. Майже очевидно, що для виробничої системи з критерієм "сумарне виробництво", оптимальна виробнича функція $FopN(f1, f2, .., fN)$ має місце властивість:

$$Fop3(f1, f2, f3) = Fop2(f1, Fop2(f2, f3)), \quad (3.15)$$

що є наслідком виконання принципу оптимальності (у Беллмана принцип оптимальності застосовується в часі - по крокам процесу, а в даному випадку — в просторі, по елементам системи). Альтернативи побудови модуля агрегування:

— модуль бере пару неперервних функцій і повертає неперервні функції;

— бере пару дискретних функцій і повертає дискретні функції.

В даному випадку вибрано другу альтернативу. Обґрунтування: модуль простіший і обчислювально-ефективніший. Далі слід вибрати форму подання виробничих функцій елементів: — для функцій одного параметричного класу — в модуль передаються тільки вектори параметрів ВФ елементів;

— функцій різних параметричних класів — з передачею в модуль векторів параметрів і параметра класу ВФ;

— з передачею імен ВФ елементів і векторів параметрів;

— повністю визначених в головній програмі ВФ елементів з передачею в модуль тільки імен ВФ. Обґрунтування: простота програмного модуля.

В практиці використання методів оптимального агрегування виникає необхідність в розробці бінарних операторів оптимального агрегування для нових актуальних ресурсних структур. На даний час [моногр ДДБор] розроблені бінарні оператори для паралельних, послідовних, циклічних ресурсних структур. Однак

виникають нові технічні системи і нові задачі управління і контролю. Раціонально виконувати розробки програмного модуля розробкам реальної системи. Світовий досвід показав, що цій області аутсорсінг «індійським програмістам» не гарантує якісної розробки програм управління процесами виробництва, постачання, обслуговування.

Далі подано специфічні етапи розробки. Третій рівень вибору — дискретизації задачі оптимального агрегування. Число точок дискретизації функцій класу «витрати, випуск» залежить від функцій модуля, в якому виконується оптимальне агрегування.

Подамо програмний модуль $bolv(v, Ns)$ для нормування матриць даних:

$$\begin{aligned} bolv(v, Ns) := \; & blv \leftarrow v \\ & \text{for } n \in 2..Ns \\ & \quad blv \leftarrow augment(blv, v) \end{aligned} \tag{3.16}$$

Задаємо параметр *Ns:=16* — максимальну розмірність системи — кількість елементів. Робимо модуль, що розраховує черговий оптимальний розподіл ресурсу при черговому кроці агрегування. Замість подвійного циклу використовуємо векторизацію - це набагато прискорює обчислення.

$$\begin{aligned} dop(rp, ra) := \; & kok \leftarrow cols(rp) \\ & kto \leftarrow rows(rp) \\ & zag \leftarrow bolv(ra, Ns) \\ & stok \leftarrow submatrix(zag, 1, kto, 1, k \\ & \qquad \longrightarrow \\ & nrzp \leftarrow (rp \cdot stok) \\ & nrzp \end{aligned} \tag{3.17}$$

Тепер можемо зробити центральну програму нашого методу - $f2c$, яка бере два масиви, що описують виробничі функції елементів (все одно — монолітних чи агрегованих), і повертає масив, що описує оптимальну виробничу функцію та відповідну вектор-функцію оптимального розподілу ресурсу.

На рисунку 3.1 подано текст підпрограми оптимізації розподілу ресурсу.

```
f2o(mf1, mf2) :=
    Xto ← rows(mf1)
    dλ ← 1 ÷ Xto
    klev ← cols(mf1)
    kpra ← cols(mf2)
    rlev ← submatrix(mf1, 1, Xto, 2, klev)
    rpra ← submatrix(mf2, 1, Xto, 2, kpra)
    for i ∈ 1 .. Xto
        mak ← 0
        for j ∈ 1 .. Xto
            i1 ← max(round((j·i)/Xto, 0), 1)
            i2 ← max[(i − i1), 1]
            Vs ← mf1[i1, 1] + mf2[i2, 1]
            if Vs > mak
                jm ← j
                mak ← Vs
        Vyxod^⟨i⟩ ← stack(mak, jm·dλ)
    Vyx ← Vyxod^T
    rnlev ← dop(rlev, Vyx^⟨2⟩)
    rnpra ← dop[rpra, (1 − Vyx^⟨2⟩)]
    Vyd ← augment(Vyx^⟨1⟩, rnlev, rnpra)
```

Рисунок 3.1 — Текст підпрограми оптимального розподілу ресурсу

Дослідження оптимального агрегування. Згідно принципу оптимальності (а він виконується для нашої задачі), скільки б ресурсу не виділялося в розвиток виробництва — цей ресурс повинен розподілятись оптимально. Обчислимо функції розподілу ресурсу між окремими продуктами чи виробництвами. Для нашого методу оптимального агрегування необхідно подати функції розвитку (ФР) в дискретному виді - як певні масиви. Задаємо: діапазон зміни обмеження по ресурсу $Rma := 150$; кількість точок обчислення ФР $Kto := 200$; крок квантування ресурсу $dx := Rma \div Kto$;

ранжовану змінну $n := 1..Kto$; формальну функцію оптимального розподілу ресурсу в одноелементній системі $r0_n := 1$.

Параметри елементів системи:

A1:=1.; W1:=0.3; S1:=6; A2:=12.; W2:=0.16; S2:=6;

A3:=1.4; W3:=0.10; S3:=6; A4:=1.6; W4:=0.06; S4:=6;

A5:=1.6; W5:=0.03; S5:=8; A6:=1.7; es:=00.3; ls:=1.

Формуємо відповідні масиви:

$fo1_n := F4(n \cdot dx, A1, W1, S1)$; $ffo2_n := F4(n \cdot dx, A2, W2, S2) - 0.03n \cdot dx$;

$fo3_n := F4(n \cdot dx, A3, W3, S3)$; $fo4_n := F4(n \cdot dx, A4, W4, S4)$;

$fo5_n := F6(n \cdot dx, A5, W5, S5)$; $fo6_n := F7(n \cdot dx, A6, es, ls)$;

$f1 := augment(fo1, r0)$; $f2 := augment(ffo2, r0)$; $f3 := augment(fo3, r0)$.

$f4 := augment(fo4, r0)$; $f5 := augment(fo5, r0)$; $f6 := augment(fo6, r0)$.

Візуальний аналіз: дослідимо типові функції "витрати — випуск" і результати їх попарного агрегування. Можна в це дерево додавати функції розвитку — скільки потрібно. Запишемо формулу агрегування в звичайній формі:

$$Ops3 := f2o(f1, f2o(f2, f3)). \qquad (3.18)$$

ННа рисунку 3.2 подано приклад обчислення функцій оптимального розподілу ресурсів в функції величини обмеження сумарного ресурсу між 4-ма підсистемами. Розподіл подано в нормованій формі (0, 1), графіки побудовані в прирощеннях. Таким чином ми бачимо безрозмірні частки ресурсу по кожній підсистемі.

Бачимо специфіку розподілу — розривність розподілів ресурсу. Побічний факт: оптимальні розподіли ресурсів розривні — класичні і нероінтелектуальні методи оптимізації для таких задач непридатні — вони пошукові і потребують гладких, випуклих функцій.

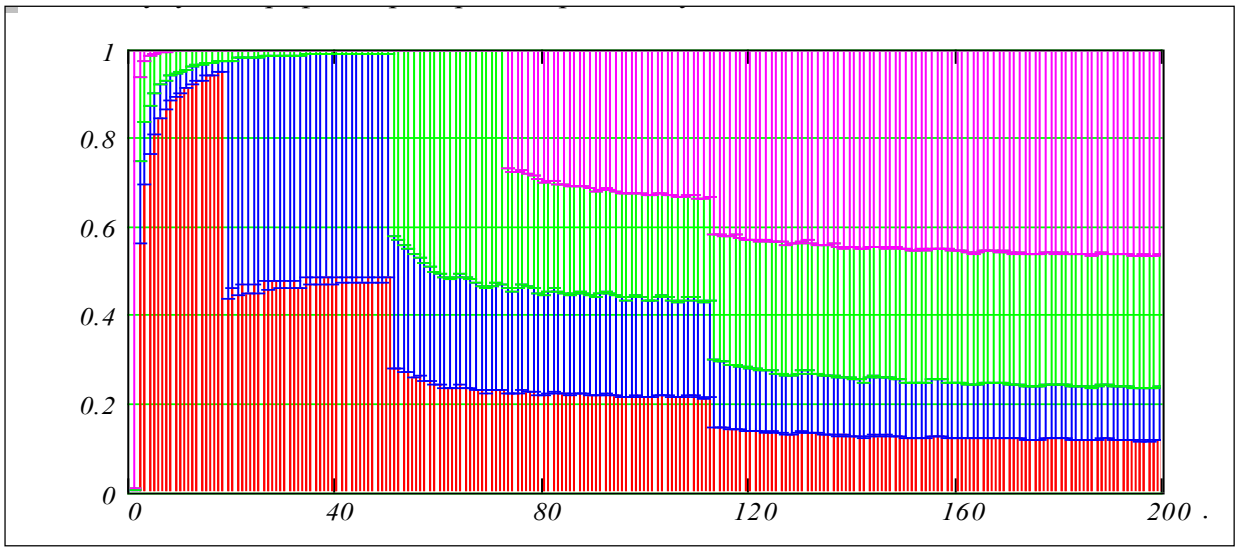
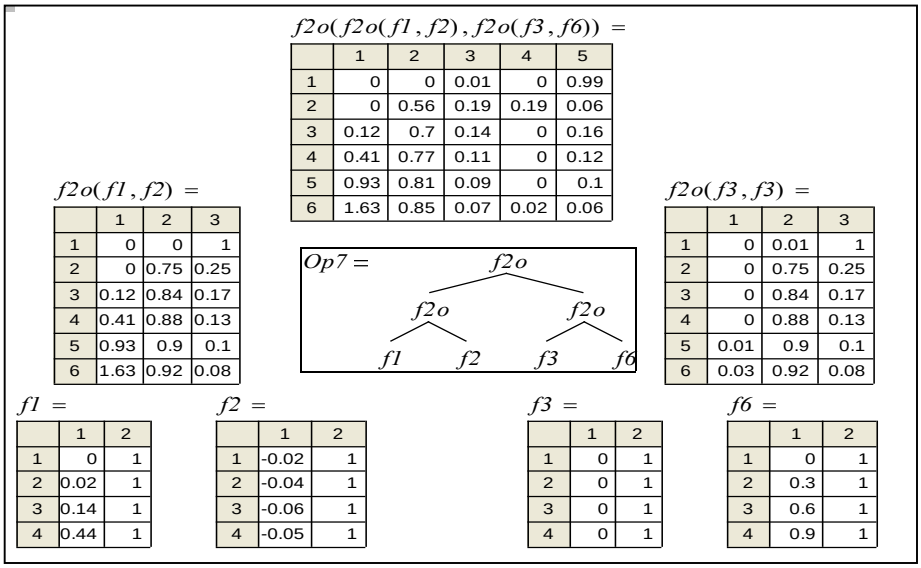


Рисунок 3.2 — Результат оптимального агрегування системи з 4-ьох елементів

На рис. 3.3 подано результати оптимального агрегування тестового прикладу в числовій формі. . Виведено разом: — структурну формулу агрегування і поетапні результати послідовного застосування оператора *f2o* до тестової задачі розглянутої вище (масиви подано в скороченому вигляді - вони мають по 128 рядків).

На рисунку 3.3 подано приклад структури даних по кроках оптимального агрегування системи з чотирьох елементів.



$f2o(f2o(f1, f2), f2o(f3, f6)) =$

	1	2	3	4	5
1	0	0	0.01	0	0.99
2	0	0.56	0.19	0.19	0.06
3	0.12	0.7	0.14	0	0.16
4	0.41	0.77	0.11	0	0.12
5	0.93	0.81	0.09	0	0.1
6	1.63	0.85	0.07	0.02	0.06

$f2o(f1, f2) =$

	1	2	3
1	0	0	1
2	0	0.75	0.25
3	0.12	0.84	0.17
4	0.41	0.88	0.13
5	0.93	0.9	0.1
6	1.63	0.92	0.08

$Op7 =$

$f2o(f3, f3) =$

	1	2	3
1	0	0.01	1
2	0	0.75	0.25
3	0	0.84	0.17
4	0	0.88	0.13
5	0.01	0.9	0.1
6	0.03	0.92	0.08

$f1 =$

	1	2
1	0	1
2	0.02	1
3	0.14	1
4	0.44	1

$f2 =$

	1	2
1	-0.02	1
2	-0.04	1
3	-0.06	1
4	-0.05	1

$f3 =$

	1	2
1	0	1
2	0	1
3	0	1
4	0	1

$f6 =$

	1	2
1	0	1
2	0.3	1
3	0.6	1
4	0.9	1

Рисунок 3.3 — Структури даних по кроках оптимального агрегування системи з чотирьох елементів (приклад)

Аналіз впливу розкидів для оптимально агрегованої системи. Подаємо черговий приклад побудови модуля для «що буде якщо аналізу» — черговий крок в побудові узагальненої моделі ризиків оптимально агрегованої виробничої системи. Крім того, це важливий елемент для користувачів-спеціалістів. Спеціалістам потрібні відкриті системи, де кожен крок кінцевого висновку можна перевірити розражунками, активно проаналізувати. Модуль для аналізу впливу розкидів має і самостійне значення, коли розподіли ймовірностей невідомі, аналіз ризиків виконують на базі оцінок ризиків.

На рисунку 3.4 подано інтерфейс для аналізу впливу розкидів оптимально агрегованих систем. Послідовно подані робочі формули оптимального агрегування, вхідні розкиди і розкид оптимально агрегованої системи. Друга частина інтерфейсу — це активний аналіз впливу розкидів: якщо розкиди можуть бути апріорно виміряні, то можна обчислити оптимальне управління для збуреної виробничої системи.

Вводимо варіації "амплітуди": *VA:=0.9* та "увігнутості": *VS:=1.5*. Ціна ресурсу: *Cin:=0.00* і обмеження по ресурсу $resurs = 100$.

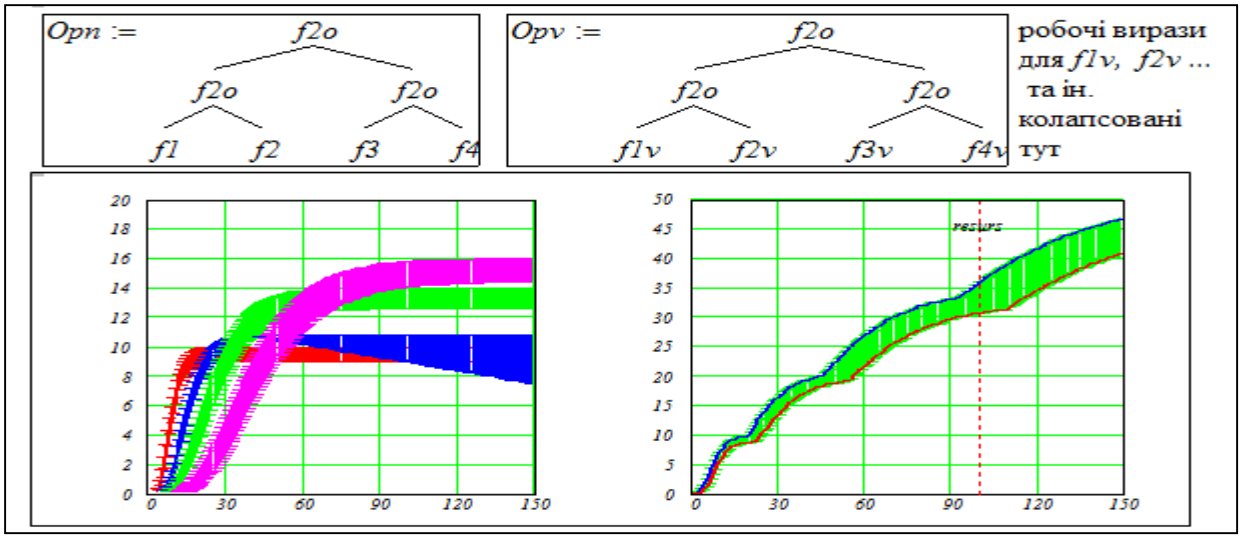


Рисунок 3.4 — Аналіз впливу розкидів параметрів оптимально агрегованої системи на оптимальну еквівалентну функцію системи

На рисунку 3.5 подана друга сторінка інтерфейсу: вплив розкидів параметрів на функції оптимального розподілу ресурсу.

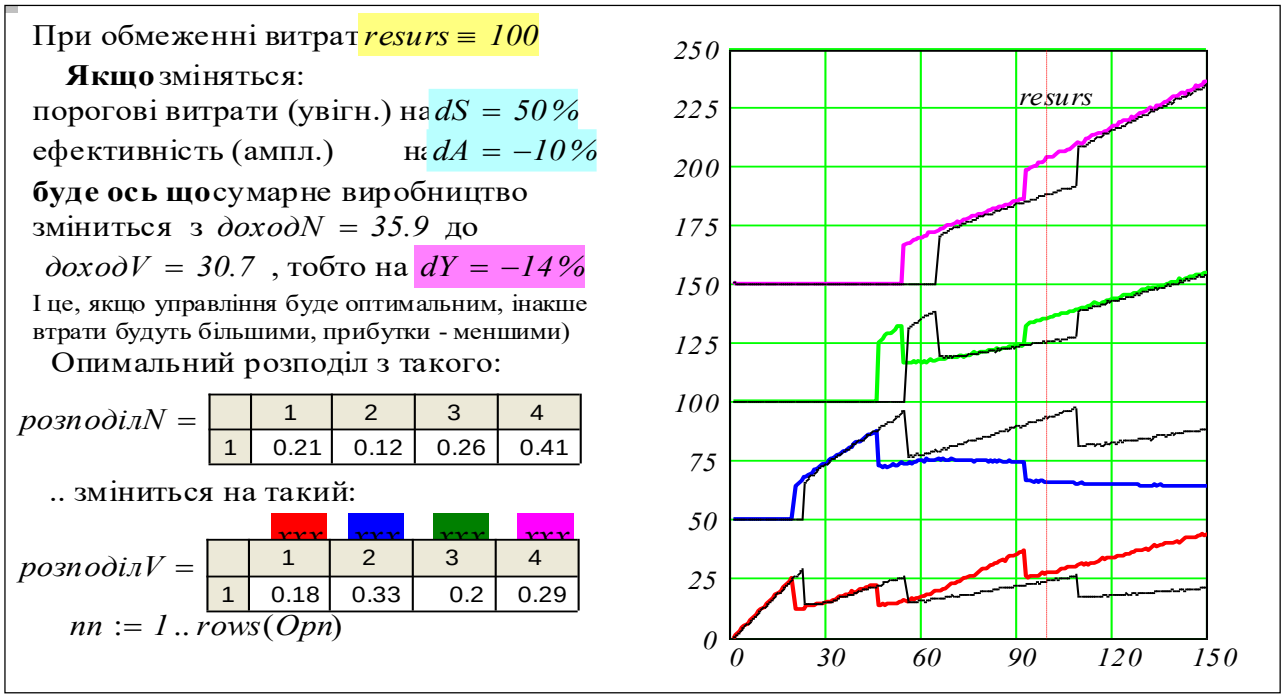


Рисунок 3.5 — Зміна оптимального управління при варіації параметрів ВС

Теоретичні основи згортки розподілів ймовірностей. Цей підрозділ — база для узагальнення і порівняння нових задач згортки розподілів - нелінійних і оптимальних.

Хай $\xi 1, \xi 2$ — дві випадкові величини з "густиною" сумісного розподілу $f_{\xi 1 \xi 2}(x_1, x_2)$ і задана борелевська функція g: $R^2 \Rightarrow R$ (відображення двовимірної множини в одновимірну). Потрібно знайти функцію (а якщо існує, то і "щільність") розподілу випадкової величини $\eta = g(\xi 1, \xi 2)$.

Користуючись тим, що ймовірність випадковому вектору потрапити в деяку область можна обчислити як об'єм під графіком щільності розподілу вектора над цією областю, сформулюємо твердження.

Теорема: Нехай $x \in R$ і область $D_x \subseteq R^2$ складається з точок таких, що $g(\xi 1, \xi 2) < x$. Тоді випадкова величина $\eta = g(\xi 1, \xi 2)$ має функцію розподілу:

$$F\eta(x) = P\left(g(\xi 1, \xi 2) < x\right) = P\left[(\xi 1, \xi 2) \notin D_x\right] = \int_{Dx1}\int_{Dx2} f_{\xi 1 \xi 2}(x_1, x_2)\, dx1\, dx2 \tag{3.19}$$

Далі припускаємо, що випадкові величини $\xi 1, \xi 2$ і тобто

$$f_{\xi 1 \xi 2}(x_1, x_2) = f_{\xi 1}(x_1) \cdot f_{\xi 2}(x_2). \tag{3.20}$$

В цьому випадку розподіл величини $g(\xi 1, \xi 2)$ повністю визначається розподілами величин $\xi 1, \xi 2$.

Формула згортки: якщо випадкові величини $\xi 1, \xi 2$ незалежні і мають абсолютно неперервні розподіли з щільностями $f_{\xi 1}(x_1)$ та $f_{\xi 2}(x_2)$, то щільність розподілу суми $\xi 1 + \xi 2$ рівна згортці щільностей $f_{\xi 1}(x_1)$ і $f_{\xi 2}(x_2)$:

$$f_{\zeta 1+\zeta 2}(t) = \int_{-\infty}^{\infty} f_{\xi 1}(u) \cdot f_{\xi 2}(t-u)\, du = \int_{-\infty}^{\infty} f_{\xi 2}(t) \cdot f_{\xi 1}(t-u)\, du \tag{3.21}$$

"Згортка" — бінарний оператор, що бере два об’єкти — розподіли ймовірностей і повертає об’єкт того ж класу — розподіл ймовірностей. Неважко перевірити, що оператор згортки — асоціативний і комутативний. Доведення формули згортки базується на теоремі і перетвореннях подвійного інтегралу. Типова задача в дослідженні стохастичних систем — проходження сигналу (потоку) з

певним розподілом ймовірностей $f1(x)$ через ймовірнісний перетворювач з певним розподілом $f2(x)$. Розподіл на виході теж визначається згорткою.

Формування стохастичних функції виробництва для випадку стандартних розподілів ймовірностей. У відповідність кожній точці ФВ — залежності "витрати — випуск" ставимо розподіл ймовірностей. Використовуємо дані попередніх розділів. Робимо узагальнену модель модель, яку можна застосувати для завдань розвитку, інноваційного розвитку, виконання проектних робіт та ін.

Реалізація. Технологію побудови стохастичної функції «витрати, випуск» подамо на прикладі функції класу "обмежена, монотонно зростаюча".

1. Задаємо детерміновану функцію:

$$F(x, vpF) := F4\left(x, vpF_1, vpF_2, vpF_3\right) \;;\; pF(x, vpF) := \frac{d}{dx} F(x, vpF) \tag{3.22}$$

2. Задаємо розподіл ймовірностей(нечіткості):

$$fpr\left(y, \mu, \sigma\right) := dnorm\left(y, \mu, \sigma\right) \tag{3.23}$$

3. Задаємо залежності параметрів розподілу від вхідної змінної *X:*

$$f\mu(x, vpF) := F(x, vpF); \tag{3.24}$$

$$f\sigma(x, vpF, kz) := kz_1 \cdot \left(pF(x, vpF) + kz_2\right) \tag{3.25}$$

4. Збираємо стохастичну функцію:

$$Ffz(x, y, vpF, kz) := fpr\left(y, f\mu(x, vpF), f\sigma(x, vpF, kz)\right) \tag{3.26}$$

5. Реалізація значення стохастичної функції:

$$Yy(x, vpF, kz) := \left| \begin{array}{l} qq \leftarrow rnorm\left[1, F(x, vpF), kz_1 \cdot \left(pF(x, vpF) + kz_2\right)\right]_1 \\ kk \leftarrow max(qq, 0) \end{array} \right. \tag{3.27}$$

Задаємо значення параметрів і виводимо для контролю і аналізу стохастичної функції *x:=0,8..400.*

Робимо дискретизовану версію функції: число точок дискретизації

y:=1..200 $Nk := 100;\quad i := 1..Nk;\quad j := 1..Nk;\quad dx := 3;\quad dy := 1$

$$kz := \begin{pmatrix} 20 \\ 0.5 \end{pmatrix};\quad vpF := \begin{pmatrix} 8 \\ 0.025 \\ 25 \end{pmatrix};\quad ffz_{i,j} := Ffz(i \cdot dx, j \cdot dy, vpF, kz)$$

На рисунку 3.6 подана графічна частина інтерфейсу для модуля введення і аналіз стохастичних функцій виробництва на базі стандартних розподілів ймовірностей. Послідовно подані:

— реалізація стохастичної ФВ;

—розкид ФВ;

— тривимірний графік стохастичної ФВ.

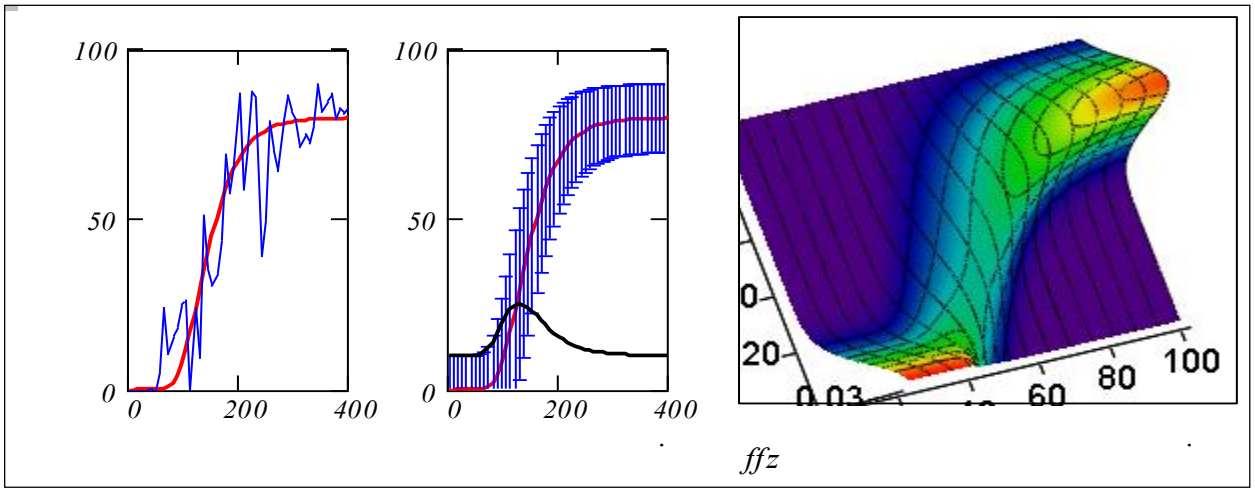


Рисунок 3.6 —Візуальний аналіз стохастичної ФВ

На першому графіку — середнє значення і реалізація цієї функції. Сусідні значення в цій моделі нечіткої функції некорельовані, проте можливо ввести випадковий зв'язок в модель. Другий графік — розподіл нечіткості. Можна використовувати простішу модель — з рівномірним розподілом:

$$myn(x) := f\mu(x, vpF) - f\sigma(x, vpF, kz); \tag{3.28}$$

$$plu(x) := f\mu(x, vpF) + f\sigma(x, vpF, kz) \tag{3.29}$$

Недолік цієї моделі стохастичної ФВ є непридатність її у випадку довільних емпіричних розподілів характерних для різних класів технологічних систем і неузгодженість з структурами даних методу оптимального агрегування.

Модифікація модуля оптимального агрегування для роботи зі

стохастичними функціями виробництва. В базовій версії беремо систему з трьох елементів. Аналіз ризиків розподіленої виробничої системи знайдемо таким чином. Вводимо вхідні дані.

Розмірність системи: $N := 3 \quad i := 1..N$

Вибираємо класи елементів: $vke := (4 \;\; 6 \;\; 7)$

Вводимо параметри ФВ елементів:

A1:=1.2; W1:=0.05; S1:=6; fo1$_n$:=F4(n·dx, A1, W1, S1);

A2:=1.4; W2:=0.02; S2:=8; fo2$_n$:=F6(n·dx, A2, W2, S2)

A3:=1.9; es:=00.3; ls:=10; fo3$_n$:=F4(n·dx, A3, es, ls).

Дискретизуємо і доповнюємо ФВ елементів для використання методу оптимального агрегування:

$f1 := augment(fo1, r0);\ \ f2 := augment(ffo2, r0);\ \ f3 := augment(fo3, r0).$

Задаємо класи і параметри розподілів ймовірностей для ФВ елементів.

Вибираємо класи розподілів ймовірностей $mke := \begin{pmatrix} 4 & 6 & 4 \\ 2 & 2 & 2 \end{pmatrix}$.

Вводимо базові параметри розподілів ймовірностей елементів. В першому наближенні вважаємо дисперсії постійними. Маємо такі залежності параметрів розподілу від вхідної змінної *X*. Задаємо число точок розподілу:

$Kr := 100;\ \ r := 1..Kr;\ \ y_r := r;$

$\sigma 1 := 2;\ \ f\mu 1_n := fo1_n;\ \ f\sigma 1_n := \sigma 1;\ \ p1_r := dnorm(y_r, 20, \sigma 1);$

$\sigma 2 := 4;\ \ f\mu 2_n := fo2_n;\ \ f\sigma 2_n := \sigma 2;\ \ p2_r := dnorm(y_r, 30, \sigma 2);$

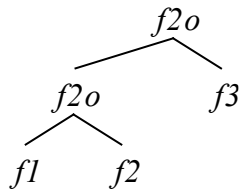
$\sigma 3 := 6;\ \ f\mu 3_n := fo3_n;\ \ f\sigma 3_n := \sigma 3;\ \ p3_r := dnorm(y_r, 50, \sigma 3).$

Будуємо графіки функцій виробництва та розподілів ймовірностей елементів. Виконаємо оптимальне агрегування. Запишемо формулу агрегування в звичайній формі:

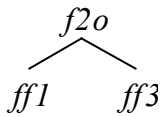
$$Ops3 := f2o(f3, f2o(f2, f1)) \tag{3.30}$$

і в структурній:

$Op3 :=$



$Op2 :=$



На рис. 3.7 представлено агрегування систем з трьох і двох елементів.

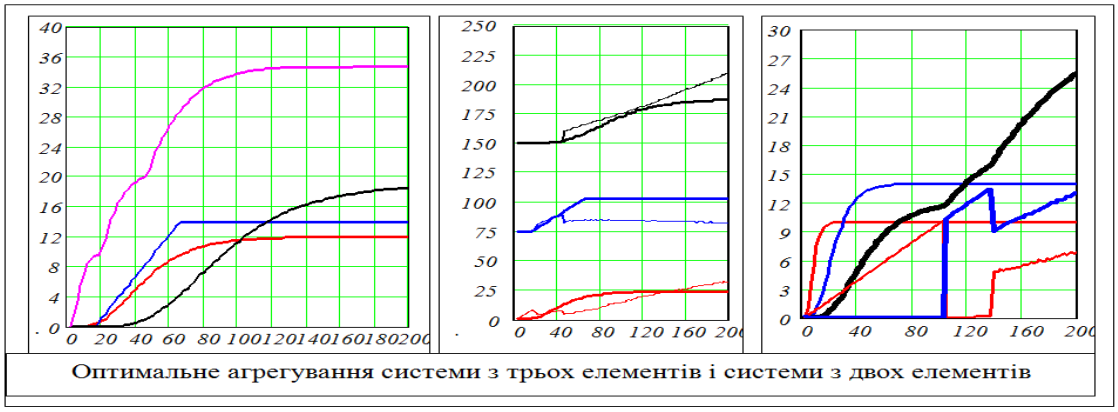


Рисунок 3.7 — Агрегування систем з трьох і двох елементів. Тестові дані

ВИСНОВКИ

Розроблено комплекс моделей і програмних модулів для оптимізації і аналізу ефективності і ризиків виробничих систем моніторингу захищеності об’єкту.

Математична суть розробки. Напрацювання теоретичних і прикладних результатів стосовно нових алгебраїчних об’єктів - стохастичних (розмитих) ФВ.

Методологічна суть розробки. Інтеграція задач прикладного системного аналізу: оптимізації та аналізу ризиків для технічних систем (розглядаємо саме ризики технологічного характеру).

Метою роботи було підвищення ефективності управління сучасними комп’ютерними системами для аналізу і реакції системи моніторингу захищеності об’єкту.

Для досягнення поставленої мети виконано розв’язання таких задач:

—проведено аналіз стану розробки моделей систем обслуговування моніторингу захищеності об’єкту;

—виконано аналіз типових ресурсних структур об’єктів – послідовних, паралельних з ресурсними і часовими зв’язками між підсистемами;

—побудовано узагальнену модель оптимального управління процесами функціонування систем на базі вбудованих генераторів випадкових процесів з заданими розподілами ймовірностей;

—виконано моделювання елементів і підсистем.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Компютеризована система моніторингу захищеності обєкту. Артоуз А.О., Колесник І. С., лектронні наукові видання, LI Науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії. Вінниця – 2022. – 1 с.

2. УДК 007: 304: 001, Серія: Соціальні комунікації, 2015 р., № 4 (24), [Текст]

3. Лабораторія штучного інтелекту MIT, 10 червня 1998 р., [Текст]

4. ГСТУ СУІБ 1.0/ISO/IEC 27001:2010, Інформаційні технології-методи захисту система управління інформаційною безпекою, офіційний переклад, ст.3, [Текст]

5. «Основи інформаційної безпеки» Маркуш Олег, [Текст]

6. Частина друга статті 10 Конвенції про захист прав людини і основоположних свобод, [Текст]

7. The Protection of Information in Computer Systems JEROME H. SALTZER, SENIOR MEMBER, IEEE, AND MICHAEL D. SCHROEDER, MEMBER, IEEE, [Текст]

8. Venter, H. S. A taxonomy for information security technologies / H. S. Venter, J. H. P. Eloff // Computers & Security. — 2003. — Vol. 22, no. 4. — P. 299–307, [Текст]

9. Anderson, J. M. Why we need a new definition of information security // Computers& Security. — 2003. — Vol. 22, no. 4. — P. 308–313, [Текст]

10. Venter, H. S.; Eloff, J. H. P. (2003). «A taxonomy for information security technologies». Computers & Security. 22 (4): 299–307, [Текст]

11. Курок Р.О., Національна академія Служби безпеки України, ІНФОРМАЦІЙНА БЕЗПЕКА В ДІЯЛЬНОСТІ СБ УКРАЇНИ: СУЧАСНІ ПРОБЛЕМИ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ, [Текст]

12. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», [Текст]

13. Інформаційна безпека (соціально-правові аспекти) / [В. Остроухов, В. Петрик, М. Присяжнюк та ін.] ; за ред. Є.Д. Скулиша. – К. : КНТ, 2010. – 776 с., с. 89,[Текст]

14. Дереко В.Н. Теоретико-методологічні засади класифікації загроз об'єктам інформаційної безпеки / В. Дереко // Інформаційна безпека людини, суспільства, держави. – 2015. – № 2 (18). – С. 16–22, [Текст]

15. National Information Assurance Training and Education Center, [Текст]

16. NIST Special Publication 800-30 Revision 1. Guide for Conducting Risk Assessments, [Текст]

17. ПОЛОЖЕННЯ про організацію системи управління ризиками в банках України та банківських групах, [Текст]

18. Стакснет [Електронний ресурс]. — [S. l. : s. n.]. — URL: https://uk.wikipedia.org/wiki/Стакснет (дата звернення: 10.05.2022).

19. В Бразилии раскрыта банда сетевых мошенников [Электронный ресурс]. —[Б. м. : б. и.]. — URL: http://www.securitylab.ru/news/215150.php (дата звернення: 10.05.2022).

20. В інтернеті з'явилися комерційні секрети "Microsoft" - Korrespondent.net [Електронний ресурс]. — [S. l. : s. n.]. — URL: http://ua.korrespondent.net/tech/247370-v-interneti-zyavilisya-komercijni-sekreti-microsoft (дата звернення: 10.05.2022).

21. Белокопытов, А.В. Современные информационные технологии: учебное

пособие [Текст] / А.В. Белокопытов. — Смоленск : ФГОУ ВПО «Смоленская сельскохозяйственная академия», 2013. — ISBN: 9785457413658.

22. Малюк, А.А. Информационная безопасность. Концептуальные и методологические основы защиты информации [Текст] / А.А. Малюк. — М. : Горячая Линия - Телеком, 2004. — ISBN: 5-93517-197-X

23. Аакер Д.А. Бизнес-стратегия: от изучения рыночной среды до выработки беспроигрышных решений. М.: Эксмо, 2007. 464 с. ISBN 978-5-699-22614-6.

24. David L. Drake, Katherine L. Morse. The Security-Specific Eight-Stage Risk Assessments Methodology. - Proceed. Of the 17 th National Computer Security Conference, 19946.

25. Боровська Т.М. Моделювання розвитку підприємства "на фоні" підприємств і споживачів сегменту ринку. / Боровська Т.М., Колесник І.С., Северілов В.А. // Вісник ВПІ. – 2009. – № 1. – С. 28-36 – ISSN 1997 9266.

26. Боровська Т. М. Основи теорії управління та дослідження операцій. Навчальний посібник / Т. М. Боровська, І.С. Колесник, В.А. Северілов. – Вінниця: УНІВЕРСУМ-Вінниця, 2008. – 242 с. – ISBN 978-966-641-275-4.

27. Боровська Т.М. Оптимізація розподілу обмеженого ресурсу у виробничій системі на базі агрегування виробничих функцій / Т.М. Боровська, І.С. Колесник, В.А. Северілов // Інформаційні технології та комп’ютерна інженерія. 2005. – № 1. – С. 12-18.

28. Дев'янин П.Н., Михальский О.О., Правиков Д.И. і ін. Теоретичні основи комп'ютерної безпеки: Навчальний посібник для вузів - М.: Радіо й зв'язок, 2000.- 192 с.

29. Загальні критерії ISO 15408: 1999–1–3.

30. Колесник І.С. Розробка імітаційних моделей для оцінки ризиків ринку./ Колесник І.С., Северілов П.В. ,Северілов В.А. // Матеріали V Міжнародної НПК „Економічна безпека сучасного підприємства”. – Вінниця: УНІВЕРСУМ-Вінниця, 2008 – С. 66-71 – ISBN 978-966-641-246-4.

ДОДАТОК А

Технічне завдання

Міністерство освіти та науки України

Вінницький національний технічний університет

Факультет інформаційних технологій та комп’ютерної інженерії

ЗАТВЕРДЖУЮ

Завідувач кафедри ОТ ВНТУ

д.т.н., проф.

_____О. Д. Азаров

“__” _____ 2022 р.

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання бакалаврської дипломної роботи

«Комп’ютеризована система моніторингу захищеності об’єкту»

08-23.БДР.001.00.000 ПЗ

Науковий керівник к.т.н., доц. каф. ОТ

_____ Колесник І. С.

Студентка групи 1КІ-18б

_____ Артоуз А. О.

Вінниця 2022

1.Найменування та область застосування

Робоча назва проекту «Комп'ютеризована система моніторингу захищеності об'єкту», розробляється для навчання студентів створювати та проектувати комп'ютерні системи.

2. Основи для розробки

Основою для розробки є дисципліни «Кодування та захист інформації», «Основи науково дослідної роботи», «Комп'ютерні системи».

3 Мета МКР і призначення розробки

3.1 Мета роботи — розробка комп'ютеризованої системи моніторингу безпеки об'єктів, а також аналіз загрози безпеки інформації

3.2 Призначення розробки — система моніторингу захищеності безпеки об'єктів призначена для забезпечення інтелектуального аналізу атак та їх наслідків, а також допомоги адміністраторам вживати контрзаходи.

4 Етапи БДР та очікувані результати

Етапи роботи та очікувані результати приведено в Таблиці А.1.

Таблиця А.1 — Етапи БДР

№ етапу	Назва етапу	Термін виконання		Очікувані результати
		початок	кінець	
1	Аналіз завдання. Вступ	11.03.22	28.03.22	Вступ
2	Аналіз сучасних загроз безпеки інформації	29.03.22	18.04.22	розділ 1
3	Аналіз безпеки об'єкту	20.04.22	27.04.22	Розділ 2
4	Оцінка рівня безпеки підприємства та побудова експертної системи	27.04.22	10.05.22	Розділ 3
5	Оформлення пояснювальної записки	12.05.22	18.05.22	ПЗ, презентація

5 Матеріали, що подаються до захисту БДР

До захисту подаються: пояснювальна записка БДР, графічні і ілюстративні матеріали, протокол попереднього захисту БДР на кафедрі, відзив наукового керівника, рецензія опонента, протоколи складання державних екзаменів, анотації до БДР українською та іноземною мовами, довідка про відповідність оформлення БДР діючим вимогам.

6 Порядок контролю виконання та захисту БДР

Виконання етапів графічної та розрахункової документації БДР контролюється науковим керівником згідно зі встановленими термінами. Захист БДР відбувається на засіданні Державної екзаменаційної комісії, затвердженою наказом ректора.

7 Вимоги до оформлювання та порядок виконання МКР

7.1 При оформлюванні БДР використовуються:

— ДСТУ 3008 : 2015 «Звіти в сфері науки і техніки. Структура та правила оформлювання»;

— ДСТУ 8302 : 2015 «Бібліографічні посилання. Загальні положення та правила складання»;

— ГОСТ 2.104-2006 «Єдина система конструкторської документації. Основні написи»;

— документами на які посилаються у вище вказаних.

Технічне завдання до виконання отримала _____ Артоуз А.О.

ДОДАТОК Б

Приклади згорток розподілів ймовірностей

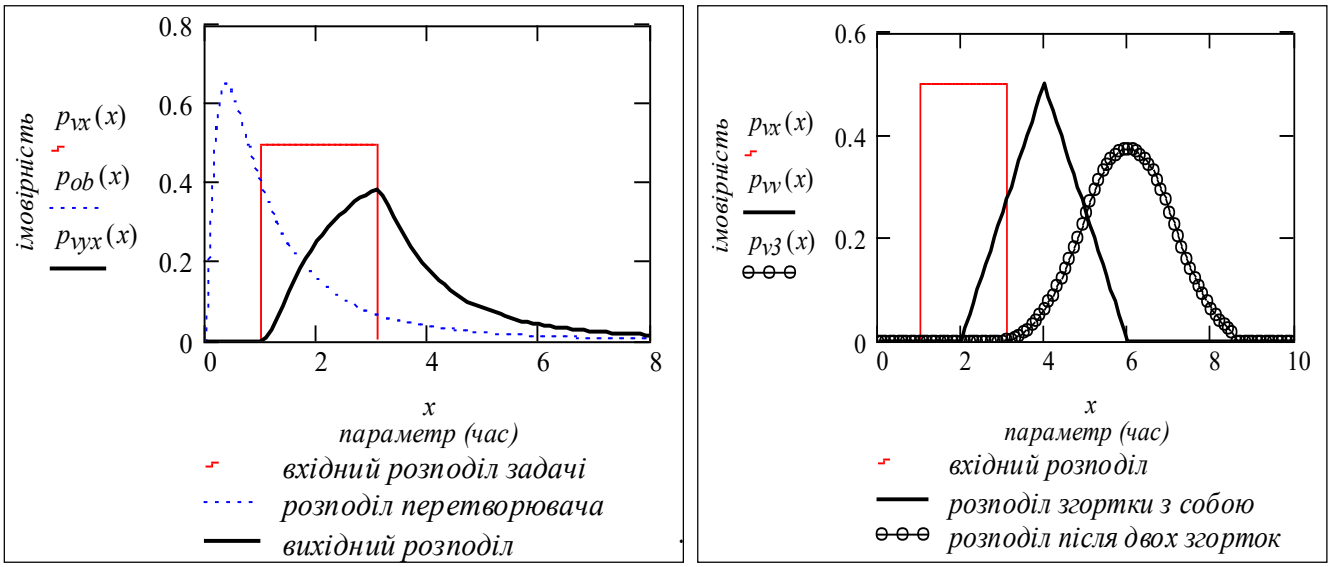


Рисунок Б.1 — Приклади згорток розподілів ймовірностей

ДОДАТОК В

Модуль генерації нормального розподілу

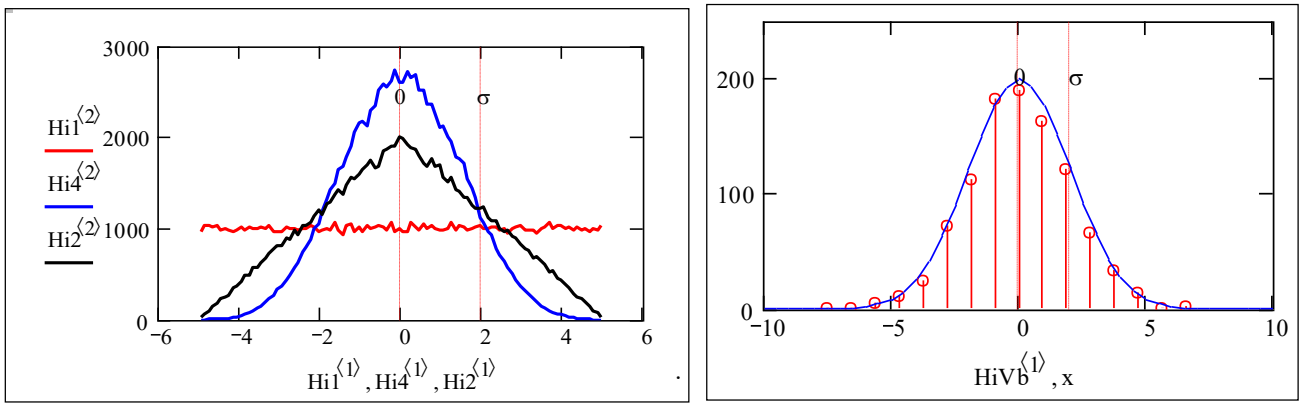


Рисунок В.1 — Модуль генерації нормального розподілу

ДОДАТОК Г

Модуль генерації Пуассонівського розподілу

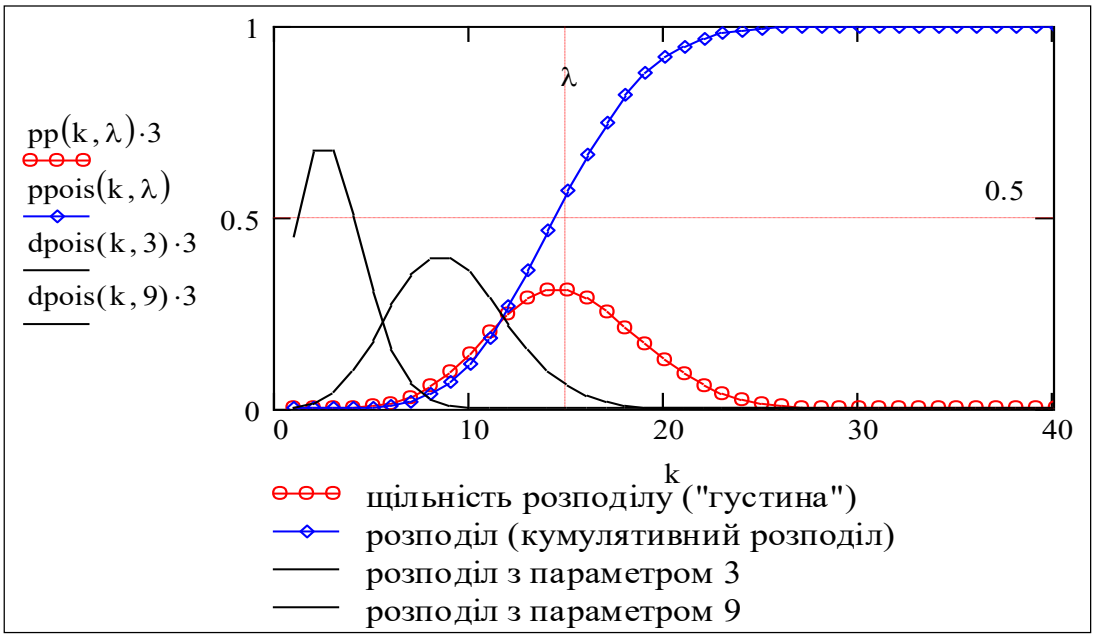


Рисунок Г.1 — Модуль генерації Пуассонівського розподілу

ДОДАТОК Д

Результати моделювання процесу з гіперболічною статистикою

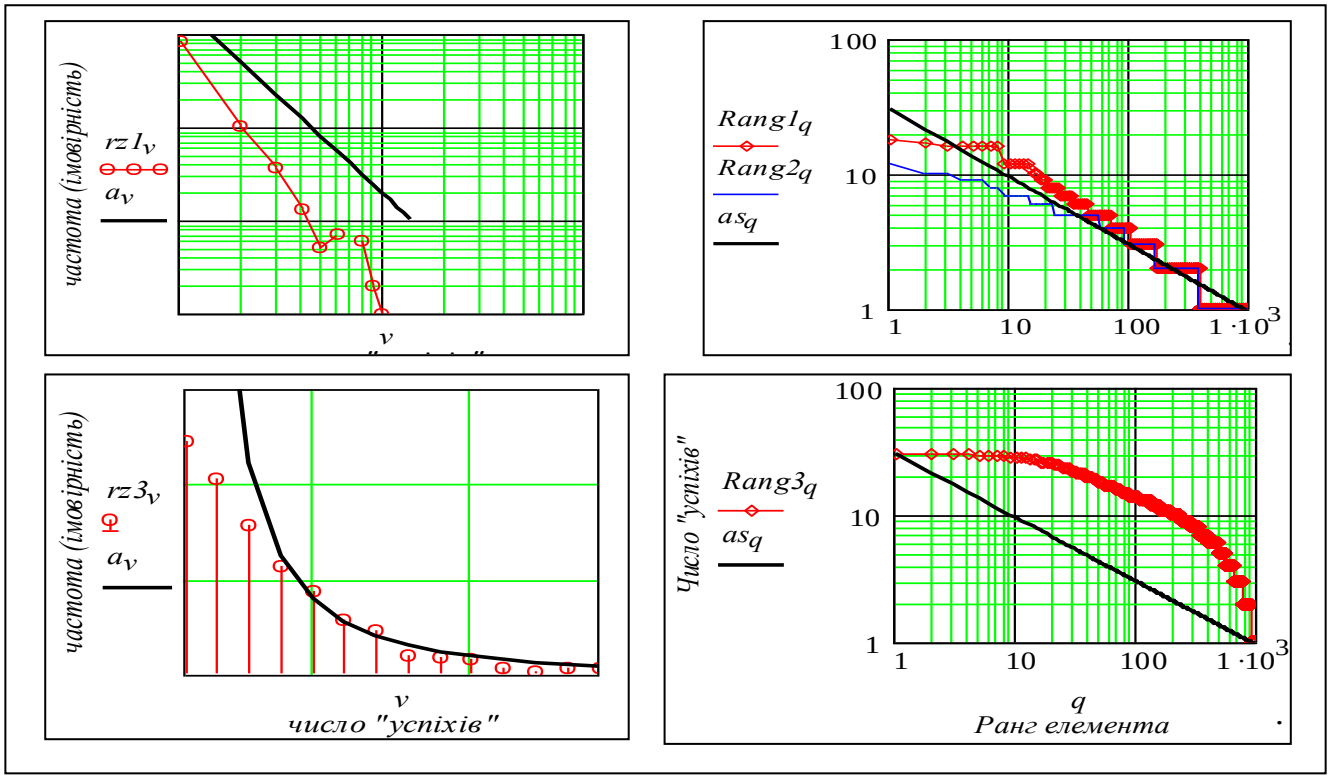


Рисунок Д.1 — Результати моделювання процесу з гіперболічною статистикою

ДОДАТОК Е

Протокол перевірки навчальної (кваліфікаційної) роботи

ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ НА
НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: «Комп'ютеризована система моніторингу захищеності об'єкту»

Тип роботи: бакалаврська дипломна робота
(БДР, МКР)

Підрозділ кафедра обчислювальної техніки
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність 81,6% Схожість 18,4%

Аналіз звіту подібності (відмітити потрібне):

- ✓ Запозичення, виявлення у роботі, оформлені коректно і не містять ознак плагіату.
- □ Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.
- □ Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Захарченко С.М.
(підпис) (прізвище, ініціали)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Артоуз А. О
(підпис) (прізвище, ініціали)

Керівник роботи _____ Колесник І. С.
(підпис) (прізвище, ініціали)