СУЧАСНІ МЕТОДИ ТА МОДЕЛІ ОБРОБКИ ДАНИХ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Монографія

За загальною редакцією доктора економічних наук, професора Пономаренка В. С.

Харків. Вид. ХНЕУ ім. С. Кузнеця, 2013

УДК 004.6
ББК 32.973.202-018.2
С91

Рецензенти: докт. техн. наук, ст. наук. співробітник Харківського університету Повітряних Сил імені Івана Кожедуба *Бараннік В. В.*; докт. екон. наук, професор, зав. кафедри економічної кібернетики Харківського національного економічного університету імені Семена Кузнеця *Клебанова Т. С.*; докт. техн. наук, професор кафедри електронних обчислювальних машин Харківського національного університету радіоелектроніки *Танянський С. С.*

Рекомендовано до видання рішенням вченої ради Харківського національного економічного університету імені Семена Кузнеця.
Протокол № 3 від 05.11.2012 р.

Авторський колектив: канд. екон. наук, доцент Беседовський О. М. – п. 1.1, п. 1.3; канд. екон. наук, професор Золотарьова І. О. – п. 1.2, розділ 7; канд. техн. наук, доцент Євсеєв С. П. – вступ, розділ 2, висновки; канд. техн. наук, доцент Дорохов О. В. – вступ, розділ 8, висновки; викладач Король О. Г. – розділ 3; канд. техн. наук, доцент Павленко Л. А. – розділ 4; канд. техн. наук, доцент Парфьонов Ю. Е. – розділ 10; ст. викладач Плеханова Г. О. – розділ 5; канд. техн. наук, доцент Тарасов О. В. – розділи 6, 12; канд. екон. наук, доцент Ушакова І. О. – розділ 9; канд. техн. наук, професор Щербаков О. В. – розділ 11.

С91 Сучасні методи та моделі обробки даних в інформаційних системах : монографія / О. М. Беседовський, І. О. Золотарьова, С. П. Євсеєв та ін. ; за заг. ред. докт. екон. наук, професора Пономаренка В. С. – Х. : Вид. ХНЕУ ім. С. Кузнеця, 2013. – 540 с. (Укр. мов.)

Розкрито сучасні підходи до моделювання бізнес-процесів підприємств, зокрема податкового обліку, прийняття управлінських рішень, комунікацій, транспортного обслуговування, питань лояльності клієнтів, інформаційного пошуку, рекламної діяльності, управління персоналом. Подано теоретико-методологічні підходи до оцінювання економічної ефективності їх упровадження. Досліджено сучасні механізми автентифікації в банківських системах, методи стиснення текстової інформації в базах даних на основі блоково-статистичних алгоритмів.

Рекомендовано для системних аналітиків, фахівців у сфері проектування, впровадження та експлуатації інформаційних систем, обробки та захисту інформації.

ISBN

УДК 004.6
ББК 32.973.202-018.2

Зміст

у КМіС, які засновані на використанні теоретико-кодових схем (ТКС) на основі методів завадостійкого кодування в режимі маскування від порушника швидкого правила декодування.

Розглянуто основні моделі та основні параметри оцінки теоретико-кодових схем (ТКС) на основі використання алгебраїчних блокових кодів щодо забезпечення безпеки даних. Проведено аналіз можливих способів модифікації ТКС щодо суттєвого зниження обсягу ключових даних і зняття основного обмеження з практичного використання теоретико-кодових схем та оцінка їх параметрів. Проаналізовано показники і критерії безпеки і достовірності передачі даних, теоретично обґрунтоване введення узагальненого показника ефективності обміну даними в ЛОМ і ГОМ. Досліджено ефективності передачі даних у комп'ютерних системах і мережах з використанням розроблених криптосистем.

Розглянуто структурну схему Національної платіжної системи, основні тенденції її розвитку, класифікація загроз інформаційної безпеки внутрішньо-платіжних систем комерційних банків України, послуги і механізми, які забезпечують інформаційну безпеку банківських транзакцій за допомогою криптографічних перетворень на основі послуг шифрування і автентифікації та цифрового підпису.

Розглянуто основні механізми забезпечення цілісності та автентичності даних, які обробляються та передаються в ВПС. Наведено загальну класифікацію кодів цілісності даних (MDC-кодів) й кодів автентичності повідомлень (MAC-кодів), аналізуються їх основні характеристики щодо забезпечення інформаційної безпеки даних на основі результатів оцінок криптографічного конкурсу NESSIE. Розглянуто основні моделі побудови MAC-кодів.

Розглянуто модель і структурну схему каскадного ключового гешування для формування кодів автентичності UMAC, а також особливості її побудови й багатоетапного формування геш-коду з використанням універсального гешування й шифрування.

продукції в натуральному виразі; максимізація завантаження спеціалізованого устаткування при наявності обмежень.

Показано, що в разі наявності точної математичної постановки завдання, де чітко визначені критерії, альтернативи, обмеження для прийняття рішень застосовуються методи теорії дослідження операцій.

4.6. Загальні принципи структуризації альтернатив 147

Наведено огляд головних принципів структуризації альтернатив: ранжування об'єктів, завдання функції вибору, завдання функції переваги, парне порівняння.

4.7. Структурування альтернатив з використанням критеріїв 148

Показано, що у загальному випадку критерій подають у вигляді деякої оцінної функції К, яка приймає значення на деякій безлічі оцінок ОПР, або у вигляді правила, за яким вибирається "якнайкраща альтернатива", яка відповідає максимальному або мінімальному значенню оцінної функції (залежно від значення критерію). Окремим випадком є прийняття рішень на підставі одного критерію.

Наведено приклад використання критеріальної таблиці при прийнятті рішень. Показано, що в разі вирішення багатокритеріального завдання, якщо перевага за одним критерієм спричиняє за собою таку ж перевагу за іншим критерієм, тобто критерії кооперуються, то вирішення завдання не є проблемою. Рішення багатокритеріального завдання також не становить особливої складності, якщо критерії нейтральні один відносно одного. У загальному випадку критерії конкурують один з одним. Аналіз таких ситуацій здійснюють за допомогою визначення множини Парето.

4.8. Альтернативи, що не домінуються, Еджворта – Парето 150

Показано, що принцип Парето полягає в тому, що оптимальний результат слід шукати тільки серед елементів множини рішень, що не домінуться. Парето-оптимальність рішення a^* означає, що воно не може бути поліпшено за жодним із критеріїв без погіршення за якимось іншим критерієм.

Наведено етапи вирішення багатокритеріального завдання з урахуванням множини непокращувальних рішень за принципом Парето.

4.9. Моделі і методи прийняття рішень в умовах багатокритеріальності 152

Наведено огляд та приклади використання методів прийняття рішень в умовах багатокритеріальності: парне порівняння на основі єдиної порядкової шкали, прийняття рішень на основі згортки критеріїв, метод головного критерію, метод лінійної (адитивної) згортки як метод упорядкування альтернатив, метод максимінної згортки, метод мультиплікативної згортки.

4.10. Прийняття рішень методом аналітичної ієрархії (МАІ) 156

Наведено загальні аспекти методу МАІ, метод обчислення індексу узгодженості (ІУ) та відношення узгодженості (ВУ), принцип перевірки адекватності моделі, яка побудована за методом МАІ.

Показано, що розроблені й успішно застосовуються пакети прикладних програм, які дозволяють виконувати: побудову ієрархії, порівняння альтернатив

на підставі вибраних критеріїв, необхідні обчислення пріоритетів рівнів, узгодженості рішень і отримати остаточний варіант ранжування альтернатив. До них відносяться такі пакети: "Expert Choice", "Decision Greed", "ИМПЕРАТОР".

Подано модель, побудовану засобами пакета "ИМПЕРАТОР", яка дозволяє ранжувати альтернативи вибору заходів з підвищення екологічної безпеки регіону.

Показано, що в теорії прийняття рішень розрізняють такі види невизначеності: стохастична або імовірнісна та повна невизначеність. Перша має місце, коли відомі імовірності настання наслідків прийняття рішень. Її називають "доброякісна невизначеність". Наведено загальні аспекти вирішення завдань в умовах ризику та метод дерева рішень.

Вирішено завдання вибору раціональної кількості устаткування в умовах стохастичної невизначеності.

Наведено головні засади теорії ігор для вирішення завдань прийняття рішень: матричні ігри антагоністів, методи рішення кінцевих ігор та приклади вирішення завдань.

Наведено класичні критерії прийняття рішень в іграх з природою в умовах повної невизначеності: Лапласа, Вальда, Севіджа, Гурвіца та приклади їх використання для вирішення завдання вибору раціональної кількості устаткування в умовах стохастичної невизначеності.

Показано, що рішення, отримані за різними методами не дають однакових результатів, що підтверджує головну тезу теорії прийняття рішень про те, що не існує абсолютно кращого рішення.

Наведено головні принципи, які покладено в основу теорії нечітких множин у прийнятті рішень. Наведено завдання прийняття рішень з вибору альтернатив, що не домінуються, у разі чіткого опису альтернатив, вибору альтернатив у разі декількох відношень переваги.

Наведено вирішення завдання вибору альтернативи з найбільшим ступенем недомінованості на підставі методу прийняття рішень при нечіткому відношенні переваги на безлічі чітко заданих альтернатив.

Розглянуто функціональність та класи сучасних програмних комплексів для управління персоналом, охарактеризовано український ринок HRM-систем (Human Resource Management). Узагальнено ключові напрями технологічного розвитку HRM-систем та запропоновано критерії вибору програмних комплексів для управління персоналом. Досліджено теоретико-методологічні підходи

щодо оцінювання економічної ефективності впровадження HRM-систем та доведено актуальність розробки моделей оцінювання ефективності HRM-систем.

Зазначено, що у зв'язку зі стрімким зростанням обсягів інформаційних ресурсів постійно виникає проблема позбавлення надлишковості даних. Констатується, що одним із шляхів вирішення цієї проблеми є розробка алгоритмів стиснення, які дозволяють підвищити ефективність збереження та передачі даних за допомогою зменшення їх надмірності

Проведено аналіз сучасного стану алгоритмів стиснення та визначено сфери їх застосування.

Констатується, що застосування алгоритмів стиснення у базах даних, особливо для зменшення об'єму текстових полів, має певні особливості і зазвичай базується на алгоритмі Хаффмана.

Запропоновано модифікацію алгоритму Хаффмана – блоково-статистичний алгоритм і теоретично обґрунтовано його ефективність порівняно з класичним алгоритмом.

Проведено експериментальне дослідження ефективності блоково-статистичного алгоритму стиснення інформації.

На основі даних різного об'єму, що підкоряються різноманітним законам розподілу частоти зустрічальності символів, проведено порівняльний аналіз запропонованого блоково-статистичного алгоритму та класичного алгоритму Хаффмана. Стверджується, що ефективність стиснення запропонованого блоково-статистичного методу вище за класичний алгоритм, та досягає свого максимуму при розподілі вхідного алфавіту на дві рівні за сумарною частотою символів групи.

Розглянуто функціонування сучасних мереж передачі даних з точки зору подання інформації, її маршрутизації і комутації. Проведено аналіз основних мережних протоколів з точки зору доцільності їх корпоративного використання, технології передачі даних, конкретного обладнання та його конфігурації.

Отримали розвиток принципи та вимоги до розробки, проектування програмного забезпечення для систем підтримки прийняття рішень у галузі транспортного обслуговування. Доведено необхідність першочергового забезпечення достовірності вводу даних, обробки помилок, підвищення швидкодії програмного забезпечення. Наведено відповідні засоби та рекомендації. Запропоновано принципи проектування форм і інтерфейсів.

Зазначено, що основна мета сучасної маркетингової стратегії направлена на формування сприятливих взаємовідносин з клієнтами. Показано кореляцію економічної лояльності з реальною поведінкою клієнтів.

Стратегія управління взаємовідносинами з клієнтами побудована на моделі взаємодії, в якій центральне місце в бізнесі займає клієнт, а основними напрямами діяльності є заходи з підтримки маркетингу, продажів та обслуговування клієнтів. Інформаційні технології дають нову платформу для поширення взаємовідносин з клієнтами. Такою платформою є соціальні мережі.

Проведено аналіз, який свідчить про те, що серед різноманіття імітаційних підходів моделювання соціальних мереж найбільш перспективними є системна динаміка, дискретно-подієве та агентне моделювання. Основа системної динаміки – побудова графічнних діаграм причинних зв’язків і глобальних впливів одних параметрів на інші в часі. Дискретно-подієве моделювання – це підхід, що пропонує абстрагуватися від безперервної природи подій і розглядати тільки основні події модельованої системи, такі, як: "очікування", "обробка замовлення", "рух з вантажем" та інші.

Найбільш перспективним для моделювання процесів, що відбуваються в соціальних мережах, є агентне моделювання. Це напрям в імітаційному моделюванні, який використовується для дослідження децентралізованих систем, динаміка функціонування яких визначається не глобальними правилами і законами, а навпаки, коли ці глобальні правила і закони є результатом індивідуальної активності членів групи.

Проведено порівняльний аналіз ринку пакетів імітаційного моделювання за різними характеристиками, на підставі якого для моделювання впливу соціальних мереж на лояльність клієнтів був обраний пакет AnyLogic 6.7.1.

Подано предметну технологію моделювання, яка включає: моделювання впливу реклами на формування лояльності клієнтів з врахуванням впливу спілкування агентів, моделювання повторних покупок та перевірку адекватності мо-

основні положення теорії Е-мереж, принципи побудови моделей та їх функціонування.

Подано опис програмної реалізації системи імітаційного моделювання, виконаної на кафедрі інформаційних систем ХНЕУ. Запропонована система є спеціалізованим інструментальним програмним засобом для створення, редагування та дослідження моделей на основі Е-мереж. Показано приклади використання цієї системи для створення імітаційних моделей.

Запропоновано декілька моделей різних елементів навчального процесу. Проведено дослідження моделей окремих видів занять, таких, як лабораторне заняття або самостійна робота студентів. Доведено можливість використання запропонованого підходу для побудови моделей процесу вивчення окремої навчальної дисципліни та навчального плану підготовки бакалаврів у цілому. Наведено окремі результати моделювання процесу адаптації студентів до системи навчання за курсом.

Зазначено, що ринок товарів і послуг, що формується в Україні, усе наполегливіше вимагає залучення й використання реклами. Проведено аналіз видів рекламної кампанії та побудовано дерево функцій процесу "Прогнозування рекламної кампанії".

Запропоновано для прогнозування рекламної кампанії у сфері культури математичну модель, параметри якої можуть контролюватися.

Встановлено, що вирішення задачі планування рекламної кампанії складається з двох підзадач: визначення пропорцій розподілу коштів по заходах та визначення пропорцій розподілу коштів по видах реклами.

Для вирішення першої задачі виникає необхідність зберігати історію зміни таких параметрів, як кількість проведених заходів, їх окупність, кількість вкладених коштів у різні види реклами. Для вирішення другого завдання необхідно мати зібрані і проаналізовані параметри за певний період діяльності в минулому. Запропонована модель, що дозволяє вирішити означені задачі.

Вступ

У теперішній час Україна активно долучилася до світового процесу інформатизації, який характеризується широким застосуванням передових інформаційних технологій у найбільш відповідальні державні та комерційні системи управління й зв'язку.

Оперативний доступ до інформаційних та обчислювальних ресурсів, що підтримуються мережею Інтернет, сьогодні розглядається як фактор подолання міжнародної економічної та культурної ізоляції, внутрішньої дезінтеграції, умовою укріплення державності, інститутів громадянського суспільства, розвитку соціальної інфраструктури.

На сьогодні в Україні вже багато що зроблено в цьому важливому напрямі діяльності: розроблена нормативно-правова база захисту інформації, проводяться роботи щодо створення інфраструктури відкритих ключів, розгортається і функціонує національна система електронного цифрового підпису.

Розділ "Сучасні технології моделювання процесів оподаткування" присвячений теоретичним засадам процесу моделювання організації податкового обліку, оптимізації організації податкового обліку та його автоматизації. У другому розділі монографії розглянуто питання інтегрованого забезпечення захисту інформації та достовірності даних, які обробляються в комп'ютерних системах і мережах, основаних на застосуванні теоретико-кодових схем (ТКС) з використанням алгеброгеометричних кодів на основі еліптичних кривих, основні моделі та основні параметри оцінки ТКС на основі використання алгебраїчних блокових кодів щодо забезпечення безпеки даних. Проаналізовано показники і критерії безпеки і достовірності передачі даних, теоретично обґрунтоване введення узагальненого показника ефективності обміну даними в ЛОМ і ГОМ.

Особлива увага в розділі "Метод забезпечення автентичності і цілісності даних на основі властивостей алгоритму UMAC-32" приділяється застосуванню нових альтернативних методів автентичності на основі використання MAC-кодів, основаних на каскадних схемах універсальних класів геш-функцій, які на відміну від цифрового підпису дозволяють забезпечити сучасні вимоги до оперативності та конфіденційності механізмам забезпечення автентичності та цілісності банківських транзакцій. Розглянуто модель і структурну схему каскадного ключового гешування для формування кодів автентичності UMAC, а також особливості її

побудови й багатоетапного формування геш-коду з використанням універсального гешування й шифрування.

У розділі "Методи та моделі прийняття управлінських рішень" розглянуто основні питання головних засад комплексної концепції прийняття рішень, наведено традиційний підхід до класифікації задач прийняття рішень та розмежування підходів до вирішення тривіальних та нетривіальних завдань, наведені сучасні моделі прийняття рішень.

У розділі "Методи та моделі вибору та оцінювання ефективності HRM-систем" розглянуто функціональність та класи сучасних програмних комплексів для управління персоналом на основі HRM-систем. Узагальнено ключові напрями технологічного розвитку HRM-систем та запропоновано критерії вибору програмних комплексів для управління персоналом.

Сформульовано проблему економного зберігання великих обсягів текстової інформації у реляційних базах даних. Наведено класифікацію алгоритмів стиснення даних і подано рекомендації відносно використання кожного підходу. Запропоновано процедури модифікації алгоритму Хаффмана для отримання більшої ефективності при стисненні текстових даних (блоково-статистичний алгоритм) та проведено моделювання з метою оцінки ефективності запропонованого алгоритму для даних з різноманітними законами розподілу частот зустрічаємості символів, які розглянуто в розділі "Метод стиснення текстової інформації в базах даних на основі блоково-статистичного алгоритму".

Розділ "Моделювання роботи комунікаційної мережі" присвячено функціонуванню мереж передачі даних, їх маршрутизації і комутації з точки технологій передачі та конфігурації обладнання. Розрахунки визначили перевагиви икористання комплексу Asterisk для практичного проектування корпоративної інформаційно-комунікаційної системи за вимогами замовників до технічних характеристик системи в цілому та її елементів, забезпечення необхідних функціональних можливостей, вартісних вимог та обмежень.

У розділі "Моделювання взаємодії споживачів і виробників транспортних послуг" розглянуто деякі аспекти розподілу споживачів за підприємствами, які пропонують транспортні послуги з перевезень. Запропоновано відповідну математичну модель з урахуванням параметрів обслуговування, виробничих можливостей надавачів транспортних послуг та вимог клієнтів. Описано створення відповідної комп’ютерної програми, тестування якої показало придатність для використання у виробничих

умовах. Досліджено питання визначення структури транспортного ринку. Обґрунтовано необхідність застосування сегментації, класифікації, структуризації, вперше запропоновано метод класифікації за ентропією. Також розглянуто модель на основі теорії ігор для визначення структури парку транспортних засобів при плануванні діяльності перевізників. Вона враховує можливі ризики, протидію конкурентів, невизначеності різного походження, помилки введення даних для транспортних задач. Наведено принципи та вимоги до розробки, проектування, програмного забезпечення для комп'ютеризованих систем підтримки прийняття рішень в галузі транспортного обслуговування.

Розділ "Моделювання інформаційного впливу соціальних мереж на лояльність клієнтів" висвітлює питання впливу соціальних мереж на лояльність клієнтів. Сучасні інформаційні технології дають нову платформу для цього. Найбільш перспективним для моделювання процесів у соціальних мережах є агентне моделювання. Проведений аналіз пакетів імітаційного моделювання визначив переваги пакета AnyLogic. Подано технологію моделювання, яка включає: моделювання впливу реклами на формування лояльності клієнтів, моделювання з урахуванням впливу спілкування агентів, моделювання повторних покупок та перевірку адекватності моделі. Побудовані модель та здійснено моделювання впливу соціальних мереж на лояльність клієнтів в середовищі пакета AnyLogic.

У розділі "Моделювання інформаційного пошуку в мережі Інтернет з використанням метаданих" розглянуто традиційні методи інформаційного пошуку, концептуальні засади семантичної "павутини", проаналізовані засоби інформаційного пошуку в семантичній "павутині". Описані критерії релевантності, показники ефективності інформаційного пошуку, розроблений програмний засіб для дослідження ефективності інформаційного пошуку. Наведені результати порівняльного аналізу ефективності інформаційного пошуку з використанням традиційного підходу до інформаційного пошуку та підходу, який ґрунтується на семантичному описі інформаційних ресурсів з використанням метаданих.

Розділ "Моделювання елементів навчального процесу вищого навчального закладу" присвяченний завданням організації навчального процесу вищого навчального закладу. Розглянуто сучасний стан моделювання елементів навчального процесу ВНЗ. Обґрунтовано використання імітаційного моделювання та запропоновано використання Е-мереж для імітаційного моделювання елементів навчального процесу.

Подано опис програмної реалізації, виконаної на кафедрі інформаційних систем ХНЕУ. Ця система є спеціалізованим інструментальним програмним засобом для створення, редагування та дослідження моделей на основі Е-мереж. Запропоновано декілька моделей різних елементів навчального процесу. Проведено дослідження моделей окремих видів занять, таких, як лабораторне заняття або самостійна робота студентів. Доведено можливість використання цього підходу для побудови моделей процесу вивчення окремої навчальної дисципліни та навчального плану підготовки бакалаврів у цілому.

У розділі "Моделювання оцінки ефективності реклами культурно-масових заходів" досліджуються шляхи ефективного прогнозування рекламної кампанії в сфері культури за допомогою математичної моделі, параметри якої можуть контролюватися керівництвом культурно-масового підприємства.

Запропоновано вирішення задачі ефективного планування рекламної кампанії, що складається з двох підзадач: визначення пропорцій розподілу грошових коштів за заходами та визначення пропорцій розподілу грошових коштів за видами реклами в аспекті одного культурно-масового заходу.

Для вирішення першої задачі виникає необхідність зберігати історію динаміки зміни таких параметрів, як кількість проведених заходів, їх окупність, кількість вкладених коштів у створення заходу, а також кількість вкладених коштів у різні види реклами.

Для вирішення другого завдання необхідно мати зібрані і проаналізовані параметри за певний період діяльності закладу в минулому. Запропоновано математична модель, що дозволяє вирішити означені задачі.

Розділ 1. Сучасні технології моделювання процесів оподаткування

1.1. Теоретичні засади моделювання бізнес-процесів підприємств

Розглянуто теоретичні засади процесу моделювання, підходи до процесів моделювання, які використовуються на сучасному етапі розвитку інформаційного суспільства. Розглянуто технології, які використовуються для моделювання бізнес-процесів. Обґрунтовано необхідність моделювання бізнес-процесів податкового обліку на підприємствах і в органах державної податкової служби. Проаналізовано сутність та наведено характеристику понять "модель" та "моделювання".

Моделювання бізнес-процесів будь-якого підприємства, установи чи організації (далі – підприємства) направлене на аналіз їх поточної діяльності та пошук шляхів удосконалення цих процесів. Саме моделювання бізнес-процесів дозволяє проаналізувати етапи цих процесів, виявити слабкі місця як у функціонуванні окремих його етапів, так і негаразди в організації взаємодії між цими етапами. Тому якісно організований бізнес-процес є тією невід'ємною складовою, яка безпосередньо впливає на ефективність діяльності всього підприємства.

Бізнес-процесам та їх моделюванню присвячена низка робіт як вітчизняних, так і зарубіжних авторів, але особливої уваги заслуговує вивчення результатів таких наукових праць. Теорії організації бізнес-процесів та їх реорганізації присвячені праці таких вчених: Абдикеєва Н. М. [1], Капустіна П. А. [90], Кондратьєва В. В., Кузнецова М. Н. [99], Кулябова Д. С., Корольової А. В. [112], Лускатової О. В. [129], Репина В. В., Єліферова В. Г. [200; 201], М. Робсона [202], М. Хаммера, Дж. Чампі [255], Д. Кєдла [286]. Моделювання бізнес-процесів досліджували: Калянов Г. Н. [89], Репин В. В., Єліферов В. Г. [201], Чернявський Д. І., Рудаков Д. В. [263], Мінухін С. В. [140; 141; 183], А. Остервальдер, І. Піньє [172] та ін.

Діяльність підприємства складається з багатьох аспектів, які характеризують всі складові діяльності підприємства та процесу управління ним – це облік, планування, прогнозування, контроль, аналіз, прийняття

рішень та ін. Вагоме місце в цій діяльності відводиться обліку, а в тому числі і податковому обліку, який, з одного боку, ведеться на кожному підприємстві, яке повинне його вести та складати відповідну податкову звітність, а з іншого боку, – цей облік ведеться контролюючими органами, щоб простежити правильність нарахування податків, повноту та своєчасність їх сплати до державного та місцевих бюджетів.

Системи бухгалтерського й податкового обліку є невід'ємними частинами системи управління будь-якого підприємства, оскільки обов'язки вести бухгалтерський облік і готувати бухгалтерську звітність, а також сплачувати податки, закріплені законодавчо. Завдання підвищення ефективності облікових систем підприємств актуальна донині, незважаючи на значні досягнення на шляху її рішення з моменту початку реформування української економіки.

Сьогодні необхідність автоматизації процесів, що входять до системи бухгалтерського й податкового обліку, не викликає сумнівів у керівників і головних бухгалтерів підприємств. Це підтверджується широкою практикою використання різних інформаційних систем для цілей бухгалтерського й податкового обліку. Це починає закріплюватися законодавчо з прийняттям Законів України "Про електронні документи та електронний документообіг" [188] та ін.

Останнім часом все активніше проходить процес автоматизації роботи та приймання звітності в податкових інспекціях. Це пояснюється як швидкістю обробки отриманих даних, так і зменшенням помилок під час їх введення до автоматизованої інформаційно-аналітичної системи контролюючого органу.

Процесам податкового обліку як на підприємствах, так і в державній податковій службі присвячено багато праць таких сучасних авторів, як: Завгородній В. П. [82], Титоренко А. Г. [3], Бусин А. А. та Мутилі І. М. [31].

Сучасний етап розвитку українського суспільства, і, відповідно, підприємств, а також технологій, котрі забезпечують їх ефективне функціонування, вимагає використання відповідних технологій на більшості (якщо не на всіх) етапах функціонування підприємств, у тому числі і на етапі моделювання. Тим паче, що технології моделювання, які використовуються, є доволі різноплановими та ефективними. Ці технології поєднуються в різні групи, які підтримують процесно-орієнтовану, об'єктно-орієнтовану методології.

В основі всього процесу моделювання бізнес-процесів лежить поняття "модель". Під моделлю розуміють спрощене уявлення реального пристрою, організації та/або процесів, явищ, що протікають у ньому (ній) [89; 183; 263].

Модель – це широке поняття, характеристика якого наведена на рис. 1.1. Розглядають такі моделі: табличні, ієрархічні, натуральні, у вигляді графів, мережні інформаційні, об’єктно-орієнтовані і процесно-орієнтовані. Окремо розглядаються комп’ютерні та наукові моделі. У рамках цієї роботи особливу увагу приділено саме об’єктно-орієнтованим і процесно-орієнтованим моделям (у першу чергу, зважаючи на те, що моделювання процесу оподаткування та контролю за ним краще розглядати саме з точки зору процесного підходу).

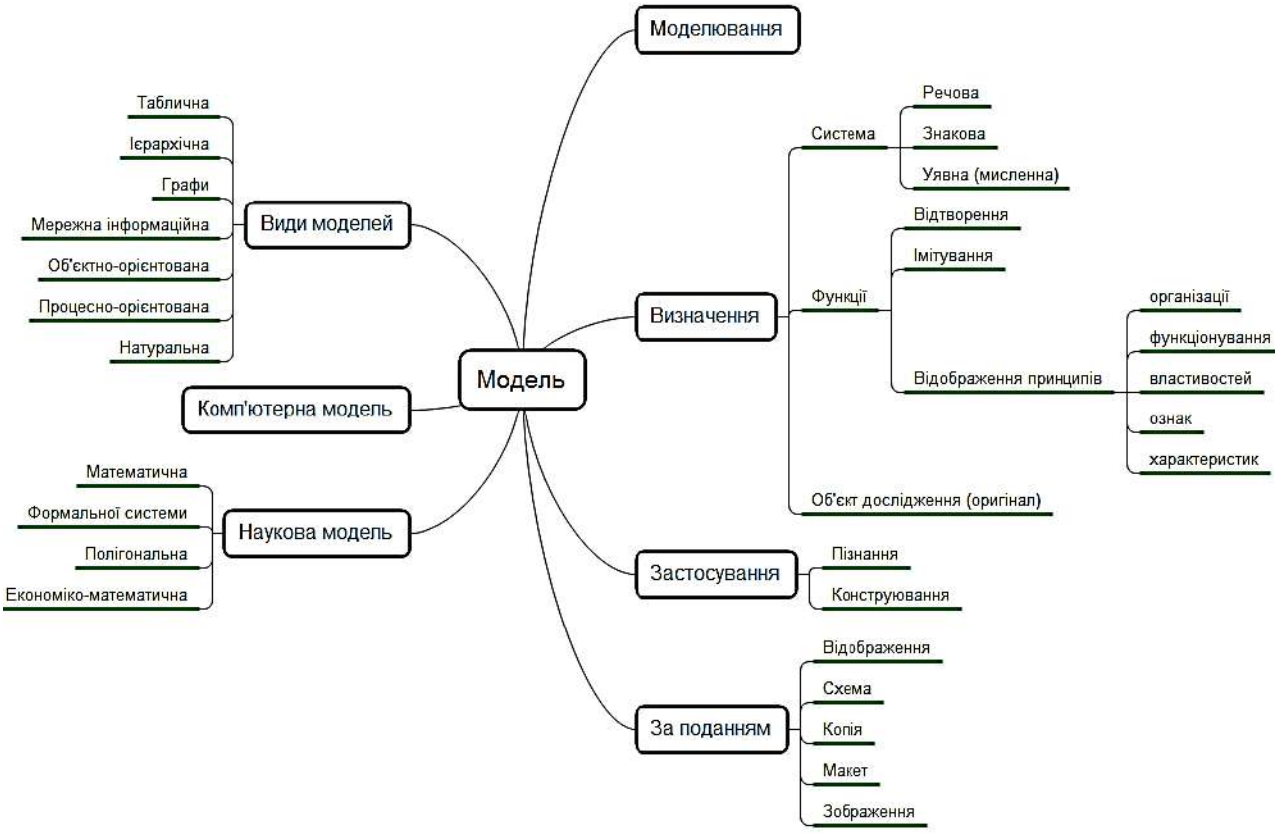


Рис. 1.1. **Характеристика поняття "модель"**

Однією з ключових характеристик поняття "модель" є поняття моделювання, за допомогою якого і відбувається опис моделі. Під моделюванням розуміють дослідження об’єктів пізнання на їх моделях; побудова і вивчення моделей реально існуючих об’єктів, процесів або явищ з метою

отримання пояснень цих явищ, а також для пе3редбачення явищ, що цікавлять дослідника [89; 183; 263].

Характеристика поняття "моделювання" за допомогою технології інтелектуальних карт наведена на рис. 1.2.

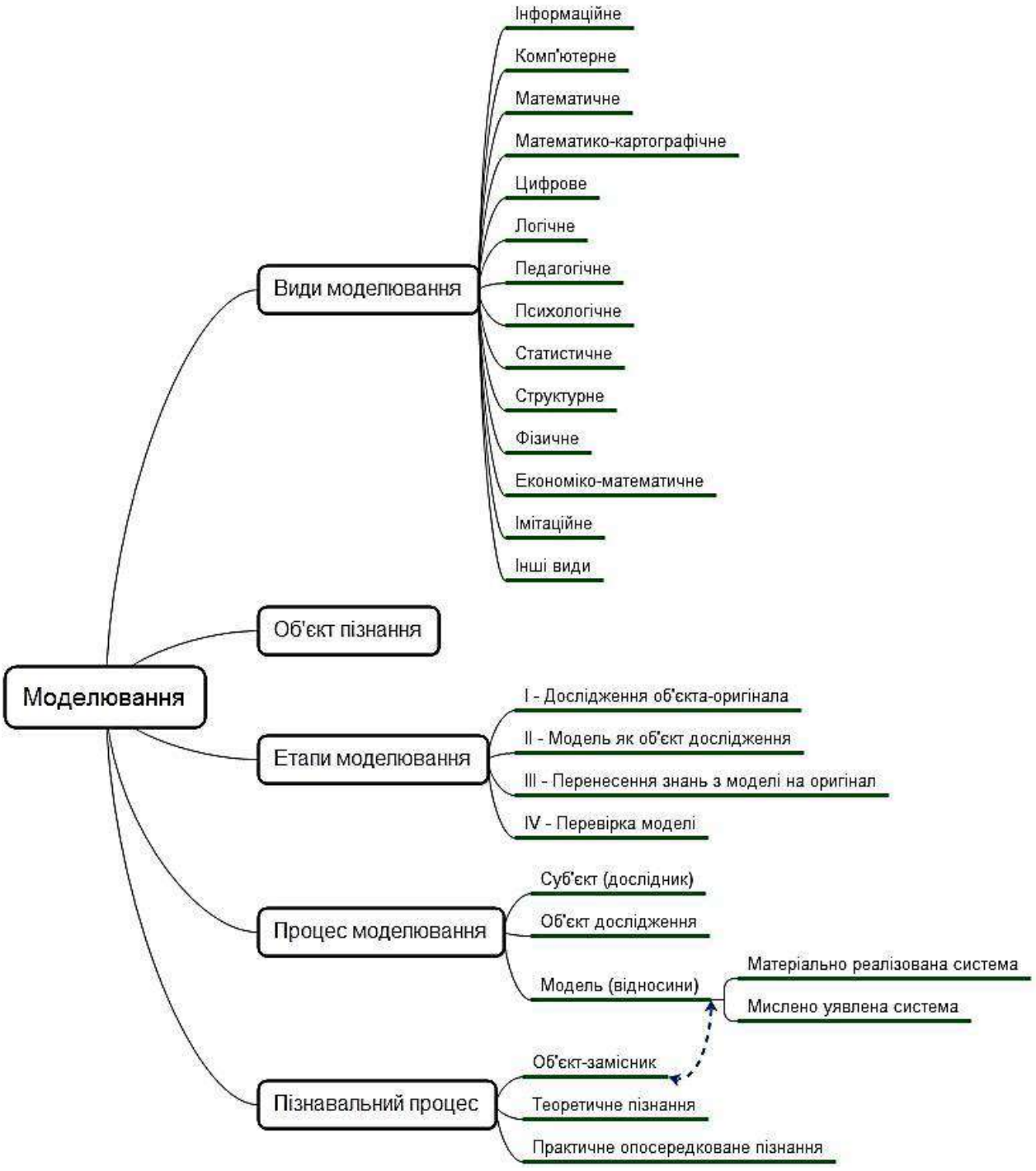


Рис. 1.2. **Характеристика поняття "моделювання"**

У рамках цього дослідження під об’єктом дослідження розглянуто процеси оподаткування на підприємствах і процеси контролю за правильністю нарахування, своєчасністю та повнотою сплати податків у податкових інспекціях.

1.2. Моделювання організації податкового обліку на підприємствах та у податкових інспекціях

Розглянуто сутність поняття "податок" і розроблено моделі податкового обліку на підприємствах і в органах державної податкової служби. Описано процес оптимізації організації податкового обліку та його автоматизації відповідно до Програми модернізації Державної податкової служби України. Проаналізовано виконання Програми модернізації на сучасному етапі.

Податковий облік може розглядатися з двох сторін. По-перше, з точки зору підприємства – платника податків. По-друге, з точки зору податкової інспекції – контролюючого органу, котрий отримує ці платежі та/або контролює їх повноту та своєчасність (рис. 1.3). Модель, яка подана на рисунку, розроблена за допомогою методології IDEF0 з використанням програмного продукту Ramus.

Вхідними ресурсами для бізнес-процесу є "облікові дані". Цей загальний опис спеціально не деталізований, щоб показати загальну характеристику всього процесу, без деталізації до конкретного виду податку. Те саме стосується і вихідних документів: "податкова звітність" і "результати контролю звітності підприємств".

В основі процесів оподаткування та податкового обліку лежить поняття "податок".

Під податком розуміють обов’язковий, безумовний платіж до відповідного бюджету, що справляється з платників податку [178] відповідно до Податкового кодексу України. У Податковому кодексі використовується ще одне поняття – збір. Під збором (платою, внеском) розуміють "обов’язковий платіж до відповідного бюджету, що справляється з платників зборів з умовою отримання ними спеціальної вигоди, у тому числі внаслідок вчинення на користь таких осіб державними органами, органами місцевого самоврядування, іншими уповноваженими органами та особами юридично значимих дій" [178].

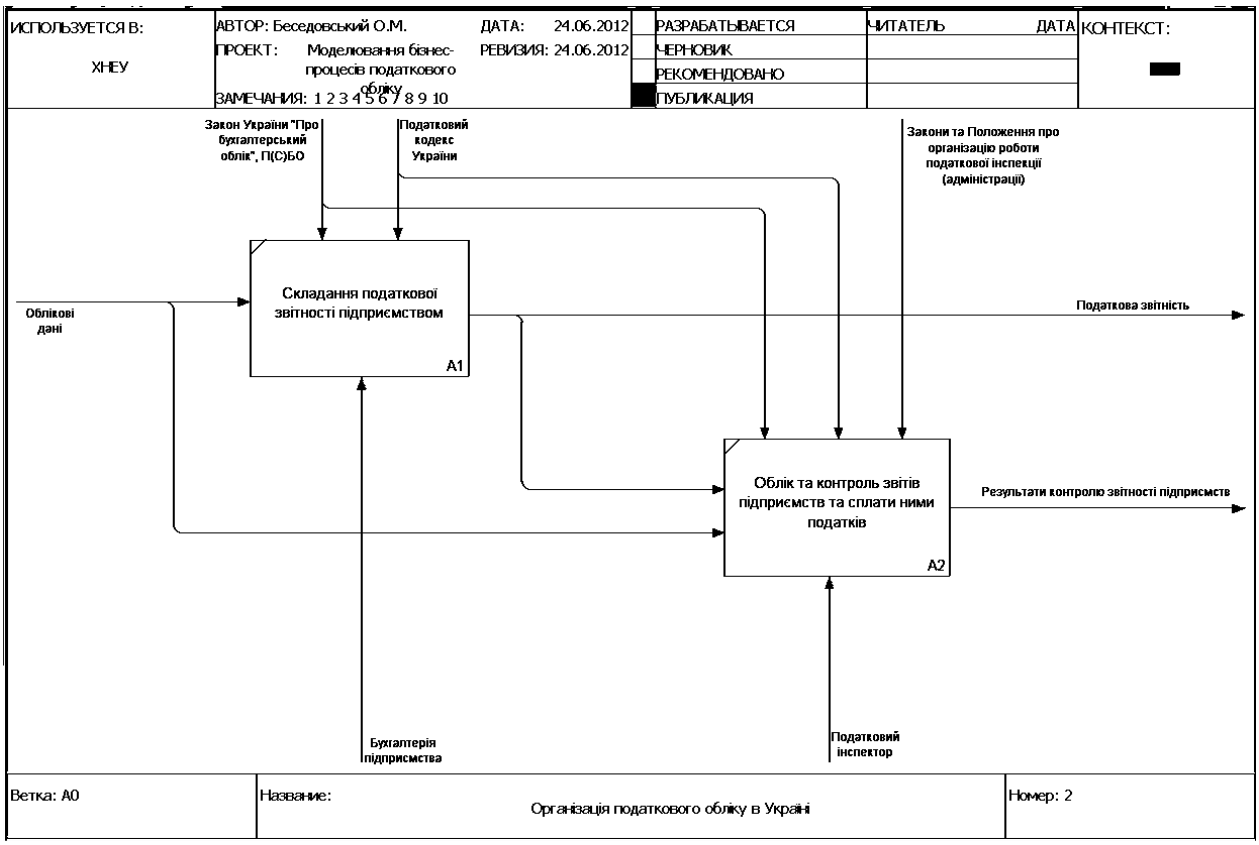


Рис. 1.3. **Взаємозв’язок підприємств і податкових інспекцій в рамках податкового обліку**

Сутність поняття "податок" наведена на рис. 1.4. Характеристика цього поняття наведена відповідно до Податкового Кодексу України.

Особливості організації податкового обліку на підприємствах України.

Підходи до побудови інформаційної системи управління підприємством, у яку входять процеси бухгалтерського й податкового обліку, можуть бути різними. На підприємстві можна створити інтегровану інформаційну систему, що споконвічно включає функції бухгалтерського й податкового обліку. Інший шлях – автоматизація процесів управління підприємством із застосуванням безлічі локальних інформаційних систем, одна або більше з яких призначені винятково для автоматизації функцій бухгалтерського й податкового обліку.

До основних особливостей процесів бухгалтерського й податкового обліку, котрі характерні для інтегрованої інформаційної системи відносять: реєстрація більшості господарських операцій і формування первинних документів провадиться в інтегрованій інформаційній системі працівни-

ками підрозділів, що не входять до складу бухгалтерії; формування автоматичних бухгалтерських проведень і записів у системі податкового обліку здійснюється одночасно з реєстрацією господарської операції.

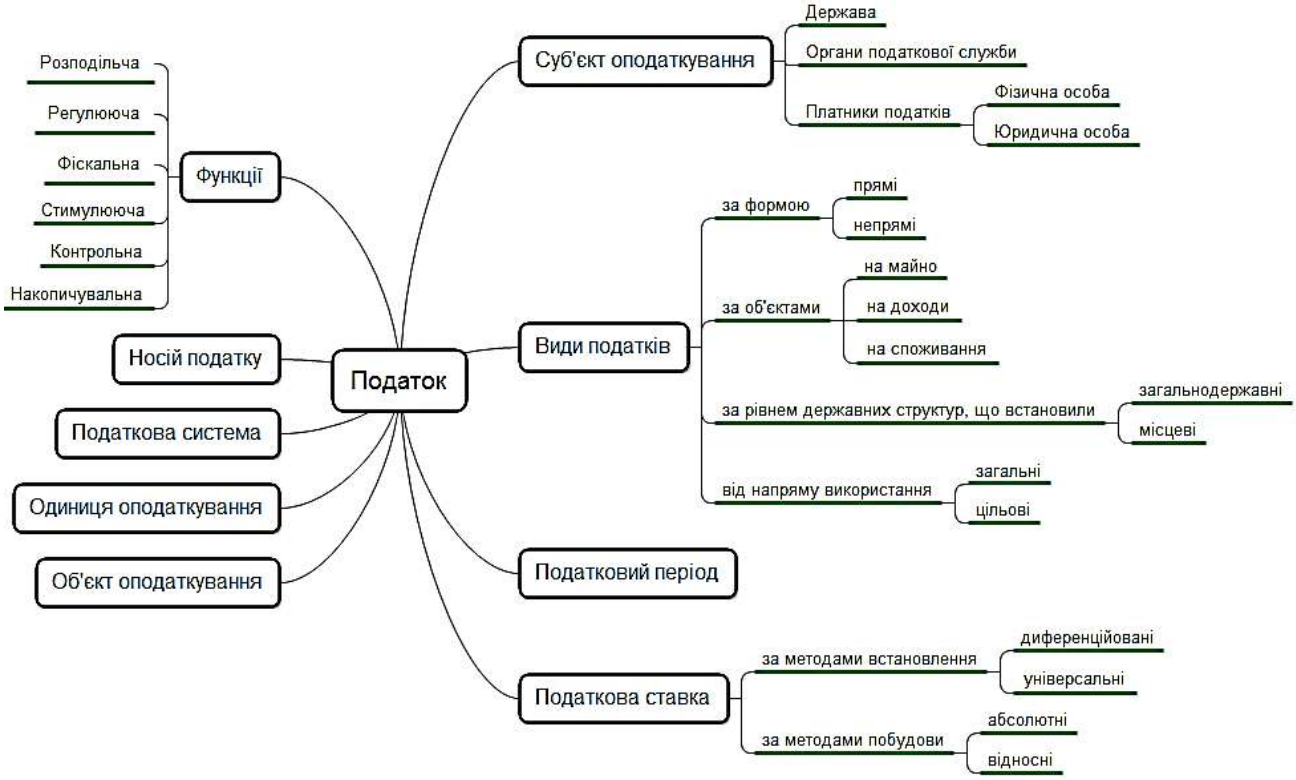


Рис. 1.4. **Сутність поняття "податок"**

При автоматизації процесів управління із застосуванням локальних інформаційних систем первинний документ і проведення в автоматизованій системі, як правило, формує бухгалтер. У випадку, коли бухгалтер не повністю виконує процес уведення в інформаційну систему первинного документа й бухгалтерського проведення, виникає ризик формування неправильного його відбиття в обліку господарської операції. У випадку формування недостовірної бухгалтерської або податкової звітності виникає проблема розподілу відповідальності між бухгалтерією й іншими структурними підрозділами підприємства. Фахівці з бухгалтерського й податкового обліку не входять у ці підрозділи, що виконують частину облікових функцій.

Головний бухгалтер відповідає за своєчасне подання повної й достовірної бухгалтерської звітності. І сучасні інтегровані інформаційні системи містять достатній інструментарій для зниження ризиків, пов’яза-

них з формуванням автоматичних бухгалтерських проведень, і оптимального рішення завдання розподілу відповідальності. Ці системи включають [31]:

1) гнучкі інструменти налаштування правил формування автоматичних проведень, які дозволяють реалізувати в інформаційній системі практично будь-які нюанси обліку;

2) інструментарій контролю правильності формування проведень, що полягає у тому, що кожне автоматично сформоване проведення може бути перевірене бухгалтером до його відбиття на рахунках бухгалтерського обліку. Це дозволяє головному бухгалтерові (керівникові бухгалтерії) успішно нести встановлену законом відповідальність.

Таким чином, процес оподаткування (або податкового обліку) на підприємствах можна представити у такому вигляді (рис. 1.5).

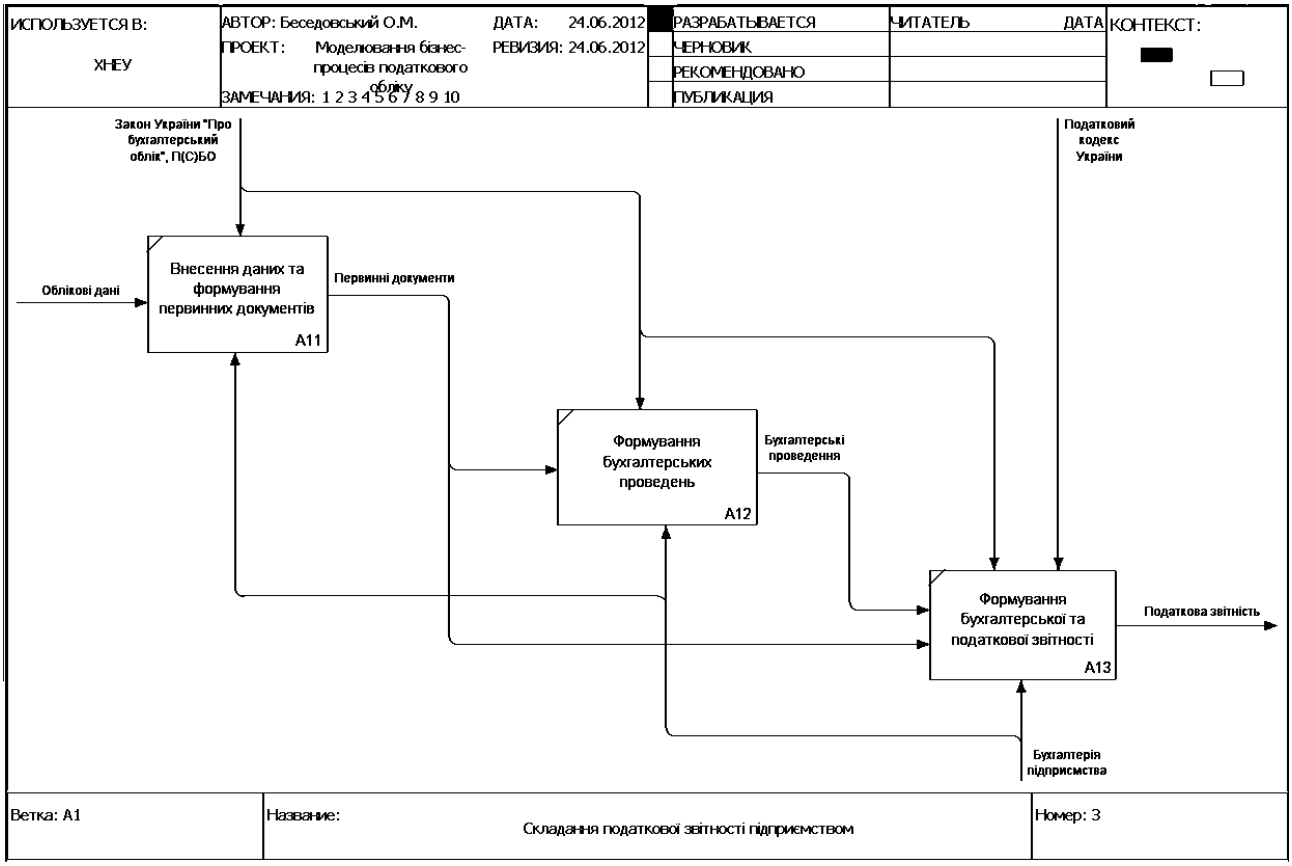


Рис. 1.5. **Процес формування податкової звітності на підприємствах**

В інтегрованих інформаційних системах існують способи зниження ризиків в області системи бухгалтерського й податкового обліку. Крім

того, інтегрована інформаційна система дає підприємству в сфері бухгалтерського й податкового обліку ряд істотних переваг. Зниження трудомісткості функцій бухгалтерії щодо реєстрації господарських операцій в інформаційній системі й формування бухгалтерської й податкової звітності – одне з них. Не менш важливий і інший аспект – можливість професійного зростання облікових працівників у результаті зміни структури їхніх функцій – переміщення центру ваги з механічних функцій на функції аналітичні й контрольні. У цілому застосування інтегрованої інформаційної системи дозволяє підприємству досягти більшого порівняно з використанням безлічі локальних інформаційних систем економічного ефекту.

Особливості організації податкового обліку в податкових інспекціях.

Усе більшого розвитку набирає тенденція автоматизації всіх аспектів діяльності державних служб України. Одним з найголовніших є автоматизація діяльності державної податкової служби (ДПС) України.

Незважаючи на процес автоматизації діяльності ДПС, процес податкового обліку на цьому рівні можна представити у такому вигляді (рис. 1.6).

З метою реалізації цього напряму в діяльності Уряду України та забезпечення реформування системи адміністрування податків Державною податковою адміністрацією України, яке спрямоване на вдосконалення взаємовідносин між Урядом, податковими службами та платниками податків, було започатковано Проект "Програма модернізації державної податкової служби України" (далі – Проект), основною метою якого є побудова податкової служби, яка б:

- була високоефективною та визнаною платниками податків;
- спиралася на визначені у податковому законодавстві правові норми відносин між платниками податків та податковою службою;
- яку б підтримувало суспільство [365].

Цей Проект повинен упроваджуватися спільно з Міжнародним банком реконструкції та розвитку. Проект почали реалізовувати з січня 2004 року.

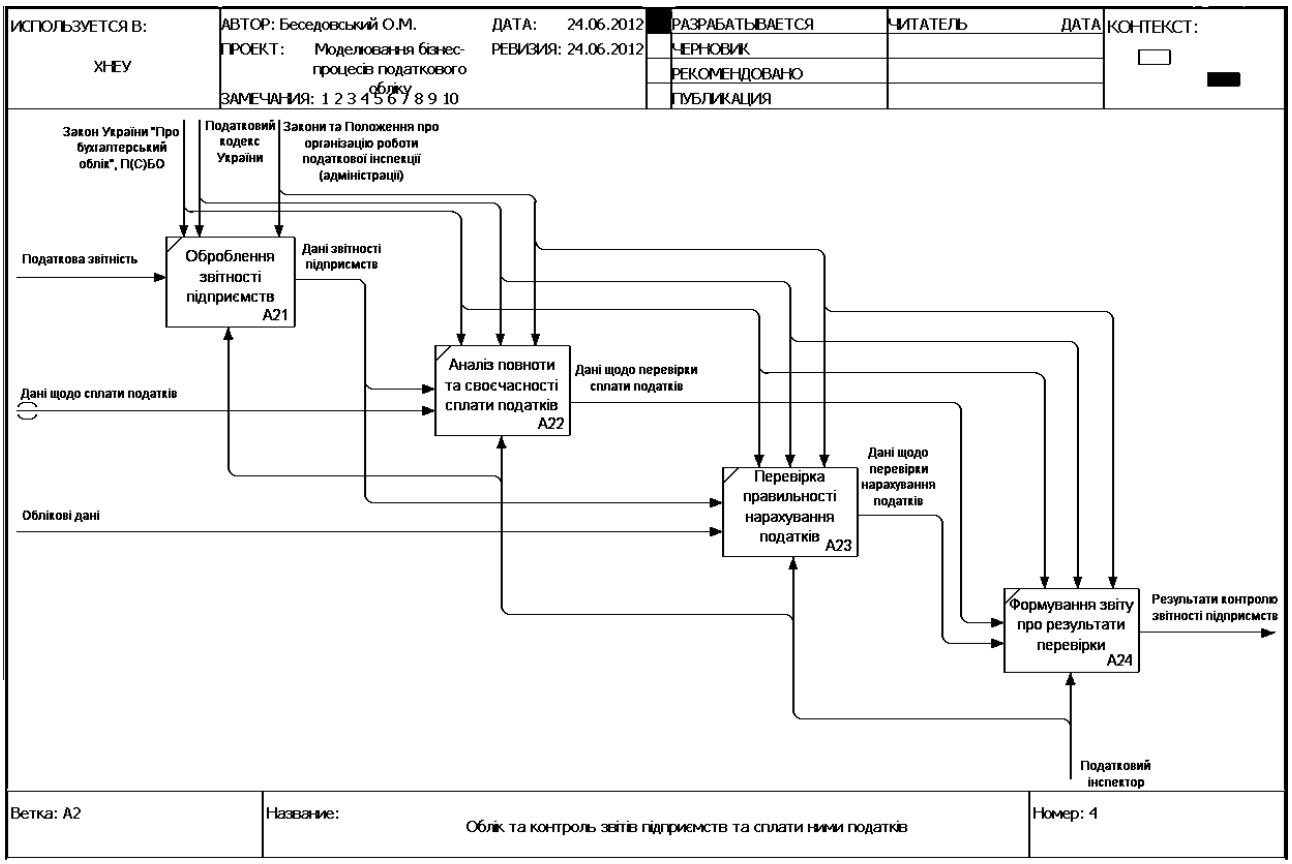


Рис. 1.6. **Податковий облік в органах державної податкової служби**

Нове бачення роботи органів податкової служби України базується на таких основних напрямах, як:

- удосконалення податкового законодавства (реалізується через прийняття Податкового Кодексу);
- удосконалення методології адміністрування податків (реалізується через введення в дію Податкового кодексу);
- удосконалення системи подання та обробки податкової звітності (подання звітності в електронному вигляді, створення інформаційної бази даних та ін.) (виконано частково, оскільки прийняття звітності в електронному вигляді відбувається, але існують певні труднощі);
- створення інтегрованої інформаційної системи органів державної податкової служби (на всіх рівнях – починаючи з загальнодержавного і завершуючи районними службами податкової інспекції);
- запровадження організаційної структури органів ДПС за функціональною ознакою.

Проект передбачено здійснити у два етапи – фаза 1 (2005 – 2009 роки), фаза 2 (2010 – 2012 роки).

Відповідно до структури Детального плану, роботи за Проектом розподілено на 7 блоків [163]:

1. Управління процесом упровадження проекту та підзвітність громадськості.

На цьому етапі проводиться оптимізація взаємодії служб ДПА з іншими урядовими та міжнародними організаціями, оптимізація їх взаємодії з метою реалізації та управління Проектом.

На основі методології оцінки роботи структурних підрозділів організацій, визначаються вимоги та критерії для оцінки роботи окремих підрозділів органів державної податкової служби. Критерії, які розроблені на даному етапі, пройшли перевірку на можливість їх використання в роботі державної податкової служби як окремої організації.

2. Удосконалення процесів адміністрування податків – короткострокові заходи.

Проводяться заходи з удосконалення адміністрування податків. На цьому етапі розробляються рекомендації щодо подальшого реформування податкового законодавства щодо нарахування та адміністрування податкових зборів.

Організація та вдосконалення процесів прийому та обробки податкової звітності в електронному вигляді. Розробляється та впроваджується програмне забезпечення для формування, прийому та обробки податкової звітності. Це відбувається як на самих підприємствах-платниках податків (шляхом передачі безкоштовних програмних модулів щодо формування електронної податкової звітності), так і в органах державної податкової служби для прийому цієї звітності.

На цьому етапі також повинна бути створена ефективна система обміну інформацією між органами податкової служби та урядовими організаціями з приводу обміну інформацією для реалізації загальних цілей; а також інформаційної системи по обміну інформацією між органами податкової служби та платниками податків для оптимізації процесів нарахування податків і представлення податкової звітності.

3. Удосконалення податкового законодавства.

На основі інформації попереднього етапу, проводиться процес удосконалення існуючого податкового законодавства з метою як оптимізації податків, так і системи по обліку та адміністрування цих податків у межах всієї країни.

4. Створення системи обслуговування платників податків.

На цьому етапі повинен бути створений Інформаційно-довідковий центр (ІДЦ) для надання "висококваліфікованих консультацій платникам податків з питань оподаткування". Робота ІДЦ має бути організована відповідно до існуючих світових стандартів з організації роботи call-центрів. Усі питання, які повинні надходити до ІДЦ, будуть роззосереджуватися відповідно до регіонів і питань, які виникають у платників податків. Це повинно підвищити якість та оперативність в наданні консультацій. Частина питань може бути записана та надаватися в записаному вигляді платникам податків, що може значно зменшити навантаження на працівників ІДЦ.

Для організації роботи ІДЦ було розроблено Концепцію щодо створення ІДЦ, яка передбачає надання таких послуг:

- надання відповідей на запитання платників податків засобами телефонного зв'язку, звичайної та електронної пошти, через веб-сайт;
- організація та проведення форумів і конференцій;
- організація та проведення "гарячих ліній";
- інформування платників податків про зміни в податковому законодавстві тощо;
- проведення опитувань серед платників податків [186].

5. Створення інтегрованої інформаційної системи.

Інтегрована інформаційна система повинна мінімізувати втручання посадовців ДПС у приймання податкової звітності та платежів, а також їх обробку, що повинно підвищити якість роботи державної податкової служби з платниками податків, насамперед через можливість звертатися з різноманітними питаннями до будь-якої служби у всіх містах України, а не тільки за місцем реєстрації, як це відбувається нині.

Зміни в процесі торкнуться також реєстрації платників податків в органах податкової служби. При реєстрації одразу будуть визначатися ті податки та податкові платежі, які будуть підлягати сплаті. Це зменшить кількість питань та звертань з приводу визначення такого переліку податків.

Повинна бути вдосконалена система податкової звітності з податків – спрощені форми податкової звітності, зменшена їх кількість, а також удосконалене роз'яснення процедури заповнення звітності, зменшена кількість неоднозначного тлумачення різноманітних рядків звітності, що, в свою чергу, повинно зменшити кількість звертань платників податків з

питаннями щодо роз'яснень цих моментів. Однак на даний час це все ще залишається прагненням, яке донині не реалізоване в дійсності.

6. Структурне та функціональне реформування органів державної податкової служби.

Передбачається реорганізація органів державної податкової служби, їх організація відповідно до функціональної ознаки.

З метою виконання робіт з оновлення попередньої та загальної організаційної структури за функціональним принципом у державній податковій інспекції [365]:

- оновлено попередню модель організаційної структури, яку в лютому 2006 року схвалено Головою ДПА України;
- розроблено загальну (концептуальну) модель організаційної структури;
- розроблено Концепцію вдосконалення організаційної структури органів ДПС.

7. Підготовка персоналу державної податкової служби України.

На цьому етапі плануються такі заходи, частина з яких вже частково реалізована:

- навчання працівників державної податкової служби щодо управління людськими ресурсами для реалізації Проекту;
- навчання працівників податкової служби для покращення роботи з інформаційними ресурсами в процесі впровадження Проекту;
- навчання працівників податкової служби для оптимізації роботи з платниками податків;
- затвердження Кодексу професійної етики працівника державної податкової служби, яким визначено правила (норми) етичної поведінки працівника органу державної податкової служби;
- частина положень Кодексу затверджена на державному рівні через включення в Податковий кодекс України.

Таким чином, реалізація програми повинна спрямувати покращення інформаційного середовища в податковому обліку України, але на даний час велика кількість положень цього Проекту так і залишається тільки на папері, хоча час упровадження положень цього Проекту вже добігає кінця.

1.3. Моделювання деяких особливостей обліку нарахування та сплати податків юридичними та фізичними особами в податкових інспекціях

Розглянуто відмінності організації податкового обліку у державній податковій службі при обліку податків юридичних осіб на прикладі податку на додану вартість та податку на прибуток підприємства. Розглянуто та проаналізовано Податковий кодекс України. Проаналізовано основні елементи кодексу. Побудовано модель процесу адміністрування податку на доходи фізичних осіб. Наведено деякі моделі процесу податкової перевірки платників податків як один з етапів адміністрування податків.

Незважаючи на загальні вимоги, що описані в Податковому Кодексі, існують деякі відмінності, що стосуються обліку нарахування та контролю сплати податків у податкових інспекціях залежно від того, хто є платником податків. Крім того, сам процес (його нерегламентована складова), залежить від того, які внутрішні (управлінські) звіти вимагає керівництво тієї чи іншої податкової інспекції.

У процесі аналізу предметної області була складена контекстна діаграма бізнес-процесу "Облік розрахунків податків і платежів до бюджету юридичними особами" (рис. 1.7), для якої були визначені такі інтерфейсні дуги:

- вхідні ресурси: дані про підприємство, дані декларації з ПДВ, дані декларації з податку на прибуток, банківська виписка;
- вихід (результат протікання бізнес-процесу): реєстр платників податків, реєстр звітів, аналітичний звіт, сумарний графік, графік за місяцями, графік за категоріями;
- управлінський вплив: інструкція з ведення обліку платежів до бюджету, інструкція з адміністрування податків, Податковий Кодекс;
- ресурси: податковий інспектор, керівник податкової інспекції.

Декомпозиція контекстної діаграми реалізована на виділенні таких робіт: формування реєстру платників, нарахування та облік податків, розрахунок та аналіз заборгованості платників до бюджету, що призводить до діаграми 1-го рівня декомпозиції (рис. 1.8).

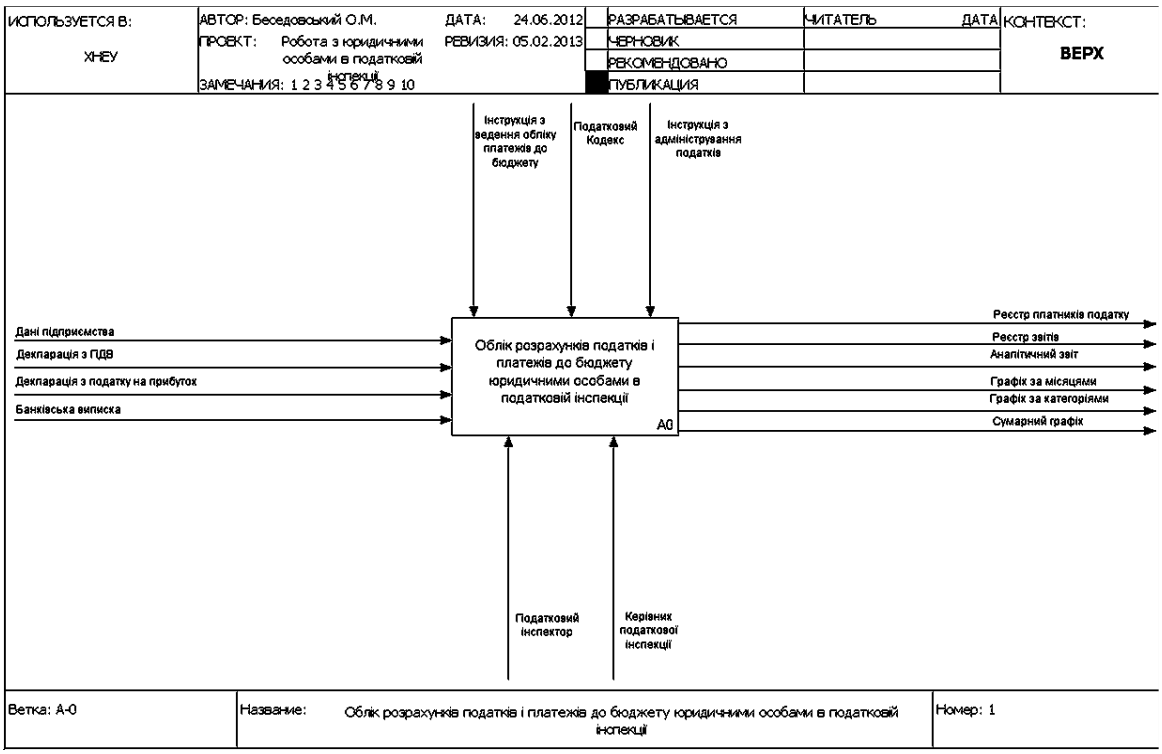


Рис. 1.7. **Контекстна діаграма моделі бізнес-процесу предметної області "Облік розрахунків податків і платежів до бюджету юридичними особами в податковій інспекції"**

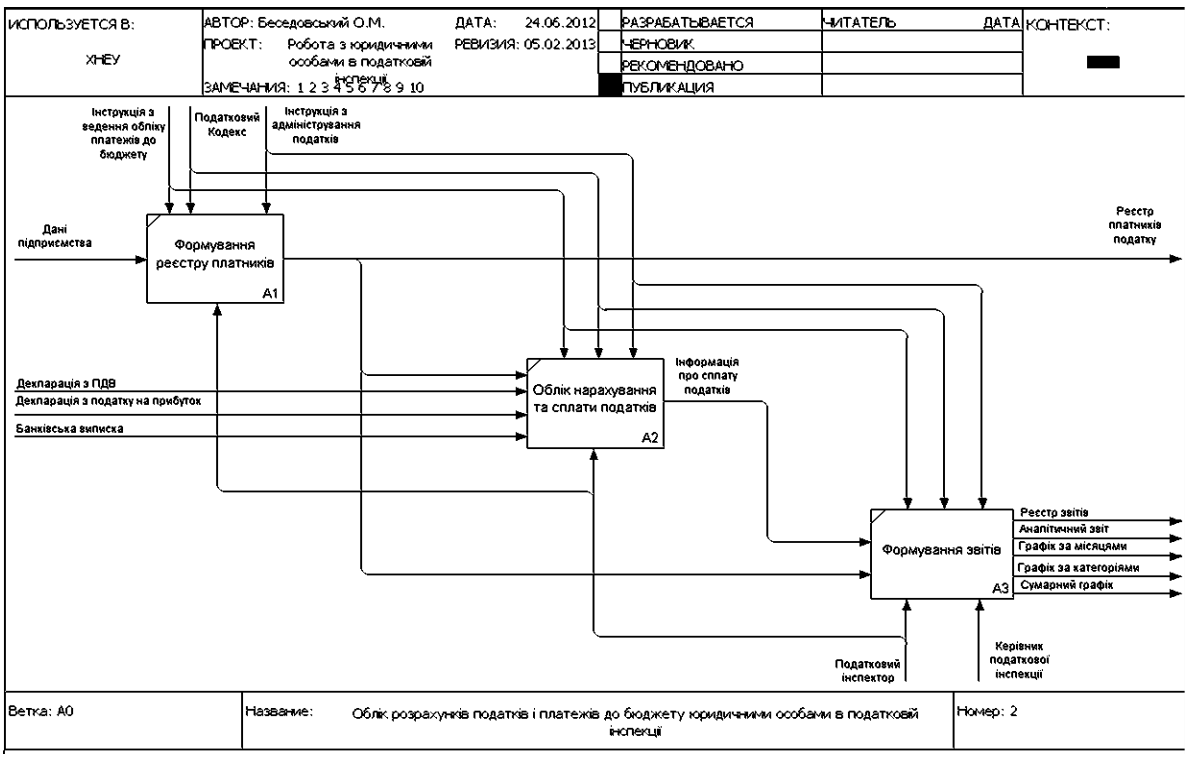


Рис. 1.8. **Декомпозиція контекстної діаграми моделі бізнес-процесів предметної області "Облік розрахунків податків і платежів до бюджету юридичними особами в податковій інспекції"**

Постійно зростаюча залежність бізнесу від інформаційних технологій передбачає підвищення вимог до роботи інформаційних систем. Сучасна інформаційна система повинна забезпечувати безперебійне надання послуг користувачам.

На сьогоднішній день основним чинником створення тривалої конкурентної переваги і зростання інвестиційної привабливості компанії стають оптимальні стратегії управління бізнесом. Ефективне управління – це саме той ресурс, який допомагає динамічно реагувати на ринкову ситуацію, яка постійно змінюється, контролювати всі сторони діяльності підприємства, оперативно виявляти "вузькі місця" і концентрувати зусилля саме там, де вони найбільш необхідні в даний момент.

З точки зору розвитку бізнесу "Облік розрахунків податків і платежів до бюджету юридичними особами в податковій інспекції" є важливою ланкою автоматизації процесів ведення і обліку даних розрахунків підприємств з податків і платежів, побудова звітів і пошуку даних.

Вимоги з точки зору розвитку бізнесу, які можна виокремити за таким бізнес-процесом:

- автоматизація процесів реєстрації підприємців;
- автоматизація процесів формування звітів;
- використання єдиної бази даних.

Вимоги користувача системи:

- можливість працювати з даними про юридичних осіб;
- розмежування прав доступу для категорій користувачів;
- можливість додавати та видаляти нових користувачів;
- формування податкової звітності;
- перегляд аналітичних даних;
- простота використання;
- швидка обробка запитів;
- достовірність інформації.

Діаграма бізнес-варіантів за завданням представлена на рис. 1.9.

Таким чином, можна сказати, що незважаючи на деякі загальні моменти, процес обліку платників, контроль нарахування податків, повноти та своєчасності їх сплати є доволі специфічним процесом, який може відрізнятися залежно від податкової інспекції. Але ці відмінності стосуються лише тих аспектів, які торкаються широти тих аналітичних звітів, які можуть формуватися, але ні якою мірою не повинні стосуватися робо-

ти з платниками податків, взаємодія з котрими регламентується Податковим кодексом та іншими нормативними документами.

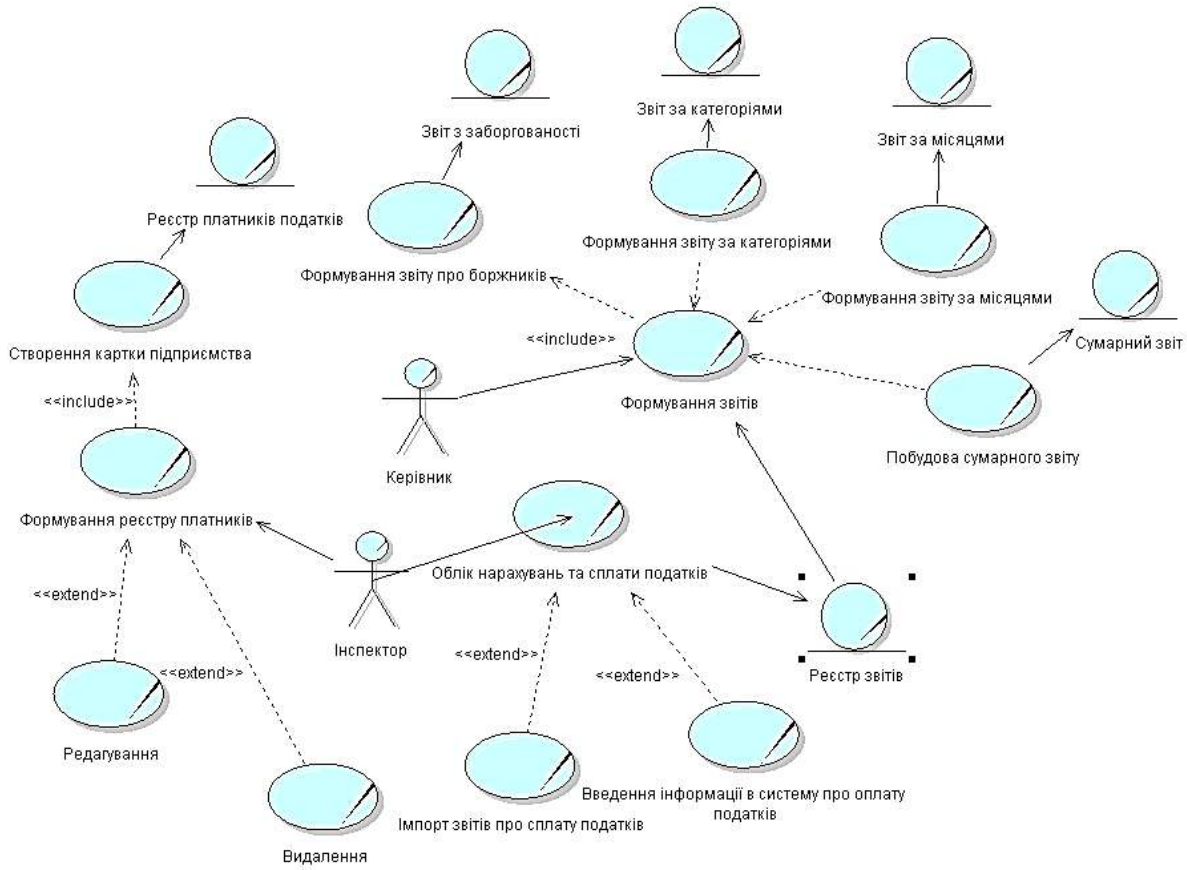


Рис. 1.9. **Діаграма бізнес-варіантів використання бізнес-процесу "Облік розрахунків податків і платежів до бюджету юридичними особами в податковій інспекції"**

Як вже зазначалося, всі відносини в Україні, що стосуються податкового обліку, регламентуються Податковим кодексом України [183]. Відповідно до цього кодексу визначаються:

- принципи, які лежать в основі функціонування Податкового кодексу (стабільність, рівність усіх платників перед законом, презумпція правомірності рішень платників податків тощо);
- сфера дії кодексу (платники податків, контролюючі органи, відповідальність, адміністрування тощо);
- елементи Податкового кодексу (об’єкт оподаткування, база оподаткування, ставка податку, платник податку та ін.);
- податкові пільги (вид, підстави, строк, розмір, шляхи надання тощо);
- перелік законодавчих актів, які регулюють відносини у сфері оподаткування наряду з Податковим кодексом України.

Характеристика всіх перелічених аспектів Податкового кодексу наведена на рис. 1.10.

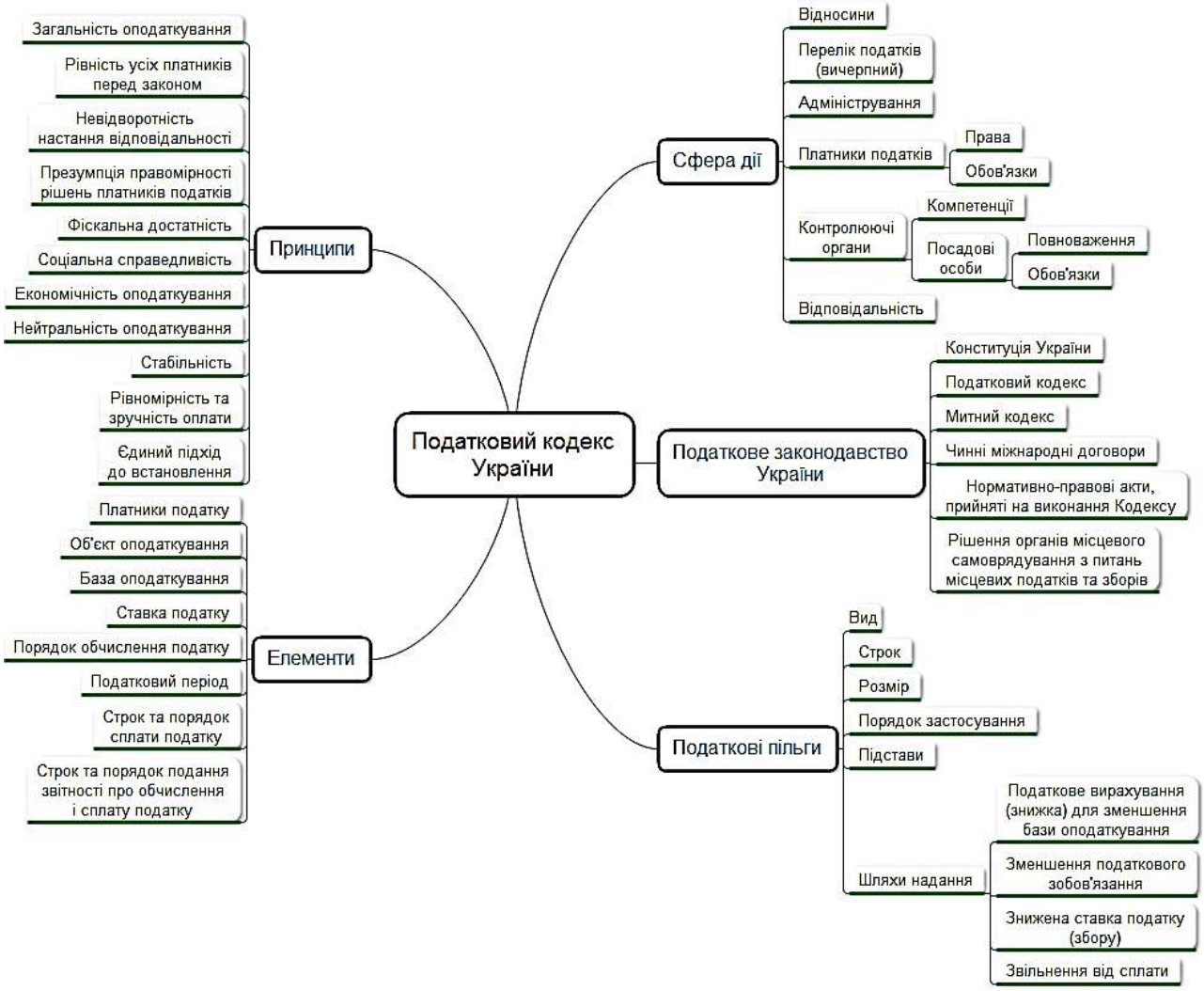


Рис. 1.10. **Сутність Податкового кодексу України (загальні положення)**

Більш детальної характеристики вимагають такі елементи Податкового кодексу, як суб’єкти оподаткування та податки.

Виокремлюють три групи суб’єктів оподаткування: держава, органи податкової служби та платники податків. Державу в рамках реалізації функцій контролю за податками представляють органи державної податкової служби, тому в подальшому суб’єкт "держава" розглядатися не буде. Платники податків можуть бути трьох видів: фізичні особи, юридичні особи і відокремлені підрозділи юридичних осіб. У свою чергу, як платники податків, так і органи державної податкової служби мають як права, так і обов’язки, які регламентуються зазначеним Податковим кодексом.

Відповідно до Податкового кодексу існує велика кількість податків та зборів, які поділяються на загальнодержавні та місцеві. Весь перелік податків та зборів, які існують в Україні, наведені на рис. 1. 11.

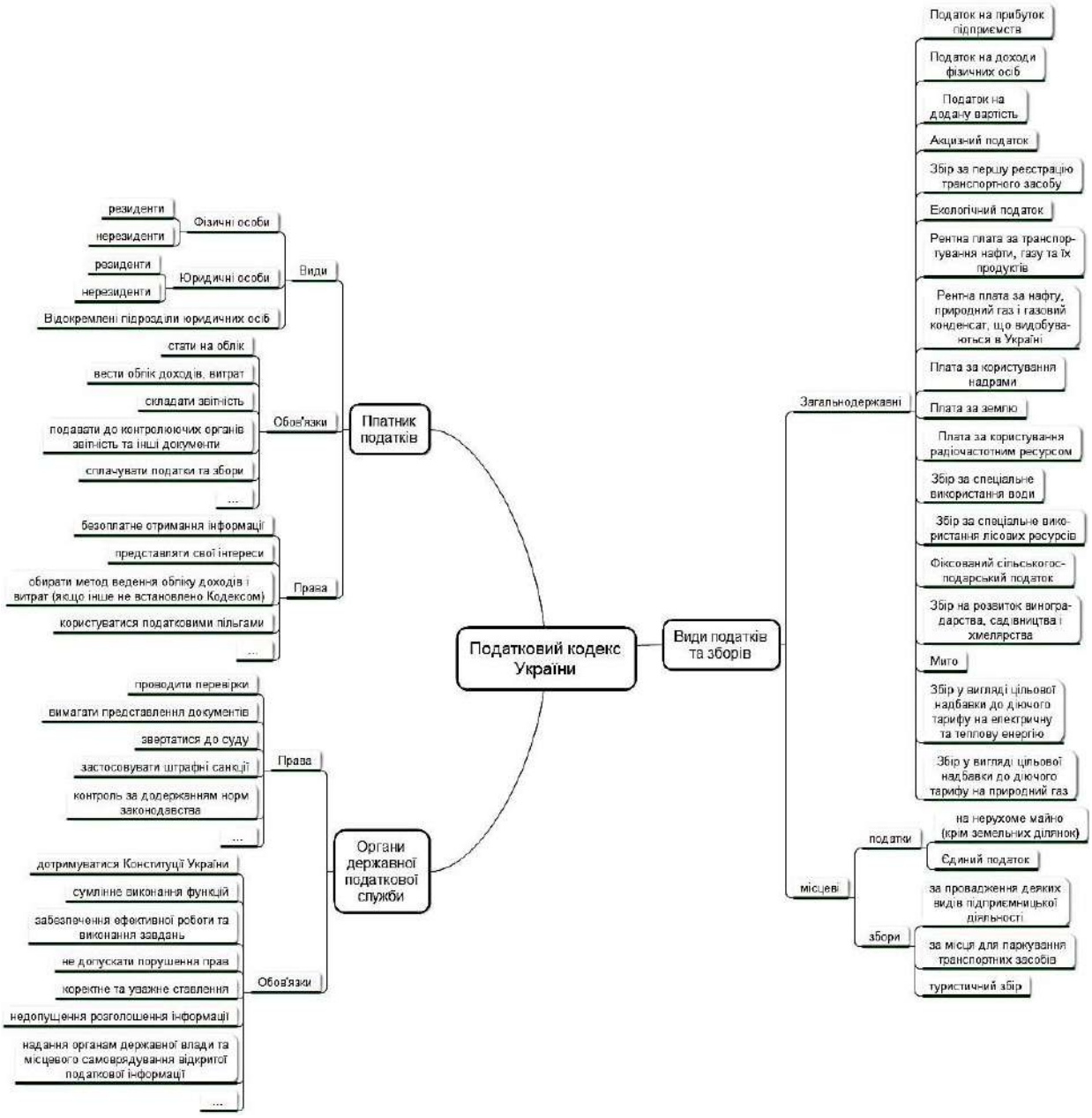


Рис. 1.11. **Сутність Податкового кодексу України (суб'єкти оподаткування та види податків)**

Наступні елементи, які вимагають більш детального аналізу, – це: податковий період (виділяють базовий податковий період та звітний період, які можуть відрізнятися відповідно до різновиду податку), строк сплату податку до бюджетів (як нормативний, так і можливість зміни строку сплати відповідно до певних обставин), податковий обов'язок, який вини-

кає при нарахуванні податку (обов'язки платника податку, які при цьому виникають, відповідальність за несвоєчасність або неповноту сплати і можливі варіанти припинення наявності податкових зобов'язань), а також організація перевірок відповідно до Податкового кодексу України (їх різновиди та принципи проведення). Більш детальне зображення цих елементів наведено на рис. 1.12.

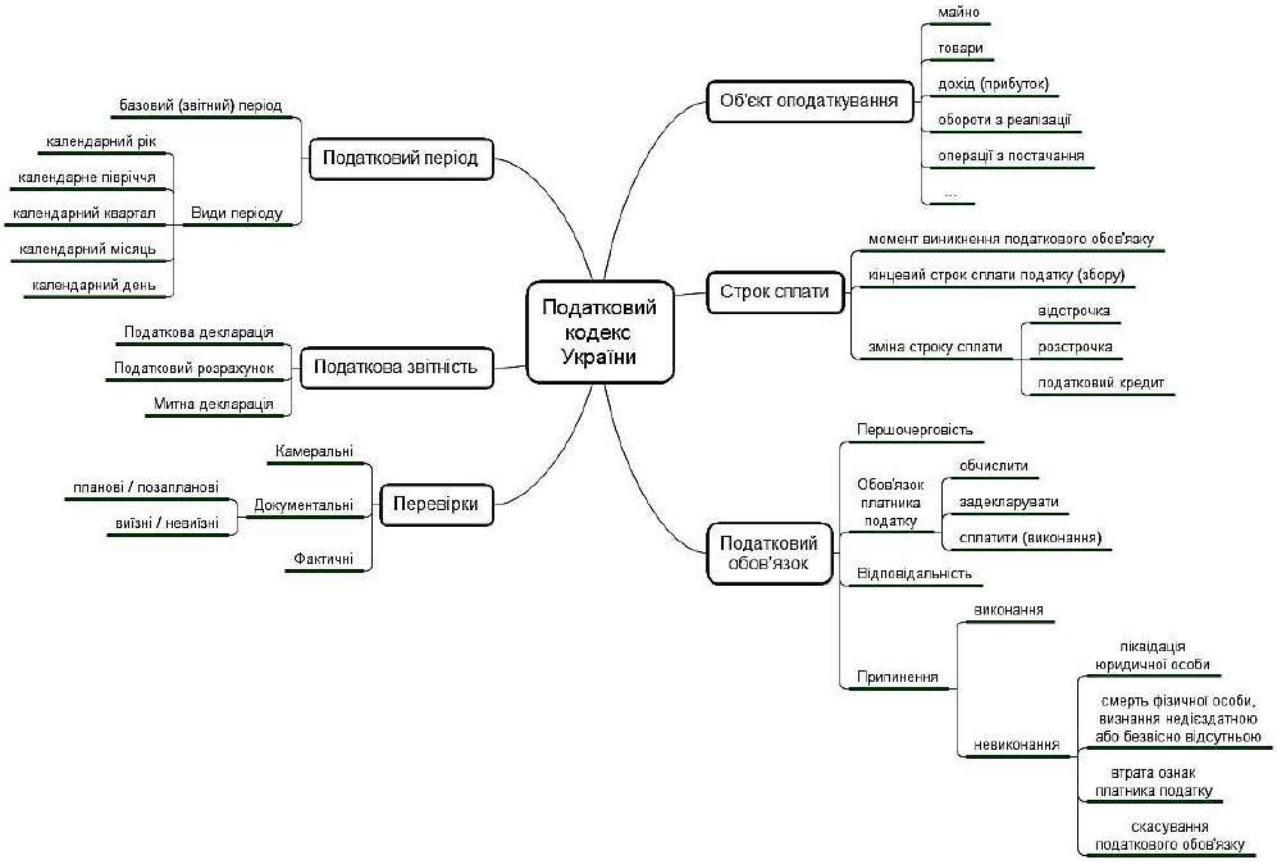


Рис. 1.12. **Сутність Податкового кодексу України (сплата податків, звітність, перевірки та ін.)**

Одним з найбільш цікавих податків з точку зору фізичних осіб є податок на доходи фізичних осіб, модель якого і буде розглянуто в даній роботі. Розглянемо процес адміністрування податку на доходи фізичних осіб від моменту реєстрації платника податку до сплати ним податкового зобов'язання.

Особливу увагу буде приділено процесу податкової перевірки, яка є стандартною процедурою, не зважаючи на той податок, розрахунки за

яким перевіряються. Крім того, такі перевірки (документальні, фактичні), найчастіше проходять як комплексні – за всіма податками та зборами.

Діаграми, на яких наведено процес адміністрування податку з доходу та перевірки правильності нарахування, повноти та своєчасності сплати наведено на рис. 1.13 – 1.17. Контекстна діаграма бізнес-процесу "Адміністрування податку на доходи фізичних осіб" наведена на рис. 1.13.

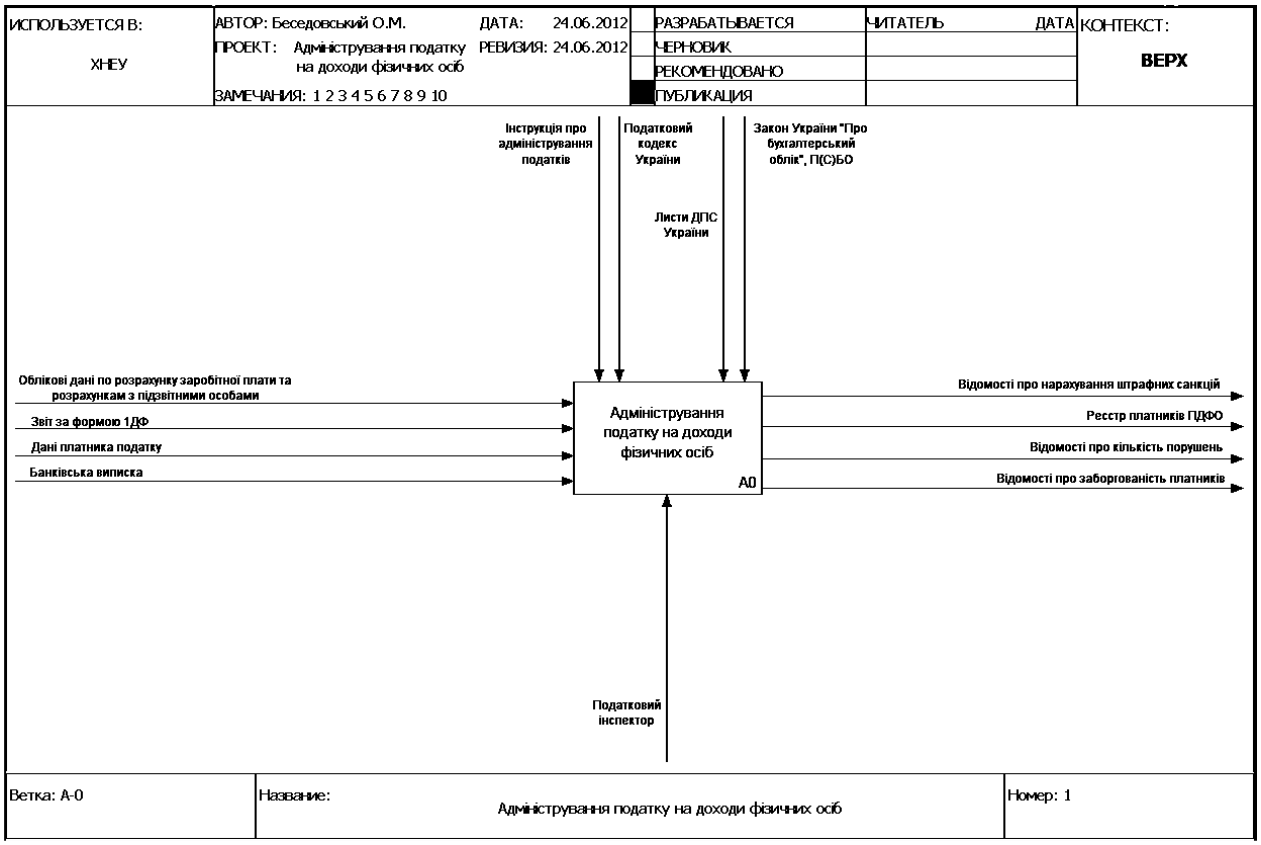


Рис. 1.13. **Бізнес-процес "Адміністрування податку на доходи фізичних осіб"**

Цей бізнес-процес можна розбити на такі завдання: реєстрації платників податків, визначення податкового зобов’язання за податком, облік сплати податкових зобов’язань, проведення податкових перевірок та нарахування штрафних санкцій (рис. 1.14). Сам процес обліку за податком розписаний тут доволі детально, тому подальшу увагу приділимо розгляду роботи "Проведення податкових перевірок".

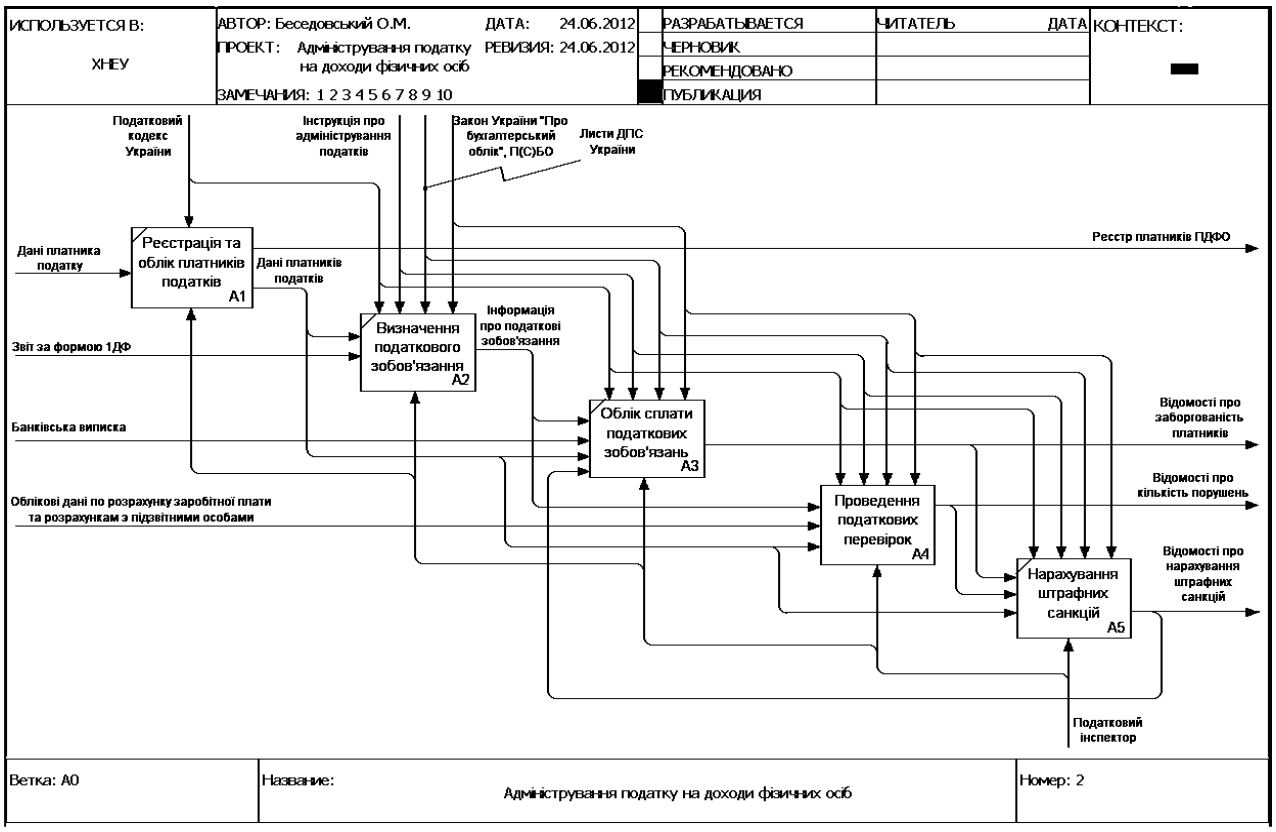


Рис. 1.14. **Декомпозиція діаграми "Адміністрування податку на доходи фізичних осіб"**

Декомпозиція роботи "Проведення податкових перевірок" наведена на рис. 1.15.

Усі податкові перевірки можна поділити на камеральні, документальні та фактичні.

Камеральні перевірки базуються на перевірці тієї документації (податкової звітності), яка подається до державної податкової служби. При цьому виїзд на місце розташування платника податку не відбувається. При цій перевірці працівники податкової служби, фактично, перевіряють правильність заповнення декларацій (звітів) та правильність розрахунку податку, який підлягає сплаті. Хід проведення камеральної перевірки за податком наведено на рис. 1.16.

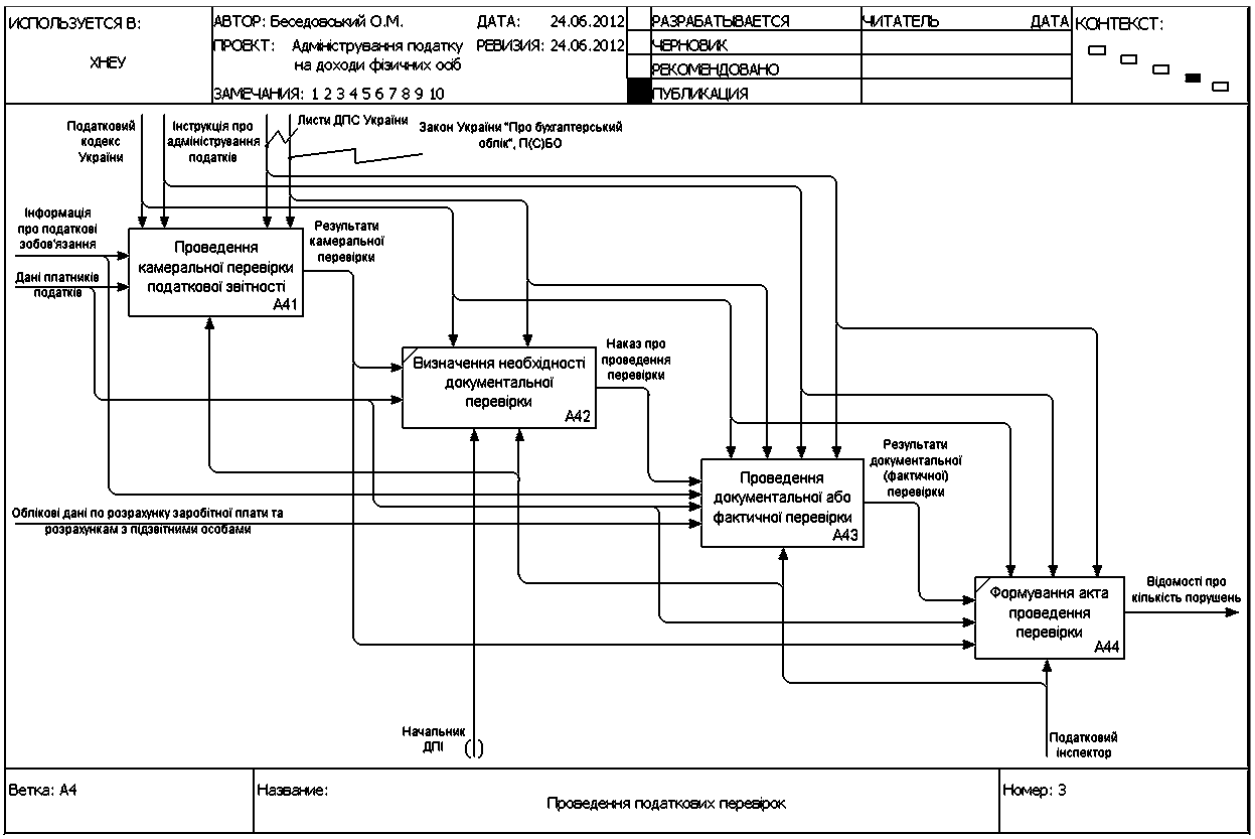


Рис. 1.15. **Діаграма "Проведення податкових перевірок"**

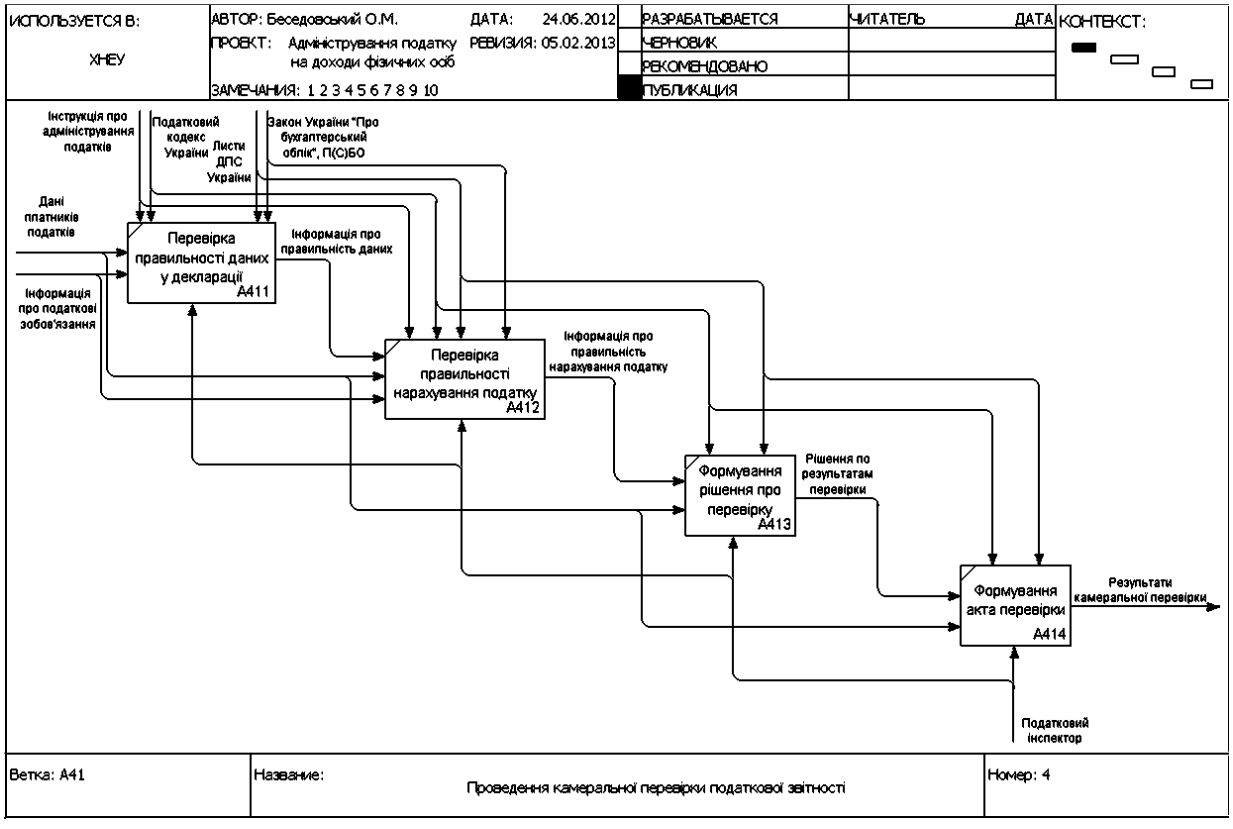


Рис. 1.16. **Діаграма "Проведення камеральної перевірки податкової звітності"**

Аналізуючи перевірки, що здійснюються державними органами у сфері підприємницької діяльності, можна виділити такі стадії [233; 379]:

- вирішення організаційних питань (визначення підконтрольного суб'єкта, оформлення наказів, повідомлення платника податку, ознайомлення платника податку з наказами);
- здійснення перевірки (перевірка первинних облікових документів, отримання пояснень за результатами перевірки);
- здійснення додаткових заходів для проведення перевірки (інвентаризація, експертизи);
- оформлення документів про результати перевірки [162].

Хід проведення документальної або фактичної перевірки наведено на рис. 1.17.

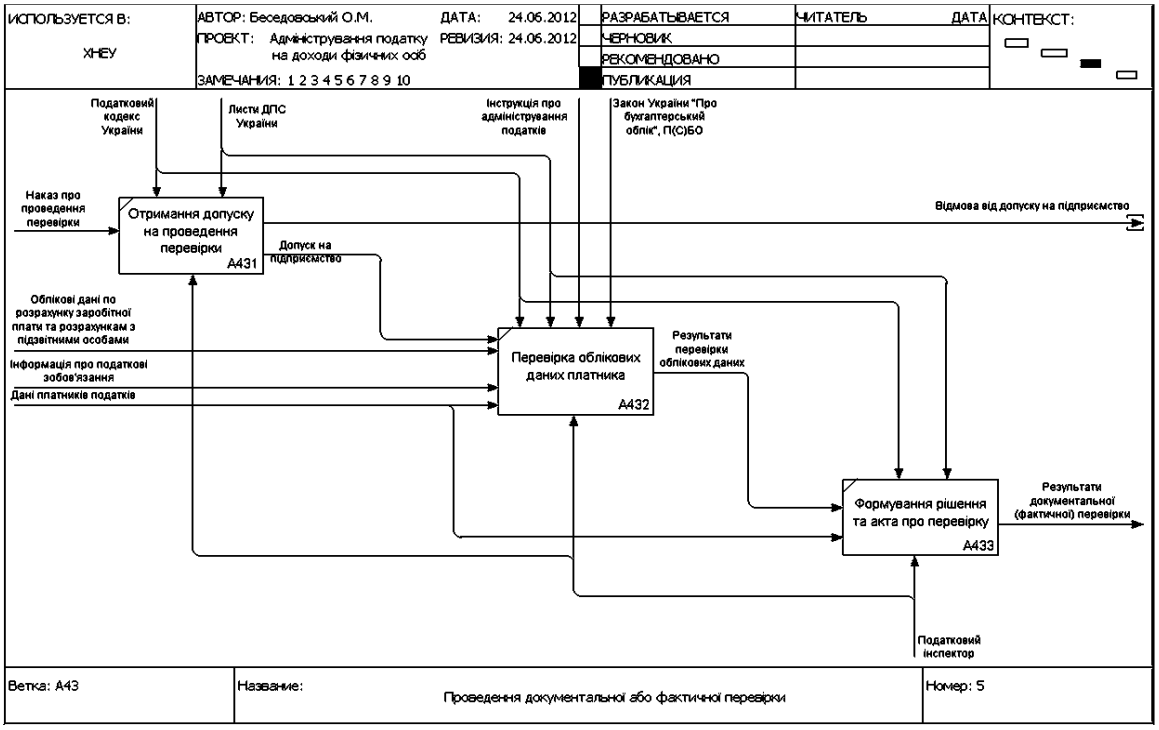


Рис. 1.17. **Діаграма "Проведення документальної або фактичної перевірки"**

Таким чином, у цьому розділі було проаналізовано такі основні поняття предметної області, як модель, моделювання, податок; побудовані інтелектуальні карти перелічених понять; виділено та обґрунтовано необхідність аналізу та моделювання бізнес-процесів оподаткування; розглянуто бізнес-процеси оподаткування на підприємствах та в органах державної податкової служби; на основі проведеного аналізу було побудовано моделі бізнес-процесів як в цілому, так і за окремими складовими роботи органів державної податкової служби – адміністрування податку з доходів фізичних осіб, а також податкових перевірок.

Розділ 2. Методи комплексного забезпечення безпеки і завадостійкості передачі даних

2.1. Інтегровані механізми захисту інформації в комп'ютерних мережах і системах

Розглянуто питання забезпечення безпеки обробки та передачі даних у комп'ютерних мережах і системах (КМіС) на основі криптографічних систем, а також забезпечення відповідної достовірності передачі даних за допомогою методів завадостійкого кодування. Проаналізовано можливість використання інтегрованих механізмів забезпечення безпеки і достовірності передачі даних у КМіС, які засновані на використанні теоретико-кодових схем (ТКС) на основі методів завадостійкого кодування в режимі маскування від порушника швидкого правила декодування.

Проблема захисту комп'ютерних мереж і систем від несанкціонованого доступу в сучасних умовах набула особливої гостроти. Стрімкий розвиток комунікаційних технологій дозволяє будувати мережі розподіленої архітектури, що поєднують велику кількість сегментів, розташованих на значній відстані один від одного. Усе це викликає збільшення числа вузлів мереж і кількості різних ліній зв'язку між ними, що, у свою чергу, підвищує ризик несанкціонованого підключення до мережі й доступу до важливої інформації [63; 260].

Збільшення обсягів оброблюваних і переданих даних у комп'ютерних системах і мережах, насамперед у банківських системах, у системах керування великими фінансовими й промисловими організаціями, підприємствами енергетичного сектору, транспорту, у системах керування й зв'язку спеціального призначення вимагає нових підходів в організації протоколів і механізмів забезпечення безпеки переданих даних [112; 113]. Вимоги до безпеки й завадостійкості обробки інформації в таких системах зростають з кожним десятиліттям, оскільки відмова системи або вихід за встановлені обмеження зазначених параметрів може призвести до значних фінансових і матеріальних втрат, зниження обороноздатності країни, збитку екології, життя й здоров'я людини.

Проведений аналіз показує [85; 176; 185; 198; 207; 209], що за останній час загальний обсяг інформації, яка оброблюється і пере-

дається в КМіС зріс багаторазово (на два-три порядки кожні п’ять – десять років у відповідно до закону Мура) і загальні тенденції свідчать, що така динаміка зберігається. Сучасні криптографічні засоби захисту інформації в таких умовах повинні забезпечувати своєчасну обробку величезних обсягів даних (десятки – сотні Мбіт/с) і задовольняти жорсткі вимоги з безпеки інформації.

Механізми забезпечення безпеки інформації в КМіС у більшості засновані на криптографічних методах, загальна класифікація яких наведена на рис. 2.1. Це методи симетричної й несиметричної криптографії, розвитку яких присвячені численні роботи [158].

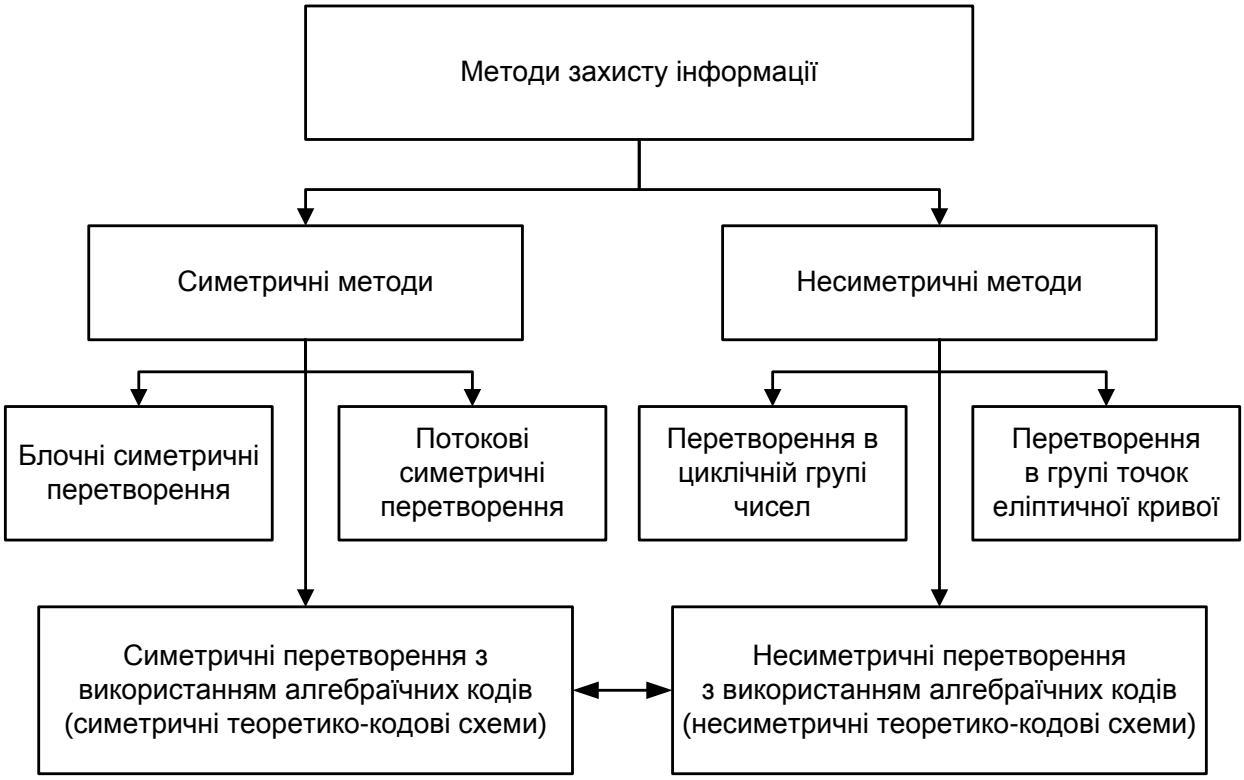


Рис. 2.1. **Загальна класифікація криптографічних методів захисту інформації**

Перспективним напрямом у розвитку криптографічних засобів захисту інформації доказової стійкості є крипто-кодові механізми, побудова яких заснована на відомості завдання зламу ключових даних до розв’язку теоретико-чисельного завдання декодування випадкового коду [96]. У роботах Сидельнікова В. М. вони одержали назву теоретико-кодових схем (ТКС) [217 – 219].

Як показує проведений аналіз їх застосування дозволяє реалізувати швидке криптографічне перетворення із забезпеченням доказової стійкості (див. табл. 2.1). Складність їх реалізації порівняна із симетричними криптоалгоритмами (блоково-симетричними шифрами (БСШ)). Крім того, їх практичне використання дозволяє застосувати інфраструктуру відкритих ключів і будувати інтегровані механізми криптографічного перетворення даних і канального кодування для комплексного забезпечення безпеки й завадостійкості передачі даних.

У табл. 2.1 наведені результати порівняльних досліджень ефективності криптографічних методів захисту інформації при фіксованому рівні стійкості:

- середньому, який полягає у складності криптоаналізу найкращим відомим алгоритмом не менш 2^{128} операцій;
- високому, що полягає у складності криптоаналізу найкращим відомим алгоритмом не менш 2^{256} операцій;
- надвисокому, що полягає у складності криптоаналізу найкращим відомим алгоритмом не менш 2^{512} операцій.

Таблиця 2.1

Результати порівняльних досліджень ефективності криптографічних методів захисту інформації при фіксованому рівні стійкості

Методи криптографічного перетворення	Модель безпеки	Довжина ключових даних, біт	Швидкість крипт. перетворень, біт/с	Додаткові функції
Блокові симетричні шифри	Практична безпека	128, 256, 512	$10^6 – 10^9$	Немає
Потокові симетричні шифри	Практична безпека	128, 256, 512	$10^7 – 10^{10}$	Немає
Несиметричні Rsa-подібні криптоалгоритми	Доказова безпека	3248 (128), 15424 (256)	$10^2 – 10^3$	Немає
Несиметричні криптоалгоритми на еліптичних кривих	Доказова безпека	283 (128), 571 (256)	$10^3 – 10^4$	Немає
Несиметричні криптоалгоритми з використанням кодових конструкцій	Доказова безпека	$0{,}5 \cdot 10^6$ (128), $2 \cdot 10^6$ (256)	$10^6 – 10^8$	Контроль помилок, підвищення завадостійкості

До додаткових функцій криптоалгоритмів (див. останній стовпчик таблиці) слід віднести можливість виявлення й/або виправлення виникаючих при передачі даних каналами зв'язку помилок. Ця функція дозволяє реалізувати комплексне забезпечення безпеки й завадостійкості передачі даних у КМіС. Як випливає з наведених у табл. 2.1 даних, подібну можливість можуть надавати тільки криптоалгоритми, засновані на використанні кодових конструкцій (крипто-кодові засоби захисту інформації). Вони будуються шляхом маскування (приховання в таємниці) від зловмисника швидкого правила декодування (поліноміальної складності) кодових слів, у результаті чого неавторизована особа без знання секретного ключа змушена використовувати складні алгоритми переборного пошуку (у загальному випадку експонентної складності) для декодування отриманої послідовності.

Таким чином, несиметричні криптоалгоритми з використанням кодових конструкцій дозволяють реалізувати криптографічний захист інформації за технологією відкритих ключів. Швидкість крипто-кодового перетворення інформації порівняна зі швидкістю шифрування (розшифрування) блоковими симетричними шифрами. Крім того, в роботах [91; 228; 229] показано, що практичне використання крипто-кодових засобів захисту інформації дозволяє на основі інтеграції механізмів канального кодування й шифрування комплексно забезпечити безпеку й завадостійкість даних, які обробляються та передаються. Отже, застосування теоретико-кодових схем з одного боку економічно вигідніше застосування цілого комплексу різних механізмів шифрування й канального кодування, що вирішують окремо взяті завдання, а з іншого – спостерігається істотне зниження сумарних обчислювальних витрат, що доводяться на одиницю інформації, яка оброблюється й передається, тобто за рахунок зниження часу обробки підвищується оперативність передачі даних.

Загальна класифікація відомих методів побудови теоретико-кодових схем наведена на рис. 2.2.

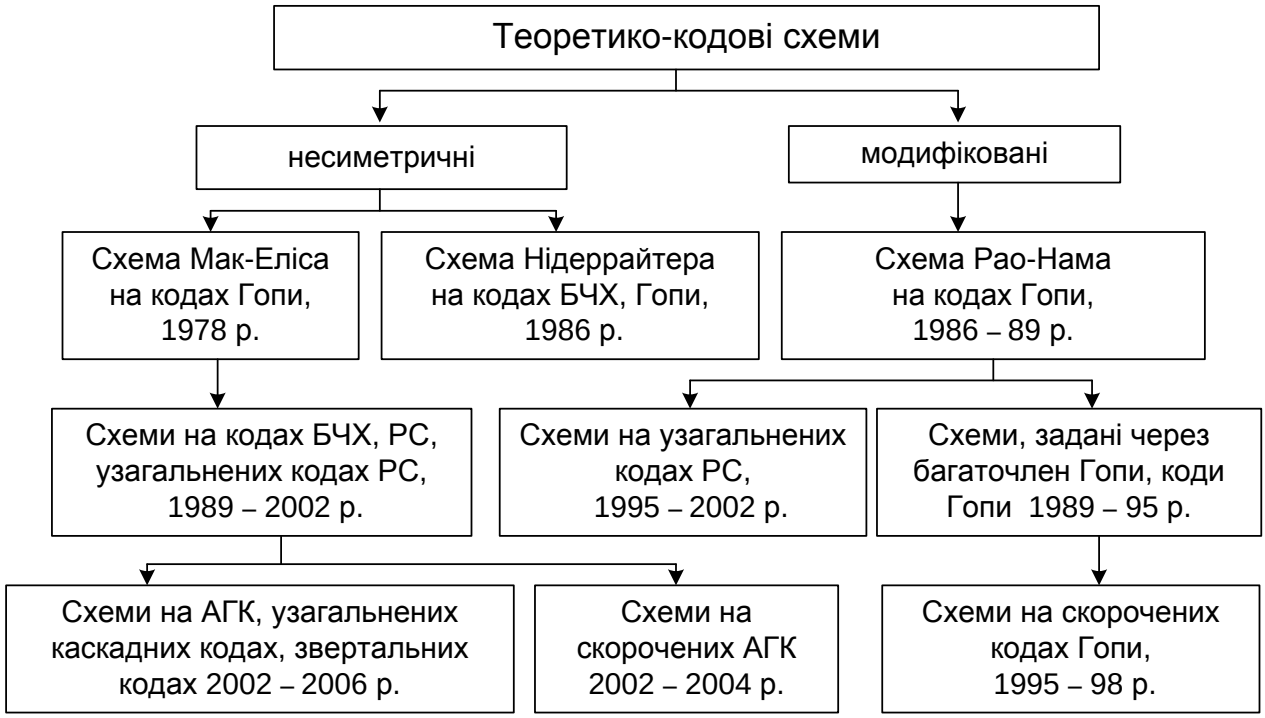


Рис. 2.2. **Загальна класифікація теоретико-кодових схем**

Проведений аналіз і порівняльні дослідження показали, що відомі несиметричні крипто-кодові засоби захисту інформації будуються за двома схемами: з маскуванням породжувальної матриці коду (схема Мак-Еліса) і з маскуванням перевірочної матриці коду (схема Нідеррайтера) [312]. Симетрична схема Рао-Нама за суттю є деяким спрощенням несиметричної конструкції Мак-Еліса. У якості вихідних об’єктів можуть виступати алгебраїчні блокові коди зі швидким (поліноміальної складності) алгоритмом декодування, такі, наприклад, як коди Гопи, Ріда-Соломона (РС), Боуза-Чоудхурі-Хоквігнема (БЧХ) [213; 214].

Найбільш ефективними зі стійкості до алгоритмів криптоаналізу є крипто-кодові засоби захисту інформації з недвійковими лінійними блоковими кодами, що виникають на алгебраїчних кривих – алгебро-геометричними кодами (АГК) [23; 25]. З одного боку, подібні конструкції стійкі до атак, запропонованих Сидельніковим В. М. [217 – 219], з іншого боку, вони забезпечують високі показники завадостійкості й оперативності передачі даних [91; 224; 228 – 230]. У той же час практичне використання крипто-кодових засобів захисту інформації з недвійковими алгебраїчними блоковими кодами припускає застосування методів і обчислювальних алгоритмів недвійкового рівноважного кодування (як за схемою Мак-Еліса, так і за схемою Нідеррайтера). Важливе

прикладне значення в галузі побудови обчислювально-ефективних криптографічних засобів захисту інформації має розробка методів і алгоритмів інтегрованих крипто-кодових засобів на їх основі для комплексного забезпечення безпеки й завадостійкості передачі даних у КМіС. Їх застосування дозволить:

- реалізувати швидкі криптографічні перетворення більших обсягів даних з використанням відкритих ключів у КМіС;
- забезпечити високий рівень стійкості до сучасних методів криптоаналізу за рахунок відомості завдання безключевого читання до розв'язання теоретико-чисельного завдання декодування випадкового коду, забезпечити доказову стійкість криптографічних засобів захисту інформації;
- будувати на канальному рівні моделі OSI інтегровані механізми криптографічного захисту інформації й завадостійкості даних у комп'ютерних системах і мережах.

2.2. Способи модифікації теоретико-кодових схем на алгебраїчних блокових кодах

Розглянуто основні моделі та основні параметри оцінки теоретико-кодових схем (ТКС) на основі використання алгебраїчних блокових кодів щодо забезпечення безпеки даних. Проведено аналіз можливих способів модифікації ТКС щодо суттєвого зниження обсягу ключових даних і зняття основного обмеження з практичного використання теоретико-кодових схем та оцінка їх параметрів. Проаналізовано показники і критерії безпеки і достовірності передачі даних, теоретично обґрунтовано введення узагальненого показника ефективності обміну даними в ЛОМ і ГОМ. Досліджено ефективності передачі даних у комп'ютерних системах і мережах з використанням розроблених криптосистем.

Перспективним напрямом у розвитку теоретико-кодових схем є розробка й дослідження способів модифікації. Їх застосування дозволяє суттєво знизити обсяг секретних ключових даних і, таким чином, зняти основні обмеження з практичного використання теоретико-кодових схем.

Першим успішним результатом у цьому напрямі є теоретико-кодові схеми Рао-Нама, запропоновані в [317]. Основна ідея, закладена в цю конструкцію, полягає у використанні одного секретного ключа – породжувальної матриці, G лінійного *блокового (n,k,d)* коду. В оригінальній схемі використовувалася породжувальна матриця, альтернантного коду Гопи. Розглянемо особливості побудови теоретико-кодової схеми Рао-Нама.

На рис. 2.3 наведена загальна схема моделі передачі секретного повідомлення між абонентами А і Б у теоретико-кодовій схемі Рао-Нама.

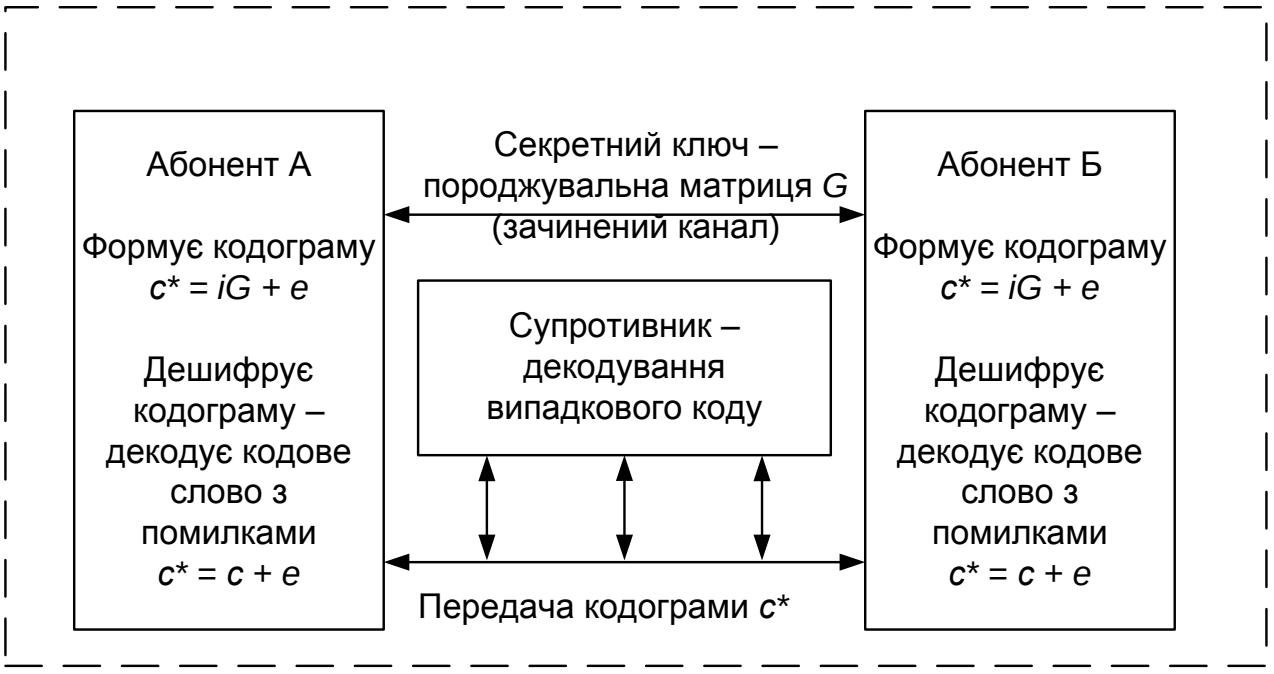


Рис. 2.3. **Схема моделі передачі кодограми в ТКС Рао-Нама**

Закриту інформацію (кодограму) у теоретико-кодовій схемі Рао-Нама визначимо у вигляді вектора c^* довжини n і обчислимо за правилом

$$c^* = I \cdot G + e.$$

Формування кодограми здійснюється шляхом кодування інформаційної послідовності I довжиною k інформаційних символів у кодове слово довжиною n кодових символів і додаванні до нього випадкового вектора помилки e. Вага вектора помилок $w(e) \le t$, де t – кількість помилок, яке може виправити (n,k,d) блоковий код, $d = 2 \cdot t + 1$.

На прийомній стороні вповноважений користувач (знаючий секретний ключ) декодує отриману кодограму – декодує кодове слово з помилками (n,k,d) алгебраїчного блокового коду. Завдання декодування алгебраїчного блокового коду (наприклад, коду Гопи) – поліноміальне розв'язне завдання. Декодування довільного лінійного коду (коду загального положення) є досить складним обчислювальним завданням. Складність його розв'язання зростає експоненціально [79; 81; 83; 85; 86]. Це положення лежить в основі теоретико-кодових схем Рао-Нама: код зі швидким алгоритмом декодування (поліноміальної складності) маскується під довільний (випадковий) лінійний код, декодування якого представляється як обчислювально складне завдання. Для вповноваженого користувача (який має секретний ключ) декодування – поліноміальне розв'язне завдання.

Проведемо оцінку параметрів теоретико-кодової схеми, яка будується із використанням алгебраїчних (n,k,d) блокових кодів над $GF(2^m)$:

розмірність секретного ключа (у бітах):

$$l_{K+} = k \cdot n \cdot m; \tag{2.1}$$

розмірність інформаційного вектора (у бітах):

$$l_I = k \cdot m; \tag{2.2}$$

розмірність кодограми (у бітах):

$$l_S = n \cdot m; \tag{2.3}$$

відносна швидкість передачі:

$$R = k / n. \tag{2.4}$$

Основним недоліком схеми Рао-Нама є великий обсяг ключа. Дійсно, для зберігання секретної породжувальної матриці (n,k,d) блокового коду *над* $GF(q)$ необхідно зберігати, у загальному випадку, $n \cdot k$ q-ічних символів. Вільною від цього недоліку є запропонована в [213; 214] теоретико-кодова схема, побудована з використанням альтернантних кодів, заданих через багаточлен Гопи.

Дослідження властивостей теоретико-кодових схем на альтернантних кодах Гопи. Теоретико-кодова схема, побудована з викорис-

танням альтернантних кодів, заданих через багаточлен Гопи вперше запропонована в роботі [86; 108; 110; 112; 253; 255]. Основна ідея полягає в побудові схеми Рао-Нама на (n,k,d)-кодах Гопи, заданих за допомогою многочлена Гопи степені $t,d = 2 \cdot t + 1$.

При цьому якщо (n,k,d)-код Гопи над $GF(q)$ дозволяє виправити t помилок, то всі кодові слова можуть бути однозначно задані многочленом Гопи степені t над $GF(q)$. У [230] показано, що кількість приведених кодів Гопи зростає експоненціально q. Отже, якщо замість породжувальної матриці коду як секретного ключа використовувати багаточлен Гопи, то одержимо стійку схему. При цьому вдається суттєво скоротити обсяг ключа. У загальному випадку, для однозначного визначення многочлена Гопи необхідно зберігати $t+1$ *q-ічних* символів.

Проведемо оцінку параметрів теоретико-кодової схеми, яка будується з використанням альтернантних (n,k,d) блокових кодів Гопи над $GF(2^m)$.

Розмірність секретного ключа (у бітах) визначається виразом:

$$l_{K+} = t \cdot m. \qquad (2.5)$$

Розмірність інформаційного вектора (у бітах), розмірність кодограми (у бітах), відносна швидкість передачі визначаються, відповідно, виразами (2.2 – 2.4).

На рис. 2.4 наведена схема моделі передачі секретного повідомлення між абонентами А і Б у схемі, побудованій з використанням альтернантних кодів, заданих через багаточлен Гопи. Основна відмінність від класичної схеми Рао-Нама полягає у використанні многочлена Гопи в якості секретного симетричного ключа. У роботах [113; 114; 120; 326] досліджені можливості теоретико-кодових схем Рао-Нама, побудованих з використанням заданих через багаточлен Гопи альтернантних кодів щодо забезпечення імітозахищеності й завадостійкості КМіС. Дійсно, якщо у виразі при формуванні кодограми використовувати випадковий вектор помилки e, такий, що $w(e) < t$, то з'являється можливість на прийомній стороні контролювати помилки в межах конструктивної величини t. Це дозволяє, з одного боку, вирішувати завдання підвищення імітозахищеності каналів керування й зв'язку, а з іншого, – підвищувати їх завадостійкість.

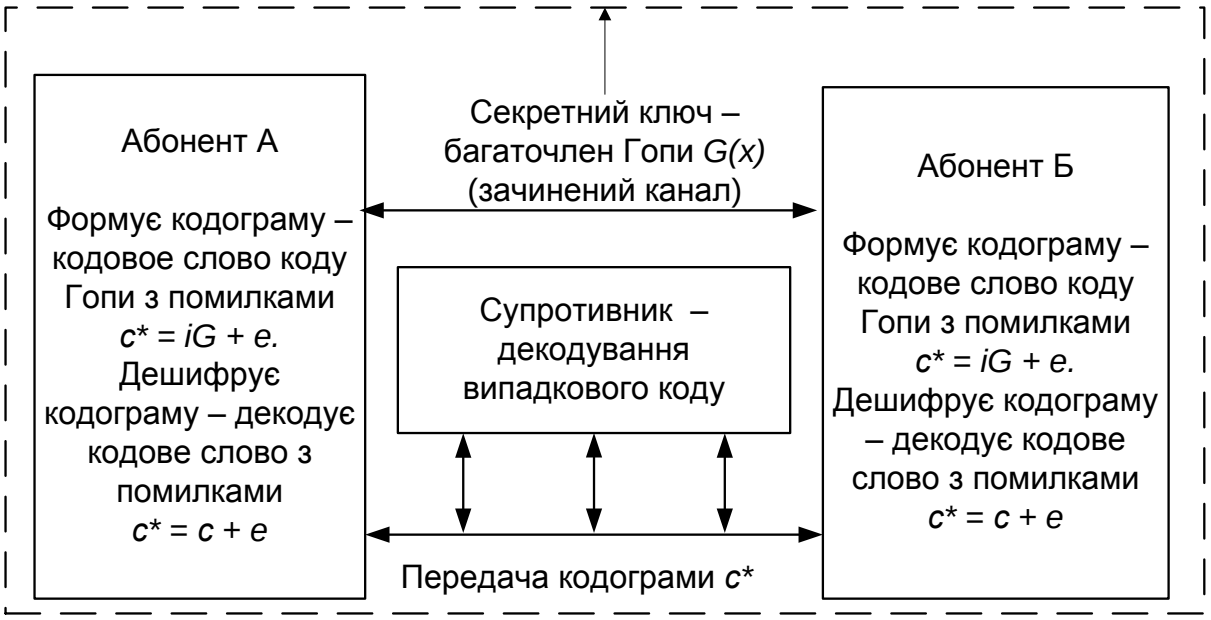


Рис. 2.4. **Схема моделі передачі кодограми в теоретико-кодовій схемі з використанням кодів Гопи**

У роботах [12; 19; 102] досліджені залежності між рівнями забезпечуваної завадостійкості й імітозахищеності при використанні теоретико-кодових схем на альтернантних кодах Гопи. Однак, як показано в роботі [245], при підвищених вимогах до імітозахищеності каналів КМіС забезпечити повною мірою завдання підвищення завадостійкості не вдається, завадостійкість такої схеми не велика. Вона поступається можливостям більшості гарних алгебраїчних кодів і є критично низькою при побудові спеціальних систем керування й зв'язку. Вільними від цих недоліків є теоретико-кодові схеми, побудовані на скорочених алгебраїчних блокових кодах.

Дослідження властивостей теоретико-кодових схем на скорочених алгебраїчних блокових кодах.

Подальший розвиток схем Рао-Нама розглянуто в роботах [66; 76; 77; 79; 81; 317]. Так, у роботі [106] зняте основне обмеження з низької величини забезпечуваної завадостійкості. Основна ідея таких схем полягає у використанні скорочених алгебраїчних блокових (n,k,d)-кодів (в оригінальній схемі використовуються скорочені коди Гопи). Символи скорочення вибираються випадково, незалежно й зберігаються в секреті (є секретним симетричним ключем). Показано, що навіть при невеликій кількості символів скорочення вдається побудувати стійку схему. Оцінка параметрів теоретико-кодової схеми, яка будується з використанням скорочених алгебраїчних (n,k,d) блокових кодів над $GF(2^m)$.

Розмірність секретного ключа (у бітах) визначається виразом:

$$l_{K+} = x \cdot m, \tag{2.6}$$

де x – кількість символів укорочення.

Розмірність інформаційного вектора (у бітах), розмірність кодограми (у бітах), відносна швидкість передачі визначаються відповідно до виразів (2.2 – 2.4).

На рис. 2.5 наведена схема моделі передачі секретного повідомлення між абонентами А і Б у системі, побудованій з використанням скорочених алгебраїчних блокових кодів. Кодограмою у такій системі є кодове слово скороченого алгебраїчного блокового коду (наприклад, коду Гопи), а всю конструктивну величину t пропонується використовувати для виправлення помилок. Таким чином, завадостійкість теоретико-кодової схеми визначається повною конструктивною величиною t блокового (n,k,d) коду, $d = 2 \cdot t + 1$. Усі виниклі в каналі зв'язку помилки e ваги $w(e) \le t$ виправляються в межах сфери пакування коду.

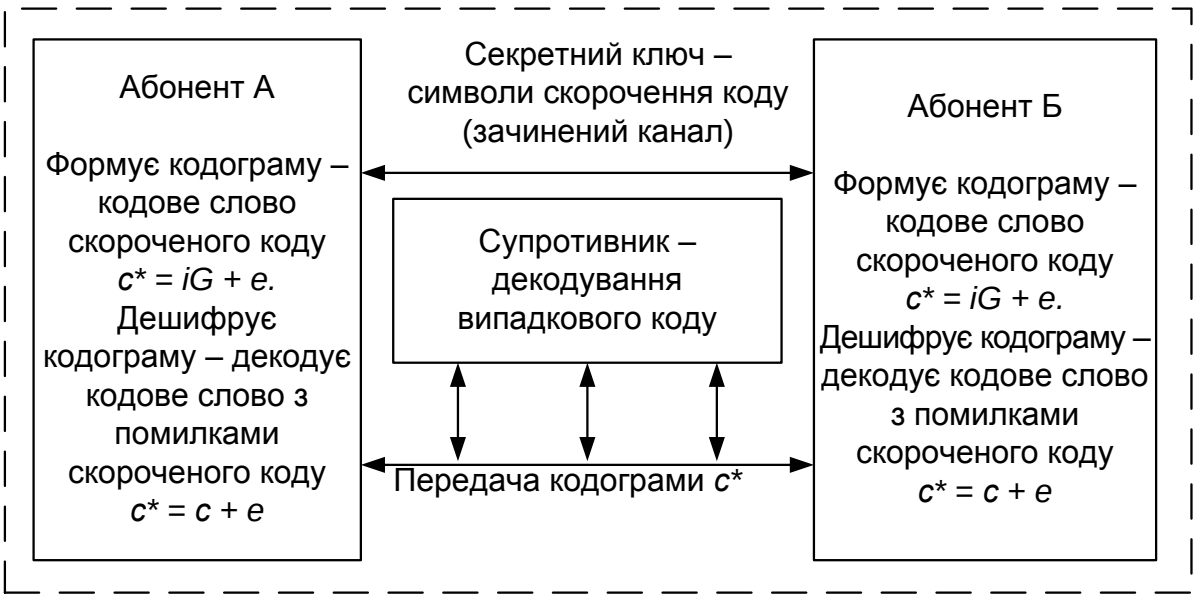


Рис. 2.5. **Схема моделі передачі кодограми в теоретико-кодовій схемі з використанням скорочених блокових кодів**

Основна перевага розглянутої на рис. 2.5 ТКС полягає у високих показниках завадостійкості. У той же час їй властивий істотний недолік – лінійність схеми. Кожна кодограма є кодовим словом лінійного скороченого блокового коду. Отже, сума двох кодограм дасть третю дозволену кодограму.

Для усунення зазначеного недоліку в роботі [106] пропонується використовувати штучні приймання внесення нелінійності (контрольні мітки часу, використання режиму зчеплення блоків та ін.). Ці заходи ускладнюють аналіз для аналітика й потенційно підвищують стійкість теоретико-кодової схеми. Однак їх використання ускладнює процес формування/зняття кодограми й, мабуть, знижує завадостійкість (наприклад, за рахунок внесення додаткової службової інформації).

Одним з перспективних напрямів у розвитку теоретико-кодових схем є використання алгебро-геометричних кодів. Далі наведені модифіковані теоретико-кодові схеми на еліптичних кодах, досліджуються їх криптографічні властивості.

Спосіб маскування еліптичних кодів у модифікованих теоретико-кодових схемах з використанням параметрів кривої як секретних даних

Скористаємося визначенням еліптичних кодів [25; 76; 77]. Визначимо такі властивості:

Властивість 1. Еліптичний (n,k,d)-код над $GF(q)$, побудований через вираз виду $\varphi: EC \to P^{k-1}$, пов'язаний характеристиками $k + d \geq n$, причому: $n \leq 2\sqrt{q} + q + 1$, $k \geq \alpha$, $d \geq n - \alpha$, $\alpha = 3 \cdot degf$.

Властивість 2. Еліптичний (n, k, d)-код над $GF(q)$, побудований через вираз виду $\varphi: EC \to P^{r-1}$, пов'язаний характеристиками $k + d \geq n$, причому: $n \leq 2\sqrt{q} + q + 1$, $k \geq n - \alpha$, $d \geq \alpha$, $\alpha = 3 \times degf$.

Нехай A – генераторна матриця еліптичного (n,k,d)-коду над $GF(q)$ виду

$$A = \begin{pmatrix} F_0(P_0) & F_0(P_1) & \dots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \dots & F_1(P_{n-1}) \\ \dots & \dots & \dots & \dots \\ F_{M-1}(P_0) & F_{M-1}(P_1) & \dots & F_{M-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,M}$$

і розмірності $M \cdot n$, $M = \alpha$, $\alpha = 3 \cdot degf$.

Задамо ТКС Рао-Нама на еліптичних кодах, побудованих через породжувальну матрицю, $G^{EC} = A$ (властивість 1). Справедливе таке твердження.

Твердження 1 [259; 260; 263; 273; 280]. Еліптичний (n,k,d)-код над $GF(2^m)$, заданий через породжувальну матрицю, $GEC = A$, *визначає* m-ічну теоретико-кодову схему Рао-Нама з параметрами:

розмірність секретного ключа (у бітах):

$$\mathrm{I}_{K+} = \alpha \cdot \left(2\sqrt{q} + q + 1\right) \cdot m; \tag{2.7}$$

розмірність інформаційного вектора (у бітах):

$$li = \alpha \cdot m; \tag{2.8}$$

розмірність кодограми (у бітах):

$$\mathrm{I}_S = \left(2\sqrt{q} + q + 1\right) \cdot m; \tag{2.9}$$

відносна швидкість передачі:

$$R = \alpha / \left(2\sqrt{q} + q + 1\right). \tag{2.10}$$

Задамо теоретико-кодову схему Рао-Нама на еліптичних кодах, побудованих через перевірочну матрицю $H^{EC} = A$. Справедливе таке твердження.

Твердження 2 [259; 260; 263; 273; 280]. Еліптичний (n,k,d)-код над $GF(2^m)$, заданий через перевірочну матрицю $H^{EC} = A$, визначає теоретико-кодову схему Рао-Нама з параметрами:

розмірність секретного ключа визначається виразом (2.7);

розмірність інформаційного вектора (у бітах):

$$I_I = \left(2\sqrt{q} + q + 1 - \alpha\right) \cdot m; \tag{2.11}$$

розмірність кодограми визначається виразом (2.9);

відносна швидкість передачі:

$$R = \left(2\sqrt{q} + q + 1 - \alpha\right) / \left(2\sqrt{q} + q + 1\right). \tag{2.12}$$

Передача кодограм у теоретико-кодовій схемі Рао-Нама на еліптичних кодах (за твердженням 1) відповідає рис. 2.5 при $G = G^{EC}$. Для передачі кодограм у теоретико-кодовій схемі Рао-Нама, побудованій з використанням результату твердження 2, необхідно попередньо обчис-

лити матрицю B, таку, що $A \times B^T = 0$. Далі, формування й передача кодограми відповідає рис. 2.5 при $G = B$.

Як випливає з доведених тверджень 1, 2, обсяг ключових даних у теоретико-кодових схемах Рао-Нама, побудованих на еліптичних кодах, відповідає обсягу відкритого ключа в несиметричних схемах. Для зниження обсягу ключових даних у теоретико-кодовій схемі на еліптичних кодах скористаємося такими особливостями побудови матриці A.

Генераторна матриця A формується в результаті відображення точок еліптичної кривої базисом генераторних функцій. У твердженнях 1, 2 використовується генераторна матриця еліптичного коду, побудованого за кривою $y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz + a_6z^3$, $a_i \in GF(q)$.

Коефіцієнти цього многочлена однозначно задають вид кривій і, відповідно, набір проективних точок, за якими будується еліптичний код (його генераторна матриця). Справедливе таке твердження.

Твердження 3 [259; 260; 263; 273; 280]. Еліптичний (n,k,d) код над $GF(q)$ однозначно задається набором $a_1...a_6$, $\forall a_i \in GF(q)$.

Доведення. Розглянемо генераторну матрицю еліптичного (n,k,d)-коду над $GF(q)$:

$$A = \begin{pmatrix} F_0(P_0) & F_0(P_1) & \dots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \dots & F_1(P_{n-1}) \\ \dots & \dots & \dots & \dots \\ F_{M-1}(P_0) & F_{M-1}(P_1) & \dots & F_{M-1}(P_{n-1}) \end{pmatrix}.$$

Кожний символ генераторної матриці формується шляхом обчислення значення генераторної функції F_j у точці P_i еліптичної кривої. Кількість M генераторних функцій визначається конструктивними характеристиками еліптичного (n,k,d)-коду. Вид функцій F_j визначається степенем α відображення точок кривої і, отже, так само задається конструктивними параметрами коду.

Таким чином, якщо задані конструктивні (n,k,d)-характеристики еліптичного коду, то унікальність генераторної матриці визначає набір точок $P_1, P_2, \dots, P_n$, у яких обчислюються значення генераторних функцій. Конкретний набір точок із простору P^2 однозначно задається видом многочлена кривої, тобто набором коефіцієнтів $a_1...a_6$, $\forall a_i \in GF(q)$.

Наслідок. Обсяг секретного ключа (у бітах) у модифікованій теоретико-кодовій схемі Рао-Нама, побудованої за еліптичними (n,k,d)-кодами над $GF(2^m)$ визначається виразом

$$l_{k+} = 5 \cdot m. \qquad (2.13)$$

Вираз (2.13) дозволяє оцінити обсяг секретних ключових даних у модифікованій теоретико-кодовій схемі Рао-Нама з еліптичними кодами. На рис. 2.6 наведені залежності обсягів ключових даних від розмірності поля $GF(2^m)$ для різних $q = 2, 4, 16, 32$. На рис. 2.6 наведені також часові витрати, необхідні для повного перебору ключових даних при швидкодії 10^{15} переборів у секунду.

Таким чином, запропонований спосіб маскування, заснований на побудові модифікованих теоретико-кодових схем на еліптичних кодах, у яких як секретні дані використовуються параметри еліптичної кривої, дозволяє суттєво знизити обсяги ключових даних порівняно з класичною схемою Рао-Нама. У той же час, потенційно стійкими вважаються схеми з $l_{k+} > 80$ біт [207]. Як випливає з наведених на рис. 2.6 залежностей, для побудови такої теоретико-кодової схеми необхідно використовувати еліптичні коди з довжиною кодового слова > 2^{20} біт.

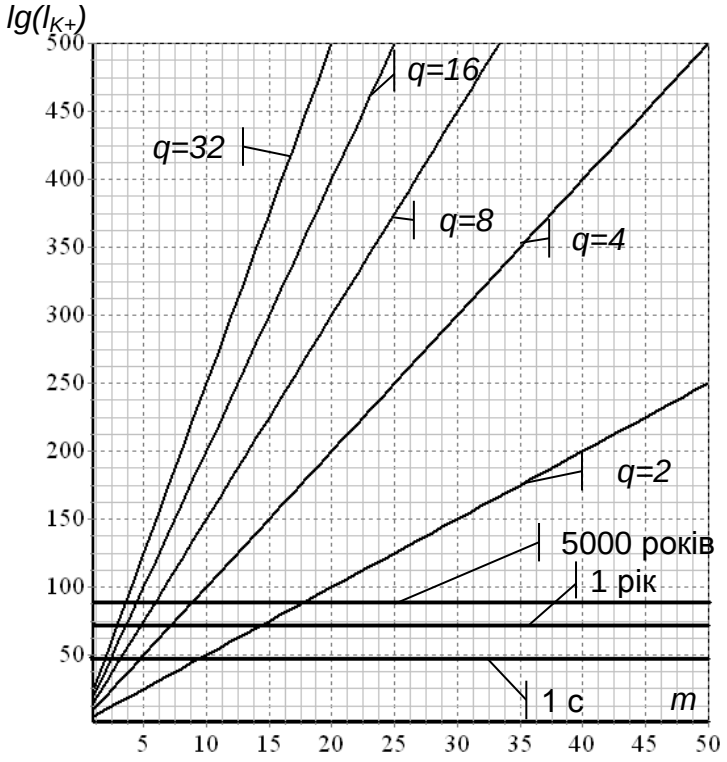


Рис. 2.6. **Залежності обсягу секретних ключових даних модифікованої теоретико-кодової схеми на еліптичних кодах**

Із практичної точки зору це обмеження може звузити область застосування запропонованих теоретико-кодових схем. Для підвищення завадостійкості й інформаційної скритності передачі інформації й зняття обмеження з довжини кодограми далі пропонується теоретико-кодова схема, побудована на модифікованих еліптичних кодах.

Спосіб маскування еліптичних кодів у модифікованих теоретико-кодових схемах з використанням символів модифікації коду як секретних даних

Відомі способи модифікації лінійних блокових кодів найбільше повно розглянуті в роботах [7; 11; 19; 21; 314; 315; 317; 321; 426]. На рис. 2.7 наведені найпоширеніші способи модифікації.

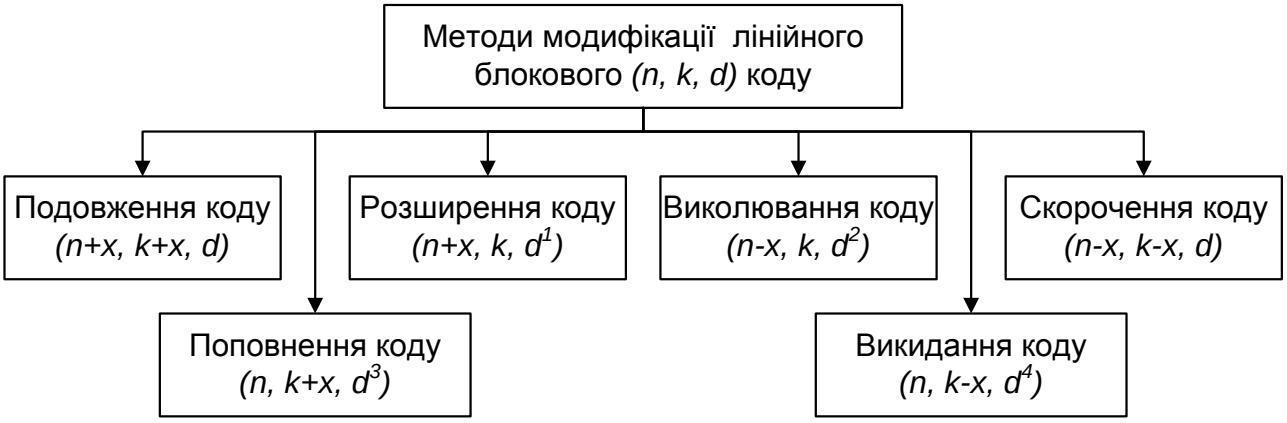


Рис. 2.7. **Способи модифікації лінійних блокових кодів**

Подовження (n,k,d) лінійного блокового коду полягає в збільшенні довжини $n+x$ шляхом додавання нових інформаційних символів $k+x$. *Розширення* (n,k,d) лінійного блокового коду полягає в збільшенні довжини $n+x$ шляхом додавання нових перевірочних символів $r+x$. *Виколювання* (n,k,d) лінійного блокового коду полягає в зменшенні довжини $n-x$ шляхом зменшення перевірочних символів $r-x$. *Скорочення* (n,k,d) лінійного блокового коду полягає в зменшенні довжини $n-x$ шляхом зменшення інформаційних символів $k-x$. *Поповнення* (n,k,d) лінійного блокового коду полягає в збільшенні довжини інформаційних символів $k+x$ без збільшення довжини коду. *Викидання* (n,k,d) лінійного блокового коду полягає в зменшенні інформаційних символів $k-x$ без збільшення довжини коду.

Потенційна стійкість теоретико-кодових схем визначається складністю декодування випадкового (n,k,d) блокового коду. Складність переставного декодування зростає експоненціально від величини $t = [(d-1)/2]$. Отже, для побудови потенційно стійких теоретико-кодових схем необхідно використовувати способи модифікації, що не допускають зниження мінімальної кодової відстані. Способи подовження й укорочення лінійних блокових кодів не змінюють мінімальну відстань, розширення (n,k,d) блокового коду приводить, як правило, до збільшення мінімальної відстані. Розглянемо ці способи докладніше.

Будь-який двійковий (n,k,d) блоковий код з непарною мінімальною відстанню можна розширити до $(n+1, k, d+1)$ з додаванням до кожного кодового слова суми всіх його компонентів як перевірки на парність [21; 219]. Відомі методи розширення (n,k,d) коду РС. Їх застосування дозволяє збільшити довжину й мінімальна кодова відстань РС коду на один і на два символи, відповідно, одержати $(q, k, q-k+1)$ і $(q+1, k, q-k+2)$ розширені РС коди над $GF(q)$. Для недвійкових еліптичних кодів способи розширення не досліджені.

Найбільш простий і зручний спосіб модифікації лінійного блокового коду, що не зменшує мінімальну кодову відстань, полягає в скорочені його довжини шляхом скорочення інформаційних символів. Нехай $I = (I_1, I_2, ..., I_k)$ – інформаційний вектор (n,k,d) блокового коду. Виберемо підмножину h інформаційних символів, $|h| = x$, $x < k$. Помістимо в інформаційний вектор I у підмножину h нулі, тобто $I_i = 0,\ \forall I_i \in h$. На інших позиціях вектора I помістимо інформаційні символи. При кодуванні інформаційного вектора символи множини h не беруть участь (вони нульові) і їх можна відкинути, а отримане кодове слово буде коротше на x кодових символів. Для модифікації (скорочення) еліптичних кодів будемо використовувати зменшення набору точок кривої. Справедливе таке твердження.

Твердження 4 [224; 259; 260; 263]. Нехай EC – еліптична крива у $GF(q)$, $g = g(EC)$ – рід кривій, $EC(GF(q))$ – множина її точок над кінцевим полем, $N = EC(GF(q))$ – їх кількість. Нехай X і h – непересічні підмножини точок, $X \cup h = EC(GF(q))$, $|h| = x$. Тоді *скорочений* еліптичний (n,k,d)-код

над *GF(q)*, побудований через відображення виду $\varphi: X \to P^{k-1}$, пов'язаний характеристиками $k + d \geq n$, причому:

$$n = 2\sqrt{q} + q + 1 - x,$$
$$k \geq \alpha - x, \qquad (2.14)$$
$$d \geq n - \alpha,\ \alpha = 3 \cdot degf.$$

Доведення. Дійсно, використовуючи результати твердження 1, побудуємо еліптичний код з параметрами: $n \leq 2\sqrt{q} + q + 1$, $k \geq \alpha - x$, $d \geq n - \alpha$, $\alpha = 3 \cdot degf$. Умова $n \leq 2\sqrt{q} + q + 1$ враховує можливість побудови еліптичних кодів на підмножині точок кривої. Якщо ця підмножина *X*, то одержимо вираз $n = 2\sqrt{q} + q + 1 - x$, а параметри еліптичного коду запишуться у вигляді (2.14).

Наслідок 1. Зафіксуємо підмножину $h_1 \subseteq h$, $|h_1| = x_1$. Нехай заданий еліптичний (n,k,d)-код над *GF(q)* побудований через відображення виду $\varphi: X \to P^{k-1}$. Тоді параметри *подовженого* на x_1 символів з *GF(q)* еліптичного коду, побудованого через відображення виду $\varphi: (X \cup h_1) \to P^{k-1}$, будуть пов'язані співвідношеннями: $n = 2\sqrt{q} + q + 1 - x + x_1$, $k \geq \alpha - x + x_1$, $d \geq n - \alpha$, $\alpha = 3 \cdot degf$.

Наслідок 2. Якщо відомий вид еліптичної кривої (набір $a_1 \ldots a_6$, $\forall a_i \in GF(q)$, то підмножини *h* і h_1 повністю визначають модифіковані еліптичні (n,k,d)-коди над *GF(q)*, побудовані через відображення виду: $\varphi: X \to P^{k-1}$ і $\varphi: (X \cup h_1) \to P^{k-1}$.

Твердження 5 [224; 259; 260; 263]. *Скорочений* еліптичний (n,k,d)-код над *GF(q)*, побудований через відображення виду $\varphi: X \to P^{r-1}$, пов'язаний характеристиками $k + d \geq n$, причому:

$$n = 2\sqrt{q} + q + 1 - x,$$
$$k \geq n - \alpha, \qquad (2.15)$$
$$d \geq \alpha,\ \alpha = 3 \cdot degf.$$

Наслідок 1. Зафіксуємо підмножину $h_1 \subseteq h$, $|h_1| = x_1$. Нехай заданий еліптичний (n,k,d)-код над *GF(q)*, побудований через відображення виду $\varphi: X \to P^{r-1}$. Тоді параметри *подовженого* на x_1 символів з *GF(q)* еліптичного коду, побудованого через відображення виду $\varphi: (X \cup h_1) \to P^{r-1}$,

будуть пов'язані співвідношеннями: $n = 2\sqrt{q} + q + 1 - x + x_1$, $k \geq n - \alpha$, $d \geq \alpha$, $\alpha = 3 \cdot degf$.

Наслідок 2. Якщо відомий вид еліптичної кривої (набір $a_1 \ldots a_6$, $\forall a_i \in GF(q)$, то підмножини h і h_1 повністю визначають модифіковані еліптичні (n,k,d)-коди над $GF(q)$, побудовані через відображення виду: $\varphi: X \to P^{r-1}$ і $\varphi: (X \cup h_1) \to P^{r-1}$.

Результати тверджень 4, 5 і їх наслідки дозволяють побудувати модифіковані (скорочені й подовжені в межах $n \leq 2\sqrt{q} + q + 1$) еліптичні (n,k,d)-коди над $GF(q)$. Задамо такий алгоритм побудови модифікованих еліптичних кодів.

Алгоритм побудови скорочених еліптичних кодів.

Крок 1. Зафіксуємо еліптичну криву над $GF(q)$. Знайдемо множину простих точок кривої $EC(GF(q))$: $(P_1, P_2, \ldots, P_N)$.

Крок 2. Зафіксуємо непересічні підмножини точок кривої X $(GF(q))$: $(P_{x1}, P_{x2}, \ldots, P_{xs})$ і $h(GF(q))$: $(P_{h1}, P_{h2}, \ldots, P_{hx})$, $X \cup h = EC(GF(q))$, $/X/ = s$, $/h/ = x$.

Крок 3. Побудуємо відображення $\varphi: X \to P^M$. Якщо $M = k$, одержимо *скорочений* еліптичний (n,k,d)-код над $GF(q)$ з параметрами $n = 2\sqrt{q} + q + 1 - x$, $k \geq \alpha - x$, $d \geq n - \alpha$, $\alpha = 3 \cdot degf$ (див. твердження 4). Якщо $M = r$, то одержимо *скорочений* еліптичний (n,k,d)-код над $GF(q)$ з параметрами: $n = 2\sqrt{q} + q + 1 - x$, $k \geq n - \alpha$, $d \geq \alpha$, $\alpha = 3 \cdot degf$ (див. твердження 5).

Алгоритм побудови подовжених еліптичних кодів.

Крок 1. Зафіксуємо еліптичну криву над $GF(q)$. Знайдемо множину простих точок кривої $EC(GF(q))$: $(P_1, P_2, \ldots, P_N)$. Побудуємо скорочений (n,k,d)-код над $GF(q)$ як результат відображення $\varphi: X \to P^M$.

Крок 2. Зафіксуємо підмножину точок кривої $h_1(GF(q))$: $(P_{x1}, P_{x2}, \ldots, P_{xx1})$, $h_1 \subseteq h$, $/h_1/ = x_1$.

Крок 3. Побудуємо відображення $\varphi: (X \cup h_1) \to P^M$. Якщо $M = k$, одержимо *подовжений* еліптичний (n,k,d)-код над $GF(q)$ з параметрами $n = 2\sqrt{q} + q + 1 - x + x_1$, $k \geq \alpha - x + x_1$, $d \geq n - \alpha$, $\alpha = 3 \cdot degf$ (див. наслідок твердження 4). Якщо $M = r$, одержимо *подовжений* еліптичний (n,k,d)-

код над *GF(q)* з параметрами: $n = 2\sqrt{q} + q + 1 - x + x_1$, $k \geq n - \alpha$, $d \geq \alpha$, $\alpha = 3 \cdot degf$ (див. наслідок твердження 5).

Використовуючи результат твердження 4 і його наслідки, задамо теоретико-кодову схему на модифікованих еліптичних кодах, побудованих через відображення виду $\varphi: X \to P^{k-1}$ і $\varphi: (X \cup h_1) \to P^{k-1}$. Справедливе таке твердження.

Твердження 6 [223; 257; 259; 260]. Скорочений еліптичний (n, k, d)-код над $GF(2^m)$, побудований через відображення виду $\varphi: X \to P^{k-1}$, визначає модифіковану теоретико-кодову схему з параметрами:

$$l_{K+} = x\left|log_2(2\sqrt{q} + q + 1)\right|; \tag{2.16}$$

$$li = (\alpha - x) \cdot m; \tag{2.17}$$

$$l_S = \left(2\sqrt{q} + q + 1 - x\right) \cdot m; \tag{2.18}$$

$$R = (\alpha - x) \left(2\sqrt{q} + q + 1 - x\right). \tag{2.19}$$

Подовжений еліптичний (n, k, d)-код над $GF(2^m)$, побудований через відображення виду $\varphi: (X \cup h_1) \to P^{k-1}$, визначає модифіковану теоретико-кодову схему з параметрами:

$$l_{k+} = (\bar{x} - x_1) \cdot \left|log_2(2\sqrt{q} + q + 1)\right|; \tag{2.20}$$

$$l_i = (\alpha - x + x_1) \cdot m; \tag{2.21}$$

$$l_S = \left(2\sqrt{q} + q + 1 - x + x_1\right) \cdot m; \tag{2.22}$$

$$R = (\alpha - x + x_1) \left(2\sqrt{q} + q + 1 - x + x_1\right). \tag{2.23}$$

Підставимо параметри модифікованих (скорочених і подовжених) еліптичних (n, k, d)-кодів над *GF(q)*, побудованих через відображення виду $\varphi: X \to P^{k-1}$ і $\varphi: (X \cup h_1) \to P^{k-1}$ (див. твердження 4) одержимо, відповідно, вираз (2.16 – 2.19) і (2.20 – 2.23).

Використовуючи результат твердження 5 і його наслідки, задамо теоретико-кодову схему на модифікованих еліптичних кодах, побудованих через відображення виду $\varphi: X \to P^{r-1}$ і $\varphi: (X \cup h_1) \to P^{r-1}$. Справедливе таке твердження.

Твердження 7 [223; 257; 259; 260]. Скорочений еліптичний (n, k, d)-код над $GF(2^m)$, побудований через відображення виду $\varphi: X \to P^{r-1}$, визначає модифіковану теоретико-кодову схему з параметрами:

розмірність секретного ключа визначається виразом (2.16);

розмірність інформаційного вектора (у бітах):

$$l_I = \left(2\sqrt{q} + q + 1 - \alpha\right) \cdot m; \qquad (2.24)$$

розмірність кодограми визначається виразом (2.18);

відносна швидкість передачі:

$$R = \left(2\sqrt{q} + q + 1 - \alpha\right) / \left(2\sqrt{q} + q + 1 - x\right). \qquad (2.25)$$

Подовжений еліптичний (n,k,d)-код над $GF(2^m)$, побудований через відображення виду $\varphi: (X \cup h_1) \to P^{r-1}$, визначає модифіковану теоретико-кодову схему з параметрами:

розмірність секретного ключа визначається виразом (2.20);

розмірність інформаційного вектора (у бітах):

$$l_I = \left(2\sqrt{q} + q + 1 - \alpha\right) \cdot m; \qquad (2.26)$$

розмірність кодограми визначається виразом (2.22);

відносна швидкість передачі:

$$R = \left(2\sqrt{q} + q + 1 - \alpha\right) / \left(2\sqrt{q} + q + 1 - x + x_1\right). \qquad (2.27)$$

Таким чином, результати тверджень 4, 5 і їх наслідки дозволяють побудувати модифіковані (скорочені й подовжені) еліптичні (n,k,d)-коди над $GF(q)$. Твердження 6 і 7 дозволяють задати теоретико-кодові схеми на модифікованих еліптичних кодах, тим самим пропонується спосіб маскування, заснований на використанні в якості секретних даних символи модифікації (скорочення або подовження) еліптичного коду, що дозволяє суттєво знизити обсяги ключової інформації.

Проаналізуємо показники і критерії безпеки і достовірності передачі даних, теоретично обґрунтовується введення узагальненого показника ефективності обміну даними в локальній обчислювальній мережі (ЛОМ) і глобальній обчислювальній мережі (ГОМ).

Аналіз показників і критеріїв безпеки і достовірності передачі даних у комп'ютерних системах і мережах

При розгляді функціонування комп'ютерної мережі загальний показник ефективності обміну даними повинен включати показник конфіденційності і приватні показники системи зв'язку – достовірність і оперативність.

Найбільш загальним підходом до забезпечення безпеки в точках уразливості комп'ютерних мереж є використання шифрування. Таким чином, забезпечення конфіденційності (інформаційної прихованості) шля-

хом реалізації механізму захисту інформації може оцінюватися як імовірнісно-часовий показник криптографічної стійкості – час ТБ, що характеризує час безпечної роботи даного криптоалгоритму за умови застосування супротивником різних методів криптоаналізу.

Безпечний час визначається за критерієм мінімального ризику:

$$T_Б = min\{T_{Б_1}, T_{Б_2}, ..., T_{Б_L}\},$$

де $T_{Б_i}$ – час безпечної роботи цього криптоалгоритму за умови застосування супротивником і-ого методу криптоаналізу; L – кількість відомих методів криптоаналізу для цього криптоалгоритму.

Відповідно до основних положень теорії складності час, що витрачається алгоритмом як функція розміру завдання, називається часовою складністю цього алгоритму. Поведінку цієї складності в інтервалі при збільшенні розміру завдання називають асимптотичною часовою складністю алгоритму. Аналогічно визначається ємнісна і асимптотична ємнісна складність алгоритму.

Позначимо B_i часову складність алгоритму, який реалізує і-ий метод криптоаналізу. Відповідний показник безпечного часу $T_{Б_i}$ запишемо у вигляді:

$$T_{Б_i} = \frac{B_i}{\xi \quad \Psi},$$

де ξ = 31622400 – числовий коефіцієнт для перерахунку секунд у роки;

Ψ – продуктивність обчислювальної системи, доступної криптоаналітику (противнику).

Тоді з урахуванням виразу складності:

$$T_Б = min\left\{\frac{B_1}{\xi \quad \Psi}, \frac{B_2}{\xi \quad \Psi}, ..., \frac{B_L}{\xi \quad \Psi}\right\},$$

що еквівалентно запису:

$$T_Б = \frac{B_{min}}{\xi \quad \Psi},$$

де B_{min} – часова складність алгоритму, який реалізує найбільш відомий метод криптоаналізу,

$$B_{min} = min\{B_1, B_2, ..., B_L\}.$$

Вимоги до безпечного часу ТБ роботи криптоалгоритму встановлюються виходячи з категорії цінності інформації, яка обробляється, її пріоритетності і приналежності. На сьогоднішній день загальноприйнятою вимогою до безпечного часу для інформації будь-якої категорії цінності є умова ТБ > 200 років.

Таким чином, загальною вимогою до безпечного часу інформації є

$$T_Б \geq T_Д,$$

де ТД – допустимо безпечний час роботи криптоалгоритму.

Під *достовірністю* (інформаційною надійністю) передачі даних розуміють ступінь відповідності прийнятих повідомлень переданим. Достовірність залежить від параметрів самої комп'ютерної мережі, ступеня її технічної досконалості і умов роботи (тип і стан каналів зв'язку, метеорологічні показники, вигляд і інтенсивність завад, організаційні заходи дотримання правил радіообміну і експлуатації апаратури). Кількісно достовірність передачі може оцінюватися:

імовірністю помилкового прийому одиничного елемента (втрата достовірності)

$$P_0 = \lim_{n_{заг} \to \infty} \frac{n_{пом}}{n_{заг}},$$

де $n_{пом}$ і $n_{заг}$ – кількість помилково прийнятих і загальна кількість переданих одиничних елементів відповідно;

імовірністю помилкового прийому пакета даних

$$P_{ошп} = \lim_{N_{заг} \to \infty} \frac{N_{пом}}{N_{заг}},$$

де $N_{пом}$ і $N_{заг}$, – кількість помилково прийнятих і загальна кількість переданих кодових (пакетів) відповідно;

імовірністю правильного прийому одиничного елемента $P_{0\,пр}$ і імовірністю правильного прийому пакета $P_{пр\,п}$, причому

$$P_{0пр} + P_0 = 1;$$
$$P_{прп} + P_{ошп} = 1.$$

Імовірності помилкового і правильного прийому одиничного елемента (P_0 і $P_{0\,пр}$) фактично є характеристиками дискретного каналу зв'язку, імовірності $P_{пом\,п}$ і $P_{пр\,п}$ є характеристиками комп'ютерної мережі в цілому, оскільки вони визначаються не тільки характером і інтенсивністю завад у каналі зв'язку, видом і швидкістю модуляції, але і способом захисту від помилок у системі.

Час доставки інформації – інтервал часу від початку надходження повідомлення даних на вхід частини комп'ютерної мережі, що передає, до початку його видачі одержувачеві даних приймаючою частиною. Час доставки tд характеризує здатність комп'ютерної мережі своєчасно доставляти інформацію. При передачі конфіденційної інформації, зокрема, до часу доставки входить час шифрування відправником пакетів даних і час розшифрування пакетів одержувачем відповідним криптоалгоритмом. Аналіз часу шифрування і розшифрування переможців конкурсів криптоалгоритмів AES і NESSIE свідчить, що для асиметричних шифрів складність реалізації криптографічних перетворень на 3 – 5 порядків вища, ніж в аналогічних систем часової стійкості (блоково-симетричних шифрів).

Таким чином, у комп'ютерних системах з автоперезапитом (вирішальним зворотним зв'язком) час доставки пакета дорівнює:

$$t_д = t_д' + \Delta t_д + t_ш + t_{розш}$$ – для симетричних криптоалгоритмів,

$$t_д = t_д' + \Delta t_д + (t_ш + t_{розш})^S$$ – для асиметричних криптоалгоритмів,

де $t_д$ – час доставки пакета з першої посилки; $\Delta t_д$ – час багаторазового повторення передачі інформації при погіршенні якості каналу;

$t_ш$ – час шифрування пакета даних криптоалгоритмом, $t_{розш}$ – час розшифрування одержувачем пакета даних; S – кратність часу шифрування (розшифрування).

Час $t_д$ доставки повідомлення на задану адресу залежить від багатьох чинників: структури каналів, надійності і завантаження мережі, методу комутації, наявності і характеру дій, що заважають і призводять до помилок і повторних передач. Він є випадковою величиною, що характеризується щільністю розподілу $f(t_д)$.

У каналах зв'язку з високою інтенсивністю помилок $P_{пом}$ підвищення достовірності приводить до збільшення часу доставки $t_д$ через збільшення кількості повторних надсилань пакета, і навпаки, зниження часу

доставки $t_д$ за рахунок зменшення кількості повторних посилок пакета веде до зниження достовірності.

Проте більшість реальних каналів передачі даних є нестаціонарними, імовірність одноразової помилки в них змінюється за часом у широких межах від 10^{-9} до 10^{-2}.

Загальною вимогою до достовірності інформації є мінімізація імовірності помилкового прийому символів повідомлення $P_{пом}$ або, що еквівалентно, максимізації імовірності правильного прийому $P_{пп}$. Водночас на сьогоднішній день вимоги до достовірності інформації, яка обробляється і передається, істотно посилилися, і відповідно до керівних документів допустима імовірність помилкового прийому символів повідомлення складає:

$$РД < 10^{-7} – 10^{-9}$$

залежно від категорії цінності інформації, яка обробляється, її пріоритетності і належності.

Таким чином, загальною вимогою до достовірності інформації є:

$$P_{\text{пом}} \leq P_{\text{Д}}.$$

Тому для оцінки ефективності функціонування комп'ютерної мережі як показник ефективності доцільно використовувати узагальнений показник функціональної ефективності.

Теоретичне обґрунтування узагальненого показника ефективності обміну даними в комп'ютерних системах і мережах.

Структура побудови показника така, що в ній об'єднано дві основні характеристики системи:

необхідна імовірність досягнення мети з необхідним показником забезпечення конфіденційності (інформаційної прихованості) в певних умовах зовнішнього середовища і при певному рівні впливу внутрішніх випадкових чинників;

витрати, які необхідно здійснити у вказаних умовах для досягнення мети з необхідною імовірністю.

Показник функціональної ефективності системи має вигляд:

$$W = \frac{P}{Q},$$

де P – імовірність досягнення цілі операції в заданих умовах;

Q – витрати, необхідні для виконання цілі операції.

У якості імовірності досягнення мети операції доцільно використовувати імовірність безпомилкової доставки пакета $P_{пр\ п}$.

$$P_{пр\ п} = (1 - P_п)^n,$$

де $P_п$ – імовірність помилки біта в каналі передачі даних;

n – кількість біт у пакеті.

Витрати, необхідні для забезпечення безпомилкової доставки пакета, визначаються надлишковістю, яка вводиться. Тому в якості надлишкового показника може виступати коефіцієнт надлишковості γ – величина, зворотна корисній (ефективній) швидкості передачі R, яка при фіксованій пропускній спроможності C вимірюється числом біт інформації, які знаходяться в одному пакеті:

$$W = \frac{P_{пр\ п}}{\gamma},$$

де $\gamma = \frac{1}{R} = \frac{t_д}{h}$, $t_д$ – час доставки пакета;

h – кількість інформаційних розрядів (біт) пакета.

Крім того, для обліку забезпечення необхідної конфіденційності (інформаційної прихованості) даних, які передаються, до складу показника ефективності необхідно ввести величину, що характеризує часову складність (стійкість) використовуваного в системі шифру – кількість операцій, необхідних для розкриття шифру зловмисником В. Оскільки дана величина має достатньо високий порядок (біля 10^{-19} -10^{-77}), зручніше використовувати її десятковий логарифм. Тоді узагальнений показник ефективності набуде вигляду:

$$W = \frac{h}{t} \cdot lgB \cdot (1 - P_п)^n.$$

Цей показник, включаючи часткові показники достовірності, конфіденційності і часу доставки даних у комп'ютерній мережі, по суті, відображає швидкість достовірної і конфіденційної передачі даних комп'ютерній мережі, що дозволяє оцінювати ефективність мережі в широкому діапазоні інтенсивностей помилок у каналі передачі даних при різних швидкостях передачі R.

Імовірність безпомилкової доставки пакета *Рпр п* за визначенням перебуває в діапазоні (0, 1). Ефективна швидкість *R* і часова складність алгоритму, який реалізує метод криптоаналізу *lg B*, у загальному випадку перебувають в діапазоні (0, +∞). Для переходу з діапазону (0, +∞) в діапазон (0, 1) зручно скористатися формулою:

$$x' = \frac{x-1}{x},$$

яка має такі властивості:

$$\lim_{x \to +0} \frac{x-1}{x} = \infty \quad \lim_{x \to 1} \frac{x-1}{x} = 0, \quad \lim_{x \to \infty} \frac{x-1}{x} = 1.$$

Замінивши значення $\frac{h}{t}$ і $lg\,B$ еквівалентними їм, отримаємо

$$\frac{\frac{h}{t}-1}{\frac{h}{t}} = \frac{h-t}{h},\ W = \frac{h-t}{h} \cdot \frac{lgB-1}{lgB} \cdot (1-P_n)^n.$$

Якщо замість показника часової складності криптоалгоритму lg B використовувати безпечний час роботи криптоалгоритму

$$T_{Бi} = \frac{B_i}{\Psi},$$

де Ψ – працездатність обчислювальної системи, доступної криптоаналітику (противнику), то

$$W = \frac{h-t}{h} \cdot \frac{t-1}{t} \cdot (1-P_П)^n = \frac{h-t}{h} \cdot \frac{\frac{B}{\psi}-1}{\frac{B}{\psi}} \cdot (1-P_П)^n = \frac{h-t}{h} \cdot \frac{B-\psi}{B} \cdot (1-P_П)^n.$$

Оскільки час доставки пакета *t* є випадковою величиною, то можливо оцінити тільки його математичне очікування *mt*.

У цьому випадку вибір оптимальної стратегії функціонування комп'ютерної мережі u* із більшості допустимих стратегій доцільно здійснювати за критерієм найбільшого середнього результату, тобто

$$W(u^*) = \max_{u_i \in U} W(u_i),$$

де $W(u_i) = \frac{n^{(u_i)} - t^{(u_i)}}{n^{(u_i)}} \cdot \frac{B^{(u_i)} - \psi^{(u_i)}}{B^{(u_i)}} \cdot P_{прп}^{(u_i)}$,

W(u$_i$) – показник ефективності комп'ютерної мережі при обраній стратегії (методі підвищення достовірності) u$_i$;

$n(u_i)$ – кількість інформаційних розрядів пакета при обраній стратегії u_i;

$t(u_i)$ – час доставки пакета t при вибраній стратегії u_i;

$B(u_i)$ – кількість операцій, необхідних для розкриття криптоалгоритму порушником при обраній стратегії u_i;

$\Psi(u_i)$ – працездатність обчислювальної системи, доступної криптоаналітику (противнику) при обраній стратегії u_i;

$P_{пр\ п(ui)}$ – імовірність правильної доставки пакета при обраній стратегії;

U – більшість допустимих стратегій (методів підвищення достовірності, які використовуються в комп'ютерній мережі).

При цьому окремі показники повинні задовольняти систему обмежень

$$\{T_Б \geq T_Д, P_{пом} \leq P_Д, t_д \leq t_Д\},$$

при мінімізації часу доставки кадру інформації.

Обрані узагальнені показники і критерії ефективності комп'ютерної мережі дозволяють досягти числових значень, що характеризують швидкість достовірної і конфіденційної передачі даних у комп'ютерній мережі і провести порівняння існуючих протоколів ГОМ за ефективністю обміну даними між двома вузлами комп'ютерної мережі.

Дослідження ефективності передачі даних у комп'ютерних системах і мережах з використанням розроблених крипто-кодових засобів захисту інформації

Оцінимо показник ефективності комп'ютерної мережі (W_i) при різних стандартних довжинах кадрів стека протоколів X.25 і параметри розробленої криптосистеми. Для підвищення значення показника функціональної ефективності комп'ютерної мережі розглянемо різні способи управління обміном даними: без зворотного зв'язку з виявленням r-кратних помилок; без зворотного зв'язку з виправленням *t*-кратних помилок; з вирішальним зворотним зв'язком і безперервною передачею кадрів (ВЗЗбп) "Повернення-на-N"; з вирішальним зворотнім зв'язком і позитивною квитанцією (ВЗЗпк).

Як вихідні дані виступають такі параметри:

а) параметри каналу передачі даних: імовірність помилки біта P_0, пропускна здатність каналу передачі даних C, довжина лінії зв'язку L; швидкість поширення сигналу в середовищі V_p.

б) параметри комп'ютерної мережі: довжина інформаційного кадру n, довжина квитанції s (для систем зі зворотним зв'язком), кратність виявлених помилок r (для систем з виявленням помилок), кратність помилки t,

що виправляється (для систем з виправленням помилок), розмір вікна Z (для систем з ВЗЗбп "Повернення-на-N"), визначена імовірність доставки пакета P_3 (для систем з ВЗЗпк).

Слід розглянути кожен з параметрів моделі. Імовірність помилки біта P_0 є характеристикою достовірності передачі інформації і змінюється в межах від 10^{-6} до 10^{-1} для різних типів каналів.

Значення пропускної спроможності каналу оберемо для систем передачі даних, що використовують радіоканали C = 9 600 біт/с.

Довжину лінії зв'язку задамо рівною L = 1 250 000 м (довжина ділянки місцевої та середньої якості відповідно до еталонної гіпотетичної моделі цифрового тракту (*Hypothetical Reference Connection – HRX*), схваленої МККТТ) і L = 2 500 000 м (довжина радіоканалу відповідно до гіпотетичної моделі радіочастотної цифрової системи передачі (*Hypothetical Reference Digital Path – HRDP*), схваленої МККР).

Швидкість поширення сигналу в середовищі задамо рівною $V_p = 3 \cdot 10^8$ м/с. Кратність виявлених помилок r = 16 відповідно до рекомендації стандарту V.41. Кратність виправлених помилок t = 8, що виправляє здатність циклічного коду з породжуючим поліномом CRC-16.

Довжину інформаційних кадрів n оберемо, виходячи зі стандартних довжин кадрів стека протоколів X.25, наведених у табл. 2.2.

Таблиця 2.2

Стандартні довжини I-кадрів протоколу LAP-B

№ п/п	Довжина поля даних інкапсульованого пакета мережного рівня, L		Режими нумерації кадрів			
			нормальний (за модулем 8)		розширений (за модулем 128)	
	байт	біт	байт	біт	байт	біт
1	16	128	20	160	21	168
2	32	256	36	288	37	296
3	64	512	68	544	69	552
4	128	1 024	132	1 056	133	1 064
5	256	2 048	260	2 080	261	2 088
6	512	4 096	516	4 128	517	4 136
7	1024	8 192	1 028	8 224	1 029	8 232
8	2 048	16 384	2 052	16 416	2 053	16 424
9	4 096	32 768	4 100	32 800	4 101	32 808

Довжина квитанції s також відповідає стандартним довжинам службових кадрів X.25: *s* = 32 біта в нормальному режимі нумерації кадрів і *s* = 40 біт у розширеному режимі нумерації. При розрахунках приймалося *n* = 160 і 1 056 біт, *s* = 32 біта.

Розмір вікна *Z* в протоколі X.25 може змінюватися в діапазоні від 1 до 7 у нормальному режимі нумерації кадрів і від 1 до 127 у розширеному. Оскільки рекомендованим значенням є *Z* = 2, то розрахунки проводилися для цього значення.

Необхідну імовірність доставки пакета приймемо рівною $P_{тр} = 0{,}95$.

Для каналів без пам'яті в комп'ютерній мережі, що використовують циклічні коди в режимі виявлення помилок (стратегія u_1), значення показника ефективності визначається як

$$W(u_1) = \frac{n^{(u_1)} - t^{(u_1)}}{n^{(u_1)}} \cdot \frac{B^{(u_1)} - \psi^{(u_1)}}{B^{(u_1)}} \cdot P_{пр\,п}^{(u_1)},$$

де $t^{(u_1)} = \frac{n}{C} + \frac{L}{V_p} + t_ш + t_{рш}$, $P_{пр\,п}^{(u_1)} = (1 - P_0)^n$,

де *n* – кількість інформаційних розрядів кадру;

C – пропускна здатність каналу;

L – довжина лінії зв'язку;

V_p – швидкість поширення сигналу в середовищі;

$t_ш$ – час шифрування кадру;

$t_{рш}$ – час розшифрування кадру;

P_0 – імовірність помилки в каналі.

Для комп'ютерної мережі без зворотного зв'язку при виправленні *t*-кратної помилки циклічним кодом *(стратегія* u_2*) значення показника ефективності визначається як*

$$W(u_2) = \frac{n^{(u_2)} - t^{(u_2)}}{n^{(u_2)}} \cdot \frac{B^{(u_2)} - \psi^{(u_2)}}{B^{(u_2)}} \cdot P_{пр\,п}^{(u_2)},$$

де $t^{(u_2)} = \frac{n}{C} + \frac{L}{V_p} + t_ш + t_{рш}$, $P_{пр\,п}^{(u_2)} = \sum_{i=0}^{t} C_n^i \cdot P_0^i (1 - P_0)^{n-i}$.

Для комп'ютерної мережі з вирішальним зворотним зв'язком і безперервним передаванням кадрів "Повернення-на-N" значення показника ефективності визначається як

$$W(u_3) = \frac{n^{(u\ 3)} - t^{(u\ 3)}}{n^{(u\ 3)}} \cdot \frac{B^{(u\ 3)} - \psi^{(u\ 3)}}{B^{(u\ 3)}} \cdot P_{пр\,п}^{(u\ 3)},$$

де

$$M\left[t^{(u\ 3)}\right] = \frac{n}{C} + \frac{L}{V_p} + t_ш + t_{рш} + \frac{\sum_{i=1}^{r} C_n^i \cdot P_0^i (1 - P_0)^{n-i} (1 - \frac{1}{2^r}) \cdot \sum_{i=r+1}^{n} C_n^i \cdot P_0^i (1 - P_0)^{n-i}}{(1 - P_0)^n} \cdot$$

$$\cdot \left(\frac{n+s}{C} + 2\frac{L}{V_p} \right),$$

$$P_{пр\,п}^{(u\ 3)} = \frac{(1 - P_0)^n}{1 - \sum_{i=1}^{r} C_n^i \cdot P_0^i (1 - P_0)^{n-i} (1 - \frac{1}{2^r}) \cdot \sum_{i=r+1}^{n} C_n^i \cdot P_0^i (1 - P_0)^{n-i}},$$

де n – довжина I-кадру;

r – кількість виявлених помилок;

s – довжина S-кадру.

Для комп'ютерної мережі з вирішальним зворотним зв'язком і позитивною квитанцією *значення показника ефективності визначається як*

$$W(u_4) = \frac{n^{(u\ 4)} - t^{(u\ 4)}}{n^{(u\ 4)}} \cdot \frac{B^{(u\ 4)} - \psi^{(u\ 4)}}{B^{(u\ 4)}} \cdot P_{пр\,п}^{(u\ 4)},$$

де

$$M\left[t^{(u\ 4)}\right] = \frac{n+s}{C} + 2\frac{L}{V_p} + t_ш + t_{рш} +$$

$$+ \frac{\sum_{i=1}^{r} C_n^i \cdot P_0^i (1 - P_0)^{n-i} (1 - \frac{1}{2^r}) \cdot \sum_{i=r+1}^{n} C_n^i \cdot P_0^i (1 - P_0)^{n-i}}{(1 - P_0)^n} \cdot \frac{n}{C},$$

$$P_{пр\,п}^{(u\ 4)} = (1 - P_0)^n \frac{1 - \left(\sum_{i=1}^{r} C_n^i \cdot P_0^i (1 - P_0)^{n-i} (1 - \frac{1}{2^r}) \cdot \sum_{i=r+1}^{n} C_n^i \cdot P_0^i (1 - P_0)^{n-i} \right)^N}{1 - \sum_{i=1}^{r} C_n^i \cdot P_0^i (1 - P_0)^{n-i} (1 - \frac{1}{2^r}) \cdot \sum_{i=r+1}^{n} C_n^i \cdot P_0^i (1 - P_0)^{n-i}},$$

де n – кількість інформаційних розрядів кадру;

s – довжина S-кадру;

$t_ш$ – час шифрування І-кадру;

$t_{рш}$ – час розшифрування І-кадру.

Результати розрахунків наведені відповідно до параметрів розробленої криптосистеми на рис. 2.8.

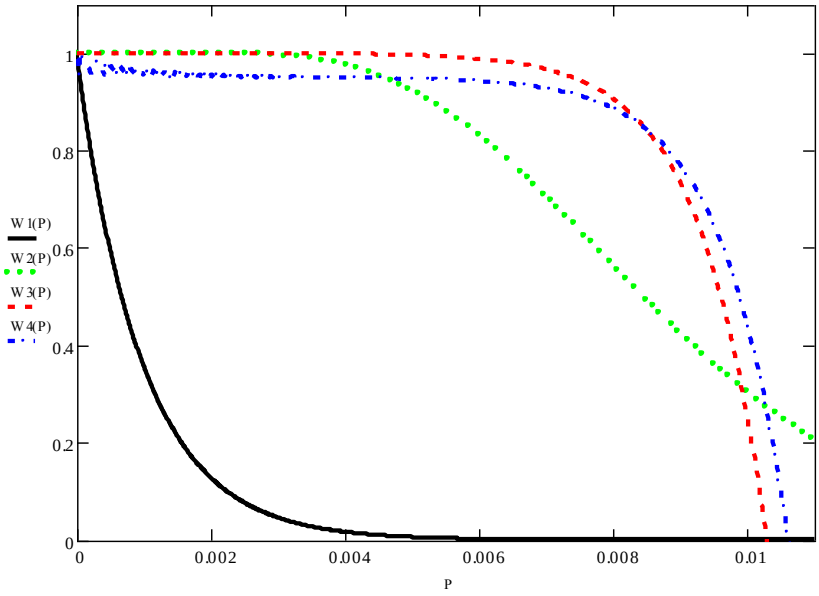


Рис. 2.8. **Залежність показника ефективності обміну даними в КС *W* від імовірності бітових помилок P_0**

Примітка. При розрахунках приймалися такі вихідні дані:

C = 56 000 біт/с; L = 1 000 км; $V_p = 3 \times 10^8$ м/с; r = 16; t = 8; n = 1 024; s = 32; Z = 2; $P_З$ = 0,95; $t_ш$ = 100 с; $t_{рш}$ = 100 с; В = 10^{24}, $\Psi = 10^{15}$.

Аналіз результатів, наведених на рис. 2.8, показує необхідність використання протоколів керування обміном даними з автоперезапитом (вирішальним зворотним зв'язком і позитивною квитанцією, з ВЗЗ і безперервною передачею кадрів "Повернення-на-N"), як у широкосмугових цифрових каналах (виділених цифрових ліній, оптоволоконних кабелях), так і в повітряних лініях передачі з $P_o = 10^{-3} – 10^{-2}$. Використання розробленої криптосистеми дозволяє інтегровано забезпечити необхідні показники завадостійкості (відмовостійкості) і безпеки (конфіденційності), що вимагаються до комп'ютерних мережах.

Детальне дослідження статистичних властивостей послідовностей помилок у реальних каналах зв'язку показало, що помилки є залежними і мають тенденцію до групування (пакетування), тобто між ними існує певна залежність – кореляція. Більшу частину часу інформація проходить каналами зв'язку без спотворень, а в окремі моменти часу виникають згущення помилок, так звані пакети (пачки, групи) помилок, усередині яких імовірність помилки виявляється значно вищою за

середню імовірності помилок, обчислену для значного часу передачі. У таких умовах способи захисту, оптимальні для гіпотези незалежних помилок, не є ефективними при використанні їх в реальних каналах зв'язку. Для обліку статистичних властивостей послідовностей помилок у реальних каналах зв'язку розглянемо модель каналу з пам'яттю.

У цій моделі у вихідні дані замість імовірності помилки біта P_0 потрібно обрати такі чотири канальні параметри: імовірність виникнення пакета помилок $P_п$, імовірність помилки всередині пакета дорівнює $P_ε$, математичне очікування – m_{ln} довжини пакета помилок, середньо-квадратичне відхилення – $σ_{ln}$ довжини пакета помилок.

При розрахунках приймалося: $P_п = 10^{-5} \div 10^{-2}$; $P_ε = 0{,}8$; $m_{ln} = 10$; $σ_{ln} = 2$.

Для каналів з пам'яттю в комп'ютерній мережі, що використовують циклічні коди в режимі виявлення помилок, значення показника ефективності визначається як:

$$W(u_1) = \frac{n^{(u_1)} - t^{(u_1)}}{n^{(u_1)}} \cdot \frac{B^{(u_1)} - \psi^{(u_1)}}{B^{(u_1)}} \cdot P_{прп}^{(u_1)},$$

де $t^{(u_1)} = \frac{n}{C} + \frac{L}{V_p} + t_ш + t_{рш}$;

$$P_{прп}^{(u_1)} = 1 - \sum_{i=0}^{\infty} \left\{ \left[1 - (1 - P_п)^{n+i} \right] \cdot \left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}} \right) - \Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\}.$$

Для комп'ютерної мережі без зворотного зв'язку при виправленні t-кратної помилки циклічним кодом значення показника ефективності визначається як:

$$W(u_2) = \frac{n^{(u_2)} - t^{(u_2)}}{n^{(u_2)}} \cdot \frac{B^{(u_2)} - \psi^{(u_2)}}{B^{(u_2)}} \cdot P_{прп}^{(u_2)},$$

де $m_t^{(u_2)} = \frac{n}{C} + \frac{L}{V_p} + t_ш + t_{рш}$,

$$P_{прп}^{(u_2)} = 1 - \sum_{i=0}^{\infty} \left\{ \left[1 - (1 - P_п)^{n-t+i} \right] \cdot \left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}} \right) - \Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\}.$$

Для комп'ютерної мережі з вирішальним зворотним зв'язком і безперервною передачею кадрів "Повернення-на-N" значення показника ефективності визначається як:

$$W(u_3) = \frac{n^{(u\ 3)} - t^{(u\ 3)}}{n^{(u\ 3)}} \cdot \frac{B^{(u\ 3)} - \psi^{(u\ 3)}}{B^{(u\ 3)}} \cdot P_{пр\,п}^{(u\ 3)},$$

де

$$t_t^{(u\ 3)} = \frac{n}{C} + \frac{L}{V_p} + t_ш + t_{рш} +$$

$$+ \frac{\sum_{i=0}^{\infty} \left\{ \left[1 - (1 - P_п)^{n+i} \right] \cdot \left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}} \right) - \Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\} \cdot \left\{ 1 - \frac{1}{2^r} \cdot \left[\frac{1}{2} - \Phi\left(\frac{r+1-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\}}{1 - \sum_{i=0}^{\infty} \left\{ \left[1 - (1 - P_п)^{n+i} \right] \cdot \left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}} \right) - \Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\}} \cdot$$

$$\cdot \left(\frac{n+s}{C} + 2\frac{L}{V_p} \right),$$

$$P_{пр\,п}^{(u\ 3)} = \frac{1 - \sum_{i=0}^{\infty} \left\{ \left[1 - (1 - P_п)^{n+i} \right] \cdot \left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}} \right) - \Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\}}{1 - \sum_{i=0}^{\infty} \left\{ \left[1 - (1 - P_п)^{n+i} \right] \cdot \left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}} \right) - \Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\} \cdot \left\{ 1 - \frac{1}{2^r} \cdot \left[\frac{1}{2} - \Phi\left(\frac{r+1-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\}}.$$

Для комп'ютерної мережі з вирішальним зворотним зв'язком і позитивною квитанцією кадрів значення показника ефективності визначається як:

$$W(u_4) = \frac{n^{(u\ 4)} - t^{(u\ 4)}}{n^{(u\ 4)}} \cdot \frac{B^{(u\ 4)} - \psi^{(u\ 4)}}{B^{(u\ 4)}} \cdot P_{пр\,п}^{(u\ 4)},$$

де

$$t^{(u\ 4)} = \frac{n+s}{C} + 2\frac{L}{V_p} + t_ш + t_{рш} + \frac{n}{C} \cdot$$

$$\times \frac{\sum_{i=0}^{\infty} \left\{ \left[1 - (1 - P_п)^{n+i} \right] \cdot \left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}} \right) - \Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\} \cdot \left\{ 1 - \frac{1}{2^r} \cdot \left[\frac{1}{2} - \Phi\left(\frac{r+1-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\}}{1 - \sum_{i=0}^{\infty} \left\{ \left[1 - (1 - P_п)^{n+i} \right] \cdot \left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}} \right) - \Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\}},$$

$$P_{пр\,п}^{(4)} = 1 - \sum_{i=0}^{\infty}\left\{\left[1-(1-P_п)^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right)-\Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}\cdot$$

$$\times\frac{1-\sum_{i=0}^{\infty}\left\{\left[1-(1-P_п)^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right)-\Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}\cdot\left\{1-\frac{1}{2^r}\cdot\left[\frac{1}{2}-\Phi\left(\frac{r+1-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}^N}{1-\sum_{i=0}^{\infty}\left\{\left[1-(1-P_п)^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right)-\Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}\cdot\left\{1-\frac{1}{2^r}\cdot\left[\frac{1}{2}-\Phi\left(\frac{r+1-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}}.$$

У результаті розрахунків отримані числові значення показника ефективності комп'ютерної мережі *W* при зміні імовірності виникнення пакета помилок $P_п$. Результати розрахунків для розробленої крипто-системи наведені на рис. 2.9.

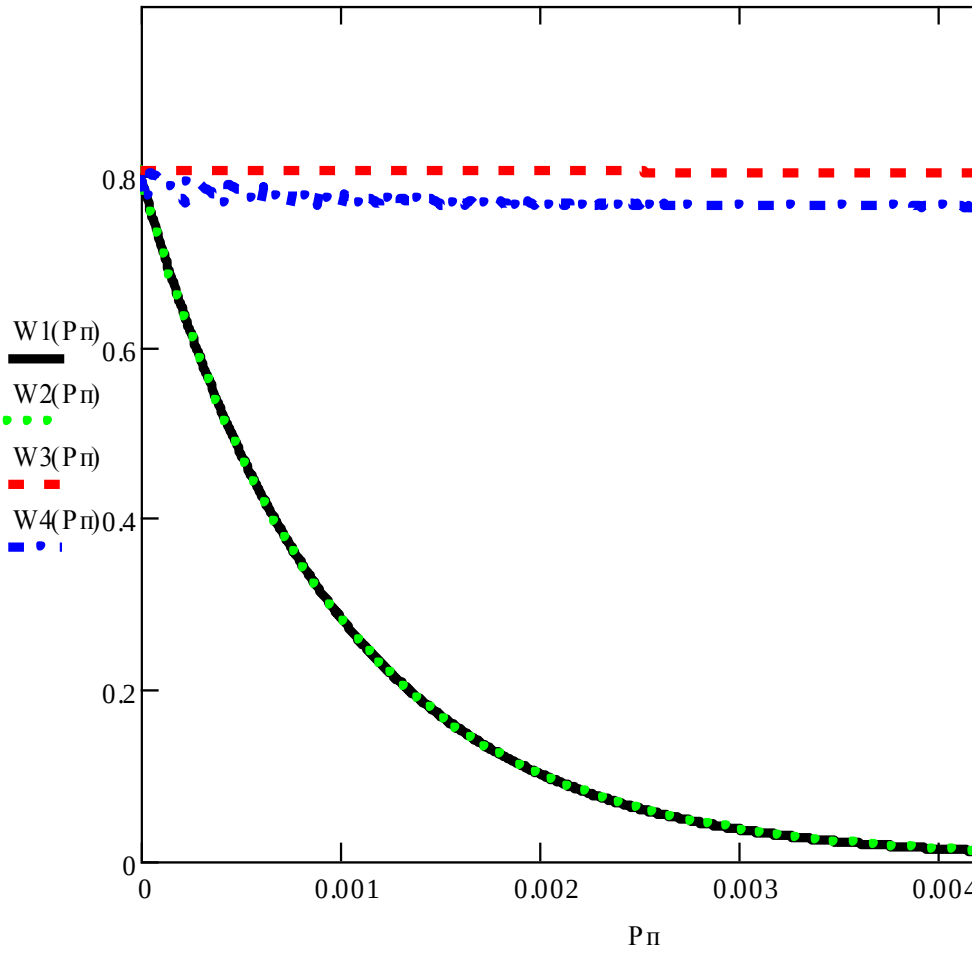


Рис. 2.9. **Залежність показника ефективності обміну даними в КМ *W* від імовірності пакетів помилок $P_п$**

Аналіз результатів рис. 2.9 свідчить, що при розгляді моделі каналу з пам'яттю різко падає показник ефективності обміну даними в КМ при використанні стратегій W_2 і W_1. Протоколи з автоперезапитом (стратегії W_3 і W_4) задовольняють вимоги узагальненого показника ефективності тільки при використанні розробленої криптосистеми в протоколах з вирішальним зворотним зв'язком і безперервним передаванням кадрів "Повторення-на-N" або з вирішальним зворотним зв'язком і позитивною квитанцією, яка дозволяє інтегровано забезпечити потрібні параметри надійності і безпеки системи. Разом з тим, аналіз рис. 2.7, 2.8 демонструє, що їх застосування знижує вимоги з оперативності – час формування пакета даних на 20 %.

У результаті досліджень показано, що застосування крипто-кодових систем при відповідних параметрах кодів дозволяє забезпечити безпеку і достовірність передачі даних у випадку використання порушником неалгебраїчних методів декодування. Крім того, практичне використання крипто-кодових засобів захисту інформації дозволяє комплексно розв'язувати завдання забезпечення безпеки і достовірності передачі даних. При значенні і довжині коду криптоаналіз обчислювально недосяжний. Складність реалізації найбільш ефективної атаки порушника складає 2^{35} групових операцій над GF(q). Таким чином, розроблені крипто-кодові системи захисту інформації ефективно забезпечують безпеку передачі даних у комп'ютерних системах і мережах.

Як видно із наведених рисунків, крипто-кодові засоби захисту інформації мають високі показники швидкодії і при формуванні криптограми, так і при її розшифруванні. При збільшенні довжини коду складність перетворення даних збільшується як поліноміальна функція.

Таким чином, розроблені крипто-кодові засоби захисту інформації дозволяють реалізувати швидке криптографічне перетворення великих об'ємів даних з використанням відкритих ключів, що, з одного боку, не потребує розповсюдження секретних ключових даних закритими каналами зв'язку, з другої сторони не потребує ускладнень існуючої апаратури передачі даних. Практично це означає, що використання розроблених криптосистем дозволяє здійснювати швидке (10 – 100 Мбіт/с) криптографічне перетворення з можливістю частої зміни ключових даних.

Розділ 3. Метод забезпечення автентичності і цілісності даних на основі властивостей алгоритму UMAC-32

3.1. Послуги і механізми забезпечення безпеки інформації відповідно до міжнародних стандартів ISO 7498, ISO/IEC 10181

Розглянуто структурну схему Національної платіжної системи, основні тенденції її розвитку, класифікація загроз інформаційної безпеки внутрішньо-платіжних систем комерційних банків України, послуги і механізми, які забезпечують інформаційну безпеку банківських транзакцій за допомогою криптографічних перетворень на основі послуг шифрування і автентифікації та цифрового підпису.

Розвиток високорентабельної економіки неможливий без упровадження сучасної системи грошового обігу та використання ефективних платіжних механізмів. Швидке зростання обсягів оброблюваних даних у сучасних ВПС, поява нових форм електронних послуг, стрімкий розвиток обчислювальної техніки висувають нові вимоги до надійності та забезпечення безпеки у ВПС.

Однак на сьогоднішній день не існує науково-обґрунтованої концепції та механізмів забезпечення фінансової безпеки банківської діяльності національної платіжної системи в цілому [37; 61; 197]. Проведений аналіз робіт у цьому напрямі показав, що проблемними питаннями у відкритих системах, у тому числі і ВПС, є питання забезпечення автентичності та цілісності конфіденційної інформації [37; 61; 197; 325; 326].

Процес розвитку ринкової економіки вимагає наявності відповідної платіжної системи, що дозволяє здійснювати розрахунки в народному господарстві відповідно до загальноприйнятих світових стандартів. У зв’язку з цим на перший план виходять надійність, безпека, а також терміновість здійснення платежів [107; 203; 223].

Національна платіжна система [107; 288] – це складна багаторівнева система централізованого управління, що забезпечує якісний стратегічно важливий канал проведення фінансових транзакцій.

Така система відноситься до складних багаторівневих систем управління критичного застосування (СУКЗ), у яких передача інформації вимагає контролю безпеки на кожному рівні [2; 325]. Важливою складовою частиною ВПС, призначеною для забезпечення послуг безпеки, є підсистема криптографічного безпеки інформації, яка реалізується відповідними протоколами і механізмами безпеки. Структурна схема СУКЗ національної платіжної системи наведена на рис. 3.1.

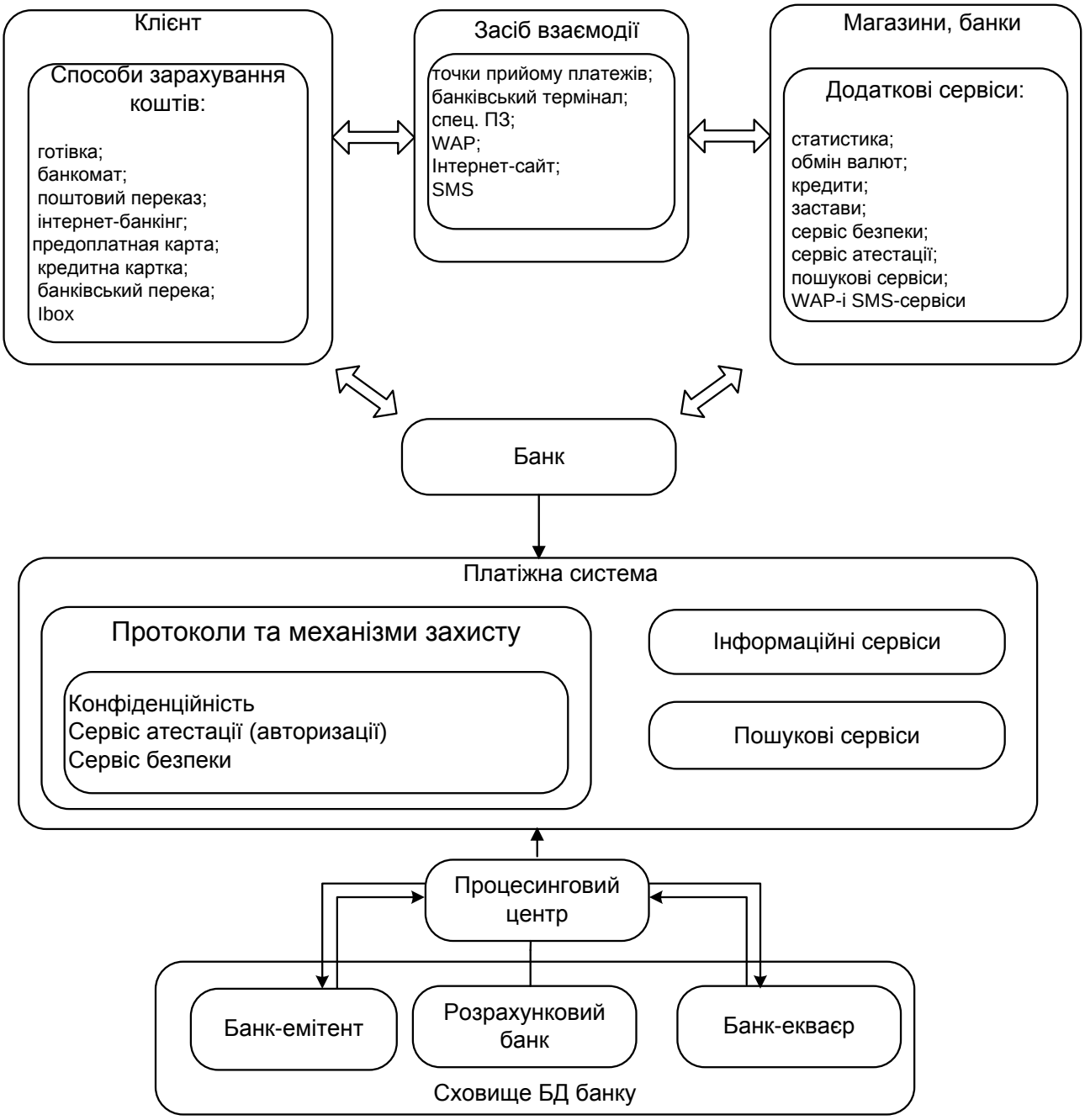


Рис. 3.1. **Структурна схема національної платіжної системи**

Проведений аналіз робіт [37; 61; 197; 326] показав, що, незважаючи на світову економічну кризу, банківські установи в усьому світі, на основі нових обчислювальних можливостей, продовжують нарощувати сферу послуг через мережі банкоматів і POS-терміналів. На рис. 3.2 наведена діаграма зростання кількості банкоматів у світі, на рис. 3.3 – в Україні [264].

Основними напрямами розвитку цього виду послуг ВПС є подальше нарощування мережі банкоматів, введення нових послуг оплати через І-бокси, розвиток електронного банкінгу та зростання продажів товарів населенню через Інтернет-магазини, що підтверджується зростанням транзакцій через мережі віддаленого доступу ВПС. На рис. 3.4 представлені результати аналізу грошового товарообігу через банкомати ВПС Україна [268].

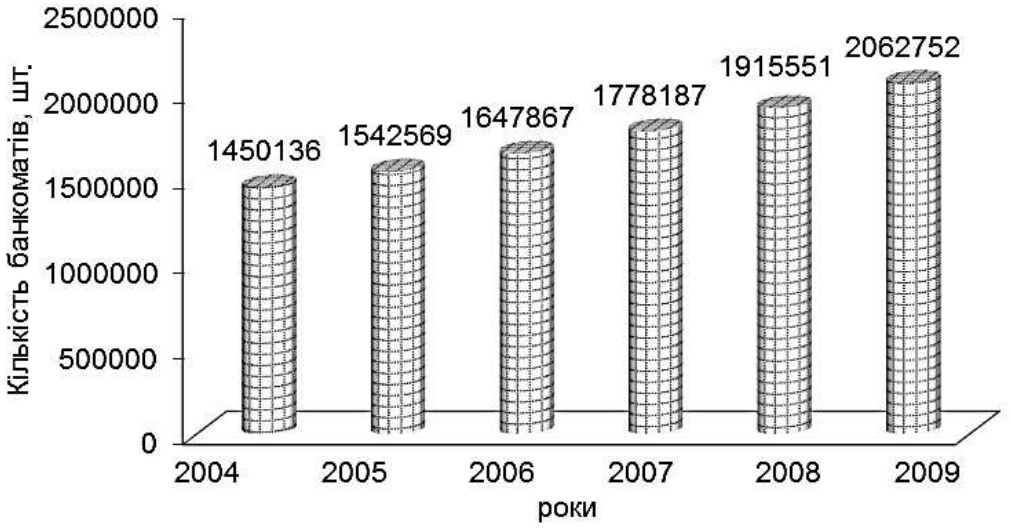


Рис. 3.2. **Зростання кількості банкоматів у світі**

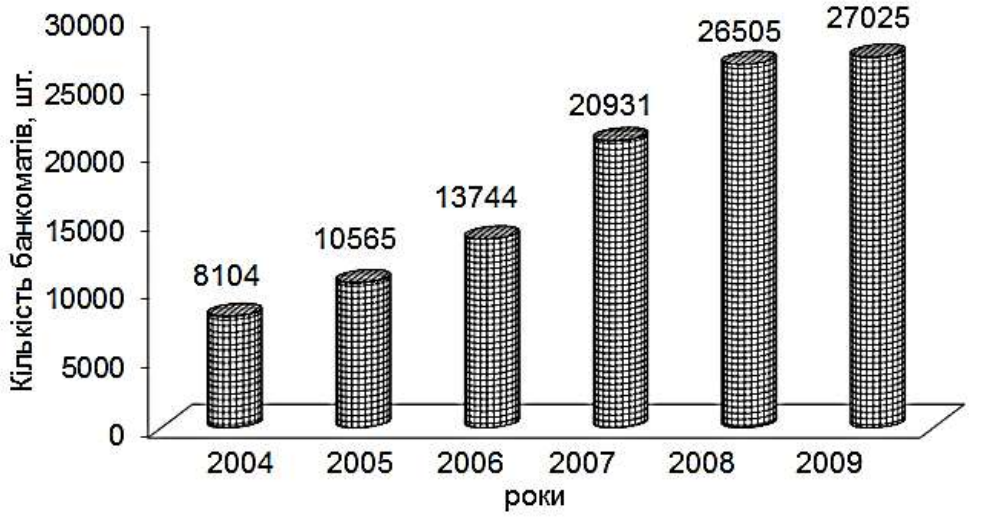


Рис. 3.3. **Зростання числа банкоматів в Україні**

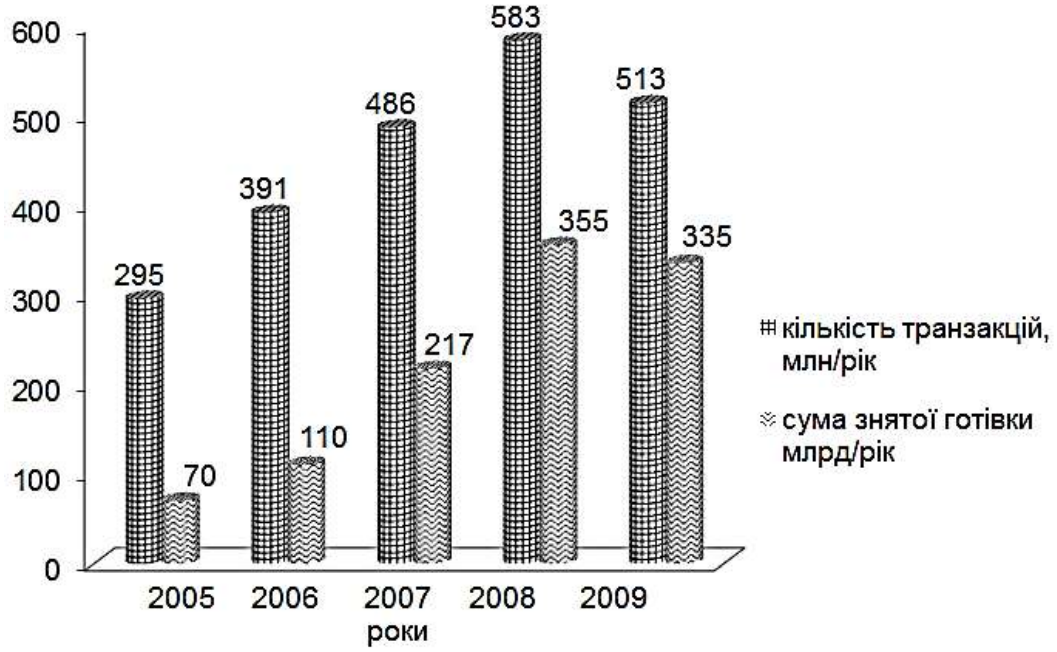


Рис. 3.4. **Зростання товарообігу через банкомати в Україні**

Проведений аналіз рис. 3.2 – 3.4 показав, що ВПС на основі досягнень комунікаційних та ІТ-технологій успішно розвивають свої функції з послуг оплати через мережі банкоматів та віддалених користувачів, продажу товарів через Інтернет-магазини і т. д. Але розвиток інформаційних технологій, глобальної мережі Інтернет, а також події (військові конфлікти, терористичні акти) останніх років, показали необхідність забезпечення інформаційної безпеки країни в цілому та її громадян зокрема. Таким чином, забезпечення безпеки ВПС, мережі зв'язку фінансово-кредитної та банківської сфер виноситься на національний рівень, що свідчить про ступінь важливості цього питання.

Сучасні методи обробки, передачі і накопичення інформації в інформаційних системах сприяли появі загроз інформаційної безпеки, пов'язаних з можливістю втрати, спотворення і розкриття даних, що адресовані або належать кінцевим користувачам.

Постійний розвиток обчислювальної техніки й збільшення її продуктивності, що підтверджується законом Мура, робить інформаційні системи вразливими до різних атак і загроз.

Загрозою інформаційній безпеці в інформаційній системі називається можливість реалізації дії на інформацію, що обробляється автоматизованою системою (АС), та призводить до спотворення, знищення, копіювання, блокування доступу до інформації, а також можливість дії на компоненти АС, що призводить до втрати, знищення або

збою функціонування носія інформації, засоби взаємодії з носієм або засобу його керування [37].

Загрози інформаційної безпеки можна класифікувати за критеріями [37]:

за метою впливу, на яку загрозу направлені насамперед;

за компонентами інформаційних систем, на які загрози націлені (дані, програми, апаратура, підтримуюча інфраструктура);

за способом здійснення (дії природного/техногенного характеру);

з розташуванням джерела загроз (внутрішні/зовнішні).

За метою впливу розрізняють три основні типи загроз інформаційної безпеки: загроза доступності, загроза цілісності та загроза конфіденційності інформації.

Загальна класифікація загроз інформаційної безпеки в ВПС наведена на рис. 3.5.

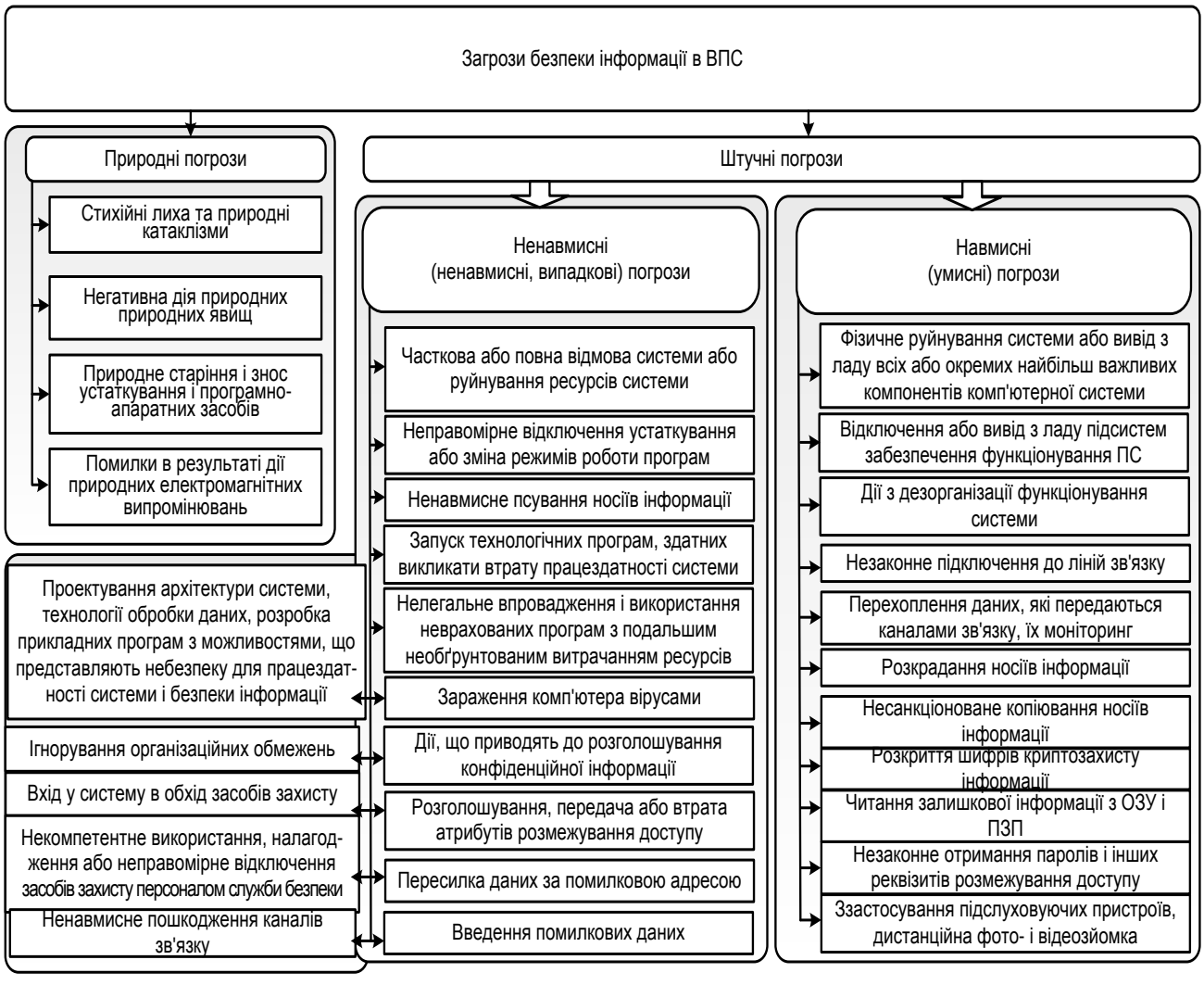


Рис. 3.5. **Класифікація основних загроз на ВПС**

Оцінка стану інформаційної безпеки свідчить, що не дивлячись на існуючі процеси зростання, їх обсяг і якісні характеристики на цьому етапі в основному не здатні задовольнити реальні потреби систем у необхідних ресурсах. У зв'язку з цим визначено основні реальні і потенційні загрози, які негативним чином впливають на процес регулювання інформаційної безпеки [2].

Аналіз рис. 3.5 показує, що джерелом ненавмисних загроз інформаційних систем можуть бути вихід з ладу апаратних чи програмних засобів, неправильні дії працівників або її користувачів, ненавмисні помилки в програмному та програмно-апаратному забезпеченні і т. д. Такі загрози можуть нанести значний збиток. Однак більш значними з точки зору ефективності функціонування є навмисні загрози, які, на відміну від випадкових, мають на меті завдання збитків інформаційній системі або користувачам [2]. Навмисні загрози можуть бути реалізовані шляхом довготривалої масованої атаки несанкціонованими запитами або вірусами, тощо. Наслідки такі: руйнування (втрата) інформації, модифікація (зміна інформації на помилкову, яка коректна за формою і змістом, але має інший сенс) і ознайомлення з нею сторонніх осіб. Ціна вказаних подій може бути досить високою.

Протидія розглянутим загрозам інформаційній безпеці є головною метою засобів захисту комп'ютерних мереж і систем.

У якості засобів захисту інформаційних систем виступають послуги інформаційної безпеки (рис. 3.6) [2; 61].

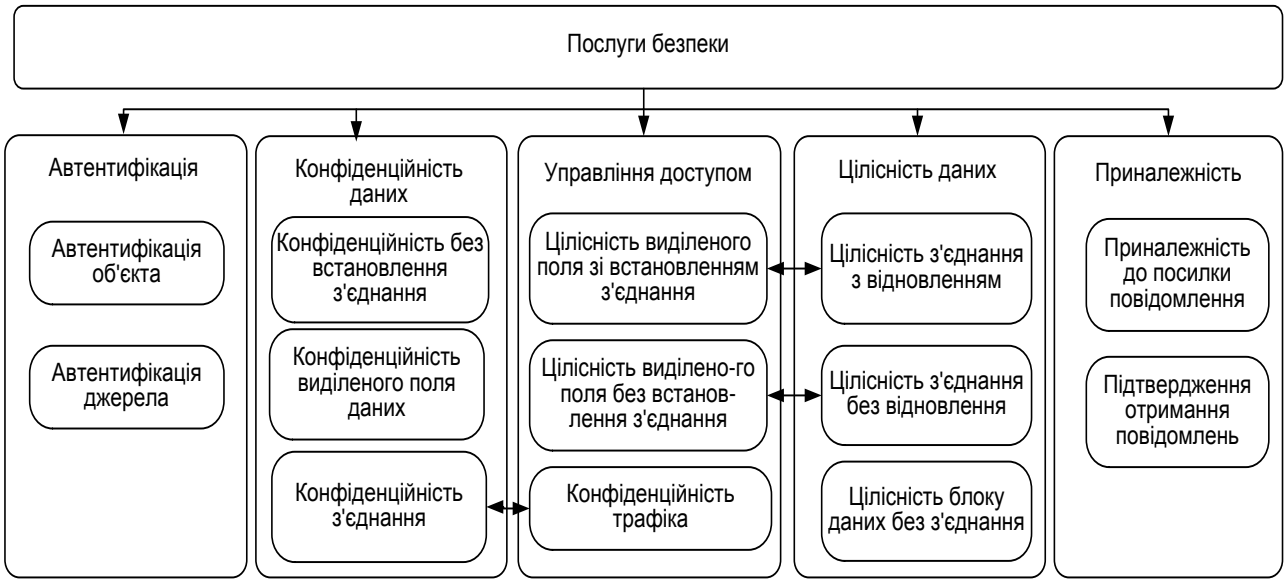


Рис. 3.6. **Послуги інформаційної безпеки**

Так, відповідно до вимог міжнародних стандартів в області криптографії (ISO 7498, ISO/IEC 10181) визначено п’ять базових послуг безпеки: автентифікація, конфіденційність даних, управління доступом, цілісність даних і приналежність [2; 61].

Кожна послуга інформаційної безпеки повинна бути забезпечена певним механізмом. Згідно з основними положеннями сучасної теорії захисту інформації для забезпечення послуг безпеки використовуються різні криптографічні механізми [2; 37; 197] (рис. 3.7).

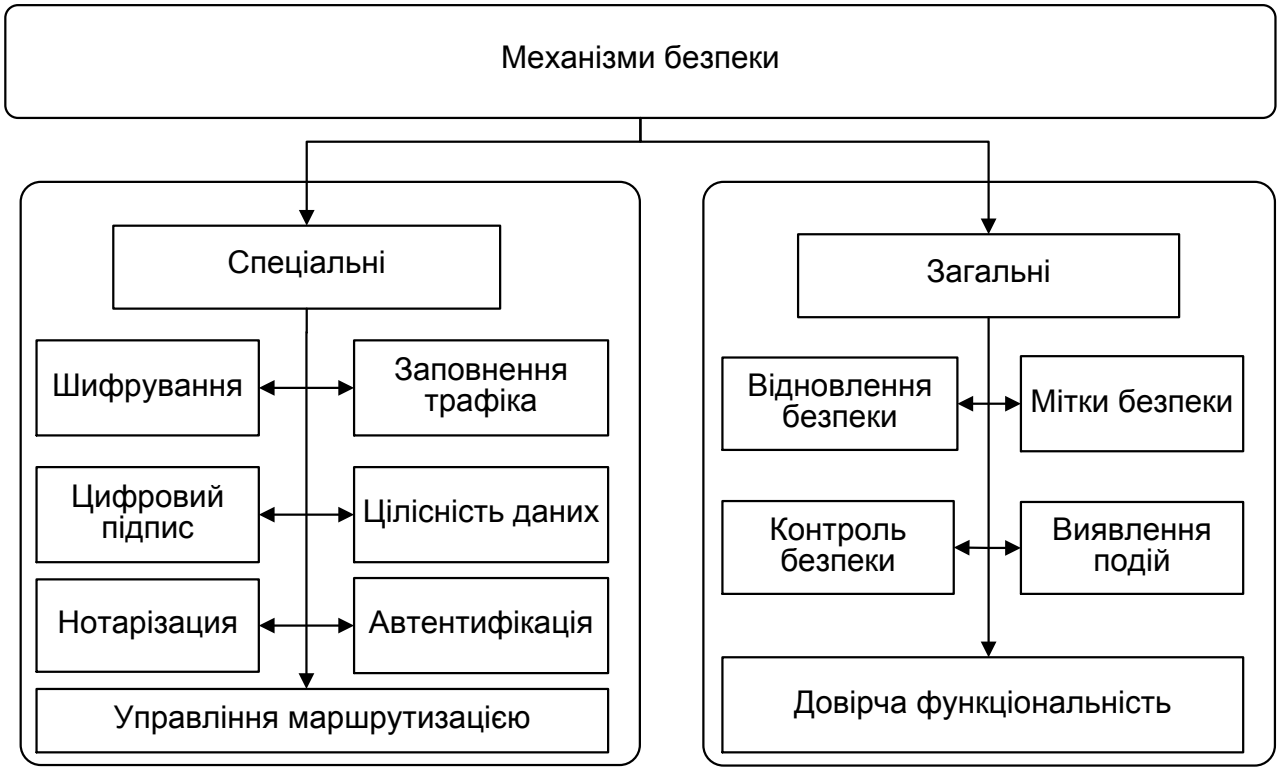


Рис. 3.7. **Механізми інформаційної безпеки**

Зображені на рис. 3.7 механізми інформаційної безпеки орієнтовані на забезпечення ефективного і необхідного рівня інформації, що передається.

У зв’язку з цим до сучасних систем інформаційної безпеки пред’являються вимоги, які повинні забезпечувати такі послуги та механізми забезпечення автентичності інформації згідно з ISO 7498-2 наведені на рис. 3.8.

На рис. 3.9 подані результати аналізу можливості несанкціонованого доступу до елементів підсистем ВПС на основі реалізації відповідних загроз.

Рис. 3.8. **Послуги і механізми забезпечення автентичності**

Проведений аналіз рис. 3.9 показав, що внутрішні загрози є однією з найбільш актуальних проблем інформаційної безпеки. Згідно зі статистикою, неправомірні дії співробітників та обслуговуючого персоналу організацій завдають найбільшої шкоди і до 90 % коштів, що виділяються на інформаційну безпеку, витрачається на забезпечення захисту від внутрішніх атак [107; 326]. Неправомірні дії користувачів призводять до значної шкоди та поділяються на:

порушення конфіденційності даних;

крадіжку інформації;

спотворення інформації;

дії, що призводять до збоїв інформаційних систем;

втрату інформації.

Відповідно до міжнародних стандартів ISO 7498, ISO/IEC 10181 для забезпечення необхідних показників безпеки визначено п’ять базових загальноприйнятих послуг, основними з яких є лише дві: автентичність і цілісність, для їх забезпечення використовуються механізми безпеки,

більшість з яких реалізується на основі криптографічних методів перетворення інформації.

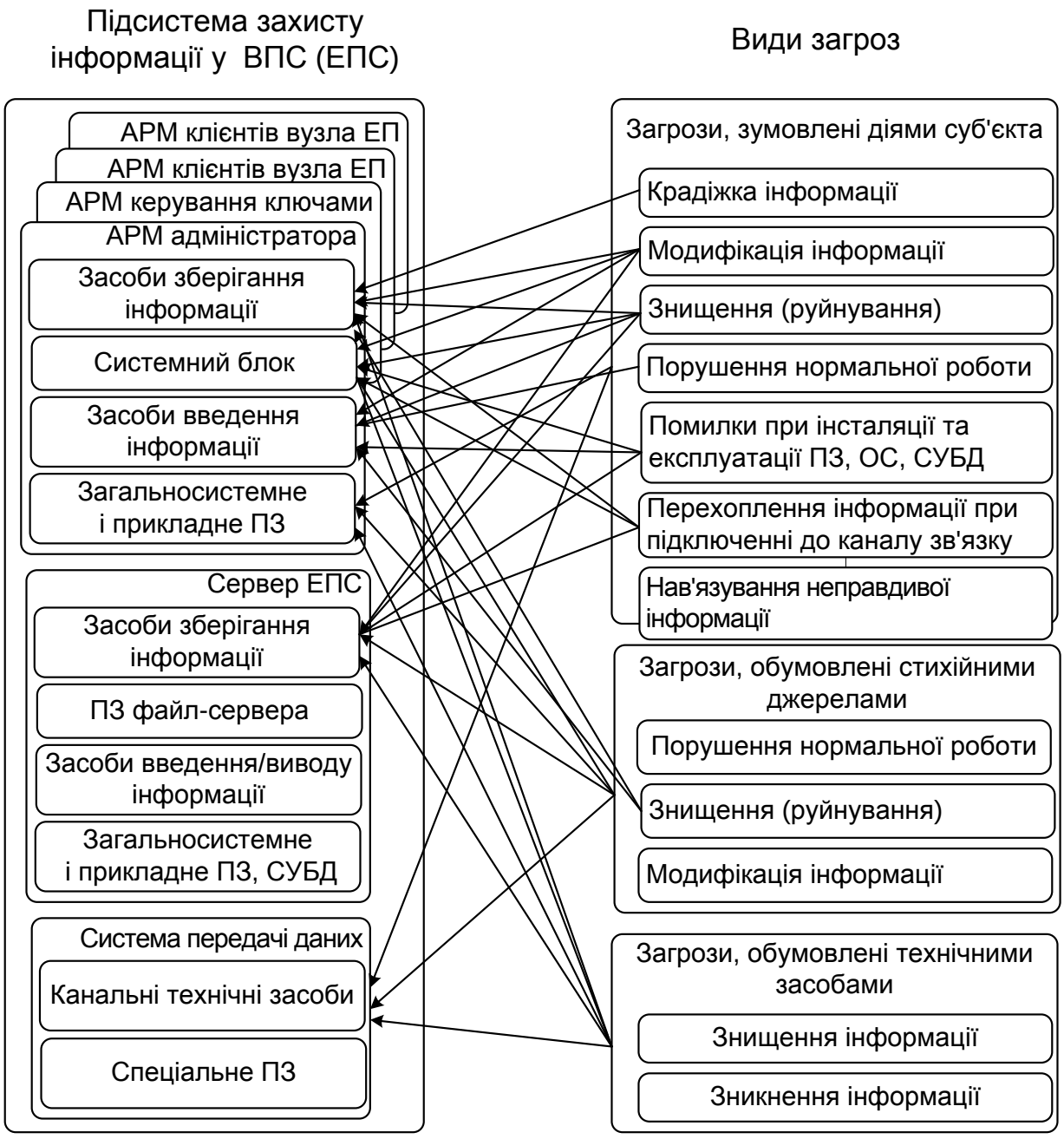


Рис. 3.9. **Аналіз можливості несанкціонованого доступу до елементів ВПС на основі реалізації відповідних загроз**

Основні механізми забезпечення цілісності та автентичності інформації у ВПС на різних рівнях засновані на використанні стандартів блочно-симетричних шифрів (DES, ГОСТ 28147-89). Прикладом програмної реалізації розглянутих механізмів є програмні засоби криптографічного захисту інформації "Грифон-Б" та "Грифон-Л" призначених для криптографічного захисту конфіденційної інформації в автоматизованих банків-

ських системах [219; 239]. Програмний засіб "Грифон-Б" призначено для криптографічного захисту конфіденційної інформації в автоматизованих банківських системах і застосовується для обміну інформацією всередині корпоративної мережі банку, з клієнтами, що працюють з системою "Клієнт-Банк", у системах обслуговування пластикових карт [107]. Програмний засіб криптографічного захисту інформації "Грифон-Л" [101] призначене для використання у сфері банківської діяльності, зокрема, для обміну конфіденційною (у тому числі фінансової) інформацією всередині корпоративної мережі банку, з клієнтами, які працюють за системою "Клієнт-Банк", у системах обслуговування пластикових карт та ін.

Основні технічні характеристики даних програмних засобів захисту наведені в табл. 3.1.

Таблиця 3.1

Основні характеристики програмних засобів захисту

Характеристики	"Грифон-Б"	"Грифон-Л"
Основні функції програми	Тест гешування, у тому числі шифрування простою заміною. Одержання чисел p, q (512 біт і 1024 біт). Тест створення і перевірки ЕЦП. Тести швидкодії (шифрування, гешування, генерації чисел, ЦП). Просте і адресне шифрування рядка або файла. Гешування рядка або файла. Генерація загальносистемних параметрів. Генерація ключа користувача. Зміна пароля на секретному ключі. Підпис рядка або файла. Загальний секретний ключ за Діффі-Хеллманом	
Стандарти	ГОСТ 28147-89. Алгоритм криптографічного перетворення. ГОСТ 34.311-95. Функція гешування. ГОСТ 34.310-95. Процедура вироблення і перевірки електронного підпису на базі асиметричного криптографічного алгоритму. Схема розподілу ключів Діффі-Хеллмана. Стандарт X9.17 для генерації сеансових ключів	
Швидкодія на ПК з процесором 633 МГц забезпечує	Шифрування області пам'яті в режимі простої заміни – не менш 5 Мб/с; гешування області пам'яті – не менш 1.5 Мб/с; обчислення ЦП – не більше 0.015 с; перевірка ЦП – не більше 0.020 с; генерація загального ключа за методом Діффі-Хеллмана – не більше 0.015 с	Шифрування області пам'яті в режимі простої заміни – не менш 2.5 Мб/с; гешування області пам'яті – не менш 1 Мб/с; обчислення ЦП при довжині ключа 512 біт – не більше 0.02 с; перевірка ЦП – не більше 0.03 с; генерація загального секретного – не більше 0.02 с

На рис. 3.10 наведений взаємозв’язок між механізмами і вживаними стандартами у підсистемі безпеки ВПС.

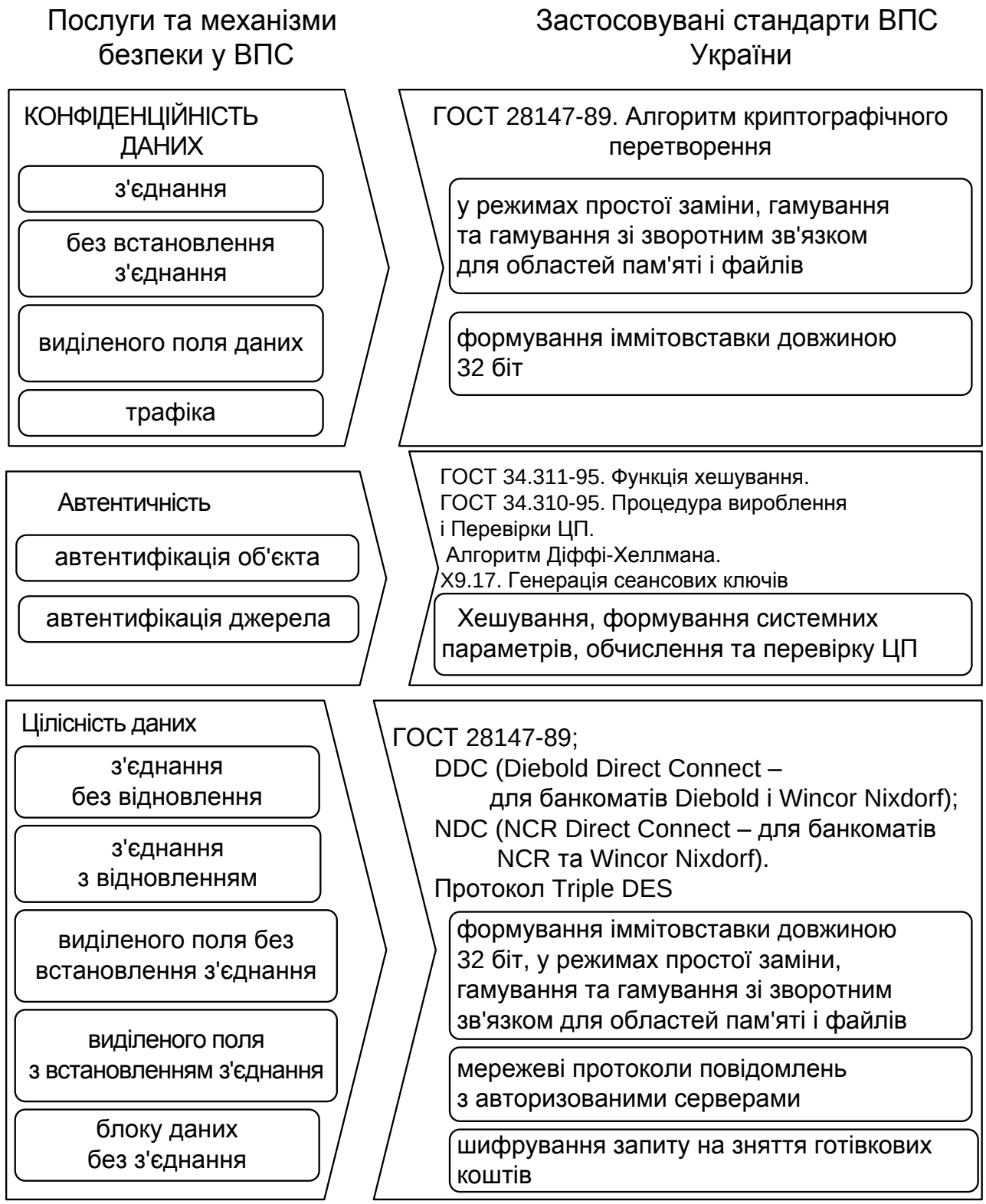


Рис. 3.10. **Взаємозв'язок між механізмами і вживаними стандартами у підсистемі безпеки ВПС**

Проведений аналіз стандартів показав, що для забезпечення конфіденційності, автентичності та цілісності використовується БСШ Російський ГОСТ28147-89 [243; 325] – застарілий алгоритм симетричного шифрування, розроблений в 1989 році, крім того крипостійкість БСШ, ґрунтується на криптостійкості S-боксів, які для даного шифру "надходять" з Російської Федерації, що істотно впливає на безпеку ВПС в цілому. На сьогоднішній день в Україні немає національних стандартів на алгоритми БСШ та формування геш-функцій, які використовуються в електронних цифрових підписах, що не дозволяє використовувати свій національний стандарт ДСТУ-4145 для забезпечення ЕЦП і БСШ, що обробляються в автоматизованих ВПС.

Таким чином, проведені дослідження показали, що подальший розвиток обчислювальних і IT-технологій призводять не тільки до збільшення зростання транзакцій та грошового обігу через банкомати та інші системи віддаленого користування ВПС, розширення послуг, що надаються через ВПС населенню, але і модернізації старих, появи нових видів загроз на елементи ВПС.

Для забезпечення безпеки банківської інформації у ВПС використовуються криптографічні симетричні і асиметричні алгоритми шифрування, які пройшли стандартизацію і сертифікацію на державному рівні. Однак відсутність Доктрини інформаційної безпеки, сертифікованих національних стандартів з основним спеціальним механізмам безпеки не дозволяють використовувати сучасні національні алгоритми, що забезпечують конфіденційність, автентичність і цілісність повідомлень, що істотно впливає на ступінь захисту інформаційних ресурсів від несанкціонованого доступу, забезпечення безпеки інформаційних і телекомунікаційних систем, як вже розгорнутих, так і створюваних на території держави, і в цілому на рівень забезпечення національної безпеки держави.

3.2. Дослідження механізмів забезпечення цілісності і автентичності інформації в автоматизованих банківських системах

Розглянуто основні механізми забезпечення цілісності та автентичності даних, які обробляються та передаються в ВПС. Наведено

загальну класифікацію кодів цілісності даних (MDC-кодів) й кодів автентичності повідомлень (MAC-кодів), аналізуються їх основні характеристики щодо забезпечення інформаційної безпеки даних на основі результатів оцінок криптографічного конкурсу NESSIE. Розглянуто основні моделі побудови MAC-кодів.

Саме питання забезпечення цілісності й автентичності інформації в сучасних банківських мережах є досить актуальним сьогодні. Оскільки методи криптоаналізу постійно вдосконалюються, потрібно проводити аналіз існуючих методів забезпечення автентифікації для усунення недоліків.

Широко поширені такі методи забезпечення автентичності повідомлення (рис. 3.11) [37; 61]: додавання до повідомлення коду автентифікації повідомлення (message authentification code, MAC-код) або зашифрованої контрольної суми; введення цифрових підписів; контрольні суми, контроль CRC, гешування і цифровий підпис – базові засоби автентифікації при цифровій передачі даних.

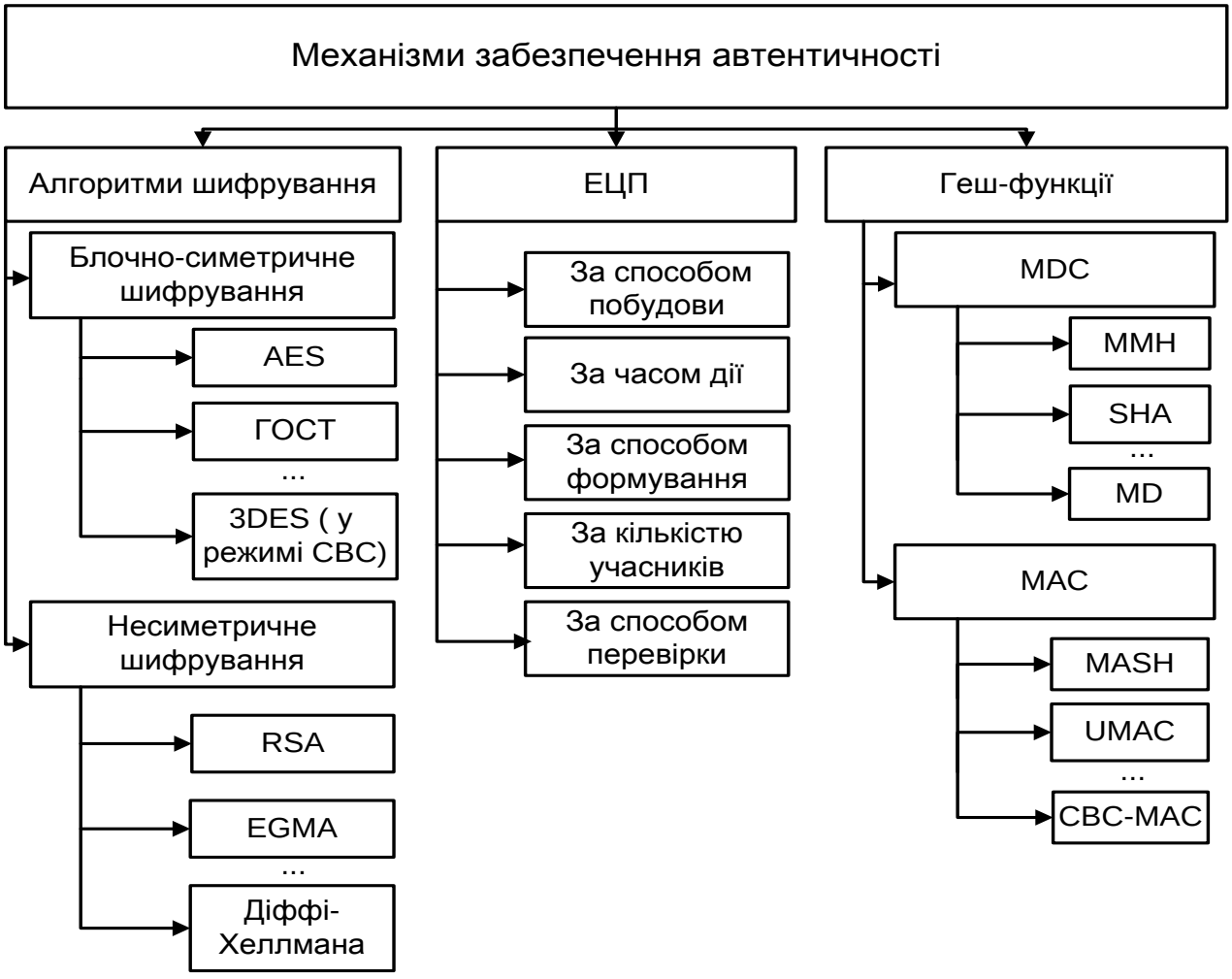


Рис. 3.11. **Механізми перевірки автентичності інформації**

Класифікацію засобів перевірки цілісності інформації наведено на рис. 3.12.

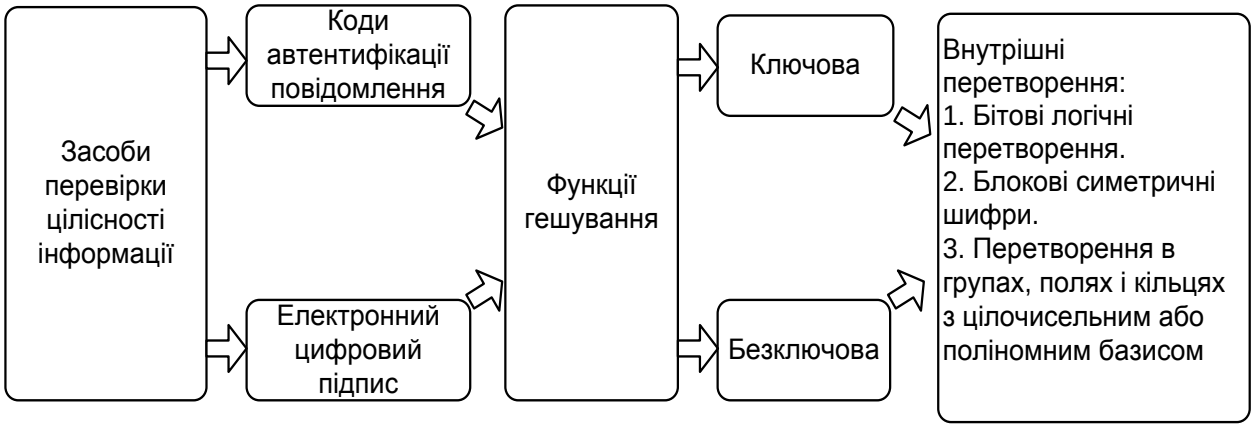


Рис. 3.12. **Класифікація засобів перевірки цілісності інформації**

При розгляді стандартів ISO 7498-2 та ISO / IEC 10181 визначено, що одним із найнадійніших способів вирішення завдань, пов'язаних з автентичністю (процедура встановлення достовірності твердження про те, що об'єкт (або суб'єкт) володіють заявленими властивостями) даних і джерел повідомлень, є процедури цифрового підпису, побудовані на основі асиметричних криптографічних алгоритмів [197; 239]. ЕЦП є рядком даних, який залежить від деякого секретного параметра (ключа), відомого тільки особі, що підписує, і від вмісту підписуваного повідомлення, представленого в цифровому вигляді [101; 326].

Таким чином, електронний цифровий підпис (ЕЦП) – це реквізит електронного документа, призначений для захисту даного електронного документа від підробки, отриманий у результаті криптографічного перетворення інформації з використанням закритого ключа електронного цифрового підпису, що дозволяє ідентифікувати власника сертифіката ключа підпису, а також установити відсутність перекручування інформації в електронному документі.

Система ЕЦП включає дві процедури: процедуру генерації підпису та процедуру верифікації підпису. У процедурі генерації підпису використовується секретний ключ відправника повідомлення, в процедурі верифікації підпису – відкритий ключ відправника. Секретний ключ

зберігається абонентом в таємниці і використовується ним для формування ЕЦП. Відкритий ключ відомий всім користувачам мережі [203; 223].

Достатньо ефективним механізмом для забезпечення автентичності повідомлень та процедури верифікації підпису є однонаправлені геш-функції.

Класифікація геш-функцій показана на рис. 3.13.

До безключових геш-функцій відносяться коди виявлення змін повідомлення (MDC-код, modification detection code), також відомі як коди виявлення маніпуляцій над повідомленнями або коди цілісності повідомлень. MDC-коди призначені для формування стислого образу або геш-коду повідомлення, який задовольняє спеціальні властивості. Вони поділяються на блочні шифри та модульну арифметику. Зрештою MDC-коди забезпечують, спільно з іншими механізмами, цілісність даних.

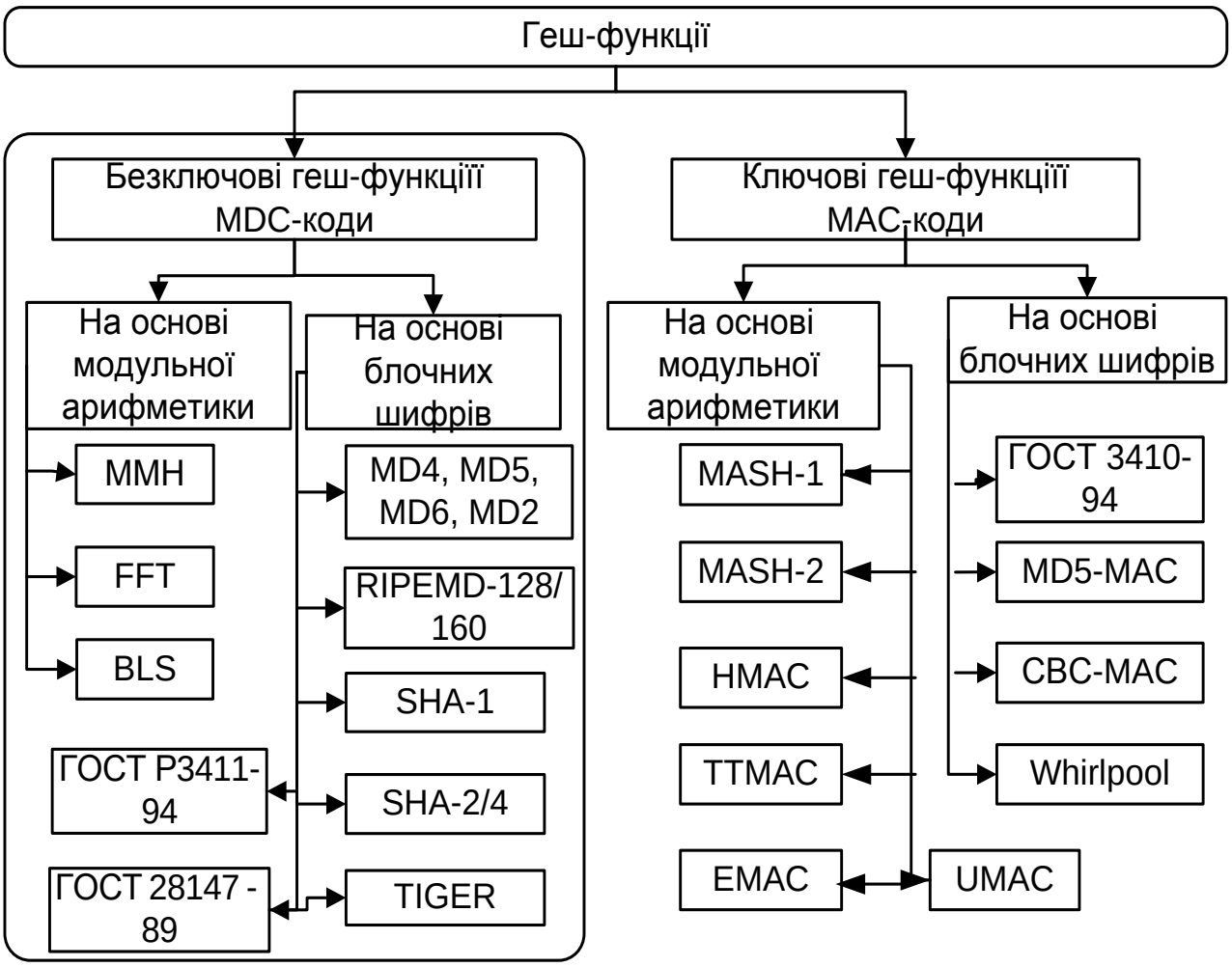


Рис. 3.13. **Класифікація геш-функцій**

Порівняльна характеристика безключових геш-функцій наведена в табл. 3.2.

Таблиця 3.2

Порівняльна характеристика безключових геш-функцій

Характеристика	MD5	MD6	SHA-1	SHA-2 (256/512)	ГОСТ 28147-89	RIPEMD-128	RIPEMD-160
Довжина дайджесту, біт	128	512	160	256/512	256	128	160
Розмір блоку обробки, біт	512	512	512	512/1024	512	512	512
Кількість ітерацій	64	168	80	64/80	32	128	160
Кількість елементарних логічних функцій	4	4	3	6/6	8	5	5
Кількість додаткових констант	64	–	4	64/64	–	4	9
Швидкість роботи на Pentium III, Мбіт/с	574,6	–	344,4	135,5 / 68,7	315,27	63.8	39.8

Аналіз табл. 3.2 показує, що суттєвим недоліком безключових геш-функцій є те, що вони не захищені від можливості підбору такого ж самого повідомлення з однаковим гешем, та мають відсутність властивості обчислювальної стійкості. Зрештою MDC-коди забезпечують, спільно з іншими механізмами, цілісність даних.

До ключових геш-функцій відносяться MAC-коди. MAC-коди призначені для забезпечення цілісності даних і автентифікації повідомлень без використання яких-небудь інших механізмів і дозволяють забезпечити автентифікацію повідомлення на основі використання методів симетричної криптографії. Алгоритми формування MAC-кодів розглядаються як геш-функції з двома вхідними параметрами, а саме повідомленням і секретним ключем. На виході такого алгоритму формується двійковий рядок фіксованої довжини. При цьому на практиці неможливо сформувати точно такий же рядок без знання ключа.

Існують три загальні підходи до побудови MAC-кодів [37].

MAC-коди, побудовані із застосуванням блокових шифрів (CBC-MAC).

MAC-коди, побудовані на основі безключових геш-функцій (HMAC, MDX-MAC).

MAC-коди, побудовані з використанням сімейства універсальних геш-функцій (UMAC).

Підходи до побудови MAC-кодів обумовлюють таку класифікацію MAC-кодів (рис. 3.14).

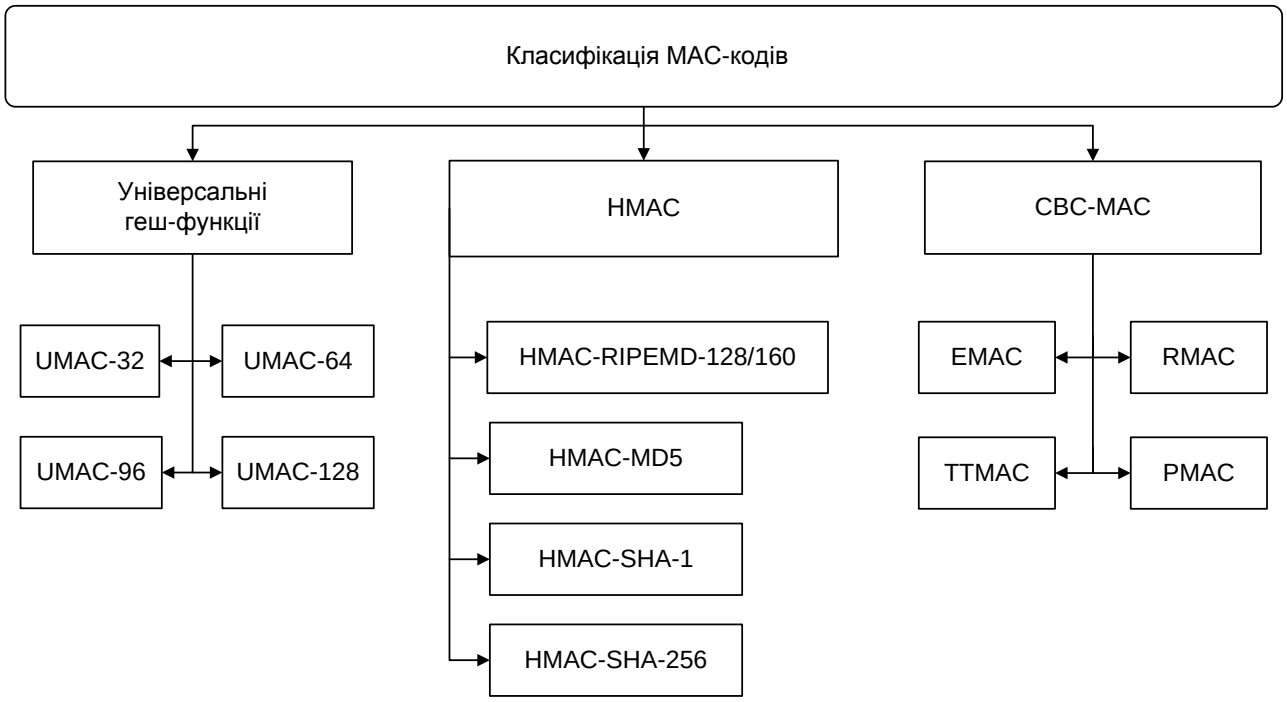


Рис. 3.14. **Класифікація MAC-кодів**

Результати досліджень у галузі захисту інформації, а також аналіз літератури [264; 288; 325; 326] показали, що одним з найбільш перспективних методів забезпечення цілісності та автентичності інформації є введення в інформацію надмірного коду на основі використання кодів автентифікації повідомлень (MAC-кодів), що дозволяє із заданою імовірністю встановлювати дійсність переданого повідомлення [61; 64].

Функції вироблення коду автентифікації повідомлень (MAC) є підкласом ключових геш-функцій і володіють додатковою властивістю обчислювальної стійкості. Функція гешування з секретним ключем h є функцією вироблення MAC-коду, якщо виконуються вимоги стискування, обчислювальної простоти (при відомому сеансовому ключі) і обчислювальної стійкості.

Обчислювальна стійкість – це неможливість знаходження геш-значення для заданого повідомлення без відомого секретного ключа, тобто для заданої ключової геш-функції h і одній або коректнішій з пар прообразів і геш-значень (x_i,$h(x_i,k)$) і невідомому секретному ключу k обчислювально неможливо знайти іншу коректну пару (x,h(x,k)) для будь-якого $x \neq x_i$.

Вимога обчислювальної стійкості припускає виконання вимоги стійкості ключа (за однією або коректнішою парою прообразів і геш-значення (x_i,$h(x_i,k)$) обчислювально неможливо відновити секретний ключ k), проте, вимога стійкості ключа не припускає виконання вимоги обчислювальної стійкості.

Для визначення і оцінки якості криптопримітивів у січні 2000 року в Бельгії почався трирічний європейський криптопроект NESSIE (New European Schemes for Signatures, Integrity, and Encryption), метою якого був відбір криптографічних алгоритмів, на базі яких, теоретично, повинні формуватися майбутні криптостандарти Європи.

Основними завданнями проекту NESSIE є відбір кращих десяти криптографічних примітивів. У цей набір входять алгоритми блокового і потокового шифрування, генератори випадкових чисел, схеми швидкої автентифікації даних (MAC), геш-функції і алгоритми цифрового підпису. У якості основних критеріїв відбору претендентів обрані реальна безпека, продуктивність, гнучкість і вимоги ринку.

Перевагою MAC є те, що він дозволяє одночасно отримати і перевірити інформацію за допомогою того ж секретного ключа. Це означає, що відправник і одержувач повідомлення повинні домовитися про ключ до початку повідомлення, як це має місце у випадку з симетричним шифруванням.

Код автентифікації повідомлення (MAC) є коротким фрагментом інформації, який використовується для перевірки достовірності повідомлення. MAC (Message Authentication Code) – код перевірки повідомлення, який використовує функцію відображення і надає дані у вигляді значень фіксованого розміру, а потім гешує саме повідомлення [61].

Алгоритм MAC приймає як введення секретний ключ і повідомлення достовірності довільної довжини і видає MAC-код, який захищає цілісність повідомлення, а також його автентичність, дозволяючи контролерам (які також володіють секретним ключем) виявляти які-небудь зміни в первинному змісті повідомлення, яке передається.

Алгоритм MAC-коду працює таким чином, що перші блоки відкритих даних, які беруть участь у виробленні MAC-коду, можуть містити службову інформацію (наприклад, адресну частину, час, синхропосилання) і не зашифровуватися.

Головною перевагою цього механізму при порівнянні з електронно-цифровим підписом є більш простий алгоритм генерації та верифікації, який дозволяє забезпечити високу швидкодію алгоритмів автентифікації повідомлень у локальних мережах та комп'ютерних системах [37].

Загальний принцип роботи MAC-кодів наведено на рис. 3.15.

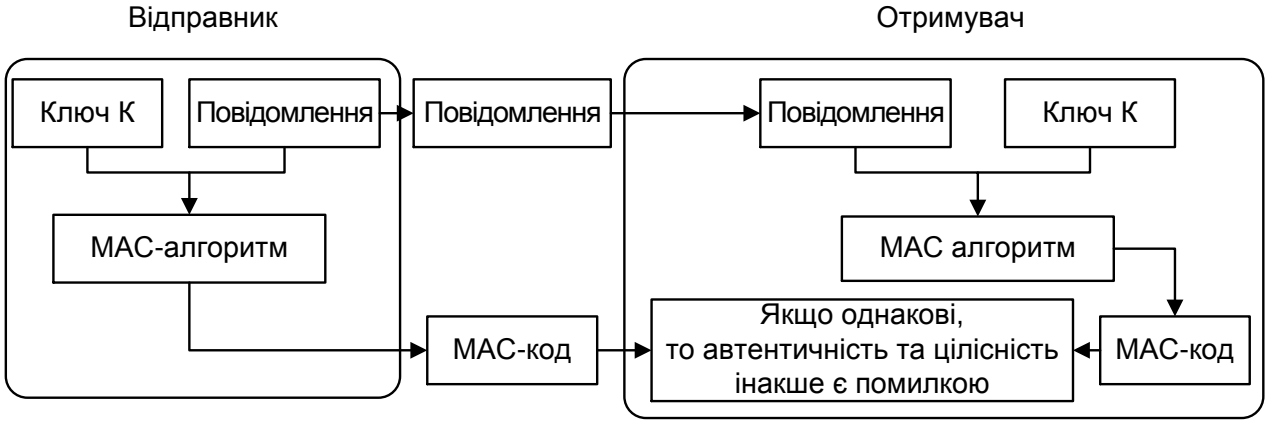


Рис. 3.15. **Принцип роботи MAC-алгоритмів**

MAC-алгоритми можуть бути виготовлені з інших криптографічних примітивів, таких, як криптографічні геш-функції (як у випадку з UMAC), або для блокових алгоритмів шифрування (OMAC, CBC-MAC і PMAC).

Для вивчення основних характеристик MAC-кодів і їх порівняльного оцінювання в науково-дослідному проекті NESSIE (IST-1999-12324) були розглянуті основні практичні алгоритми MAC-кодів і відібрані чотири кращі:

Two-Track-MAC: K.U.Leuven, Бельгія і Debis AG, Німеччина;

TTMAC (також відомий як Two-Track-MAC) має найвищий рівень безпеки MAC примітивів розглянутих у NESSIE. Дизайн TTMAC заснований на геш-функції RIPEMD-160 (з невеликими змінами). Безпека може бути доведена в припущенні, що основна функція стиснення є псевдовипадковою. TTMAC має конкретне виконання переваги: вона особливо ефективна в разі коротких повідомлень, а також має оптимальну спритність ключів.

CBC-MAC (ISO/IEC 9797-1), до яких відносяться EMAC та RMAC;

EMAC (також відомий як DMAC) має таку перевагу, що дозволяє повторне використання існуючих блокових шифрів реалізації (у CBC-режимі з додатковим шифруванням у вигляді перетворення на виході). Безпека може бути доведена в припущенні, що основний блоковий шифр є псевдовипадковим. Продуктивність і спритність ключів є розумними (EMAC кращий для коротких повідомлень, оскільки довжина блоку менша порівняно зі схемами, заснованими на геш-функції). NESSIE рекомендує використовувати цю конструкцію з 128-бітним блоковим шифром, включеним в NESSIE.

HMAC (ISO/IEC 9797-1);

HMAC має таку перевагу, що дозволяє повторне використання існуючих реалізацій геш-функції. Безпека може бути доведена на таких припущеннях: основна геш-функція стійка до колізій з невідомим початковим значенням; функція стиснення забезпечена ключами на початкове значення безпечного MAC примітиву (для повідомлень з одного блоку); функція стиснення є слабкою псевдовипадковою функцією. Ці припущення слабкіші, ніж припущення, необхідні для TTMAC і EMAC. Продуктивність і спритність ключів є розумними. NESSIE рекомендує використовувати цю конструкцію з колізіонно-стійкою геш-функцією, включеною в NESSIE.

UMAC: розробка корпорації Intel (США), Університету з штату Невада в Рено (США), Науково-дослідної лабораторії IBM (США), Technion (Ізраїль) і Університету з Каліфорнії в Девісі (США);

Для перевірки автентичності довгого потоку повідомлень UMAC на сьогоднішній день є найшвидшим з MAC примітивів розглянутими NESSIE (за рахунок більшої складності і гіршої спритності ключів порівняно з іншими примітивами). UMAC заснований на універсальному сімействі геш-функцій й доказовою безпекою: розрив примітиву означатиме і розрив блокового шифру, який використовується в схемі як псевдо-випадкова функція (поточна специфікація в якості блокового шифру вибирає AES).

Основними характеристиками алгоритмів формування MAC-кодів, за якими виконується їх порівняльна оцінка відповідно до рекомендацій проекту NESSIE є:

рівень захищеності MAC кодів від загальних атак;

швидкодія алгоритмів формування MAC-кодів;

статистичні властивості розподілів MAC-кодів.

У табл. 3.3 наведено аналіз тестування швидкості роботи алгоритмів гешування.

Таблиця 3.3

Аналіз тестування швидкості роботи алгоритмів гешування

Функція гешування	Кількість циклів	Мова реалізації	Швидкість роботи на Celeron 600 MHz	Швидкість роботи на Pentium III 1000 MHz
ГОСТ 34311-95	–	C + ASM	49,408 Мбіт/с	83,056 Мбіт/с
UMAC	–	C C + ASM	989,371 Мбіт/с 3518,900 Мбіт/с	1648,953 Мбіт/с 5885,057 Мбіт/с
Rijndael CBC-MAC	14	C	139,376 Мбіт/с	231,255 Мбіт/с
ГОСТ 28147-89 (OFB)	16	C + ASM	189,559 Мбіт/с	315,270 Мбіт/с

Проведений аналіз показав, що найбільш перспективним алгоритмом обробки інформації є UMAC, який забезпечує обробку величезних розмірів даних за секунди (10^9 біт/с). При додатковому використанні алгоритму AES, вірогідність зламу значно зменшується.

Порівняльні дослідження методів безпечного гешування, представлених на конкурс NESSIE

В Європі в рамках проекту NESSIE (New European Schemes for Signature, Integrity, and Encryption) проходив конкурс на розробку європейських криптографічних стандартів. Як відомо, у 2001 році в США за результатами конкурсу, організованого Національним інститутом стандартизації та технологій США, був прийнятий новий стандарт блочного шифрування AES-Rijndael. Цей алгоритм був визнаний після дворічних досліджень і відкритого обговорення в рамках проекту AES (Advanced Encryption Standard) в якості кращого і в даний час прийнятий в якості федерального стандарту США (FIPS 197) [325].

Проект AES як концептуальний підхід до розробки якісних криптографічних примітивів показав досить високу ефективність у широкому

сенсі. Саме тому європейське співтовариство пішло по цьому шляху для розробки нових європейських стандартів.

Одними з криптографічних примітивів, що висувалися на конкурс NESSIE, були алгоритми формування MAC-кодів та геш-функцій.

Головні критерії відбору, які використовувались на конкурсі:

безпека – найважливіший критерій, тому що безпека алгоритмів шифрування – головне призначення цих алгоритмів. Процес оцінки безпеки враховував і вплив подій поза проектом NESSIE (таких, як нові напади або методи аналізу);

ринкові вимоги пов'язані з потребою в алгоритмі, його зручності і простоті використання, можливості міжнародного використання;

продуктивність алгоритму шифрування на певному обладнанні. Для програмного забезпечення розглядали 8-бітові процесори (як в недорогих платіжних картках з вбудованим мікропроцесором), 32-бітові процесори (наприклад, старе сімейство Pentium), сучасні 64-бітові процесори;

гнучкість алгоритму.

Нині в Україні інтенсивно впроваджуються різні системи електронного документообігу. Обов'язковим їх реквізитом є наявність ЕЦП, при виробленні якого, в свою чергу, використовується функція гешування. З цією метою використовується міждержавний стандарт ГОСТ 34.311-95 [59; 344]. Розглядаються питання гармонізації та використання функцій гешування, що визначені в ISO/IEC 10118, перше за все SHA-2. Але, фундаментальним вирішенням проблеми появи в Україні ефективного алгоритму або алгоритмів гешування, є врахування як теоретичних так і практичних результатів конкурсу NIST SHA-3 Competition.

На даний момент існує велика кількість криптографічних сервісів, які потребують різних ступенів захисту і відповідно різних довжин геш-значень, що передбачено, наприклад, у стандарті SHA-2 [283; 325]. Крім того, важливо мати можливість реалізації геш-функції на різних апаратних платформах, у тому числі з обмеженим об'ємом пам'яті та низькою розрядністю процесора (наприклад, смарт-картка). На рівні стандарту важливо, щоб один алгоритм поєднував у собі усі названі функціональні можливості. Наявність кількох стандартизованих алгоритмів ускладнює розробку інформаційно-телекомунікаційних систем і призводить до конфліктів між системами різних розробників.

Використовуючи досвід проведених та перспективних міжнародних конкурсів на нові криптографічні стандарти (NIST SHA-3 Competition, NESSIE), необхідно визначити мінімальний перелік вимог, якому має

відповідати геш-функція. Перелік вимог умовно поділяється на дві частини: вимоги до стійкості та вимоги до функціональності алгоритму. Вимоги до стійкості мають відповідати простому правилу – не повинно існувати жодної атаки на алгоритм складністю менше ніж атака "груба сила". Наступні критерії є ключовими для забезпечення захищеності, про що свідчать матеріали міжнародних конкурсів на нові криптографічні стандарти [37; 197; 239]:

складність знаходження колізії $2^{n/2}$;

складність відновлення прообразу 2^n ;

складність знаходження другого прообразу не менше 2^n ;

стійкість до атак length extension;

стійкість до усічених колізій;

стійкість до атак мультиколлізій;

відсутність атак розпізнавання для генераторів псевдовипадкових послідовностей, що використовують HMAC, побудованих на базі геш-функції зі складністю, меншою ніж знаходження другого прообразу і кількістю запитів до генератора не менше $2^{n/2}$;

надійність математичної бази.

Вимоги до функціональності алгоритму гешування формуються зважаючи на ймовірну галузь застосування. Перш за все, необхідно забезпечити сумісність нового стандарту з уже діючими на території України стандартами ЕЦП, а також передбачити можливість суміщення з рядом міжнародних стандартів та перспективних стандартів, що можуть бути прийняті в межах України.

Функціональність нового стандарту гешування має відповідати такому переліку вимог:

довжина виробленого геш-значення;

максимальна швидкодія;

максимальна кількість процесорів, що може бути ефективно використана для паралельних обчислень;

мінімальні вимоги до обчислювальних ресурсів;

можливість реалізації алгоритму на різноманітних програмних, програмно-апаратних та апаратних платформах;

простота архітектури алгоритму.

Новий національний стандарт, який має бути розробленій, планується використовувати у широкому колі криптографічних додатків, які висувають до нього ряд специфічних вимог технічного характеру. Галузь застосування нового алгоритму охоплює:

використання виробленого геш-значення у якості інструмента контролю цілісності інформації при передачі, зберіганні та розповсюдженні. Найбільш відомими прикладами є протоколи встановлення та розповсюдження ключів, механізми надання послуги неспростовності, асиметричні шифри, системи електронного цифрового підпису з додатком або відновленням повідомлення та ін.;

вироблення кодів автентифікації повідомлень за технологією HMAC;

використання геш-функції у якості генератора псевдовипадкових послідовностей.

Наведений перелік є нормальною міжнародною практикою використання геш-функцій як криптографічних алгоритмів для вирішення завдань криптографічного захисту інформації.

У фінальному звіті міжнародного криптографічного конкурсу NESSIE зазначена функція гешування Whirlpool (на основі власного вбудованого блочно-симетричного шифру) і відібрані чотири кращі алгоритми формування MAC-кодів: UMAC, Two-Track-MAC, CBC-MAC, HMAC [203; 325].

UMAC – код автентифікації повідомлення був розроблений Тедом Кроветцом (Ted Krovetz), Джоном Блеком (John Black), Шаї Халеві (Shai Halevi), Хьюго Кравцеком (Hugo Krawczyk) і Пилипом Рогевеєм (Phillip Rogaway) [288; 153]. Алгоритм заснований на сімействах універсальних геш-функцій і забезпечує доказову безпеку MAC-коду, безпека забезпечується стійкістю застосовуваного блочно-симетричного шифру (БСШ) AES у режимі CBC (зчеплення блоків відкритого тексту в другому шару функції UHASH-16 або UHASH-32).

На рис. 3.16 наведена модель роботи алгоритмів UMAC16/32.

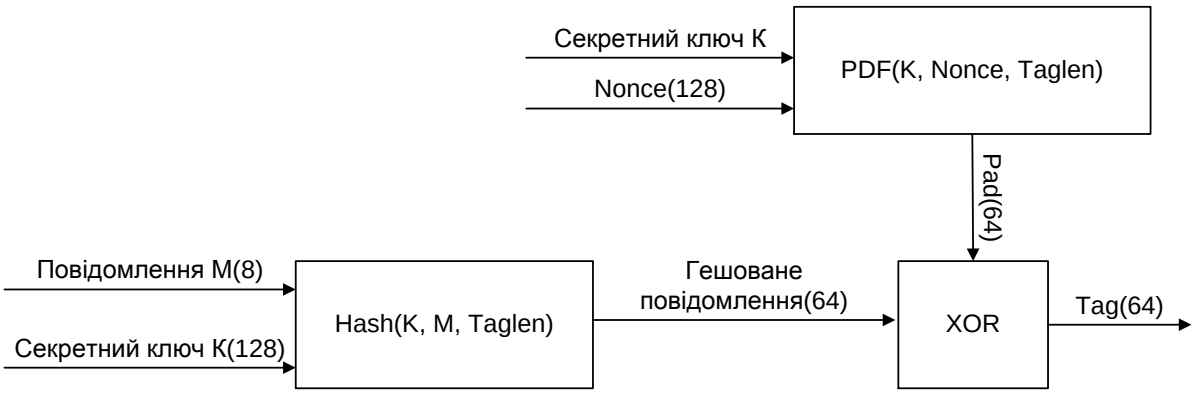


Рис. 3.16. **Модель роботи алгоритму UMAC16/32**

Алгоритм дозволяє забезпечити більш високу швидкість (особливо для довгих повідомлень) і підтверджувану безпеку ціною більшої складності.

Для опису процедур формування MAC-коду розглянемо UMAC (1999 року). Повідомлення M довільної довжини надходить на двошарову функцію UHASH, у якій на першому шарі за допомогою універсального класу геш-функцій NH повідомлення розбивається на блоки певної довжини (за винятком останнього блоку, що може мати меншу довжину). Кожен блок обробляється адитивним ключовим матеріалом (один ключ використовується для кожного блоку), процедура стиску здійснюється шляхом множення пари блоків повідомлення на ключ. Усі стислі блоки потім конкатенуються і довжина інформаційного блоку зростає до встановленого значення [283].

На другому шарі за допомогою функції PRF (псевдо довільної функції), використовуючи або режим CBC із БСШ AES, або використовуючи алгоритм HMAC, одержуємо MAC-код фіксованої довжини. Таким чином, сімейство універсальних геш-функцій NH використовується як прискорювач на HMAC або CBC-MAC.

Крім того, можна використати конструкцію Тойпліца (Toeplitz), для зниження ймовірності підробки (застосовуючи NH кілька разів із ключами, які перемішані між собою, і конкатенуючи результати), і/або використати дворівневе гешування для зменшення кількості необхідних ключів. Існують також деякі інші варіації, що дозволяють оптимізувати деякі види структур.

Значна частина обмежень UMAC (1999 року) виходить із того, що повідомлення стискається до встановленого коефіцієнта, а не встанов-

леної довжини. У першому випадку, код автентифікації обчислюється шляхом обчислення функції PRF(геш||залишок), у другому випадку може бути обчислений шляхом геш (PRF(залишок), що має деякі переваги (використання PRF обмежене мінімумом, у нього немає входу необмеженої довжини). NH, сімейство універсальних геш-функцій, використаних в UMAC (1999 року), могло також бути стисло до встановленої вихідної довжини, у цьому випадку потрібний буде ключ (згенерований PRG) довжиною, рівною повідомленню (ціле повідомлення повинне розглядатися як єдиний блок у даному описі) [61; 325; 326].

Версія UMAC (2000 року) є переможцем криптографічного європейського конкурсу NESSI, уводить додаткову складність для рішення проблеми стиску повідомлення до встановленої довжини так, що MAC може обчислюватися геш (PRF (залишок)). Частина PRF працює, кодуючи залишок блоковим шифром. Частина гешу (також називана UHASH) стискає повідомлення, що складається із трьох різних шарів:

на першому шарі використовується швидке сімейство геш-функцій NH для стиску повідомлення до встановленого коефіцієнта;

на другому шарі геш-коду установленої довжини використовується сімейство геш-функцій RP, що не так швидко, як NH, але генерує вихід установленої довжини з використанням ключа встановленої довжини (для цього використовується режим CBC БСШ AES);

на третьому шарі використовується сімейство геш-функцій IP, що зводить довжину свого входу до більш підходящого розміру.

Універсальне сімейство геш-функцій RP ґрунтується на поліноміальних обчисленнях. Рядок, що складається з n слів довжиною m біт може розглядатися як поліном ступеня n в області значень, де кожне слово рядка служить коефіцієнтом. Для обчислення гешу необхідно обчислити поліном для довільно обраної крапки (ключа).

Для ефективності обчислення виконуються в області максимальних значень, однак менше, ніж 2^m. Функція застосовується для розширення області до довільного рядка, при цьому використовується гібридна схема, у якій RP є поліноміальними геш-кодами: невеликий діапазон значень використовується для коротких повідомлень, а більший – для більше довгих повідомлень. З погляду безпеки, імовірність колізії трохи підвищується порівняно зі шаром універсального класу геш-функцій NH алгоритму [326].

Шар з універсальним сімейством геш-функцій IP скорочує довжину свого входу, оскільки слой гешу RP генерує виходи, що значно більші порівняно з передбачуваною ймовірністю колізій (для найдовших автентифікованих повідомлень більшість бітів вихідних рядків, шаруючись RP, будуть нулями).

Алгоритми UMAC16 і UMAC32 засновані на тришарових схемах гешу UHASH 16 і UHASH 32 відповідно і використовуються для кодування залишку БСШ AES (Rijndael). При цьому функція PRG, що обчислює із ключа користувача, одержує ключове значення, необхідне у внутрішній операції UHASH і також заснована на AES, у режимі зворотного зв'язку.

UHASH 16 використовує 16-бітові слова, подаючи їх як підписані цілі. Шар гешу NH діє на блоках 2 Кб, стиснутих в 32-бітові величини (відповідає коефіцієнту стиску 512). Імовірність помилки виявилася не більше 2^{15}. Результат проходить шар гешу RP, що обчислює вихідний рядок установленої довжини 128 біт. Сімейство геш RP є конструкцією, що використовує три області значень із 32-бітовими, 64-бітовими і 128-бітовими первинними модулями відповідно. Довжина повідомлення обмежується максимумом 2^{64} біт, і доведено, що цей шар значно збільшує ймовірність зіткнення (близько 2^{19}). Якщо автентифіковане повідомлення досить невелике, по-перше, відпадає необхідність у шарі RP і цей шар пропускається як оптимізація. Шар гешу IP додає своє 128-бітове уведення до 16-бітового виходу, створюючи ймовірність зіткнення майже 2^{15}. Тришарова конструкція повторюється множиною разів з незалежними ключами для збільшення довжини коду автентифікації та зниження шансів підробки MAC-коду. За замовчуванням кількість повторень – чотири рази, і додавання 16-бітових вихідних величин дає 64-бітовий MAC-код з імовірністю підробки 260.

Основні розходження з алгоритмом UHASH 32 полягають у використовуванні 32-бітових слів і дворазовому повторенні тришарових схем (за замовчуванням). Це дає різні можливості на практиці (використання більшої множини значень), але аналіз, головним чином, залишається колишнім.

Переваги перед попередньою версією UMAC (1999 року) полягає у використовуванні мінімізованого шифрувального примітива (AES), що (у результаті) дає більшу ефективність для коротких повідомлень і забезпечує додаткову гнучкість верифікації: можна вибрати кількість пара-

лельних ітерацій в обчисленні MAC, тим самим варіюючи обчислювальним часом для забезпечення заданого рівня безпеки.

Two-Track-MAC – код автентичності повідомлення, призначений для перевірки достовірності і цілісності переданих даних. Основною його метою є запобігти змінам повідомлень третьою стороною під час передачі.

В основі Two-Track-MAC лежить геш-функція RIPEMD-160. Її особливість полягає в шифруванні повідомлення за двома незалежними шляхами (на рис. 3.17 позначені як L і R). Такий підхід дозволяє збільшити розмір внутрішнього стану. У результаті чого отримаємо більше можливих значень внутрішньої функції шифрування. Це дозволяє ускладнити атаки, засновані на переборі всіляких значень.

Порівняно з MDx-MAC, який так само заснований на RIPEMD-160 Two-Track-MAC набагато ефективніше для коротких повідомлень (512 або 1024 біт), і також ефективніше на довгих повідомленнях.

Іншою важливою перевагою TTMAC є можливість швидкої зміни ключа шифрування. Це дозволяє збільшити стійкість системи без зниження швидкості. При досить частій зміні ключа зловмиснику не вдасться зібрати великої кількості пар повідомлення – MAC-код, що дуже знижує ймовірність підбору ключа або MAC-коду.

Модель роботи алгоритму Two-Track-MAC наведена на рис. 3.17.

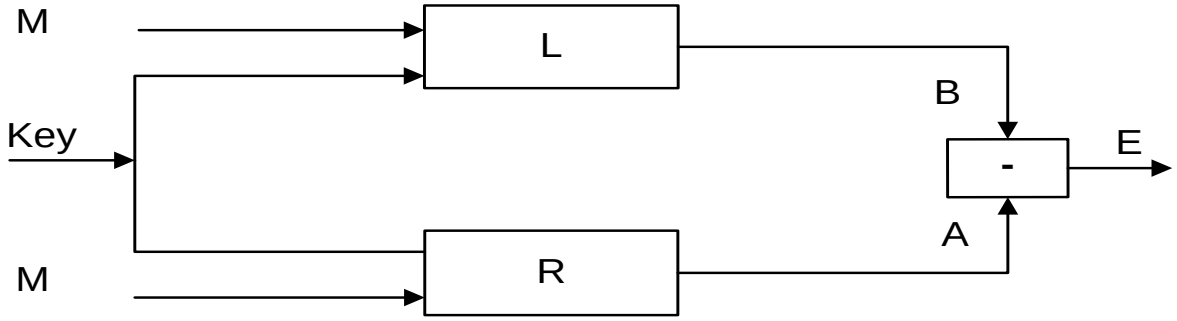


Рис. 3.17. **Модель роботи алгоритму Two-Track-MAC**

CBC-MAC (ISO/IEC 9797-1), до яких відносяться EMAC та RMAC.

Блоковий шифр E є функцією $E : K_E \cdot \{0,1\}^n \rightarrow \{0,1\}^n$, де кожна E (K, •) = Ek (•) є перестановкою на $\{0,1\}^n$, K_E це безліч можливих ключів, а n довжина блоку.

CBC MAC найбільш простий і добре відомий алгоритм, щоб зробити MAC з блочного шифру E. Нехай M = M [1] ◦ M [2] ◦ … ◦ M [m] буде рядком повідомлення, де | M [1] | = | M [2] | = … = | M [m] | = n. Тоді CBC_K (M), CBC MAC з M з ключами K, визначається як Y [m], де Y [i] = E_K (M [i] $\oplus$ Y[i –1]) для i = 1,..., m і Y [0] = 0^n.

У наявних реалізаціях MAC-алгоритмів CBC MAC Bellare, Kilian, і Rogaway запропонували EMAC.

EMAC (також відомий як DMAC) має таку перевагу, що дозволяє повторне використання існуючих блокових шифрів реалізації (у CBC-режимі з додатковим шифруванням у вигляді перетворення на виході). Безпека може бути доведена в припущенні, що основною блоковий шифр є псевдовипадковим. Продуктивність і спритність ключів є розумними (EMAC кращий для коротких повідомлень, оскільки довжина блоку менша порівняно зі схемами, заснованими на геш-функції). NESSIE рекомендує використовувати цю конструкцію з 128-бітним блоковим шифром, включеним у NESSIE.

Модель роботи алгоритму CBC-MAC наведено на рис. 3.18.

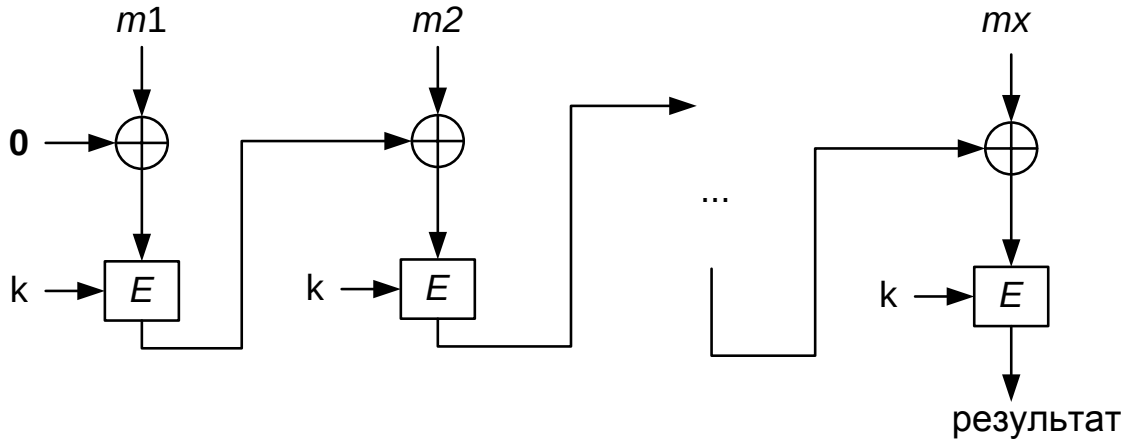


Рис. 3.18. **Модель роботи алгоритму CBC-MAC**

HMAC (ISO/IEC 9797-1).

Формування MAC-кодів за допомогою HMAC:

$$HMAC(K,M) = h((K \oplus opad) \,||\, h(K \oplus ipad) \,||\, M),$$

де h – геш-функція; K – секретний ключ, доповнений нулями до розміру блоку; M – повідомлення для ідентифікації; II – конкатенація; opad – 0x5c5c..5c (довжина дорівнює розміру блоку); ipad – 0x3636..36 (довжина дорівнює розміру блоку).

HMAC має таку перевагу, що дозволяє повторне використання існуючих реалізацій геш-функції. Безпека може бути доведена на таких припущеннях: основна геш-функція стійка до колізій з невідомим початковим значенням; функція стиснення забезпечена ключами на початкове значення безпечного MAC примітиву (для повідомлень з одного блоку); функція стиснення є слабкою псевдовипадковою функцією. Ці припущення слабкіші, ніж припущення, необхідні для TTMAC і EMAC. Продуктивність і спритність ключів є розумними. NESSIE рекомендує використовувати цю конструкцію з колізіонно-стійкою геш-функцією, включеною в NESSIE.

Модель роботи алгоритму HMAC наведено на рис. 3.19.

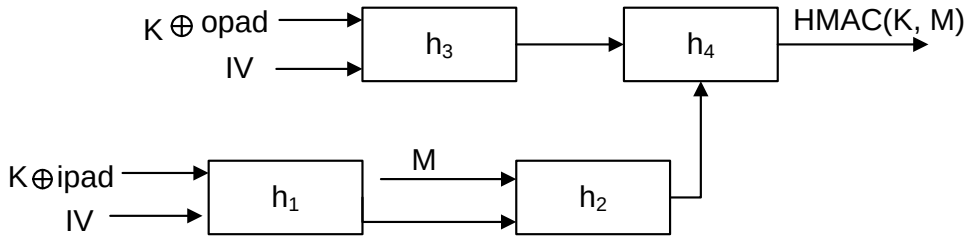


Рис. 3.19. **Модель роботи алгоритму HMAC**

Серед основних недоліків алгоритмів є погане розсіювання та використання для генерації ключа алгоритму DES (AES). Щодо використання алгоритмів DES та AES для отримання стійкої ключової послідовності, то це накладає обмеження на швидкість гешування самого алгоритму MAC-коду [288; 325; 326].

У табл. 3.4 наведено аналіз тестування швидкості роботи алгоритмів гешування.

Таблиця 3.4

Аналіз тестування швидкості роботи алгоритмів гешування

Функція гешування	Кількість циклів	Мова реалізації	Швидкість роботи на Celeron 600 MHz	Швидкість роботи на Pentium III 1000 MHz
Whirlpool	10	C	28,013 Мбіт/с	46,961 Мбіт/с
SHA-2 (512)	80	C	41,159 Мбіт/с	68,701 Мбіт/с
SHA-2 (256)	64	C	81,308 Мбіт/с	135,557 Мбіт/с

ГОСТ 34311-95	–	C+Assembler	49,408 Мбіт/с	83,056 Мбіт/с
HAVAL	96(128, 160)	C	337,842 Мбіт/с	564,809 Мбіт/с
SHA-1	80	C, Assembler	206,285 Мбіт/с 361,581 Мбіт/с	344,433 Мбіт/с 605,558 Мбіт/с
RIPEMD-160	160	C	147,465 Мбіт/с	246,568 Мбіт/с
MD5	64	C	278,715 Мбіт/с	574,635 Мбіт/с
MD4	48	C	344,086 Мбіт/с	467,793 Мбіт/с
UMAC	–	C C+Assembler	989,371 Мбіт/с 3518,900 Мбіт/с	1648,953 Мбіт/с 5885,057 Мбіт/с
Rijndael CBC-MAC	14	C	139,376 Мбіт/с	231,255 Мбіт/с
ГОСТ 28147-89 (OFB)	16	C+Assembler	189,559 Мбіт/с	315,270 Мбіт/с

Як видно з аналізу табл. 3.4 Two-Track-MAC уступає за швидкістю тільки UMAC алгоритму приблизно в 3 – 7 разів, але має в 2,5 рази більший розмір MAC коду.

У табл. 3.5 наведено можливі значення довжин ключа і геш-коду для різних алгоритмів сімейства MAC.

Таблиця 3.5

Довжина ключа k і довжина геш-коду n для MAC-кодів

Алгоритм	k (ключ)	n (геш-код)
UMAC	128	64
TTMAC	160	≤ 160
EMAC-AES	128,192,256	≤ 128
RMAC-AES	128,192,256	≤ 128
HMAC-SHA-1	≤ 512	≤ 160

Алгоритм EMAC заснований на AES CBC-MAC вважається стандартом для вхідних у цю категорію шифрів. Схема використає AES (Rijndael) блоковий симетричний шифр і генерує величину MAC до 128 біт. RMAC є випадковим варіантом схеми EMAC, що забезпечує кращу протидію атаці на основі внутрішніх помилок. Відмінність – у вихідному перетворенні (шифрування виробляється на ключі, отриманому порозрядним доповненням K2 і R. Two-Track-MAC заснований на геш-функції RIPEMD-160 з модифікаціями. Алгоритм працює, шляхом ітераційного використання функції стиску [203; 239].

У табл. 3.6 наведено основні результати оцінки швидкодії Two-Track-MAC алгоритму для різних операційних платформ. Швидкість

обчислень визначається кількістю циклів процесора, затрачуваних на один байт оброблюваного повідомлення.

Таблиця 3.6

Швидкодія MAC алгоритмів

Алгоритм	Довжина MAC-коду (біт)	Довжина ключа (біт)	Тип ПЕВМ				
			Pentium2	PIII/Linux	Pentium4	Xeon	AMD
1	2	3	4	5	6	7	8
TTMAC	160	160	21	21	40	37	21
UMAC-16	64	128	6.1	6.0	6.2	6.1	6.2
UMAC-32	64	128	2.5	2.9	6.7	6.6	1.9

Закінчення табл. 3.6

1	2	3	4	5	6	7	8
HMAC-Whirlpool	512	512	86	72	98	103	100
HMAC-MD4	128	512	4.7	4.7	6.4	6.4	4.7
HMAC-MD5	128	512	7.2	7.3	9.4	9.4	7.4
HMAC-RIPE-MD	160	512	23	18	27	26	21
HMAC-SHA-0	160	512	16	15	23	23	13
HMAC-SHA-1	160	512	16	15	25	24	12
HMAC-SHA-2	256 384 512	512	40 84 84	39 84 84	40 124 124	39 132 132	33 72 72
HMAC-Tiger	192	512	24	21	28	26	20
CBC MAC-Rijndael (EMAC)	128	128	24	26	26	27	31
CBC MAC-DES	64	56	62	61	72	69	54
CBC MAC-Shacal	512	160	31	31	67	74	29

Аналіз табл. 3.5 показує, що схеми ключового гешування UMAC на основі поліноміальних функцій дозволяють одержати найвищу швидкість гешування, крім цього вони є переможцем Міжнародного криптографічного конкурсу NESSIE.

Проаналізувавши характеристики MDC-кодів і MAC-кодів можна зробити висновок, що MAC-коди є більш стійкими і на відміну від MDC-кодів не потребують додаткових алгоритмів для шифрування повідомлення. Тому більш перспективним є дослідження ключових геш-функцій.

3.3. Модель отримання геш-коду на основі використання UMAC-32

Розглянуто модель і структурну схему каскадного ключового гешування для формування кодів автентичності UMAC, а також особливості її побудови й багатоетапного формування геш-коду з використанням універсального гешування й шифрування.

Загальна схема кодів автентичності повідомлень UMAC.

Одна з перших версій алгоритму формування кодів автентичності повідомлень з використанням універсального гешування (UMAC – Message Authentication Code using Universal Hashing) була подана в роботі [326]. Надалі, після деякого доопрацювання, алгоритм UMAC був поданий у фінальному звіті європейського конкурсу NESSIE − New European Schemes for Signatures, Integrity, and Encryption (нові європейські схеми для підписів, цілісності, і шифрування) [37]. Одна з останніх електронних версій алгоритму UMAC доступна в електронному вигляді [203]. Розглянемо загальну схему формування кодів автентичності повідомлень з використанням алгоритму UMAC, проаналізуємо основні аналітичні співвідношення, що описують внутрішню структуру і вживані перетворення при формуванні кодів автентичності повідомлень.

Загальна схема формування кодів автентичності повідомлень з використанням алгоритму UMAC.

Код автентичності повідомлень (позначимо його Tag) за специфікацією алгоритму UMAC формується за допомогою обчислення такої функції:

$$Tag = UMAC\,(K, M, Nonce, Taglen) = Y \oplus Pad,$$

де K − секретний ключ, довжина якого $Keylen$ дорівнює стандартній довжині секретного ключа використовуваного блокового симетричного шифру (специфікацією UMAC рекомендується використовувати алгоритм шифрування AES (FIPS-197), в цьому випадку довжина секретного ключа $Keylen$ належить множині допустимих значень $\{16, 24, 32\}$ байт); M − інформаційне повідомлення, яке підлягає автентифікації, подане у вигляді масиву-рядка, розмірністю від одного до 2^{67} біт (2^{64} байт); *Nonce* – неповторюване (упроваджуються для всіх інформаційних повідомлень M) восьмибайтове число; $Taglen$ − ціле число з множини допустимих значень $\{4, 8, 12, 16\}$, що задає довжину коду автентичності повідомлень Tag в байтах; $Hash(K, M, Taglen)$ − функція ключового універсального гешування

інформаційного повідомлення M з використанням секретного ключа K; $PDF(K, Nonce, Taglen)$ − функція формування псевдовипадкової підкладки (Pad) за введеним значенням і секретним ключем; "$\oplus$" − побітове додавання (XOR) результату ключового гешування повідомлення і сформованої підкладки $Pad = PDF(K, Nonce, Taglen)$, тобто

$$Tag = Hash(K, M, Taglen) \oplus PDF(K, Nonce, Taglen).$$

Довжина геш-коду Y, підкладки Pad та коду Tag належить множині допустимих значень $\{32, 64, 96, 128\}$ біт. Ці фіксовані значення $Taglen$ відповідають випадку формування кодів автентичності повідомлень UMAC-32, UMAC-64, UMAC-96 або UMAC-128 відповідно.

Для різних версій UMAC схема роботи алгоритму універсального гешування виглядає таким чином, як показано на рис. 3.20.

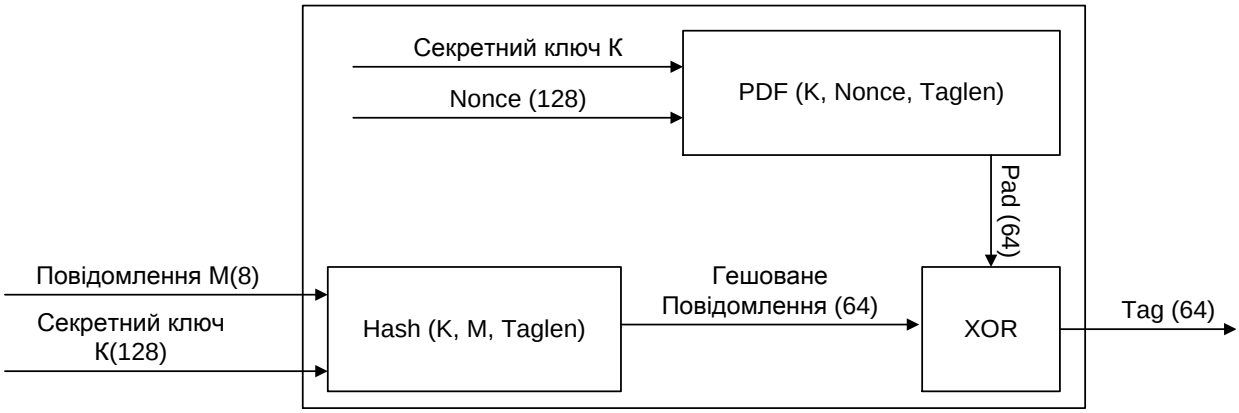


Рис. 3.20. **Загальна модель універсальних геш-функцій UMAC-16/32**

З рис. 3.20 видно, що базовою частиною формування MAC-коду є функція UHASH (універсальне гешування), яка використовується в обох версіях UMAC-16 та UMAC-32.

Перший рівень гешування

Перший рівень гешування виконує розбиття масиву-рядка M розмірності до 2^{64} байт на блоки M_i по 1 024 байт з подальшим перетворенням кожного блоку функцією $NH(K_{L1}, M_i)$. Отримані результати $Hash_{L1_i} = NH(K_{L1}, M_i)$ конкатенуються (об'єднуються) у рядок $Y_{L1} = Hash_{L1}(K_{L1}, M)$, який коротше інформаційної послідовності в 128 разів. Цей рядок і є результатом гешування першого рівня:

$$Y_{L1} = Hash_{L1}(K_{L1}, M) = NH(K_{L1}, M_0) \| NH(K_{L1}, M_1) \| ... \| NH(K_{L1}, M_{n\ 1}),$$

де $n = \left\lceil \frac{Length(M)}{1024} \right\rceil$, $Length(M)$ – байтова довжина інформаційного повідомлення *M.*

Значення функції $Hash_{L1_i} = NH(K_{L1}, M_i)$ обчислюється за таким правилом. Інформаційний блок M_i розбивається на чотирибайтові підблоки так, що:

$$M_i = M_{i_1} \| M_{i_2} \| ... \| M_{i_t},$$

де $t = \left\lceil \frac{Length(M_i)}{4} \right\rceil$. У цьому випадку $t = \left\lceil \frac{1024}{4} \right\rceil = 256$.

Аналогічним чином ключова послідовність K_{L1} подається у вигляді послідовностей чотирибайтових підблоків:

$$K_{L1} = K_{L1_1} \| K_{L1_2} \| ... \| K_{L1_t}.$$

Після чого, беручи початковий стан $Hash_{L1_i} = 0$, для всіх $j = 1,9,17...,t\ \ 7$ виконуються такі операції:

$$Hash_{L1_i} = Hash_{L1_i} +_{64} ((M_{i_{j+0}} +_{32} K_{L1_{j+0}}) \cdot_{64} (M_{i_{j+4}} +_{32} K_{L1_{j+4}})),$$
$$Hash_{L1_i} = Hash_{L1_i} +_{64} ((M_{i_{j+1}} +_{32} K_{L1_{j+1}}) \cdot_{64} (M_{i_{j+5}} +_{32} K_{L1_{j+5}})),$$
$$Hash_{L1_i} = Hash_{L1_i} +_{64} ((M_{i_{j+2}} +_{32} K_{L1_{j+2}}) \cdot_{64} (M_{i_{j+6}} +_{32} K_{L1_{j+6}})),$$
$$Hash_{L1_i} = Hash_{L1_i} +_{64} ((M_{i_{j+3}} +_{32} K_{L1_{j+3}}) \cdot_{64} (M_{i_{j+7}} +_{32} K_{L1_{j+7}})),$$

де $+_{64}$, $+_{32}$ – операції додавання за модулем 2^{64} і 2^{32}, відповідно;

$\cdot_{64}$ – операція множення за модулем 2^{64}.

У результаті обчислень формується восьмибайтове значення $Hash_{L1_i}$.

На першому шарі виконується розбиття вхідного повідомлення за допомогою методу функції NH гешування за такою схемою (рис. 3.21):

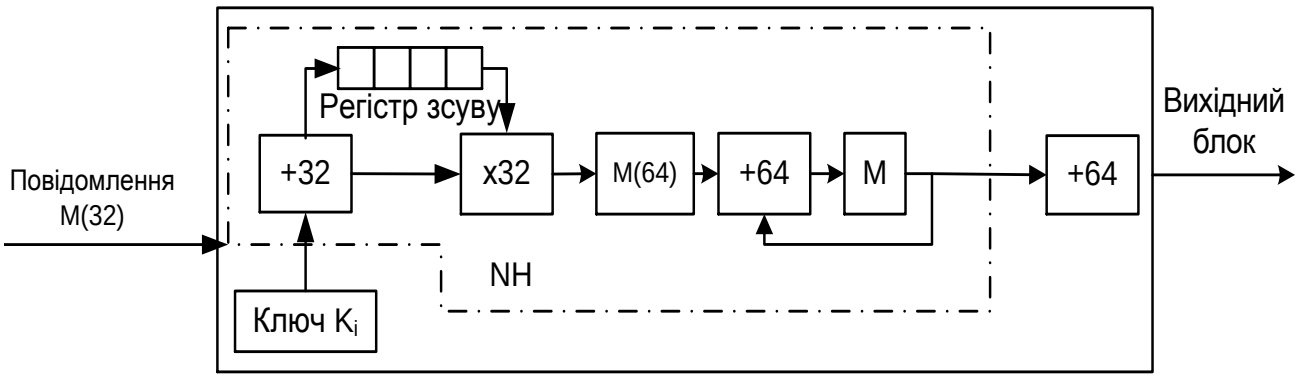


Рис. 3.21. **Схема роботи першого шару L1 Hash Function**

Розрахуємо вручну ключі на першому рівні гешування:

$$n = \left\lceil \frac{Numbyte}{Blocklen} \right\rceil = \frac{1024 + 16 \cdot 3}{32} = \frac{1072}{32} = 33{,}5 \approx 33$$

$\Rightarrow i = 1,2,\ldots,33$

$T_i = Index \| i.$

Для генерації ключа використовувався алгоритм Rijndael, що лежить в основі блоково-симетричного шифру AES.

Rijndael є блоковим шифром, який розроблений бельгійськими вченими Джоаном Дименом і Вінцентом Ріджменом [2]. Rijndael може використовуватися з розмірами ключів і блоків, рівними 128, 192 і 256 бітів. Rijndael був вибраний серед чотирьох інших кандидатів на застосування в якості стандарту AES завдяки своїй високій стійкості, ефективності, продуктивності, гнучкості і малим вимогам до пам'яті комп'ютерних систем.

Для першого рівня гешування $Index = 1, \Rightarrow T_i$.

Дані, отримані при розрахунку, наведені в табл. 3.7.

Таблиця 3.7

Розрахунок ключів на першому шарі гешування для UMAC

Блок даних T	Конкатенація $Index \| i$	Результат	Згенерований ключ	Блок даних T	Конкатенація $Index \| i$	Результат	Згенерований ключ
T_1	1 || 1	0000000100000001	329D	T_{18}	1 || 18	0000000100010010	0E02
T_2	1 || 2	0000000100000010	E43B	T_{19}	1 || 19	0000000100010011	0F3C

T_3	1 || 3	0000000100000011	6FC8	T_{20}	1 || 20	0000000100010100	1C04
T_4	1 || 4	0000000100000100	4974	T_{21}	1 || 21	0000000100010101	CEA0
T_5	1 || 5	0000000100000101	AD75	T_{22}	1 || 22	0000000100010110	4AB0
T_6	1 || 6	0000000100000110	EAA0	T_{23}	1 || 23	0000000100010111	0D85
T_7	1 || 7	0000000100000111	4E21	T_{24}	1 || 24	0000000100011000	8EFE
T_8	1 || 8	0000000100001000	C505	T_{25}	1 || 25	0000000100011001	B880
T_9	1 || 9	0000000100001001	F8A1	T_{26}	1 || 26	0000000100011010	03F3
T_{10}	1 || 10	0000000100001010	ABBE	T_{27}	1 || 27	0000000100011011	682E
T_{11}	1 || 11	0000000100001011	0F3F	T_{28}	1 || 28	0000000100011100	0720
T_{12}	1 || 12	0000000100001100	86A3	T_{29}	1 || 29	0000000100011101	5AE8
T_{13}	1 || 13	0000000100001101	C295	T_{30}	1 || 30	0000000100011110	D24D
T_{14}	1 || 14	0000000100001110	4DA4	T_{31}	1 || 31	0000000100011111	FB94
T_{15}	1 || 15	0000000100001111	8996	T_{32}	1 || 32	0000000100100000	9C41
T_{16}	1 || 16	0000000100010000	DCDE	T_{33}	1 || 33	0000000100100001	81FA
T_{17}	1 || 17	0000000100010001	9035				

Ключ формується методом конкатенації всіх розрахованих ключів: $K' = K'_1 \| K'_2 \| ... \| K'_n$.

Другий рівень гешування

Другий рівень гешування використовує поліноміальне ключове гешування, докладно розглянуте в роботах [300; 315]. Результатом роботи цього рівня є обчислення геш-коду

$$Y_{L2} = Hash_{L2}(K_{L2}, Y_{L1}) = Poly(Wordbits, Maxwordrange, k, M_P),$$

тобто на вхід гешування другого рівня подається рядок $Y_{L1} = Hash_{L1}(K_{L1}, M)$.

У якості вихідних даних функція поліноміального гешування використовує: $Wordbits \in [64,128]$; $Maxwordrange$ – позитивне ціле число, менше $2^{Wordbits}$; k – залежить від ключа K_{L2} ціле число з діапазону $[0,..., prime(Wordbits)-1]$, $prime(x)$ – найбільше просте число, менше 2^x; $M_P = Y_{L1} = Hash_{L1}(K_{L1}, M)$ – дані, що підлягають поліноміальному гешуванню.

За специфікацією алгоритму UMAC як $prime(x)$ використовуються такі константи: $prime(36) = 2^{36} - 5$, $prime(64) = 2^{64} - 59$, $prime(128) = 2^{128} - 159$. Бітову довжину M_P позначимо $Bytelength(M_P)$. Залежно від довжини M_P використовуються такі особливості в реалізації другого рівня гешування:

якщо довжина даних M_P, що надійшли, не перевершує 2^{17} байт, тоді поліноміальне гешування *Poly* виконується з параметрами $Wordbits = 64$; $Maxwordrange = 2^{64} - 2^{32}$; $k = k64$ – рядок, утворений першими восьми байтами ключа K_{L2} та спеціальною восьмибайтовою маскою;

якщо довжина даних M_P, що надійшли, перевершує 2^{17} байт (але не перевершує 2^{64} байт), тоді перші 2^{17} байт даних обробляються функцією поліноміального гешування $Poly(64,2^{64} - 2^{32}, k64, M_P)$, а байти даних, що залишилися, обробляються функцією *Poly* з параметрами $Wordbits = 128$; $Maxwordrange = 2^{128} - 2^{96}$; $k = k128$ – рядок, утворений останніми
16 байтами ключа K_{L2} та спеціальною 16 байтною маскою.

Гешовані дані M_P розбиваються на блоки по $Wordbytes = Wordbits/8$ байт:

$$M_P = M_{P_1} \| M_{P_2} \| ... \| M_{P_n},$$

де $n = Bytelength(M_P)/Wordbytes$.

Результатом гешування є значення поліноміальної функції

$$Y_{L2} = \left(M_{P_n} + kM_{P_{n-1}} + ... + k^{n-1}M_{P_1} + k^n\right) \bmod(p),$$

яке обчислюється ітеративною процедурою (для всіх $i = 1,2,...,n$):

$$Poly_i = \left(kPoly_{i-1} + M_{P_i}\right) mod(p),\ Poly_0 = 1,\ p = prime(Wordbits),$$

за допомогою схеми Горнера

$$M_{P_n} + kM_{P_{n-1}} + ... + k^{n-1}M_{P_1} + k^n = (((k + M_{P_1})k + M_{P_2})k + ... + M_{P_{n-1}})k + M_{P_n}.$$

Обчислення геш-значення $Y_{L2} = Poly_n$ є цілим числом з діапазону $[0,..., prime(Wordbits) - 1]$.

Розрахунки значення ключів для другого рівня гешування:

$$n = \left\lceil \frac{Numbyte}{Blocklen} \right\rceil = \frac{24 \cdot 4}{32} = \frac{96}{32} = 3$$

$=> i = 1,2,3$

$T_i = Index \| i.$

Для другого рівня гешування $Index$=2, => T_i.

Дані, отримані при розрахунку, наведені в табл. 3.8.

Таблиця 3.8

Розрахунок ключів на другому шарі гешування для UMAC

Блок даних T	Конкатенація $Index \| i$	Результат	Згенерований ключ
T_1	2 || 1	0000001000000001	608E
T_2	2 || 2	0000001000000010	EC56
T_3	2 || 3	0000001000000011	9FF3

$K_{L2} = K1 \| K2 \| K3$

Загальна схема роботи алгоритму цього шару універсальної геш-функції подана на рис. 3.22:

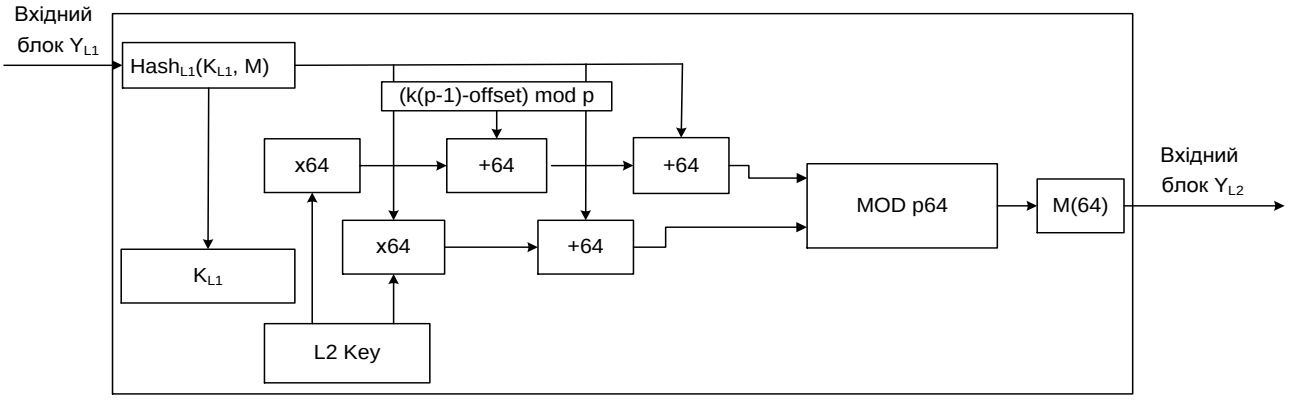


Рис. 3.22. **Схема роботи другого шару L2 Hash Function**

Третій рівень гешування

Третій рівень гешування $Hash_{L3}(K_{L3_1}, K_{L3_2}, Y_{L2})$ виконується над результатом поліноміального гешування і перетворює подані на його вхід дані довжини до 16 байт у геш-код Y фіксованої довжини 32 біта.

У якості вихідних даних третього рівня гешування виступають дві ключові послідовності K_{L3_1} і K_{L3_2} довжини 64 і 4 байти відповідно, а також вхідна 16 байтна послідовність Y_{L2}.

Гешовані дані Y_{L2} і ключова послідовність K_{L3_1} рівномірно розбиваються на вісім блоків, кожен з яких постає як ціле число Y_{L2_i} і $K_{L3_{1i}}$, $i = 1,2,...,8$.

Геш-значення Y_{L3} обчислюється таким чином:

$$Y_{L3} = \left(\left(\left(\sum_{i=1}^{m} Y_{L2_i} K_{L3_{1_i}} \right) mod(prime(36)) \right) mod(2^{32}) \right) xor(K_{L3_2}),$$

де $(x)xor(y)$ − операція "виключає АБО" над значеннями x і y.

Розрахунок формування ключів:
Формування K_{L31}:

$$n = \left\lceil \frac{Numbyte}{Blocklen} \right\rceil = \frac{64 \cdot 8}{16} = \frac{512}{16} = 32$$

$$=> i = 1,2,3,...,32$$

$$T_i = Index \,||\, i.$$

Для третього рівня гешування $Index$=3, => T_i:
Дані, отримані при розрахунку, наведені в табл. 3.9.

Таблиця 3.9

Розрахунок першого ключа на третьому шарі гешування для UMAC

Блок даних T	Конкатенація $Index \,\|\|\, i$	Результат	Згенерований ключ	Блок даних T	Конкатенація $Index \,\|\|\, i$	Результат	Згенерований ключ
T_1	3 || 1	0000001100000001	8A13	T_{18}	3 || 17	0000001100010001	161F
T_2	3 || 2	0000001100000010	056A	T_{19}	3 || 18	0000001100010010	E6F4
T_3	3 || 3	0000001100000011	534D	T_{20}	3 || 19	0000001100010011	C0A0
T_4	3 || 4	0000001100000100	DE16	T_{21}	3 || 20	0000001100010100	6012
T_5	3 || 5	0000001100000101	91B2	T_{22}	3 || 21	0000001100010101	EC5A
T_6	3 || 6	0000001100000110	6B5E	T_{23}	3 || 22	0000001100010110	C606
T_7	3 || 7	0000001100000111	1E7A	T_{24}	3 || 23	0000001100010111	7823

T_8	3 || 8	0000001100001000	21ED	T_{25}	3 || 24	0000001100011000	F379
T_9	3 || 9	0000001100001001	C060	T_{26}	3 || 25	0000001100011001	7E88
T_{10}	3 || 10	0000001100001010	1B0B	T_{27}	3 || 26	0000001100011010	CE5E
T_{11}	3 || 11	0000001100001011	6BE0	T_{28}	3 || 27	0000001100011011	027B
T_{12}	3 || 12	0000001100001100	458C	T_{29}	3 || 28	0000001100011100	B60B
T_{13}	3 || 13	0000001100001101	F7A8	T_{30}	3 || 29	0000001100011101	6928
T_{14}	3 || 14	0000001100001110	6F0D	T_{31}	3 || 30	0000001100011110	1CC4
T_{15}	3 || 15	0000001100001111	F91C	T_{32}	3 || 31	0000001100011111	E2C5
T_{16}	3 || 16	0000001100010000	4AF1	T_{33}	3 || 32	0000001100100000	5BA9

$K_{L31} = K1 \,||\, K2 \,||\, K3 \,..\, ||\, K32$

Формування K_{L32}:

$$n = \left\lceil \frac{\text{Numbyte}}{\text{Blocklen}} \right\rceil = \frac{4 \cdot 8}{16} = \frac{32}{16} = 2 \Rightarrow i = 1$$

$$T_i = Index \,||\, i.$$

Для третього рівня гешування $Index$=4, => T_i:

Дані, отримані при розрахунку, наведені в табл. 3.10.

Таблиця 3.10

Розрахунок другого ключа на третьому шарі гешування для UMAC

Блок даних T	Конкатенація $Index \,\|\|\, i$	Результат	Згенерований ключ
T_1	4 || 1	0000010000000001	F530
T_2	4 || 2	0000010000000010	E33E

Призначення третього шару полягає в перетворенні вхідного вектора В завдовжки 16 байт у рядок рівний 4 байт. Загальна схема роботи третього шару L3 Hash Function приведена на рис. 3.23.

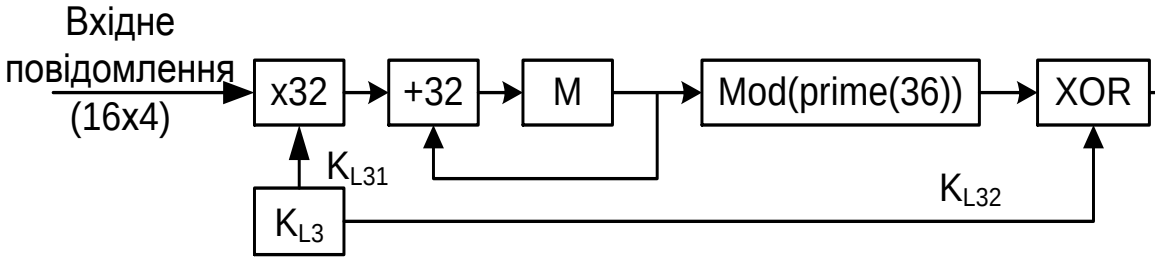


Рис. 3.23. **Схема роботи третього шару L3 Hash Function**

Схема формування ключів (KDF: Key-Derivation Function)

Алгоритм роботи функції вироблення підключів KDF може бути представлений у вигляді рис. 3.24.

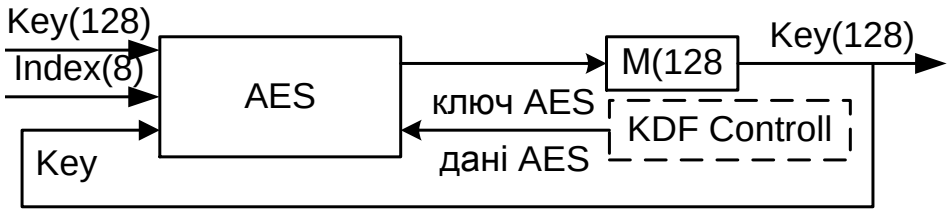


Рис. 3.24. **Схема роботи функції KDF**

Спеціальна функція $KDF(K, Index, Numbyte)$ призначена для формування послідовностей псевдовипадкових біт даних, які використовуються на різних рівнях формування кодів автентичності повідомлень як ключові дані відповідних функцій гешування.

У якості вихідних даних функції генерації ключових псевдовипадкових послідовностей використовується секретних ключ K довжини $Keylen$ байт і два позитивних цілих числа $Index$ і $Numbyte$, значення яких не перевершує 2^{64}.

Для формування псевдовипадкових ключових послідовностей використовується блоковий симетричний шифр. Позначимо процедуру шифрування блоку даних T довжини $Blocklen$ байт з використанням секретного ключа K довжини $Keylen$ байт у вигляді деякої функції $Enchiper(K,T)$. Тоді процедуру формування псевдовипадкової ключової послідовності $K' = KDF(K, Index, Numbyte)$ можна представити у вигляді такого ітеративного (для всіх $i = 1,2,...,n$) перетворення:

$$T_i = Index \| i,$$
$$K'_i = Enchiper(K, T_i),$$
$$K' = K'_1 \| K'_2 \| ... \| K'_n,$$

де $n = \left\lceil \frac{Numbyte}{Blocklen} \right\rceil$; $a \| b$ – конкатенація (приєднання) рядків a і b.

Сформована послідовність псевдовипадкових ключових біт даних K' має довжину $Numbyte$ байт, кратну довжині блоку $Blocklen$ байт.

Схема формування псевдовипадковою підкладки (PDF: Pad-Derivation Function).

У функції універсального гешування використовується функція PDF (генератор псевдовипадкових чисел). Схема роботи алгоритму генератора представлена на рис. 3.25.

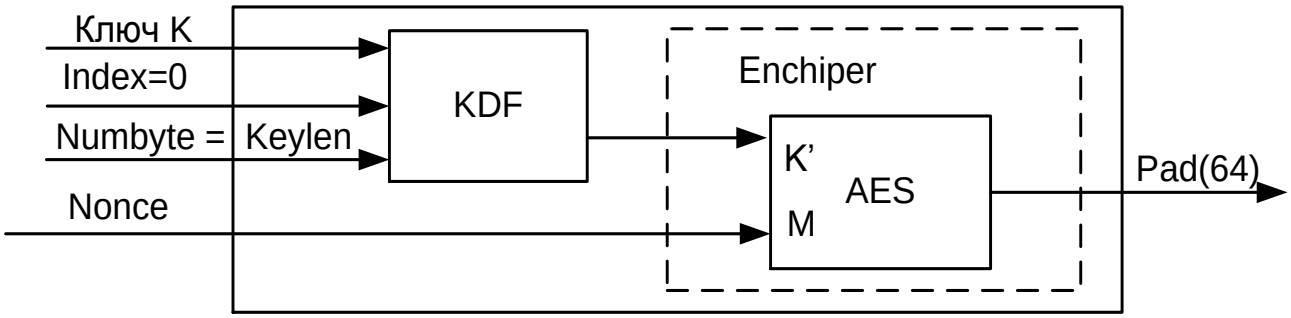


Рис. 3.25. **Схема роботи функції PDF**

Функція $PDF(K, Nonce, Tagler)$ призначена для формування псевдовипадкової підкладки Pad, яка використовується на заключному етапі формування коду автентичності повідомлення.

У якості вихідних даних використовується секретний ключ K довжини $Keylen$ байт і неповторюваних (для всіх введених інформаційних повідомлень M) восьмибайтове число $Nonce$, а також ціле число $Taglen$, що задає розмір (довжину в байтах) сформованого коду автентичності Tag.

Процедура формування псевдовипадкової підкладки $Pad = PDF(K, Nonce, Tagler)$ полягає у формуванні підключа $K' = KDF(K, Index, Numbyte)$, $Index = 0$, $Numbyte = Keylen$, з використанням розгля-

нутої вище процедури формування послідовностей псевдовипадкових ключових біт і шифрування значення *Nonce* на сформованому підключення *K'*, тобто:

$Pad = PDF(K, Nonce, Taglen) = Enchiper(KDF(K, 0, Keylen), Nonce)$.

Процедура формування псевдовипадкової підкладки *Pad* побудована так, що результуюче значення *Pad* має довжину *Taglen* байт незалежно від значень *Blocklen* і *Nonce*.

Таким чином, розглянута схема формування кодів автентичності повідомлень UMAC використовує багаторівневу конструкцію універсального гешування $Hash(K,M,Taglen)$ і процедуру формування псевдовипадкової підкладки *Pad*. Застосування універсального гешування дозволяє забезпечити рівноімовірності формування геш-образів для всієї множини використовуваних ключових даних, на чому і базується доказ безпеки алгоритму [61]. Формування псевдовипадкової підкладки криптографічно стійким алгоритмом (наприклад, з використанням блокового симетричного шифру AES) забезпечує крипостійкість алгоритму UMAC на рівні стійкості застосовуваного криптоалгоритму [197]. Отже, розглянута схема формування UMAC має потенційно високі показники ефективності.

Однак на сьогоднішній день не досліджені колізійні властивості алгоритму UMAC після застосування завершальної процедури накладення на сформовані геш-коди $Y = Hash(K,M,Taglen)$ псевдовипадкових підкладок $Pad = PDF(K, Nonce, Tagler)$. Далі показано, що результуючі коди справжності повідомлень $Tag = UMAC(K,M,Nonce,Taglen) = Y \oplus Pad$ формуються нерівноімовірно для всієї множини використовуваних ключових даних. Отже, алгоритм формування UMAC після застосування останнього шару накладення псевдовипадкових підкладок втрачає властивість "універсальності" гешування, його колізійні властивості істотно погіршуються.

3.4. Дослідження ефективності безпечного гешування на основі UMAC-32

Запропоновано методику дослідження колізійних властивостей кодів автентифікації повідомлень UMAC на основі зменшеної моделі окремих шарів використовуваних перетворень і оцінювання розподілу

колізій (зіткнень) формованих образів (кодів). Застосування зменшених моделей використовуваних шарів перетворень дозволяє, зберігши алгебраїчну структуру криптоалгоритму, проводити дослідження основних показників його ефективності.

Зменшена модель формування кодів дійсності повідомлень UMAC (міні-UMAC)

Схема формування кодів автентифікації повідомлень UMAC використовує у своїй структурі кілька шарів перетворення, у тому числі блоковий симетричних шифр (рекомендований до використання шифр AES). Розроблювальна зменшена модель UMAC повинна включати відповідні шари перетворення зі збереженням їх алгебраїчної структури при виконанні масштабування до міні-версії. Природнім представляється досліджувати колізійні характеристики формованих образів (кодів) на кожному із шарів перетворення, у тому числі формованих за допомогою блокового симетричного шифру псевдовипадкових підкладок Pad, проаналізувати їх вплив на колізійні властивості кодів автентифікації повідомлень зменшеної моделі UMAC.

Схема формування кодів UMAC складається з таких шарів:

трирівневе універсальне гешування для формування геш-кодів $Y = Hash(K, M, Tagler)$;

криптографічне перетворення з використанням блокового симетричного шифру для формування псевдовипадкової підкладки $Pad = PDF(K, Nonce, Tagler)$;

заключне перетворення для формування кодів автентифікації повідомлень $Tag = UMAC(K, M, Nonce, Tagler) = Y \oplus Pad$.

Розглянемо кожний шар схеми формування кодів автентифікації повідомлень UMAC на предмет їх масштабування.

Міні-версію трирівневого універсального гешування побудуємо без зміни структури алгебраїчних перетворень простим зменшенням розмірності блоків оброблюваних даних у вісім раз.

Відповідна довжина геш-коду Y_{mini} зменшеної моделі першого шару буде кратна 4 бітам, його значення сформуємо за допомогою об'єднання (конкатенації) чотирьох послідовностей $Y_{mini\,L3_i}$

$$Y_{mini} = Y_{mini_{L3_1}} \| Y_{mini_{L3_2}} \| Y_{mini_{L3_3}} \| Y_{mini_{L3_4}},$$

де $Y_{mini_{L3_i}}$ – результат багаторівневого гешування повідомлення зменшеної моделі першого шару міні-UMAC.

Розглянемо процес формування одного блоку $Y_{mini_{L3_i}}$ (другий рівень гешування в зменшеній моделі виконувати не будемо):

$$Y_{mini_{L3_i}} = Y_{mini_{L3}} = Hash_{mini_{L3}}\left(K_{mini_{L3_1}}, K_{mini_{L3_2}}, Hash_{mini_{L1}}\left(K_{mini_{L1}}, M_{mini}\right)\right),$$

де $K_{mini_{L1}}$, $K_{mini_{L3_1}}$, $K_{mini_{L3_2}}$ – ключові послідовності міні-UMAC;

$Hash_{mini_{L1}}$ і $Hash_{mini_{L3}}$ – зменшені версії гешування першого й третього рівнів відповідно.

На першому рівні масив-рядок M_{mini} розмірності 32 біта перетвориться функцією $NH(K_{L1}, M_i)$. Цей рядок і є результатом гешування першого рівня: $Y_{mini_{L1}} = NH_{mini}\left(K_{mini_{L1}}, M_{mini}\right)$.

Значення функції $NH_{mini}\left(K_{mini_{L1}}, M_{mini}\right)$ обчислюється за таким правилом. Інформаційний блок M_{mini} розбивається на вісім чотирибітових підблоків $M_{mini} = M_{mini_1} \| M_{mini_2} \| \ldots \| M_{mini_8}$.

Аналогічним чином ключова послідовність K_{L1} подається у вигляді послідовностей з восьми чотирибітових підблоків:

$$K_{mini_{L1}} = K_{mini_{L1_1}} \| K_{mini_{L1_2}} \| \ldots \| K_{mini_{L1_8}}.$$

Після чого (ухвалюючи початковий стан $Hash_{L1} = 0$) виконуються такі операції:

$$Hash_{mini_{L1}} = Hash_{mini_{L1}} +_8 ((M_{mini_0} +_4 K_{mini_{L1_0}}) \times_8 (M_{mini_4} +_4 K_{mini_{L1_4}})),$$
$$Hash_{mini_{L1}} = Hash_{mini_{L1}} +_8 ((M_{mini_1} +_4 K_{mini_{L1_1}}) \times_8 (M_{mini_5} +_4 K_{mini_{L1_5}})),$$
$$Hash_{mini_{L1}} = Hash_{mini_{L1}} +_8 ((M_{mini_2} +_4 K_{mini_{L1_2}}) \times_8 (M_{mini_6} +_4 K_{mini_{L1_6}})),$$
$$Hash_{mini_{L1}} = Hash_{mini_{L1}} +_8 ((M_{mini_3} +_4 K_{mini_{L1_3}}) \times_8 (M_{mini_7} +_4 K_{mini_{L1_7}})),$$

де $+_8$, $+_4$ – операції додавання за модулем 28 і 24 відповідно;

$\times_8$ – операція множення за модулем 28.

У результаті обчислень формується восьмибітне значення $Y_{miniL1} = Hash_{miniL1}$.

Третій рівень гешування перетворить подані на його вхід восьмибітні дані Y_{miniL1} у геш-код Y_{miniL3} довжини 4 біта. У якості ключових послідовностей виступають K_{miniL3_1} і K_{miniL3_2} довжини 16 і 4 біта відповідно.

Гешовані дані $Hash_{miniL1}$ й ключова послідовність K_{miniL3_1} рівномірно розбиваються на чотири блоки, кожний з яких подається як ціле число Y_{miniL2_i} й $K_{miniL3_{1_i}}$, $i = 1,2,...,4$.

Геш-значення Y_{miniL3} обчислюється таким чином:

$$Y_{miniL3} = \left(\left(\left(\sum_{i=1}^{4} Y_{miniL2_i} K_{miniL3_{1_i}} \right) mod(17) \right) mod(2^4) \right) \cdot or(K_{miniL3_2}),$$

де $(x)xor(y)$ – операція, "що виключає АБО" над значеннями x й y.

Коротко розглянемо цю зменшену модель шифру й обґрунтуємо її використання для формування псевдовипадкової підкладки в міні-UMAC.

Розмір блоку відкритого тексту рівний 16 біт, які позначимо чотирма шістнадцятковими числами h_0, h_1, h_2, h_3. Зазначимо, що h_0 складається з перших чотирьох біт вхідного потоку. Однак коли h_0 розглядається як шістнадцяткова цифра, то перший біт розглядається як біт вищого порядку. Наприклад, вхідний блок 1000 1100 0111 0001 буде поданий $h_0 = 8$, $h_1 = c$, $h_2 = 7$, $h_3 = 1$.

Розмір ключа також рівний 16 біт. Позначимо його як 4 шістнадцяткові числа k_0, k_1, k_2, k_3.

Кроки шифру застосовуються до стану – масиву 2×2 шістнадцяткових цифр. Однак для розглянутої далі операції $\tilde{\sigma}$ стан буде подано як масив 8×2 біт, тобто кожна шістнадцяткова цифра буде розглядатися як стовпець 4 біт з бітом вищого порядку зверху.

Вхідний блок завантажується в стан відображенням h_0, h_1, h_2, h_3 в $\begin{bmatrix} h_0 & h_2 \\ h_1 & h_3 \end{bmatrix}$. Наприклад, вхідний блок 1000 1100 0111 0001 буде завантажений як

$\begin{bmatrix} 8 & 7 \\ c & 1 \end{bmatrix}$, де матриця 8×2 буде $\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix}$.

Baby-Rijndael включає трохи ідентичних за структурою раундів (за замовчуванням їх 4). Перед шифруванням вхідний блок завантажується в стан, який описано, й розраховуються раундові ключі. Шифрування має загальну структуру:

$$E(a) = r_4 \cdot r_3 \cdot r_2 \cdot r_1(a \oplus k_0),$$

де a позначає стан, k_0, k_1, k_2, k_3, k_4 – раундові ключі й $r(a) = (t \cdot \tilde{\sigma}(S(a))) \oplus k_i$, за винятком r_4, де пропущене множення на t.

Наприкінці шифру стан вивантажує в 16-бітний блок у такому ж порядку, у якому він завантажувався.

Тепер опишемо окремі компоненти шифру.

Subbytes: операція S є вибіркова таблиця, яка застосовується до кожної 16-річній цифрі стану:

$$\begin{bmatrix} h_0 & h_2 \\ h_1 & h_3 \end{bmatrix} \xrightarrow{S} \begin{bmatrix} S(h_0) & S(h_2) \\ S(h_1) & S(h_3) \end{bmatrix},$$

де функція S задається табл. 3.11.

Таблиця 3.11

Вибіркова таблиця, що реалізує S-Блок Baby-Rijndael

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S(x)$	a	4	3	b	8	e	2	c	5	7	6	f	0	1	9	d

Shiftrows: Операція $\tilde{\sigma}$ просто міняє входи в другому рядку стану:

$$\begin{bmatrix} h_0 & h_2 \\ h_1 & h_3 \end{bmatrix} \xrightarrow{\tilde{\sigma}} \begin{bmatrix} h_0 & h_2 \\ h_3 & h_1 \end{bmatrix}.$$

Mixcolumns: матриця t є наступною 8×8 матрицею біт:

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Для цього перетворення стан розглядається як 8×2 бітова матриця. Стан множиться ліворуч на t, використовуючи матричне множення за модулем 2: $a = ta$.

Keyschedule: на початку шифру й наприкінці кожного раунду стан побітно складається (тобто за модулем 2) з раундовим ключем. Стовпці раундових ключів визначені рекурсивно в такий спосіб:

$$w_0 = \begin{pmatrix} k_0 \\ k_1 \end{pmatrix},\ w_1 = \begin{pmatrix} k_2 \\ k_3 \end{pmatrix},$$

$$w_{2i} = w_{2i-2} \oplus S(reverse(\quad w_{2i-2})) \quad \oplus r_i,$$

$$w_{2i+1} = w_{2i-1} \oplus w_{2i}$$

для всіх $i = 1,2,3,4$, де $r_i = \begin{pmatrix} 2^{i-1} \\ 0 \end{pmatrix}$, а функція $reverse$ заміняє два входи в стовпець. Функція S та ж, що й уже описана.

Слід зазначити, що всі додавання виконуються побітно за модулем 2. Нарешті, для $i = 1, 2, 3, 4$ раундовий ключ k_i є матриця, чиї стовпці є w_{2i} й w_{2i+1}.

Використання розглянутої зменшеної моделі блокового симетричного шифру AES дозволяє провести експериментальні дослідження колізійних властивостей формованих псевдовипадкових підкладок за всією безліччю секретних ключів. Так, псевдовипадкова підкладка Pad_{mini} міні-UMAC формується за допомогою шифрування неповторюваного для кожного інформаційного повідомлення M_{mini} числа $Nonce$.

Результуюче значення Pad_{mini} має довжину 16 біт, так само довжина, що Y_{mini} яка і відповідає, геш-коду.

Міні-версія заключного перетворення для формування кодів автентифікації повідомлень міні-UMAC полягає в порозрядному підсумовуванні за модулем 2 значень Y_{mini} і Pad_{mini}: $Tag_{mini} = Y_{mini} \oplus Pad_{mini}$.

Таким чином, масштабування застосовуваних перетворень на відповідних шарах схеми формування кодів автентифікації повідомлень, дозволяє побудувати зменшену модель UMAC, експериментально досліджувати колізійні властивості формованих образів (кодів).

На рис. 3.24 схематично зображений процес масштабування при розробці міні-версії UMAC.

Коефіцієнт масштабування при розробці міні-моделі UMAC обраний таким чином, щоб довжина формованих геш-кодів Y, псевдовипадкових підкладок Pad і кодів автентифікації повідомлень $Tag = Y \oplus Pad$ дорівнювала довжині блоку міні-версії блокового симетричного шифру AES, тобто 16 бітам. Вибір такого коефіцієнта масштабування дозволяє, з одного боку, зберегти алгебраїчну структуру основних перетворень алгоритму UMAC, у тому числі й вхідного в його схему алгоритму AES, а з іншого боку це дає можливість провести експериментальні дослідження з використанням методів статистичної перевірки гіпотез і математичної статистики, розглядаючи обмежений набір елементів Y, що Pad і $Tag = Y \oplus Pad$ й відповідають результати за оцінкою числа колізій як вибірку з генеральної сукупності.

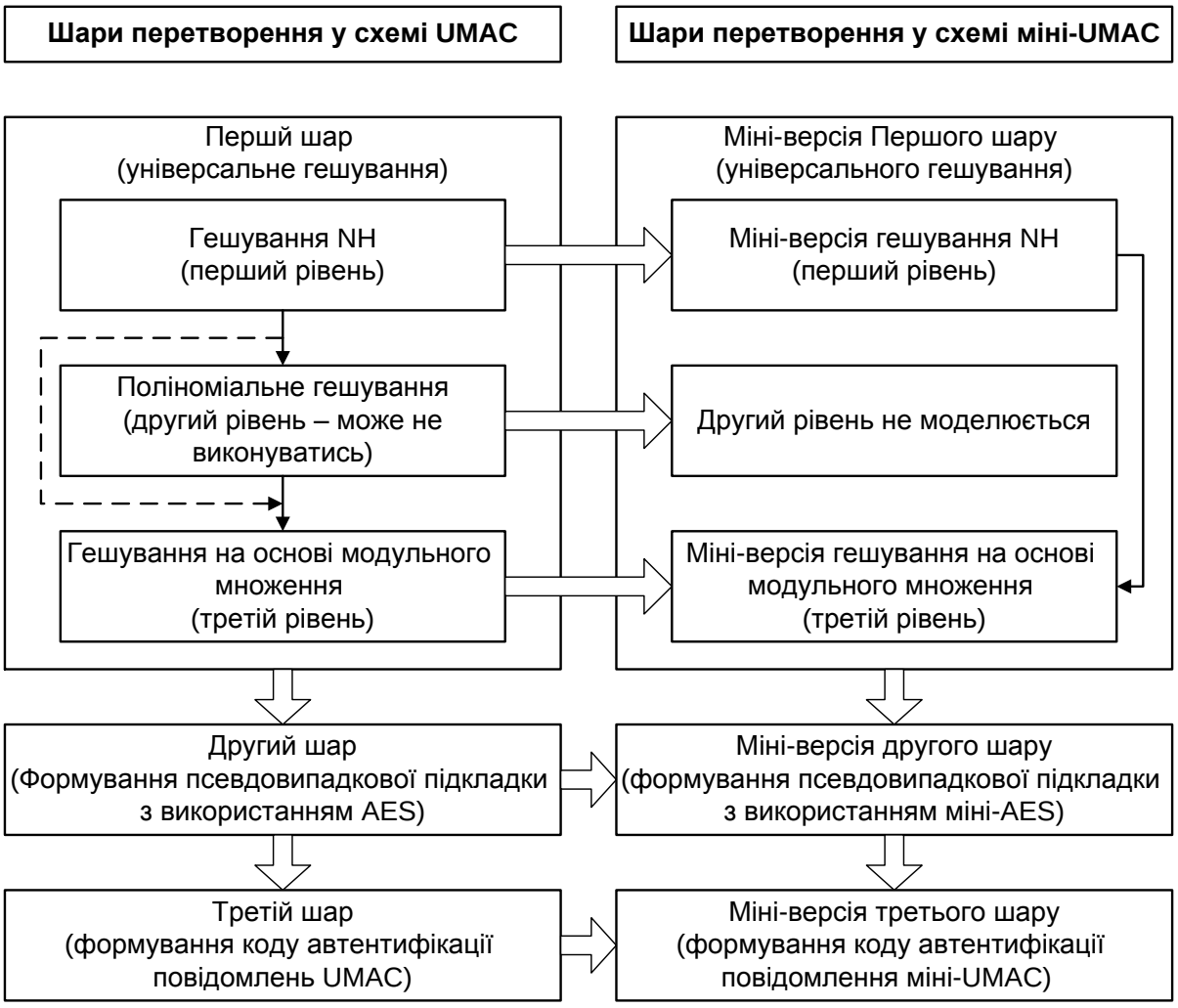


Рис. 3.24. **Схема масштабування UMAC**

Для проведення статистичного дослідження колізійних властивостей сформованих елементів введемо методику, в основі якої лежить емпірична оцінка максимумів числа ключів (правил гешування), при яких:

1. Для довільних $x_1, x_2 \in A$, $x_1 \neq x_2$ виконується рівність:

$$h(x_1) = h(x_2). \tag{3.1}$$

2. Для довільних $x_1 \in A$ та $y_1 \in B$ виконується рівність:

$$h(x_1) = y_1. \tag{3.2}$$

3. Для довільних $x_1, x_2 \in A$, $x_1 \neq x_2$ та $y_1, y_2 \in B$ виконується рівність:

$$h(x_1) = y_1, h(x_2) = y_2. \quad (3.3)$$

Оцінка за першим критерієм відповідає перевірці здійсненності умови для універсального класу геш-функцій, оцінка за другим і третім критерієм умов для строго універсального класу геш-функцій.

Введемо такі позначення:

$$n_1(x_1, x_2) = \left|\{h \in H : h(x_1) = h(x_2)\}\right|,\ x_1, x_2 \in A,\ x_1 \neq x_2;$$
$$n_2(x_1, y_1) = \left|\{h \in H : h(x_1) = y_1\}\right|,\ x_1 \in A,\ y_1 \in B;$$
$$n_3(x_1, x_2, y_1, y_2) = \left|\{h \in H : h(x_1) = y_1, h(x_2) = y_2\}\right|,\ x_1, x_2 \in A,\ x_1 \neq x_2,$$
$$y_1, y_2 \in B.$$

Перший показник $n_1(x_1, x_2)$ характеризує число правил гешування, при яких для заданих $x_1, x_2 \in A$, $x_1 \neq x_2$, виконується рівність (3.1), тобто число ключів, при яких існує колізія (збіг геш-кодів) для двох вхідних послідовностей x_1 і x_2.

Другий показник $n_2(x_1, y_1)$ характеризує число правил гешування, при яких для заданих $x_1 \in A$, $y_1 \in B$, виконується рівність (3.2), тобто число ключів, при яких для вхідної послідовності x_1 значення геш-коду y_1 не змінюється.

Третій показник $n_3(x_1, x_2, y_1, y_2)$ характеризує число правил гешування, при яких для заданих $x_1, x_2 \in A$, $x_1 \neq x_2$, $y_1, y_2 \in B$, виконується рівність (3.3), тобто число ключів, при яких для двох вхідних послідовностей x_1 та x_2 відповідні їм значення геш-кодів y_1 і y_2 не змінюються.

Оскільки число ключів, при яких можуть виконуватися рівності (3.1), (3.2) та (3.3), не повинне перевершувати відповідних їм значень $P_{кол}\ |H|$, $|H|/|B|$ та $P_{кол}|H|/|B|$, то розглядатимемо максимальне число таких ключів для кожного з розглянутого набору елементів.

Обмежимося вивченням статистичних характеристик максимумів цих величин, а потім порівняємо отримані результати з числом $P_{кол} \times H$ (для першого критерію), з числом $|H|/|B|$ (для другого критерію) і числом $P_{кол}|H|/|B|$ (для третього критерію).

Таким чином, в якості статистичних показників оцінки колізійних властивостей, за якими будемо проводити експериментальні дослідження, пропонується використовувати:

математичні очікування $m(n_1)$, $m(n_2)$ та $m(n_3)$ максимумів числа правил гешування, при яких виконуються рівності (3.1), (3.2) та (3.3), відповідно;

дисперсії, $D(n_1)$, $D(n_2)$ та $D(n_3)$, що характеризують розсіювання значень числа правил гешування, при яких виконуються рівності (3.1), (3.2) та (1.3), щодо їх математичних сподівань $m(n_1)$, $m(n_2)$ та $m(n_3)$, відповідно.

Оцінювання колізійних властивостей за наведеними критеріями будемо робити в середньостатистичному сенсі. Іншими словами, при постановці експерименту будемо використовувати обмежений набір елементів $x_1, x_2 \in A$, $x_1 \neq x_2$, і відповідних їм геш-образів $y_1, y_2 \in B$, розглядаючи відповідні результати як вибірку з генеральної сукупності.

Оцінкою для математичного сподівання m випадкової величини X є середнє арифметичне значення X_i (або статистичне середнє).

$$\tilde{m} = \frac{1}{N} \sum_{i=1}^{N} X_i,$$

де N − кількість реалізацій випадкової величини X.

Оцінка дисперсії випадкової величини X визначається виразом

$$\tilde{D} = \frac{1}{N-1} \sum_{i=1}^{N} (X_i - \tilde{m})^2.$$

У силу центральної граничної теореми теорії ймовірностей при великих значеннях кількості реалізацій N середнє арифметичне буде мати розподіл, близький до нормального з математичним очікуванням

$$m[\tilde{m}] \approx \tilde{m}$$

і середнім квадратичним відхиленням

$$\sigma[\tilde{m}] \approx \frac{\sigma}{\sqrt{N}},$$

де σ − середнє квадратичне відхилення оцінюваного параметру.

При цьому вірогідність того, що оцінка відхилиться від свого математичного сподівання менше, ніж на (довірча ймовірність), дорівнює:

$$P(|\tilde{m} - m| < \varepsilon) \approx 2\Phi\left(\frac{\varepsilon}{\sigma[\tilde{m}]}\right), \qquad (3.4)$$

де $\Phi(x)$ − функція Лапласа, визначається виразом

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_0^x e^{\frac{t^2}{2}} dt. \qquad (3.5)$$

Таким чином, при проведенні експериментальних досліджень колізійних властивостей будемо використовувати методи статистичної перевірки гіпотез і математичної статистики.

1. З генеральної сукупності випадкової величини *X* сформуємо вибірку обсягу *N: X1, X2, ..., XN*:

для середньостатистичного оцінювання математичного сподівання $m(n_1)$ і дисперсії $D(n_1)$ в якості випадкової величини виступає максимум $n_1(x_1, x_2)$ за всіма $h(x_1) = h(x_2)$ для заданих x_1 і x_2, отже, вибірку сформуємо відбором з *N* пар елементів, $x_1, x_2 \in A$, $x_1 \neq x_2$;

для середньостатистичного оцінювання математичного сподівання $m(n_2)$ і дисперсії $D(n_2)$ в якості випадкової величини виступає максимум за всім $y_1 = h(x_1)$, отже, вибірку сформуємо відбором з *N* пар елементів $x_1 \in A$, $y_1 \in B$;

для середньостатистичного оцінювання математичного сподівання $m(n_3)$ і дисперсії $D(n_3)$ в якості випадкової величини виступає максимум $n_3(x_1, x_2, y_1, y_2)$ за всіма парами $y_1 = h(x_1)$ та $y_2 = h(x_2)$, отже, вибірку сформуємо відбором з N четвірок елементів $x_1, x_2 \in A$, $x_1 \neq x_2$, $y_1, y_2 \in B$.

2. При експериментальних дослідженнях колізійних властивостей гешування:

за першим критерієм будемо оцінювати середнє арифметичне $\tilde{m}(n_1)$ спостережуваних значень максимумів $n_1(x_1, x_2)$ і дисперсію $\tilde{D}(n_1)$;

за другим критерієм будемо оцінювати середнє арифметичне $\tilde{m}(n_2)$ спостережуваних значень максимумів $n_2(x_1, y_1)$ і дисперсію $\tilde{D}(n_2)$;

за третім критерієм будемо оцінювати середнє арифметичне $\tilde{m}(n_3)$ спостережуваних значень максимумів $n_3(x_1, x_2, y_1, y_2)$ і дисперсію $\tilde{D}(n_3)$.

3. Обґрунтуємо достовірність отриманих середньостатистичних оцінок. Для цього зафіксуємо точність ε і розрахуємо значення функції

Лапласа, яка, відповідно до виразу (3.4), дає відповідні довірчі ймовірності:

$$P(\left|\tilde{m}(n_1)-m(n_1)\right|<\varepsilon \lesssim 2\Phi\left(\frac{\varepsilon}{\sigma[\tilde{m}(n_1)]}\right),\ \sigma[\tilde{m}(n_1)]\approx\frac{\sqrt{\tilde{D}(n_1)}}{\sqrt{N}};$$

$$P(\left|\tilde{m}(n_2)-m(n_2)\right|<\varepsilon \lesssim 2\Phi\left(\frac{\varepsilon}{\sigma[\tilde{m}(n_2)]}\right),\ \sigma[\tilde{m}(n_2)]\approx\frac{\sqrt{\tilde{D}(n_2)}}{\sqrt{N}};$$

$$P(\left|\tilde{m}(n_3)-m(n_3)\right|<\varepsilon \lesssim 2\Phi\left(\frac{\varepsilon}{\sigma[\tilde{m}(n_3)]}\right),\ \sigma[\tilde{m}(n_3)]\approx\frac{\sqrt{\tilde{D}(n_3)}}{\sqrt{N}}.$$

При зворотній постановці завдання, тобто для фіксованої довірчої ймовірності $P_д$ при обсязі вибірки N довірчий інтервал визначимо таким чином:

$$\tilde{m}-t_\rho\cdot\sigma[\tilde{m}]<m<\tilde{m}+t_\rho\cdot\sigma[\tilde{m}], \qquad (3.6)$$

де t_ρ – корінь рівняння $2\Phi(t_\rho)=P_д$.

Іншими словами, в цьому випадку межі довірчого інтервалу будуть відповідати заданій довірчій ймовірності $P_д$, а точність оцінок визначається як $\varepsilon=t_\rho\cdot\sigma[\tilde{m}]$.

Для цього випадку при заданій імовірності $P_д$ маємо:

$$\tilde{m}(n_1)-t_\rho\cdot\frac{\sqrt{\tilde{D}(n_1)}}{\sqrt{N}}<m(n_1)<\tilde{m}(n_1)+t_\rho\cdot\frac{\sqrt{\tilde{D}(n_1)}}{\sqrt{N}},\ \varepsilon=t_\rho\cdot\frac{\sqrt{\tilde{D}(n_1)}}{\sqrt{N}};$$

$$\tilde{m}(n_2)-t_\rho\cdot\frac{\sqrt{\tilde{D}(n_2)}}{\sqrt{N}}<m(n_2)<\tilde{m}(n_2)+t_\rho\cdot\frac{\sqrt{\tilde{D}(n_2)}}{\sqrt{N}},\ \varepsilon=t_\rho\cdot\frac{\sqrt{\tilde{D}(n_2)}}{\sqrt{N}};$$

$$\tilde{m}(n_3)-t_\rho\cdot\frac{\sqrt{\tilde{D}(n_3)}}{\sqrt{N}}<m(n_3)<\tilde{m}(n_3)+t_\rho\cdot\frac{\sqrt{\tilde{D}(n_3)}}{\sqrt{N}},\ \varepsilon=t_\rho\cdot\frac{\sqrt{\tilde{D}(n_3)}}{\sqrt{N}}.$$

На основі описаної методики досліджують статистичну безпеку ключових геш-функцій. Визначені рекомендації вибору параметрів геш-кодів використовуються в процедурі гешування повідомлення в ЕЦП для забезпечення необхідного рівня цілісності й автентичності даних.

Слід зазначити, що не доведено існування таких геш-функцій, для яких обчислення за такою методикою заданого значення геш-функції теоретично неможливо. Зазвичай знаходження значення геш-функції є

лише обчислювально складним завданням. На сьогоднішній момент немає математичного обґрунтування цієї методики для UMAC-32.

Алгоритм UMAC був розроблений так, щоб забезпечити паралельні обчислення в SIMD архітектурі. SIMD архітектура забезпечується регістрами, які, в деяких інструкціях, можуть поводитися зі словами малого розміру, як з векторами. Одна із найшвидших реалізацій UMAC використовує MMX інструкції Pentium, які поводяться з 64 бітовим регістром, як з чотиривимірним вектором по 16 біт.

Залежно від установки початкових параметрів алгоритму UMAC вивчено п’ять схем: UMAC-STD-30, UMAC-STD-60, UMAC-MMX-15, UMAC-MMX-30 і UMAC-MMX-60.

Результати випробувань схем UMAC (1999) з оцінкою швидкості обчислень подані в табл. 3.12 [268].

Таблиця 3.12

Швидкість обчислення UMAC, яка вимірюється в Гбіт/с (циклу/байт)

Алгоритм	Pentium II	PowerPC	Альфа
UMAC-STD-60	1.49 (1.93)	1.81 (1.58)	1.03 (2.78)
UMAC-STD-30	2.79 (1.03)	2.28 (1.26)	1.79 (1.60)
UMAC-MMX-60	2.94 (0.98)	4.21 (0.66)	0.287 (10.0)
UMAC-MMX-30	5.66 (0.51)	7.20 (0.39)	0.571 (5.02)
UMAC-MMX-15	8.47 (0.33)	10.5 (0.27)	0.981 (2.85)
CBC-MAC-RC6	0.162 (17.7)	0.210 (13.7)	0.068 (42.5)
HMAC-SHA1	0.227 (12.6)	0.228 (12.6)	0.117 (24.5)

Аналіз табл. 3.12 показує, що найбільша швидкість обчислення на різних апаратних платформах займають схеми алгоритму UMAC, на Pentium II та PowerPC – схема UMAC-MMX-15, а на Альфа – UMAC-STD-60.

Підвищення швидкості обчислень, особливо при повідомленнях малої довжини, було досягнуте в UMAC (2000), де запропоновано дві схеми: UMAC-32 (без SIMD паралелізму) і UMAC-16 (з SIMD паралелізмом), що дозволило досягти продуктивності в три рази більшої, ніж при перших версіях UMAC-STD і UMAC-MMX, наведено в табл. 3.13.

Таблиця 3.13

Продуктивність алгоритмів UMAC для різних довжин даних

Алгоритм	43 байт	256 байт	1500 байт	256 Кбайт
UMAC-32	16.3	3.8	2.1	1.9
UMAC-STD	52.9	12.3	3.8	1.9
UMAC-16	14.0	2.7	1.2	1.0
UMAC-MMX	35.9	4.5	1.7	1.0

Висока швидкість забезпечується за рахунок того, що MAC-код обчислюється за схемою: результат гешування $\oplus$ PRF (показник новизни), який посилається одержувачу разом з повідомленням і показником новизни.

Максимальний коефіцієнт стиснення досягається на повідомленнях 4 Кбайт. UMAC виконується краще всього на довгих повідомленнях тому, що геш-функція є тоді більш ефективною через скорочення кількості обчислень, що доводяться на псевдовипадкову функцію PRF. У якості PRF функції застосовується одна з криптографічних геш-функцій у режимі CBC-MAC або HMAC. Деякий виграш у швидкості з'являється вже при довжинах повідомлення в пару сотень байт.

У табл. 3.14 представлені основні результати щодо параметрів і оцінки швидкодії основних алгоритмів формування MAC-кодів для різних операційних платформ [203; 223; 239].

Таблиця 3.14

Швидкодія алгоритмів формування MAC-кодів

Алгоритм	Довжина MAC коду (біт)	Довжина ключа (біт)	Тип ПЕОМ				
			Pentium 2	PIII/Linux	Pentium 4	Xeon	AMD
TTmac	160	160	21	21	40	37	21
Umac-16	64	128	6.1	6.0	6.2	6.1	6.2
Umac-32	64	128	2.5	2.9	6.7	6.6	1.9
HMAC-MD5	128	512	7.2	7.3	9.4	9.4	7.4
HMAC-SHA-1	160	512	16	15	25	24	12
HMAC-Tiger	192	512	24	21	28	26	20
CBCMAC-DES	64	56	62	61	72	69	54

Аналіз алгоритмів формування MAC-код показав, що для нових криптографічних систем можна рекомендувати MAC-коди, засновані на застосуванні безключових геш-функцій (HMAC коди) і MAC-коди, засно-

вані на використанні сімейства універсальних геш-функцій (UMAC-16, UMAC-32).

На рис. 3.25 наведена пропускна здатність, вимірювана в машинних циклах за байт, для аутентифікації і гешування повідомлень різної довжини. Результати були зібрані на 700 МГц Pentium III.

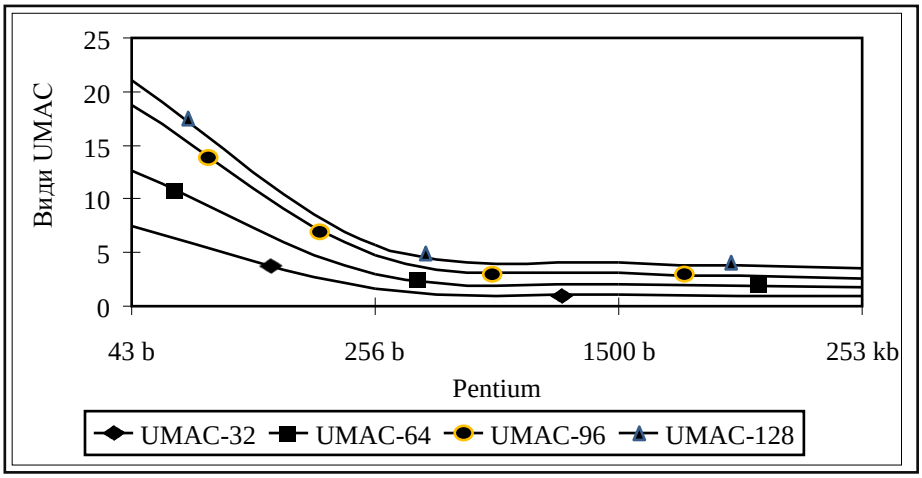


Рис. 3.25. **Порівняльна характеристика видів UMAC**

Аналіз рис. 3.25 показує, що UMAC-32, на відміну від інших версій, є найшвидшим серед інших версій оскільки він використовує "полегшену" безпеку: аутентифікаційні теги з 32-біт забезпечують корисні гарантії безпеки, коли підробки не катастрофічні, і обчислювальне середовище обмежене. Теги цієї довжини були стандартними для роздрібних банківських послуг, але великі теги є більш безпечними для багатьох додатків.

На рис. 3.26 представлена порівняльна характеристика MAC-кодів.

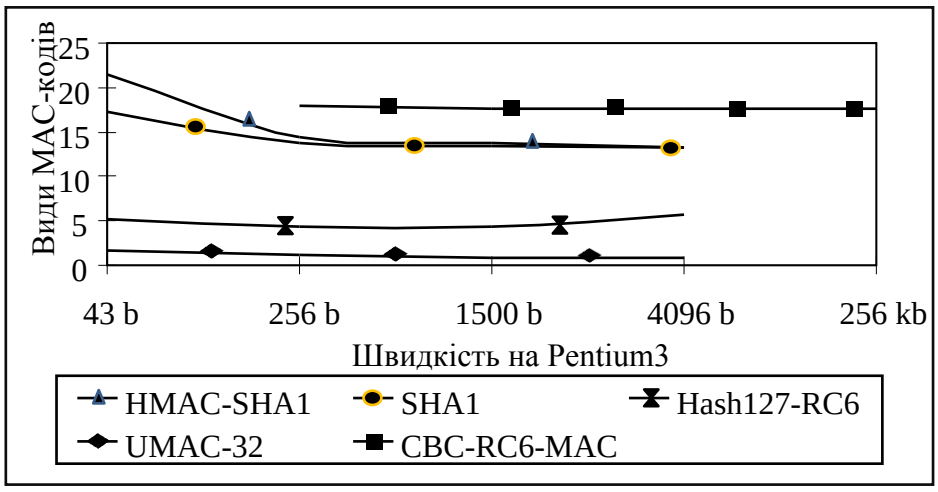


Рис. 3.26. **Порівняльна характеристика MAC-кодів**

Аналіз рис. 3.26 показує, що UMAC-32 не має суттєвих залежностей між довжиною повідомлення і швидкістю генерації MAC-коду, що не можна сказати про інші алгоритми.

Таким чином, порівняльний аналіз методів формування кодів контролю цілісності й автентичності даних показав, що найбільш ефективним механізмом при побудові MAC слід вважати багатошарові конструкції з використанням методів універсального гешування й блокових симетричних шифрів (на прикладі схеми UMAC). Такі механізми дозволяють забезпечити надзвичайно високу швидкість обробки інформаційних даних (> 10^9 біт/с), а застосування методів криптографічного перетворення інформації забезпечує їх високу безпеку. Застосування універсального гешування в багатошаровій конструкції MAC дозволяє забезпечити рівноймовірність формування геш-образів (кодів контролю цілісності й автентичності даних) для всієї множини використовуваних ключових даних.

Розділ 4. Методи та моделі прийняття управлінських рішень

4.1. Раціональний вибір і ефективне рішення

Проведено аналіз та узагальнення понять "раціональний вибір", "корисність управлінського рішення", які базуються на головних засадах теорії прийняття рішень та теорії корисності.

Завдання вибору або прийняття рішень є одним із центральних у будь-якій сфері людської діяльності [5; 119; 120; 125; 165 – 167]. Рішення приймаються для досягнення конкретної мети або бажаних результатів, які необхідно отримати в ході планованої операції. Одне з основних допущень при цьому полягає в тому, що особа, що приймає рішення (ОПР), робить раціональний вибір або ухвалює якнайкраще рішення. Поведінка людини при виборі і механізм порівняльної оцінки альтернатив є проблематикою спеціальної гілки науки, яка отримала назву теорії корисності [59].

Згідно з цією теорією, корисність – це суб'єктивна оцінка альтернативи – міра, за допомогою якої ОПР цілеспрямовано визначає її якість.

У різних фахівців завжди є мета, щодо якої визначається корисність об’єкта оцінки [15; 23; 125; 157]. Тому існує декілька визначень поняття "корисність". Корисність – цілеспрямована міра, визначувана щодо завдання оцінки, яка ставиться керівником процесу оцінки, і що фіксується в документації. Користь може бути виражена, наприклад, у зростанні прибутку, в поліпшенні екологічного стану навколишнього середовища, в збільшенні сегмента ринку, в підвищенні продуктивності праці, в підвищенні іміджу ОПР, престижу його фірми тощо. Інакше корисність – це величина, яку в процесі вибору максимізувала відповідальна особа або особа, яка слідує аксіомам раціонального вибору [15]. У цілому можна сказати, що корисність – це уявна міра психологічної і споживацької цінності різних благ.

Корисність управлінського рішення полягає у виборі найбільш адекватного зовнішнім і внутрішнім умовам розвитку підприємства рішення.

Якнайкраще рішення є тією з альтернатив, серед наявних варіантів досягнення мети, яка розглядається ОПР як найголовніший претендент на звання "рішення". Вербально "якнайкраще рішення" можна визначити як альтернативу, яку ОПР, стійко виділяє серед інших, якій вона постійно віддає перевагу порівняно з будь-якою іншою з наявних альтернатив. Проте якнайкращих рішень може бути декілька. При цьому вважають, що вони всі між собою однакові за перевагою (еквівалентні). Множинність якнайкращих альтернатив виникає з неможливості їх розрізнити при даному рівні деталізації переваг ОПР, як у разі множини Парето. Отже, для виділення єдиної якнайкращої альтернативи є тільки один шлях – послідовне уточнення переваг ОПР за додатковими аспектами (так званий принцип вкладених відносин).

Ефективність рішення – це суб’єктивна оцінка ОПР ступеня корисного ефекту даного рішення з метою усунення проблеми, що стоїть перед ним.

У будь-якому випадку перед ОПР постає завдання кількісного оцінювання міри переваги альтернатив однієї перед одною, для чого використовується функція корисності. Побудова функції корисності залежить від наявності інформації про предмет вибору і умови його функціонування.

Основою будь-якого процесу управління є інформація, якою володіє ОПР. Проблеми з недоліком інформації створюють умови невизначеності, і є перешкодою для отримання узагальненої оцінки відносної ефек-

тивності, важливості, цінності або корисності ухвалюваних рішень. Вплив невизначеності може позначатися по-різному [7].

Питаннями розробки загальних методів і моделей аналізу ситуацій і прийняття рішень займається математична дисципліна теорія прийняття рішень (ТПР) [4; 15; 22; 36; 48; 87; 93; 135; 165 – 169; 343 – 344; 347; 359; 379; 401; 405].

4.2. Головні концепції теорії прийняття рішень в управлінні складними об’єктами

Наведено огляд головних засад комплексної концепції прийняття рішень, яка вимагає врахування всіх істотних аспектів проблемної ситуації і раціональної інтеграції як логічного мислення й інтуіції людини, так і математичних і технічних засобів.

Одним з найважливіших початкових положень ТПР є теза про те, що не існує абсолютно кращого рішення. Якнайкращим рішенням може вважатися лише для даного ОПР, відносно поставленої мети, тільки в даному місці і в даний момент часу. Основне завдання ТПР полягає не в тому, щоб замінити людину в процесі вироблення рішення, а в тому, щоб допомогти їй розібратися в суті складної ситуації.

Об’єктом дослідження ТПР є ситуація прийняття рішень, або так звана проблемна ситуація (ПС).

Предметом дослідження ТПР є загальні закономірності розроблення рішень у проблемних ситуаціях, а також закономірності, властиві процесу моделювання основних елементів проблемної ситуації.

Основним призначенням ТПР є розробка для практики науково обґрунтованих рекомендацій щодо організації і технології побудови процедур підготовки і прийняття рішень у складних ситуаціях із застосуванням сучасних методів і засобів (у першу чергу, комп’ютерних систем).

Методологічну основу ТПР складають елементи системного підходу, які реалізуються в елементах наукової бази системного аналізу. Тобто це сукупності конкретних, методичних підходів, практичних методів і алгоритмів, які мають практичну спрямованість та дозволяють реалізувати теоретичні концепції і головні ідеї системного підходу в рамках соціально-економічних, екологічних, технічних проблем.

В основі сучасної ТПР лежить комплексна концепція прийняття рішень, яка вимагає врахування всіх істотних аспектів проблемної ситуації і раціональної інтеграції як логічного мислення й інтуїції людини, так і математичних і технічних засобів [119].

Згідно з цією концепцією прийняття рішення – це свідомий вибір з ряду варіантів (альтернатив). Вибір – дія, що дозволяє організувати цілеспрямовану діяльність людини. Рішення – результат вибору, який реалізований у певній нормативно-правовій формі (порада, рекомендація, наказ, програма тощо). Прийняття рішень – це процедура вибору альтернативи із заданої множини на підставі певного критерію або безлічі критеріїв. Альтернатива – кожна з двох або більше можливостей, таких, що виключають одна одну. Критерій (від грецького – засіб для вислову думок) – ознака, на підставі якої проводиться оцінювання, визначення або класифікація чого-небудь; мірило оцінювання. Особа, яка приймає рішення (ОПР) – це людина (або група осіб), які володіють правами вибору рішення і несуть відповідальність за його наслідки. Власник проблеми, який, на думку оточуючих, повинен вирішувати проблему, і несе повну відповідальність за результат її рішення. Це може бути керівник компанії, фірми, головний інженер, головний технолог і т. д. Він не є особою, яка фактично ухвалює рішення. Керівник активної групи – керівник групи фахівців, що мають загальні інтереси і прагнуть зробити вплив на процес вибору. Експерт – професіонал у певній проблемній області. Консультант щодо ухвалення рішень – координатор процесу прийняття рішень.

ОПР організує всі процедури прийняття рішень із залученням вказаних фахівців і ухвалює рішення.

Прийняття рішення полягає у виконанні послідовності таких процедур:

1) аналіз проблеми, вибір мети, задля якої проводиться вибір;

2) оцінка ступеня узгодженості мети (від повної узгодженості до повної суперечності);

3) формулювання множини альтернатив, з яких здійснюється вибір;

4) аналіз і оцінка наслідків реалізації кожної з альтернатив;

5) формулювання критерію порівняння, тобто правила, за допомогою якого визначається перевага альтернатив;

6) визначення режиму вибору: однократний або багатократний;

7) оцінка ситуації, в якій проводиться вибір (визначеність або невизначеність, її вигляд);

8) визначення типу відповідальності (індивідуальна або групова);

9) реалізація вибраного варіанта дій (результату, рішення).

Вибір критерію є складним, відповідальним завданням. Проте об'єктивно існують критерії, без яких практично неможливо оцінювати перевагу результатів будь-якої економічної або комерційної операції. Це такі критерії, як: час, витрати, прибуток, ефективність.

Показник або оцінка критерію – значення, які приймає критерій і які відображають у свідомості ОПР ступінь переваги або непереваги тих або інших властивостей результату операції. Оцінки критерію виражаються в прийнятих для їх вимірювання спеціальних шкалах. При прийнятті рішень, перш за все, необхідно сформувати модель проблемної ситуації, тобто сформулювати завдання прийняття рішення (ЗПР).

Одним з найважливіших початкових положень ТПР є теза про те, що не існує абсолютно кращого рішення. Якнайкращим рішення може вважатися лише для даного ОПР, відносно поставленої ним мети, тільки в даному місці і в даний момент часу. Основне завдання ТПР полягає не в тому, щоб замінити людину в процесі вироблення рішення, а в тому, щоб допомогти їй розібратися в суті складної ситуації.

4.3. Класифікація завдань прийняття рішень

Наведено традиційний підхід до класифікації завдань прийняття рішень та розмежування підходів до вирішення тривіальних і нетривіальних завдань. Розрізнено такі категорії завдань прийняття рішень: в умовах визначеності, в умовах невизначеності (в умовах ризику або в умовах стохастичної невизначеності, в умовах повної невизначеності, в умовах нечітко заданої інформації), багатокритеріальні задачі.

Традиційний підхід до класифікації завдань прийняття рішень заснований на безлічі ознак, що характеризують кількість і якість доступної інформації [7]. При цьому завдання прийняття рішень подаються таким кортежем:

$$< T, A, K, X, F, G, D >,$$

де *T* – постановка завдання (наприклад, синтезувати і вибрати якнайкращий варіант системи в значенні її функціональних властивостей; виявити найінформативніші параметри функціонування системи для оптимального управління; вибрати якнайкращу альтернативу зі значень параметрів функціонування системи для стабілізації її роботи);

A – безліч допустимих альтернатив для реалізації певних функцій або функціональних властивостей системи;

K – безліч критеріїв вибору (множина може включати один (скалярний) критерій або може містити декілька критеріїв (векторний критерій). Відповідно до цього завдання прийняття рішень поділяють на завдання зі скалярним критерієм і завдання з векторним критерієм або багатокритеріальні завдання;

X – безліч методів вимірювання переваг альтернатив (використання номінальної класифікаційної шкали; використання рангової шкали; використання кількісної шкали; експертне оцінювання за допомогою коментарів; експериментальне оцінювання; оцінювання на основі продукційних правил);

F – відображення безлічі допустимих альтернатив, що реалізовують функції, в безліч критеріальних оцінок. Відображення А в К може бути детермінованим; вірогіднісним; невизначеним. Відповідно до цього завдання ділять на завдання в умовах визначеності, в умовах ризику, в умовах невизначеності;

G – система переваг вирішального елемента (ОПР) (формування переваг однією особою або колективом). Відповідно до цього розрізняють: завдання індивідуального і завдання колективного прийняття рішень;

D – вирішальне правило, що відображає систему переваг вирішального елемента.

Відповідно до різних варіантів відображень А в К розрізняють такі класи завдань прийняття рішень.

1. Завдання прийняття рішень в умовах визначеності.

До цього класу відносяться завдання, для вирішення яких є достатня і достовірна кількісна інформація. У цьому випадку застосовуються методи математичного програмування. Умовами застосування цих методів є такі:

- завдання добре формалізоване, тобто існує адекватна математична модель реального світу;
- існує єдина цільова функція (критерій оптимізації), що дозволяє судити про якість порівнюваних альтернативних варіантів;

- існує можливість кількісного оцінювання значень цільової функції;
- завдання має певні ступені свободи (ресурси оптимізації) – параметри функціонування системи, які можливо змінювати в деяких межах у цілях поліпшення значення цільової функції.

2. Завдання прийняття рішень в умовах ризику.

Мають місце, коли існує можливість описати настання того або іншого результату з певною вірогідністю. Такі завдання називають завданнями прийняття рішень в умовах ризику. Для побудови розподілу вірогідності настання результатів необхідно мати представницьку статистику результатів спостережень або знання експертів. Звичайно для їх вирішення застосовуються методи одновимірної або багатовимірної корисності. Ці завдання займають проміжне становище між завданнями в умовах визначеності і невизначеності.

3. Завдання прийняття рішень в умовах невизначеності.

Ці завдання мають місце, коли інформація, необхідна для прийняття рішень, є неточною, неповною, некількісною, багатокритеріальною, а формальні моделі досліджуваної системи дуже складні або відсутні.

Цю класифікацію доцільно доповнити поняттями тривіальні та нетривіальні завдання прийняття рішень.

Завдання прийняття рішень називається тривіальною, якщо вона характеризується одним критерієм K і всім альтернативам A_i приписані конкретні числові оцінки відповідно до значень вказаного критерію (рис. 4.1) [7].

Завдання прийняття рішень перестає бути тривіальною, якщо при одному критерію кожній альтернативі відповідає не точне оцінювання, а інтервал можливих оцінок (рис. 8.2), що створює умови невизначеності.

Рис. 4.1. **Вибір альтернативи при одному критерію і точному числовому оцінюванні значень альтернатив**

Якщо при одному критерію кожній альтернативі відповідає розподіл $f(K/Ai)$ на значеннях вказаного критерію, то створюються умови ризику (рис. 4.2).

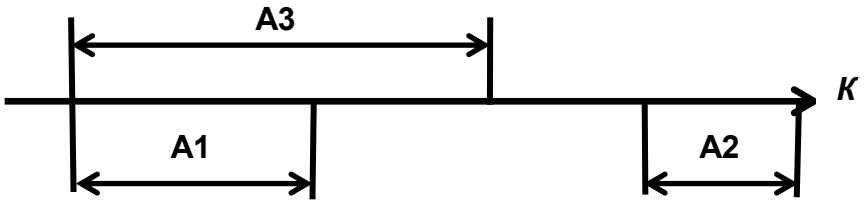


Рис. 4.2. **Вибір альтернативи при одному критерію та інтервальному оцінюванні значень альтернатив**

Наявність невизначених чинників, особливо в поєднані з багатокритеріальністю, істотно ускладнює прийняття рішень. Навіть якщо діє найбільш вивчений у теоретичному відношенні чинник – випадковість, і навіть якщо завдання однокритеріальне, то прийняти рішення не просто, оскільки потрібно враховувати відношення ОПР до ризику, до можливості понести втрати або збитки через несприятливий збіг обставин. Для випадку з іншими по своїй природі невизначеностями (поведінкової, природної) ситуація прийняття рішення ще більш ускладнюється. Наприклад, частка на ринку збуту, на яку може розраховувати ОПР, часто є невизначеною. На "суміжних сегментах" ринку конкуренти, як правило, переслідують власну мету, часто невідому ОПР, що робить процес вироблення рішення надзвичайно складним.

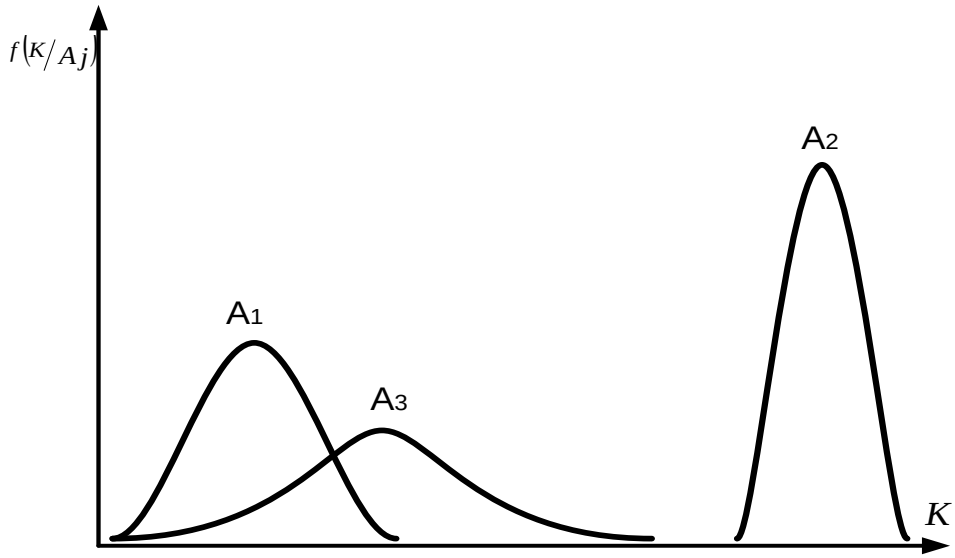


Рис. 4.3. **Вибір альтернативи при одному критерію в умовах ризику**

Отже, нетривіальними є завдання прийняття рішень в умовах наявності багатьох критеріїв, ризику та невизначеності.

4.4. Методи теорії дослідження операцій при прийнятті рішень

Наведено сферу застосування теорії дослідження операцій при вирішенні завдань прийняття рішень. У цьому разі вибір полягає у відшуканні оптимального рішення, яке максимізує (або мінімізує) цільову функцію, яка моделює ступінь переваги в значенні досягнення мети. Тобто моделі цієї теорії дозволяють вирішувати завдання прийняття рішень в умовах визначеності.

Для прийняття рішення широко використовуються методи прикладної наукової дисципліни – теорії дослідження операцій. Істотна відмінність у предметі дослідження теорії прийняття рішень і дослідження операцій полягає в тому, що застосування формальних методів дослідження операцій може бути почато тільки після отримання точного формулювання мети. Рішення полягає у відшуканні оптимального рішення, яке максимізує (або мінімізує) цільову функцію, яка моделює ступінь переваги в значенні досягнення мети. Таким чином, моделі цієї теорії дозволяють вирішувати завдання прийняття рішень в умовах визначеності. Теорія прийняття рішень як об'єкт дослідження аналізує проблему й формулює мету. Наступними етапами є вибір якнайкращого рішення й інтерпретація його для практики. ТПР закінчує застосування свого апарату тільки після вивчення ступеня визначеності проблеми, яка стояла перед ОПР, і фіксації практичного досвіду.

Існує коло завдань, заснованих на теорії дослідження операцій, для яких побудовані відпрацьовані математичні моделі, що дозволяють знаходити рішення без участі ОПР. Це завдання розподілу ресурсів, транспортні завдання, завдання масового обслуговування, управління запасами і ряд інших.

Моделі лінійного і нелінійного програмування застосовуються при прийнятті рішень в умовах визначеності, коли точно відомі всі параметри моделі [36; 114; 115]. Наприклад, при оптимальному плануванні на основі моделі лінійного програмування вигляду (4.1) необхідно мати значення параметрів: $c_j, a_{ij}, b_i, d_j, D_j$.

$$E = \sum_{j=1}^{n} c_j \cdot x_j \uparrow max(min); \qquad (4.1)$$

$$\sum_{j=1}^{n} a_{ij} \cdot x_j \le b_i; \quad i = 1,...,m;$$

$$d_j \le x_j \le D_j; \; j = 1,...,n,$$

де E – прибуток підприємства;

c_j – вартість реалізації одиниці продукції;

a_{ij} – витрати ресурсів;

b_i – запас i-го ресурсу.

У практичних розрахунках ці величини приймаються детермінованими. Насправді тільки граничні значення d_j, D_j шуканої змінної x_j є детермінованими. Решта змінних є випадковими.

Наприклад, якщо ресурс b_i – предмет поставки, то його величина залежить від термінів і об'ємів поставки.

Якщо ресурсом є устаткування, то його кількість залежить від надійності устаткування; потреби в ресурсах або витрати ресурсів a_{ij} залежать від якості продукції і т. д. Тому прийняття рішення про оптимальний випуск продукції на підставі моделі (4.1) насправді є прийняттям рішення в умовах невизначеності.

Завдання (4.1) з випадковими параметрами називають завданням стохастичного програмування (СТП). Для її вирішення необхідно мати в розпорядженні параметри випадкових величин. Розглядають два підходи до вирішення таких завдань.

У першому випадку відомі діапазони зміни випадкової величини. Такі завдання називаються завданнями прийняття рішень в умовах повної невизначеності.

У другому випадку відомий закон розподілу випадкової величини і його параметри. Такі завдання називаються завданнями прийняття рішень в умовах ризику.

У разі прийняття рішень в умовах повної невизначеності на основі лінійної моделі (4.1) параметри d_j, D_j вважають детермінованими.

Якщо на підставі попередніх періодів для кожного з параметрів моделі (4.1) вдалося встановити такі межі:

$$\min c_j \le c_j \le \max c_j,$$

$$mina_{ij} \le a_{ij} \le maxa_{ij},$$

$$minb_i \le b_i \le maxb_i,$$

то розрахунок плану для двох крайніх випадків дозволяє отримати два варіанта рішень: гірший (песимістичний) та кращий (оптимістичний).

У першому випадку ресурси приймають мінімальне значення $min\, b_i$, а їх витрата – максимальне значення $max\, a_{ij}$. Тоді очікуваний прибуток E залежить від нижньої межі $min\, c_j$ вартості реалізації продукції та сам знаходиться на нижній межі. Підставивши ці значення в модель (8.1), отримаємо звичайне завдання лінійного програмування для випадку песимістичного плану, виконання якого гарантовано, але прибуток низький.

У другому випадку кращим (оптимістичним) є план, де ресурси мають максимальне значення $max\, b_i$, а їх витрата – мінімальне значення $min\, a_{ij}$, прибуток E залежить від максимального значення $max\, c_j$ та сам має максимальне значення. План в цьому випадку дасть значний ефект, але його виконання не гарантовано.

Наведений підхід повною мірою відноситься і до моделей нелінійного програмування.

4.5. Завдання прийняття рішень про оптимальний план випуску продукції в умовах визначеності

Наведено вирішення трьох завдань прийняття рішення в умовах визначеності з такими критеріями: максимізація прибутку; максимізація випуску продукції в натуральному виразі; максимізація завантаження спеціалізованого устаткування при наявності обмежень.

Показано, що в разі наявності точної математичної постановки завдання, де чітко визначені критерії, альтернативи, обмеження для прийняття рішень застосовуються методи теорії дослідження операцій.

Випуск продукції P_j характеризується наявністю ресурсів і нормами витрати a_{ij}, наведеними в табл. 4.1.

Необхідно знайти оптимальний план випуску продукції на підставі таких критеріїв:

максимізація прибутку;

максимізація випуску продукції в натуральному виразі;

максимізація завантаження спеціалізованого устаткування (типу 1 і типу 2).

Таблиця 4.1

Початкові дані для вирішення завдань пошуку оптимального плану випуску продукції

Найменування ресурсу	Вид продукції				Запас ресурсів
	P_1	P_2	P_3	P_4	
Спеціалізоване обладнання типу 1, нормо-час	7	5	10	12	1 600
Спеціалізоване обладнання типу 2, нормо-час	15	13	18	20	3 200
Складальні роботи, людино-год.	2	1	2	3	2 40
Комплектуючі вироби, шт.	1	2	4	3	400
Витрати на виготовлення 1 шт., грн	220	300	400	420	-
Відпускна ціна за 1 шт., грн	300	450	600	500	-
Мінімальний випуск, шт.	2	10	-	15	-
Максимальний випуск, шт.	40	-	50	15	-

Математична модель завдання за різними критеріями та наявними обмеженнями має такий вигляд.

За критерієм максимізації прибутку:

$$E_1 = \sum_{j=1}^{4} (C_j - S_j) \cdot x_j \to max, \qquad (4.2)$$

де C_j – відпускна ціна одиниці продукції;

S_j – витрати на виготовлення одиниці продукції;

x_j – план виготовлення продукції.

За критерієм максимізації випуску продукції в натуральному виразі:

$$E_2 = \sum_{j=1}^{4} x_j \rightarrow max. \qquad (4.3)$$

За критерієм максимізації навантаження обладнання:

$$E_3 = \sum_{i=1}^{2} \sum_{j=1}^{4} a_{ij} \cdot x_j \quad _i max, \qquad (4.4)$$

де a_{ij} – значення i-го ресурсу (спеціалізованого обладнання) для виготовлення j-ої продукції.

Обмеження на спеціалізоване обладнання типу 1:

$$\sum_{j=1}^{4} a_{1j} \cdot x_j \le 1600. \qquad (4.5)$$

Обмеження на спеціалізоване обладнання типу 2:

$$\sum_{j=1}^{4} a_{2j} \cdot x_j \le 3200. \qquad (4.6)$$

Обмеження на складальні роботи:

$$\sum_{j=1}^{4} a_{3j} \cdot x_j \le 240. \qquad (4.7)$$

Обмеження на комплектуючі вироби:

$$\sum_{j=1}^{4} a_{4j} \cdot x_j \le 400. \qquad (4.8)$$

Обмеження на планові значення змінних:

$$2 \le x_1 \le 40,\ x_2 \ge 10,\ x_3 \le 50,\ x_4 = 15. \qquad (4.9)$$

Рішення для цих варіантів наведено в табл. 4.2.

Таблиця 4.2

Результат вирішення завдань оптимізації плану випуску продукції

Рішення	P_1	P_2	P_3	P_4	
План випуску продукції в разі максимізації прибутку	12	172	0	15	–

План випуску продукції в разі максимізації випуску продукції в натуральному виразі	12	172	0	15	–
План випуску продукції в разі максимізації завантаження спеціалізованого обладнання	12	172	0	15	–
Максимальний прибуток: **27 883,33 грн**					
Максимальний випуск продукції: **199 шт.**					
Максимальне навантаження спеціалізованого обладнання: **3 826,67** нормо-год.					

Отримані результати дозволяють ОПР прийняти рішення про такий план випуску продукції:

для продукції P_1 – 12 шт.;

для продукції P_2 – 172 шт.;

для продукції P_3 – 0 шт.;

для продукції P_4 – 15 шт.

Проте є широке коло завдань, що не укладаються в рамки теорії дослідження операцій. Це багатокритеріальні завдання і завдання прийняття рішень в умовах стохастичної і повної невизначеності.

4.6. Загальні принципи структуризації альтернатив

Наведено огляд головних принципів структуризації альтернатив: ранжування об'єктів, завдання функції вибору, завдання функції переваги, парне порівняння.

Основою прийняття рішень щодо варіантів рішень або вибору тих або інших альтернатив є їх порівняння або опис переваг ОПР. Далі наведені найпоширеніші з цих способів [7].

Ранжування об'єктів – представлення елементів множини A у вигляді послідовності в порядку убування (або незростання) їх переваги. При цьому не оговорюють "на скільки" один елемент переважає інший. Ранжування дозволяє вибрати з досліджуваної сукупності чинників найістотніший.

Завдання функції переваги або безпосереднє оцінювання – кожному об'єкту ставиться відповідно деяке число, наприклад, оцінка його якості в балах. Наприклад, оцінка студента на іспиті.

Завдання функції вибору $X^* = F(X)$, яка для будь-якої підмножини X множини A $(X \in A)$ дає підмножину $(X^* \in X)$ кращих, з погляду ОПР, елементів множини X. Наприклад, функція мети в оптимізаційних завданнях теорії дослідження операцій.

Парне порівняння – це встановлення переваги об'єктів при порівнянні всіх можливих пар. Тут не потрібно, як при ранжуванні, упорядковувати всі об'єкти. Необхідно в кожній з пар виявити більш значущий об'єкт або встановити їх рівність. При використанні методу частіше за все складається матриця розміром *n x n*, де *n* – кількість порівнюваних об'єктів, яку називають бінарним відношенням.

4.7. Структурування альтернатив з використанням критеріїв

Показано, що у загальному випадку критерій подають у вигляді деякої оцінної функції К, яка приймає значення на деякій безлічі оцінок ОПР, або у вигляді правила, за яким вибирається "якнайкраща альтернатива", яка відповідає максимальному або мінімальному значенню оцінної функції (залежно від значення критерію). Окремим випадком є прийняття рішень на підставі одного критерію.

Наведено приклад використання критеріальної таблиці при прийнятті рішень. Показано, що в разі вирішення багатокритеріального завдання, якщо перевага за одним критерієм спричиняє за собою таку ж перевагу за іншим критерієм, тобто критерії кооперуються, то вирішення завдання не є проблемою. Рішення багатокритеріального завдання також не становить особливої складності, якщо критерії нейтральні один відносно одного. У загальному випадку критерії конкурують один з одним. Аналіз таких ситуацій здійснюють за допомогою визначення множини Парето.

Звичайно для опису переваг ОПР використовуються числові функції, які називаються критеріями, визначені на безлічі результатів вибору. Значення критерію характеризує ступінь інтенсивності деякої властивості результату, важливого з погляду поставленої мети. У загальному випадку критерій подають у вигляді деякої оцінної функції К, приймаючої значення на деякій безлічі оцінок ОПР, або у вигляді правила, за яким

обирається "якнайкраща альтернатива", яка відповідає максимальному або мінімальному значенню оцінної функції (залежно від значення критерію). Окремим випадком є прийняття рішень на підставі одного критерію. Такий варіант можливий у випадку завдань в умовах повної визначеності, коли критерій виражають у вигляді функції мети, тоді вибір альтернатив полягає в рішенні оптимізаційного завдання. У реальних ситуаціях доводиться приймати рішення на підставі множини критеріїв [119; 120; 162; 166; 167; 179; 368; 369; 398; 405; 409; 410; 414; 415].

Наприклад, при покупці устаткування розглядаються декілька критеріїв: вартість, надійність, продуктивність та інші. Наявність декількох критеріїв робить завдання прийняття рішень багатокритеріальним. Далі наведений приклад, який ілюструє необхідність визначення важливості критерію при виборі рішення. Кількість балів, яку набрали абітурієнти на зовнішньому незалежному оцінюванні (ЗНО):

Тараненко: математика – 88, література – 69.

Писаренко: математика – 63, література – 92.

Стратегія S_1 – прийняти у ВНЗ Тараненко, стратегія S_2 – прийняти у ВНЗ Писаренко. З погляду технічного ВНЗ переважає стратегія S_1, з погляду гуманітарного – стратегія S_2.

Завдання багатокритеріального прийняття рішень визначається безліччю можливих рішень A, векторним критерієм K і відносинами переваг на множині A.

Мета рішення завдання – пошук "оптимальної в певному розумінні альтернативи" $a^* \in A$ або групи альтернатив з урахуванням відносин переваги на основі векторного критерію, який визначає ОПР.

Звичайно для порівняння альтернатив на підставі критеріїв використовується критеріальна таблиця (табл. 4.3).

Таблиця 4.3

Критеріальна таблиця

	k_1	k_2	…	k_n
a_1	x_{11}	x_{12}	…	x_{1n}
a_2	x_{21}	x_{22}		x_{2n}
…	…	…	…	…
a_m	x_{m1}	x_{m2}	…	x_{mn}

У рядках знаходяться альтернативи, в стовпцях – критерії, на перетині рядків і стовпців – оцінка альтернатив за відповідними критеріями.

У теорії багатокритеріального аналізу метод структуризації альтернатив називають вирішальним правилом. Пошук рішення багатокритеріального завдання не є проблемою, якщо перевага за одним критерієм спричиняє за собою таку ж перевагу за іншим критерієм, тобто критерії кооперуються. Наприклад, при покупці комп'ютера покупець прагне придбати престижний, дорогий інструмент, або навпаки скромний та недорогий інструмент.

Рішення багатокритеріального завдання також не представляє особливої складності, якщо критерії нейтральні один відносно одного. Наприклад, при покупці комп'ютера покупець прагне придбати надійний, з сучасним дизайном інструмент. У загальному випадку критерії конкурують один з одним. Наприклад, невисока вартість і престижність комп'ютера. Аналіз таких ситуацій здійснюють за допомогою визначення множини Парето [119; 120; 166; 167; 179].

4.8. Альтернативи, що не домінуються, Еджворта – Парето

Показано, що принцип Парето полягає в тому, що оптимальний результат слід шукати тільки серед елементів множини рішень, що не домінуться. Парето-оптимальність рішення α^* означає, що воно не може бути поліпшено за жодним із критеріїв без погіршення за якимось іншим критерієм.

Наведено етапи вирішення багатокритеріального завдання з урахуванням множини непокращувальних рішень за принципом Парето.

Нехай оцінка трьох альтернатив виконувалася на основі двох критеріїв: вартість і надійність (табл. 4.4).

Тут альтернатива A_3 є найпереважнішою, оскільки вона не гірша решти альтернатив за всіма критеріями.

Альтернатива a_i є домінуючою відносно альтернативи a_k, якщо за всіма критеріями оцінки альтернативи a_i не гірше, ніж альтернативи a_k, а хоча б за одним критерієм оцінка a_i краще.

Таблиця 4.4

Оцінка трьох альтернатив за двома критеріями

Альтернативи	Критерій	
	Вартість	Надійність
A_1	Невисока	Низька
A_2	Висока	Висока
A_3	Низька	Висока

У прикладі альтернатива A_3 є домінуючою відносно альтернатив A_1 і A_2.

Альтернативи A_1 і A_2 не знаходяться у відношенні домінування: за вартістю краще альтернатива A_1, за надійністю – альтернатива A_2. Ці альтернативи незрівнянні.

Альтернатива a_i, для якої не існує альтернативи a_k, кращої за всіма критеріями одночасно, називається недомінуємою або оптимальною за Парето. Альтернативи, що належать множині Еджворта – Парето, прийнято називати незрівнянними – кожна з них перевершує будь-яку іншу за якимось з критеріїв.

У прикладі дві альтернативи A_1 і A_2 належать множині Парето або множині Еджворта – Парето.

Вільфредо Парето (1848 – 1923) – італійський економіст-соціолог, який першим звернув увагу на те, що починати впорядкування багатокритеріальних альтернатив треба з видалення явно гірших. З ім'ям В. Парето пов'язано ще одне математичне поняття "діаграма Парето" – гістограма, впорядкована за убуванням "стовпчиків".

Ф. Еджворт – англійський вчений, спеціалізувався на питаннях математичної економіки. Поняття "Парето-оптимальне рішення" в разі двох критеріїв Еджворт ввів до того, як в загальному вигляді його було сформульовано В. Парето. Принцип Парето полягає в тому, що оптимальний результат слід шукати тільки серед елементів множини рішень, що не домінують [119; 120].

Серед альтернатив можуть виявитися і такі, у яких оцінки за всіма критеріями гірші, ніж у інших. Такі альтернативи не є конкурентоспроможними, їх викреслюють з таблиці. Залишаються альтернативи, які хоча б

за одним критерієм не гірше, ніж інші або альтернативи, що не домінюються. Множину Парето ще називають множиною непокращуваних рішень.

Парето-оптимальність рішення a^* означає, що воно не може бути поліпшене за жодним з критеріїв без погіршення за якимось іншим критерієм.

При пошуці однієї переважної альтернативи необхідні додаткові відомості про критерії, які змогли б зменшити множину Парето.

Рішення багатокритеріального завдання зводиться до таких етапів.

1. Визначення безлічі непокращуваних рішень за Парето.
2. Отримання додаткової інформації про критерії.
3. Використання додаткової інформації, поки множина Парето не міститиме одну альтернативу або їх групу і "згортання" критеріїв.

4.9. Моделі і методи прийняття рішень в умовах багатокритеріальності

Наведено огляд та приклади використання методів прийняття рішень в умовах багатокритеріальності: парне порівняння на основі єдиної порядкової шкали, прийняття рішень на основі згортки критеріїв, метод головного критерію, метод лінійної (адитивної) згортки як метод упорядкування альтернатив, метод максимінної згортки, метод мультиплікативної згортки.

Існує ряд методів прийняття рішень в умовах багатокритеріальності [48; 59; 119; 120; 135; 159; 166; 167; 224]. Тут розглядаються деякі з них.

4.9.1. Парне порівняння на основі єдиної порядкової шкали

Отримана безліч альтернатив підлягає структуризації. Поширеним методом впорядкування альтернатив є парне порівняння на основі якісної інформації з використанням "єдиної порядкової шкали". Наприклад, необхідно упорядкувати студентів за оцінками, отриманими з математики і фізкультури, виходячи з п’ятибальної системи оцінок (табл. 4.5.) Для цього виконується впорядкування поєднання оцінок. Порівняння будь-якої пари студентів зводиться до пошуку в таблиці поєднань значень критеріїв і відповідних їм рангів. У табл. 4.6 наведені результати ранжування студентів за результатами здачі екзаменів з двох дисциплін.

Таблиця 4.5

Єдина порядкова шкала для ранжування студентів

Ранг	Математика	Фізкультура
1	5	5
2	5	4
3	5	3
4	4	5
5	4	4
6	4	3
7	3	5
8	3	4
9	3	3

Таблиця 4.6

Ранжування студентів за результатами складання двох екзаменів

№	Студент	Оцінка з математики	Оцінка з фізкультури	Ранг
1	Анікєєв	5	3	3
2	Бекетов	5	5	1
3	Руденко	3	4	8
4	Рижов	4	4	5
5	Соковенко	5	4	2
6	Степанов	3	3	9
7	Талуєв	3	5	7
8	Тимірязєв	4	5	4
9	Усов	4	3	6

Таблиця такого типу називається "єдиною порядковою шкалою".

Недоліком методу є громіздкість побудови шкали при великій кількості критеріїв.

4.9.2. Методи прийняття рішень на основі згортки критеріїв

4.9.2.1. Метод головного критерію. У методі головного критерію вибирається один з критеріїв, який якнайповніше відображає мету прийняття рішень [119; 120; 159; 165 – 167].

Решта критеріїв враховується тільки з погляду можливої вказівки їх нижніх меж.

Таким чином, багатокритеріальне завдання прийняття рішень замінюється однокритеріальним завданням з критерієм K_i, де оптимальне рішення відповідає вибору альтернативи a^*, для якої виконується умова:

$$a^* = \arg\max_{a \in A} K_j(a) \qquad (4.10)$$

при обмеженнях $K_j(a) \geq \lambda_k, k \neq i,$

де λ_k – нижня межа k-го критерію.

Далі наведений приклад використання методу головного критерію при прийнятті рішення про вибір кандидатів на посаду.

Використовується трьохбальна система оцінювання кандидатів на посаду за двома критеріями: "Освіта" і "Досвід" (табл. 4.7).

Таблиця 4.7

Критеріальна таблиця вибору кандидатів на посаду

Кандидати	Критерії	
	Освіта	Досвід
1	1	3
2	2	2
3	2	1
4	1	2
5	3	1

Перш за все, необхідно вибрати з безлічі альтернатив такі, що не домінуються. Для цього необхідно виконати парне порівняння усіх альтернатив. Перша та друга альтернативи незрівнянні. Перша альтернатива домінує четверту альтернативу, тому альтернативу 4 відкидають. Порівняння другої і третьої альтернатив дозволяє відкинути третю альтернативу. Альтернативи 1, 2, 5 незрівнянні або такі, що не домінуються, або утворюють множину Парето. Надалі розглядаються тільки альтернативи 1, 2, 5. Припустимо, другий критерій є головним, тоді оптимальним буде перший кандидат, оскільки значення $K_1 = 3$ більше всіх. При використанні обмежень на решту критеріїв рішення буде іншим.

Якщо $K_1 > 2 \quad (\lambda_1 = 2)$, то в цьому випадку максимум K_2 досягається для альтернатив 2 і 4. Але для альтернативи 4 не виконується введене обмеження. Тому оптимальною є друга альтернатива.

4.9.2.2. Лінійна (адитивна) згортка як метод упорядкування альтернатив. Найпоширеніший спосіб впорядкування альтернатив – "лінійна згортка" (зважена згортка) [119; 120; 159; 165 – 167]. Кожному критерію привласнюють певну вагу $(w_1, w_2, ..., w_n)$. Обчислюють зважені суми за кожним рядком критеріальної таблиці за формулою:

$$K(a_i) = \sum_{j=1}^{n} x_{ij} w_j, \qquad (4.11)$$

де $\sum_{j=1}^{n} w_j = 1.$

При цьому оптимальне значення альтернативи відповідає формулі (4.10).

Ранжування виконується за значенням K_i.

Лінійна згортка є прикладом найпростішої функції корисності. Далі наведений приклад застосування методу лінійної згортки.

Для прикладу оцінки кандидатів на деяку посаду вектор ваги критеріїв має вигляд: w_j: (0,4; 0,6).

Значення елементів лінійної згортки:

$$K_1 = 0{,}4 \cdot 1 + 0{,}6 \cdot 3 = 2{,}2;$$
$$K_2 = 0{,}4 \cdot 2 + 0{,}6 \cdot 2 = 2;$$
$$K_5 = 0{,}4 \cdot 3 + 0{,}6 \cdot 1 = 1{,}8.$$

Перший кандидат є найкращим.

Методу властиві такі недоліки [36; 179].

1. Низька оцінка за одним із критеріїв може бути компенсована високою оцінкою за іншим.

2. Не завжди вдається коректно оцінити вагу критеріїв.

4.9.2.3. Максимінна згортка. Більш універсальним методом вибору на підставі кількох критеріїв є максимінна згортка [4; 166; 167; 208; 343; 344]:

$$a^* = \arg\max \min_{i=1,\ldots,m;\ j=1,\ldots,n} x_{ij} w_j . \qquad (4.12)$$

Далі наведений приклад оцінки кандидатів на посаду методом максимінної згортки:

$$K_1 = \min\{0{,}4 \cdot 1;\ 0{,}6 \cdot 3\} = 0{,}4;$$
$$K_2 = \min\{0{,}4 \cdot 2;\ 0{,}6 \cdot 2\} = 0{,}8;$$
$$K_5 = \min\{0{,}4 \cdot 3;\ 0{,}6 \cdot 1\} = 0{,}6.$$
$$a^* = \max K_i .$$

Другий кандидат є найкращим на підставі максимінного критерію.

4.9.2.4. Мультиплікативна згортка. Мультиплікативна згортка використовується в моделях, заснованих на постулаті "низька оцінка хоча б за одним критерієм спричиняє за собою низьке значення функції корисності" [119; 120; 159; 165 – 167]. Згортка має вигляд:

$$K_i(a) = \prod_{j=1}^{n} (x_{ij})^{w_j}, \qquad (4.13)$$

де w_j – вага критерію,

$$0 \le x_{ij} \le 1, \quad \sum_{j=1}^{n} w_j = 1.$$

Рішення a^* є найкращим, якщо для усіх $a \in A$ виконується умова:

$$a^* = \arg\max_i K_i(a).$$

Для прикладу оцінки кандидатів на посаду при векторі ваги критеріїв (0,4; 0,6) значення критеріїв для альтернатив 1, 2, 5 такі:

$$K_1 = 1^{0,4} + 3^{0,6} = 2{,}93,$$
$$K_2 = 2^{0,4} + 2^{0,6} = 2{,}84,$$
$$K_5 = 3^{0,4} + 1^{0,6} = 2{,}55.$$

У цьому випадку перший кандидат є якнайкращим.

Побудова узагальненого критерію або "функції цінності" або "функції корисності" – неоднозначне завдання, для вирішення якого розроблено безліч методів [108; 218; 219; 253; 257 – 260].

4.10. Прийняття рішень методом аналітичної ієрархії (MAI)

Наведено загальні аспекти методу MAI, метод обчислення індексу узгодженості (ІУ) та відношення узгодженості (ВУ), принцип перевірки адекватності моделі, яка побудована за методом MAI.

Показано, що розроблені й успішно застосовуються пакети прикладних програм, які дозволяють виконувати: побудову ієрархії, порівняння альтернатив на підставі вибраних критеріїв, необхідні обчислення пріоритетів рівнів, узгодженості рішень і отримати остаточний варіант ранжування альтернатив. До них відносяться такі пакети: "Expert Choice", "Decision Greed", "ИМПЕРАТОР".

Подано модель, побудовану засобами пакета "ИМПЕРАТОР", яка дозволяє ранжувати альтернативи вибору заходів з підвищення екологічної безпеки регіону.

4.10.1. Загальні аспекти методу MAI

Метод аналізу ієрархій (MAI) – міждисциплінарний розділ науки, створений працями американського ученого Томаса Сааті, його учнів і послідовників [7; 119; 120; 135; 210]. Ця методологія відповідає природному ходу людського мислення. MAI зараз є найпопулярнішим підходом до рішення багатокритеріальних завдань. Це пояснюється тим, що багато реальних проблем можна представити у вигляді ієрархічної структури мети, підлеглих варіантів рішень (альтернатив). Крім того, MAI використовує матриці парних порівнянь, побудова яких не є складним завданням для експертів. Завдання прийняття рішення зводиться до такого.

Існують:

1) декілька однотипних альтернатив (об’єктів, дій тощо);

2) головний критерій (головна мета) порівняння альтернатив;

3) декілька груп однотипних чинників (приватних критеріїв, об’єктів, дій тощо), що впливають відомим чином на відбір альтернатив;

4) множина направлених зв’язків, вказуючих на впливи рішень, критерія і чинників один на одного.

Вимагається кожній альтернативі поставити відповідно пріоритет (число) – отримати рейтинг альтернатив. Чим переважніша альтернатива за вибраним критерієм, тим вище її пріоритет або ранг.

Результатом є вектор рангів альтернатив. Сам вибір може виконуватися ОПР одним із варіантів: вибір (вибрати або відкинути декілька варіантів з групи можливих); розподіл ресурсів (кожний з даних варіантів враховується відповідно до його пріоритету).

Структура моделі прийняття рішень у методі аналізу ієрархій становить схему (граф), а MAI є систематичною процедурою для ієрархічного представлення компонент проблеми. Метод полягає в декомпозиції проблеми на все більш прості складові і подальшій обробці послідовності думок ОПР щодо парних порівнянь. У результаті одержують відносний ступінь впливу компонент нижнього рівня на компоненти верхнього рівня. Ці оцінки виражаються чисельно. MAI включає процедури синтезу множинності думок, отримання пріоритетності критеріїв і знаходження альтернативних рішень. Отримані значення є оцінками в шкалі відносин і відповідають жорстким оцінкам (оцінкам у сильних шкалах). MAI включає такі основні етапи:

1. Декомпозиція проблеми.
2. Побудова ієрархічної структури моделі проблеми.
3. Експертне оцінювання переваг.
4. Побудова локальних пріоритетів.
5. Оцінка узгодженості думок.
6. Синтез локальних пріоритетів.
7. Висновки і пропозиції для прийняття рішень.

При практичній роботі з MAI, зокрема при роботі з пакетом "ИМПЕРАТОР" [8], використовуються такі терміни.

Вузол – загальна назва для всіх можливих вирішень (альтернатив), головного критерію (головної мети) рейтингування рішень, усіх чинників, від яких так чи інакше залежить рейтинг. Назва вузла співпадає з назвою відповідного рішення, критерію або чинника. Рішення, критерій і чинники є "вузлами" проблеми прийняття рішення.

Рівень – група всіх однотипних (рівноправних, однорідних, гомогенних тощо) вузлів. Назва рівня відображає призначення, функцію групи

вузлів у ситуації прийняття рішення. Кожний вузол визначається не тільки своєю назвою, але і назвою рівня, якому він належить.

Фокус або мета – верхній рівень моделі ієрархії. Проміжні рівні складають допоміжні критерії.

Нижній рівень складають сценарії або альтернативи, з яких потрібно зробити вибір. Значущість (важливість) елементів проміжного рівня залежить від верхнього елемента. Значущість елементів нижнього рівня залежить від елементів проміжного рівня.

Наступний за фокусом рівень можуть займати актори (дійові особи або організації), що роблять вплив на вибір альтернатив. Наступний рівень займають дії акторів.

Зв'язок – вказівка на наявність впливу одного вузла (домінуючого) на інший (підлеглий). На схемі зв'язок зображається лінією. Напрям зв'язку (і відповідної стрілки) співпадає з напрямом впливу. З погляду теорії графів зв'язок – дуга направленого графа. Зв'язок від вузла-чинника до вузла-рішеня означає, що перевага (важливість, оптимальність) рішення оцінюється ОПР з погляду дії даного чинника згідно зі шкалою Сааті.

Кластер – група вузлів одного рівня, підлеглих деякому вузлу іншого рівня – вершині кластера (домінуючому вузлу). Кластери утворюються при розстановці зв'язків між вузлами, при цьому відбувається формування кластерної структури. Важливість вузлів кластера один щодо одного оцінюється відповідно до того, який вузол є вершиною кластера. Кластер визначається: 1) своєю вершиною, 2) назвою рівня, 3) списком вузлів. Пріоритет вузла в кластері – позитивне число, що служить для кількісного виразу важливості (ваги, значущості, переваги тощо) даного вузла в кластері щодо інших вузлів кластера відповідно до критерію, укладеного у вершині кластера. Сума всіх пріоритетів вузлів кластера дорівнює одиниці. Тому часто пріоритети можна трактувати як вірогідність, частки загального ресурсу тощо залежно від випадку.

На практиці зустрічаються два типи домінантних ієрархій. Перший тип: ієрархія прямого процесу, яка проектує існуючий стан проблеми на найвірогідніше або логічне майбутнє. Другий тип: ієрархія зворотного процесу визначає програми управління, що дозволяють досягти бажаного майбутнього. У табл. 4.8 в узагальненому вигляді наведені рівні ієрархії для двох типів ієрархії.

Таблиця 4.8

Рівні ієрархії в MAI

Ієрархія прямого процесу	Ієрархія зворотного процесу
1. Макромета, яка повинна бути досягнута в результаті рішення проблеми	1. Попередні (бажані) сценарії
2. Соціальні, політичні, економічні й інші обмеження (чинники)	2. Проблеми і можливості
3. Сили, які рухають чинниками	3. Актори і коаліції
4. Актори, які керують силами	4. Мета акторів
5. Мета акторів	5. Політики акторів
6. Політики акторів	6. Програми досягнення мети
7. Контрастні сценарії	
8. Узагальнений сценарій	

4.10.2. Метод парних порівнянь у MAI. Міра узгодженості

Для парного порівняння об’єктів складають квадратну матрицю [135; 210]:

Альтернативи	A_1	A_2	…	A_j	…	A_n
A_1	a_{11}	a_{12}	…	a_{1j}	…	a_{1n}
A_2	a_{21}	a_{22}	…	a_{2j}	…	a_{2n}
…	…	…	…	…	…	…
A_i	a_{i1}	a_{i2}	…	…	…	a_{in}
…	…	…	…	…	…	…
A_n	a_{n1}	a_{n2}	…	a_{nj}	…	a_{nn}

Елемент матриці a_{ij} – міра переваги об’єкта A_i над об’єктом A_j, яка виражається експертом у сильних шкалах або у шкалі Сааті. Діагональні елементи матриці завжди дорівнюють 1. Для матриці парних порівнянь завжди виконується умова:

$$a_{ij} = 1/a_{ji}.$$

Тому експерт заповнює тільки верхню наддіагональну частину матриці парних порівнянь.

Розрізняють дві ситуації експертних оцінок порівняльної важливості об’єктів. Перша ситуація має місце, коли міра порівнюваних властивостей виражена в сильних шкалах. У цьому випадку, якщо міра

властивості об'єкта A_i рівна ω_i, а міра об'єкта A_j рівна ω_j, то міра переваги A_i порівняно з A_j рівна ω_i / ω_j. Матриця переваг у цьому випадку є узгодженою. Узгодженість означає, що якщо порівнюються n об'єктів, то достатньо $n(n-1)$ думок щодо їх порівняння, де кожний з порівнюваних об'єктів представлений, принаймні, один раз. Уся решта думок може бути виведена з отриманих. Наприклад, для матриці парних порівнянь трьох об'єктів A_1, A_2, A_3 шляхом вимірювань було отримане, що A_1 перевершує A_2 в 3 рази і в 6 разів об'єкт A_3.

Достатня кількість порівнянь дорівнює: *3 – 1 = 2*. Матриця порівнянь представлена:

Альтернативи	A_1	A_2	A_3
A_1	1	3	6
A_2	1/3	1	2
A_3	1/6	1/2	1

Оскільки $A_1/A_2 = 3$ та $A_1/A_3 = 6$, то $A_1 = A_2 \cdot 3$ і $A_1 = A_3 \cdot 6$ і $A_2 \cdot 3 = A_3 \cdot 6$, тому $A_2/A_3 = 2$ та $A_3/A_2 = 1/2$.

Таку узгодженість називають повною. Повна узгодженість включає як порядкову, так і кардинальну узгодженість.

Порядкову узгодженість називають транзитивною (якщо A_i є переважнішою ніж A_j, а A_j є переважнішою, ніж A_k, то A_i є переважнішою ніж A_k). У розглянутому прикладі – це: якщо *6 > 3*, а *3 > 1*, то *6 > 1*. Кардинальна узгодженість означає, що $a_{ij} \cdot a_{jk} = a_{ik}$. У прикладі це: $a_{12} \cdot a_{23} = a_{13}$, тобто $3 \cdot 2 = 6$.

Друга, найпоширеніша ситуація, полягає в тому, що властивості об'єктів слабо структуровані і можуть бути оцінені тільки в шкалі порядку. У цьому випадку експерти використовують шкалу Сааті. У цьому разі неможливо досягти повної узгодженості через різні кваліметричні шкали у різних об'єктів тому розглядають два показники: індекс узгодженості (ІУ) і відношення узгодженості (ВУ).

4.10.3. Індекс узгодженості (ІУ), відношення узгодженості (ВУ)

У загальному випадку узгодженість зворотно-симетричної матриці еквівалентна до вимоги рівності її максимального власного значення λ_{max} числу порівнюваних об'єктів n $(\lambda_{max} = n)$. Тому як міру розузгодженості розглядають нормоване відхилення λ_{max} від n, яке називається індексом узгодженості:

$$IУ = (\lambda_{max} - n)/(n - 1). \quad (4.14)$$

Оцінювання прийнятності отриманого узгодження виконується порівнянням його з випадковим індексом (ВІ).

Випадковий індекс – це індекс узгодженості, розрахований для квадратної n-вимірної позитивної зворотно-симетричної матриці, елементи якої згенерували датчиком випадкових чисел, розподілених за рівномірним законом для інтервалу значень: 1/9, 1/8, 1/7, 1/6, 1/5, 1/4, 1/3, 1/2, 1, 2, 3, 4, 5, 6, 7, 8, 9.

У табл. 4.9 подані значення випадкового індексу ВІ для різних матриць порядку від 2 до 15.

Таблиця 4.9

Значення випадкового індексу

Порядок матриці	2	3	4	5	6	7	8	9	10	11	12	13	14	15
ВІ	0	0,58	0,9	1,12	1,24	1,32	1,41	1,45	1,49	1,51	1,54	1,56	1,57	1,59

Відношення узгодженості обчислюється за формулою:

$$ВУ = IУУ/В. \quad (4.15)$$

Якщо значення ВУ менше ніж 0,1, то ступінь узгодженості вважається добрим.

У деяких випадках прийнятним ступенем узгодженості можна вважати діапазон (0,1 – 0,3). Якщо $ВУ > (0,1 – 0,3)$, то експерту рекомендується переглянути свої думки.

Аналіз результатів експертних оцінок полягає в отриманні вектора пріоритетів порівнюваних об'єктів.

З математичної точки зору необхідно обчислити головний власний вектор матриці.

Після нормалізації він стає вектором пріоритетів.

Точний спосіб обчислення головного власного вектора матриці складається зі зведення матриці в доволі високі ступені і розподілі суми кожного рядка на загальну суму елементів матриці.

Альтернативи	A_1	A_2	…	A_j	…	A_n	Головний власний вектор	Вектор пріоритетів
A_1	a_{11}	a_{12}	…	a_{1j}	…	a_{1n}	V_1	P_1
A_2	a_{21}	a_{22}	…	a_{2j}	…	a_{2n}	V_2	P_2
…	…	…	…	…	…	…	…	…
A_i	a_{i1}	a_{i2}	…	a_{ij}	…	a_{in}	V_i	P_i
…	…	…	…	…	…	…	…	…
A_n	a_{n1}	a_{n2}	…	a_{nj}	…	a_{nn}	V_n	P_n

Наближений спосіб, що дає добрі наближення, полягає в такому:

для матриці, яка наведена вище, компонент головного власного вектора обчислюється як середнє геометричне значень у рядку за формулою:

$$Vi = \sqrt[n]{\prod_{j=1}^{n} aij}. \qquad (4.16)$$

Компонент i вектора пріоритетів обчислюється як нормоване значення головного власного вектора:

$$Pi = \frac{Vi}{\sum_{i=1}^{n} Vi}. \qquad (4.17)$$

Наближені значення λ_{max} для оцінювання відношення узгодженості можна отримати за формулою:

$$\lambda max = \sum_{j=1}^{n} Mj \cdot Pj, \qquad (4.18)$$

де $Mj = \sum_{j=1}^{n} aij$ – сума елементів *j*-го стовпця матриці;

P_j – вектор пріоритетів аналізованої матриці.

Отримане значення λ_{max} дозволяє обчислити для зворотно-симетричної матриці індекс узгодженості за формулою (4.14) і потім відношення узгодженості за формулою (4.15).

4.10.4. Адекватність моделі, яка побудована за методом MAI

Адекватність моделі – це властивість, що полягає в здатності моделі відтворювати з необхідною повнотою ті властивості якості об’єкта, які є істотними для мети аналізу [135].

Щодо моделі, отриманої згідно з MAI, до поняття адекватності відноситься перевірка двох моментів:

1) відношення узгодженості (ВУ) повинне бути менше 0,1 (прийнятним вважається діапазон значень (0,1 – 0,3));

2) модель стійка відносно до незначних змін її структури.

Стійкість вектора пріоритетів – якісна характеристика чутливості значень пріоритетів до малих змін даних або структури моделі.

Очевидно, дані, що використовуються для прийняття рішень, завжди більш-менш неточні.

Тому чим менше чутливість значень пріоритетів, тим більше обґрунтованість використання цих пріоритетів для підтримки прийняття рішення.

Якщо при малих змінах даних або структури рейтинг змінюється неістотно, то він вважається стійким.

Розроблені й успішно застосовуються пакети прикладних програм, що дозволяють виконувати: побудову ієрархії, порівняння альтернатив на підставі вибраних критеріїв, необхідні обчислення пріоритетів рівнів, узгодженості рішень і отримати остаточний варіант ранжування альтернатив.

До них відносяться такі пакети: "Expert Choice", "Decision Greed", "ИМПЕРАТОР".

На рис. 4.4 наведено модель, побудовану засобами пакета "ИМПЕРАТОР", яка дозволяє ранжувати три альтернативи.

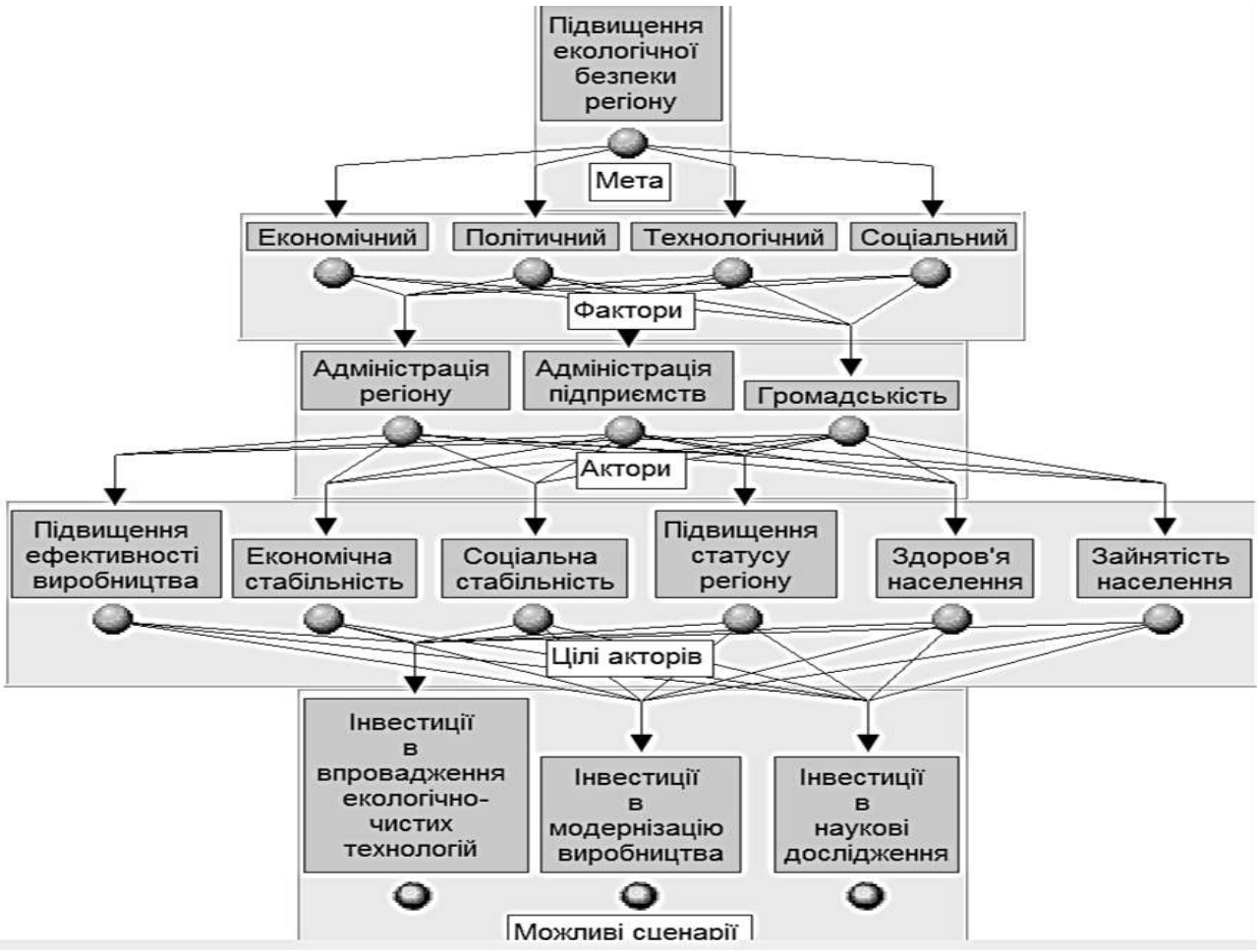


Рис. 4.4. **Модель ранжування трьох альтернатив за методом MAI**

4.11. Моделі та методи прийняття рішень в умовах нечіткої інформації, невизначеності та ризику

Показано, що в теорії прийняття рішень розрізняють такі види невизначеності: стохастична або імовірнісна та повна невизначеність. Перша має місце, коли відомі імовірності настання наслідків прийняття рішень. Її називають "доброякісна невизначеність". Наведено загальні аспекти вирішення завдань в умовах ризику та метод дерева рішень.

Вирішено завдання вибору раціональної кількості устаткування в умовах стохастичної невизначеності.

4.11.1. Виграш і ризик при прийнятті рішень в умовахневизначеності

У теорії прийняття рішень розрізняють такі види невизначеності: стохастична або імовірнісна невизначеність та повна невизначеність.

Перша має місце, коли відомі імовірності настання наслідків прийняття рішень. Її називають "доброякісна невизначеність" [36]. Друга має місце, коли інформація, необхідна для прийняття рішень, є неточною, неповною, нечіткою, некількісною, а формальні моделі досліджуваної системи або занадто складні, або відсутні.

При прийнятті рішень в умовах нечіткої інформації, невизначеності і ризику, як і в завданнях теорії статистичних рішень, розглядаються платіжні матриці (для дискретного випадку), або платіжна функція (в безперервному випадку). Значення в платіжній матриці, або в платіжній функції залежать від 2-х чинників: стан природи, варіанти рішень ОПР.

У матриці платежів розглядаються m можливих стратегій: $A_1, A_2, ..., A_m$. У стовпцях – стратегії природи: $П_1, П_2, ..., П_n$; a_{ij} – виграш при кожній парі стратегій:

Рішення	Стан природи			
	$П_1$	$П_2$	…	$П_n$
A_1	a_{11}	a_{12}	…	a_{1n}
A_2	a_{21}	a_{22}	…	a_{2n}
…	…	…	…	…
A_m	a_{m1}	a_{m2}	…	a_{mn}

Необхідно вибрати таку стратегію ОПР A_i, яка є найбільш вигідною порівняно з іншими, або таку, що максимізує деяку критеріальну функцію, що відображає систему переваг ОПР.

Оскільки стан природи не визначено при здійсненні певного вибору, то ОПР ризикує.

У цьому випадку в теорії прийняття рішень вводиться поняття "ризик". Ризиком r_{ij} гравця, що використовує стратегію A_i в умовах $П_j$, називається різниця між виграшем, який він одержав би, якби знав умови $П_j$, і виграшем, який він отримає, не знаючи їх.

Щоб отримати значення ризику r_{ij} необхідно доповнити матрицю виграшів рядком з β_j максимальними значеннями виграшів за стовпцями і побудувати матрицю ризиків з елементами:

$$r_{ij} = \beta_j - a_{ij}. \qquad (4.20)$$

У цьому випадку необхідно прийняти рішення, яке мінімізує значення ризику.

Таким чином, розрізняють дві постановки завдання про вибір рішення: у першій необхідно отримати максимальний виграш, у другій – мінімальний ризик [289].

Найпростіший випадок невизначеності "доброякісна" або стохастична невизначеність, коли стани природи мають певні імовірності p_j, які відомі ОПР. У цьому випадку необхідно вибрати стратегію, для якої середнє значення виграшу, взяте за рядком, є максимальним.

$$a_i = \sum_{j=1}^{n} a_{ij} \cdot p_j \Rightarrow max. \qquad (4.21)$$

Та ж стратегія, яка звертає в максимум середній виграш, звертає в мінімум середній ризик:

$$r_i = \sum_{j=1}^{n} r_{ij} \cdot p_j \Rightarrow min. \qquad (4.22)$$

Таким чином, у разі стохастичної невизначеності обидва підходи ("від виграшу" і "від ризику") дають одне і те ж оптимальне рішення.

Необхідно зауважити, що поняття "ризик" традиційно пов’язують з певною імовірністю або зі стохастичною невизначеністю настання тієї чи іншої небажаної події.

Тому визначення терміна "ризик" таке: "Небажана подія, що полягає в збитку або втраті, що наступає з певною імовірністю" [36].

Коли імовірності станів природи не піддаються оцінці, то для прийняття раціонального рішення роблять спробу знайти не найгірше рішення. У цьому випадку все залежить від точки зору ОПР на ситуацію, від позиції дослідника, від того, якими втратами загрожує невдалий вибір рішення. У випадку, коли імовірності p_j існують, але ОПР вони невідомі, розроблені спеціальні критерії прийняття рішень: критерій Лапласа, критерій Вальда, критерій Гурвіца, критерій Севіджа [36; 157; 159].

4.11.2. Прийняття рішень в умовах ризику

Завдання прийняття рішень в умовах ризику займають проміжне становище між завданнями прийняття рішень в умовах визначеності і в умовах повної невизначеності [7; 22; 48; 59; 72].

У цьому випадку розглядаються кілька станів природи, аналітик робить припущення про імовірність настання кожного з них. Наприклад, існує $m \cdot (m > 1)$ станів природи і p_j – оцінка імовірності настання події j. У загальному випадку значення імовірностей оцінюються на підставі статистичних даних за минулий час, де були зафіксовані прояви події протягом певного періоду спостережень.

Очікуване значення випадкової величини обчислюється як зважене середнє всіх можливих значень цієї випадкової величини, де ваги є імовірностями прийняття випадковою величиною даних значень.

Оскільки результат прийняття того чи іншого рішення залежить від станів природи, очікуваний результат, пов'язаний з рішенням і, обчислюється як сума добутків виграшу a_{ij} та імовірності p_j.

Таким чином, очікуваний результат A_i прийняття рішень обчислюється за формулою:

$$A_i = \sum_{j=1}^{m} a_{ij} \cdot p_j . \qquad (4.23)$$

Далі вибирається вирішення, яке максимізує очікуваний результат: $A = max(A_i)$.

При наявності випадкових факторів у завданні прийняття рішень необхідно враховувати не тільки переваги ОПР відносно різних наслідків, але і її ставлення (схильність) до ризику.

Моделі прийняття рішень, що відображають реальні виробничі ситуації, як правило, надзвичайно складні.

Раціональний вибір означає, що рішення ОПР є результатом послідовного процесу мислення. Процес розробки і аналізу моделі прийняття рішень в умовах ризику полягає в такому: 1) створення структури моделі; 2) визначення значень імовірностей можливих результатів; 3) визначення значень корисності можливих результатів; 4) оцінювання альтернатив і вибір стратегії.

Традиційно такі завдання вирішуються із застосуванням методу дерева рішень [7; 59; 72; 119; 120; 166; 167; 173; 379; 426].

4.11.3. Дерево рішень як метод прийняття рішень в умовах стохастичної невизначеності (в умовах ризику)

Дерево рішень – це графічна модель аналізу рішень в умовах ризику. Типове дерево рішень складається з вузлів рішень (квадрат) і вузлів випадкових подій або рішень випадку (кружок).

Гілки, що виходять із вузла рішення, представляють можливі рішення, а гілки, що виходять із вузла подій, відповідають різним випадковим подіям. На гілках дерева позначають значення імовірностей, у кінцевих гілок представляють результат дії. Дерево будують зліва направо.

У закінченому дереві рішень шлях від початкового вузла дерева до якого-небудь кінцевого вузла представляє послідовність рішень і можливих випадкових подій. Обчислення в дереві рішень виконуються за схемою зворотного перерахування, починаючи від кінцевих вузлів і закінчуючи початковим вузлом дерева. Цей метод називають методом "згортання" дерева. При цьому для вузлів подій обчислюються очікувані значення від випадкових подій, а для вузлів рішень як значення вибирається максимальне очікуване значення, обчислене для гілок, що виходять із вузла рішень.

Таким чином, по дереву рішень визначається оптимальна стратегія – послідовність рішень, які повинні виконуватися при виникненні тих або інших випадкових подій.

4.11.4. Задача вибору раціональної кількості устаткування в умовах стохастичної невизначеності

Проблеми підприємства пов’язані зі збільшеними платежами за недотримання екологічних норм (застаріле технологічне обладнання і, відповідно, застаріла технологія основного виробництва). Підприємство передбачає придбання нового обладнання по $40 \cdot 10^3$ грн, за кожний агрегат. Вигода від установки кожного агрегату складе $75 \cdot 10^3$ грн. Усе обладнання повинно бути введено в дію протягом певного часу.

Але всі агрегати не можуть бути введені в дію одночасно. Якщо підприємство закупить агрегатів більше, ніж зможе ввести в дію за відведений час, то понесе збитки, які дорівнюють вартості обладнання, яке не було введено в дію. Якщо буде закуплено недостатню кількість

агрегатів, будуть наростати екологічні проблеми. За оцінкою експертів, екологічні проблеми, пов'язані з неможливістю введення (за відведений час) в дію кожного агрегату становлять $50 \cdot 10^3$ грн. Імовірність введення в дію кількості агрегатів: 0 шт., 100 шт., 200 шт., 300 шт. оцінюються експертами в такий спосіб: $p(0) = 0,1;\ p(100) = 0,3;\ p(200) = 0,4;\ p(300) = 0,2$.

Необхідно знайти оптимальну кількість обладнання, придбання і введення в дію якого, дозволить підвищити прибуток підприємства.

Завдання відноситься до завдань прийняття рішень в умовах ризику: кожне з рішень пов'язане з певними втратами грошових коштів з певним ступенем імовірності.

У моделі чотири можливі значення рішення щодо придбання обладнання пов'язані з чотирма значеннями кількості агрегатів, які можуть бути введені в дію. У табл. 4.10 наведена матриця A значень a_{ij} прибутку підприємства (грн), де кожному з варіантів кількості придбаного устаткування відповідає варіант кількості устаткування, яке можливо ввести в дію.

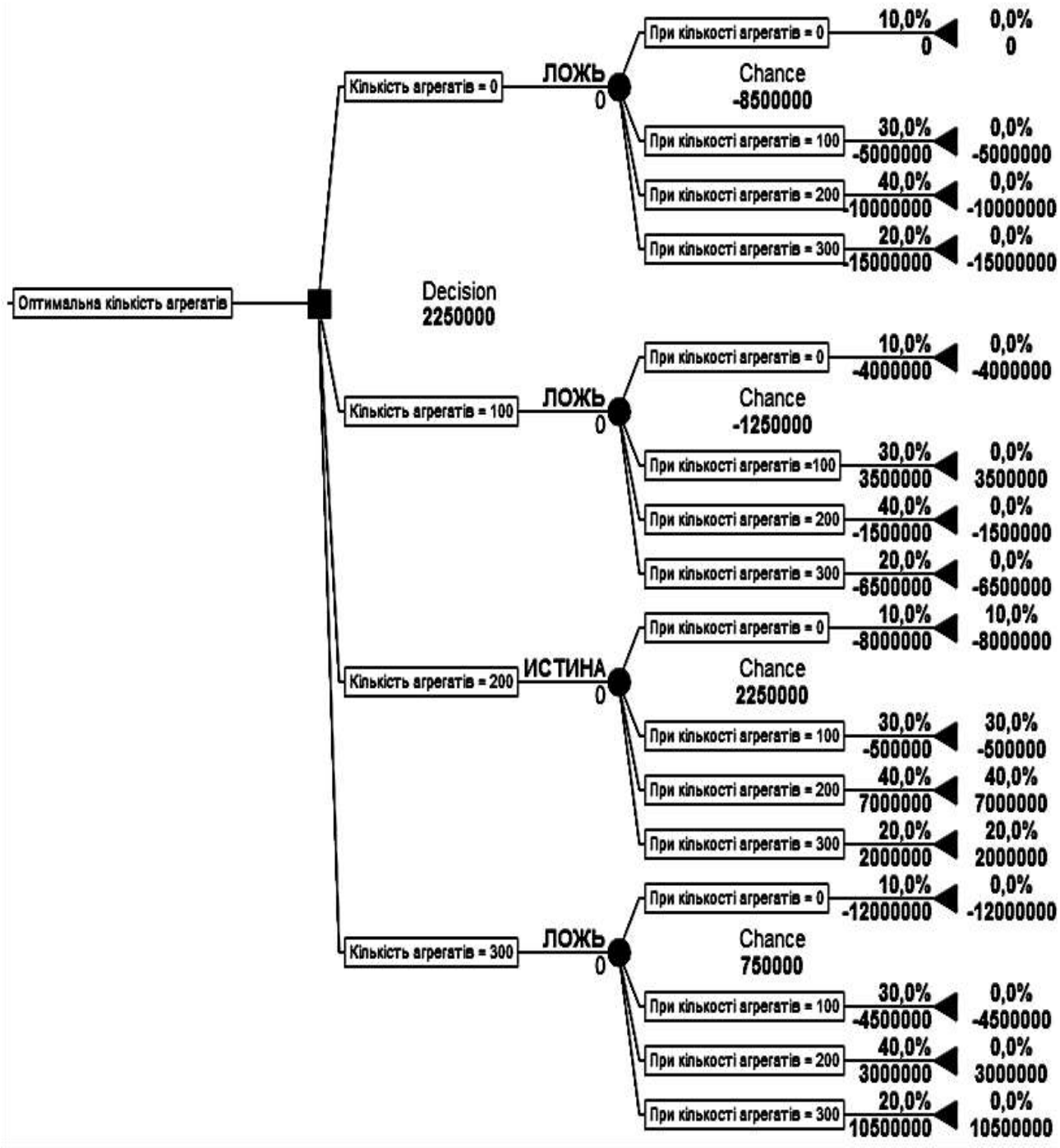


Рис. 4.5. **Результат вирішення завдання методом дерева рішень**

Таблиця 4.10

Варіанти значень прибутку підприємства (грн)

Рішення (кількість придбаного устаткування)	Стан природи (кількість устаткування, яке можливо ввести в дію)			
	0,00	100,00	200,00	300,00
0	0,00	-5 000 000,00	-10 000 000,00	-15 000 000,00
100	-4 000 000,00	3 500 000,00	-1 500 000,00	-6 500 000,00
200	-8 000 000,00	-500 000,00	7 000 000,00	2 000 000,00
300	-12 000 000,00	-4 500 000,00	3 000 000,00	10 500 000,00

На рис. 4.5 наведено дерево рішень для завдання вибору оптимальної кількості агрегатів, побудовано у середовищі пакета Precision Tree [195].

Оптимальна кількість агрегатів, яку необхідно придбати для максимізації прибутку підприємства, становить 200 штук.

4.12. Теорія ігор у прийнятті рішень

Наведено головні засади теорії ігор для вирішення завдань прийняття рішень: матричні ігри антагоністів, методи рішення кінцевих ігор та приклади вирішення завдань.

4.12.1. Ігрові методи прийняття рішень

Розділ математики "Теорія ігор і статистичних рішень" має в своєму розпорядженні методи вирішення завдань прийняття рішень в умовах повної або "поганої" невизначеності [36; 425].

У деяких випадках ці методи дозволяють знайти оптимальні рішення, але частіше вони дозволяють просто глибше розібратися в ситуації, оцінити кожне рішення з різних точок зору й ухвалити рішення, якщо не єдино правильне, то продумане. Найпростішими з ситуацій, що містять "погану невизначеність" є конфліктні ситуації, коли стикаються інтереси двох або більш сторін, що переслідують різну мету, причому виграш кожної сторони залежить від того, як поведуться інші. Це різні ситуації бойових дій, ситуації конкурентної боротьби, ситуації в спорті і т. д. Теорія ігор (ТІ) є математичною теорією конфліктних ситуацій.

Мета ТІ – розробка рекомендацій до розумної поведінки учасників конфлікту або пошук на цій основі оптимальних рішень.

Гра – це математична модель ігрової ситуації, деяка спрощена схема, де зафіксовані самі гравці, правила гри, певні виграші після кожного ходу, правила закінчення гри. Конфліктуючі сторони називаються гравцями, одне здійснення гри – партія, результат гри – виграш або програш. Причому виграш або програш має кількісний вираз.

Якщо стикаються інтереси двох учасників – гра парна, якщо більшої кількості гравців – множинна. Учасники множинної гри можуть утворювати коаліції. Множинна гра з двома постійними коаліціями перетворюється в парну. Розвиток гри в часі представляють як ряд послідовних ходів учасників.

Ходом гри називається вибір гравцем одного з передбачених правилами гри дій. Розрізняють ходи особисті і випадкові. При особистому ході гравець самостійно вибирає дію. При випадковому ході вибір здійснюється яким-небудь механізмом випадкового вибору (киданням монети, грального кістки і т. д.). Стратегією гравця називається сукупність правил, що визначають вибір варіанта дій при кожному особистому ході.

Залежно від числа стратегій гри, вони діляться на кінцеві і нескінченні. Наприклад, у грі в шахи набір стратегій кінцевий, але такий великий, що повний їх перелік практично неможливий.

Оптимальною стратегією гравця називається така, яка забезпечує йому якнайкраще становище в грі, тобто максимальний виграш.

Задача ТІ – виявлення оптимальних стратегій гравців. Основне припущення, виходячи з якого знаходяться оптимальні стратегії, полягає в тому, що супротивник щонайменше так само розумний, як і сам гравець.

Гра називається грою з нульовою сумою, якщо сума виграшей усіх гравців дорівнює нулю (кожний гравець виграє за рахунок інших). Найпростіша гра з нульовою сумою – парна гра – називається антагоністичною грою (або грою із суровим суперництвом).

4.12.2. Матричні ігри антагоністів

Хай у грі беруть участь два гравці *A* і *B*. У гравця *A* є *m* можливих стратегій $A_1, A_2, \ldots A_m$, у супротивника – *n* можливих стратегій: $B_1, B_2, \ldots B_n$,. Це гра *m x n*. У табл. 4.11 наведені стратегії гравців і значення a_{ij} – виграшів гравця *A*, якщо він користується стратегією A_i, а супротивник при цьому користується стратегією B_j (табл. 4.11).

Таблиця 4.11

Стратегії гравців і значення a_{ij}

Стратегії	B_1	B_2	…	B_n
A_1	a_{11}	a_{12}	…	a_{1n}
A_2	a_{21}	a_{22}	…	a_{2n}
…	…	…	…	…
A_m	a_{m1}	a_{m2}	…	a_{mn}

Складання такої матриці означає, що багатоходова гра зведена до одноходової – від гравця вимагається зробити вибір своєї стратегії.

Далі наведений приклад гри 4 х 5 у матричній формі (табл. 4.12).

Таблиця 4.12

Стратегії гравців і значення a_{ij}

Стратегії	B_1	B_2	B_3	B_4	B_5
A_1	3	4	5	2	3
A_2	1	8	4	3	4
A_3	10	3	1	7	6
A_4	4	5	3	4	8

Виходячи з основного принципу теорії ігор – принципу обережності (перестраховочного правила "завжди розраховуй на гірше"), необхідно вибрати стратегію, при якій мінімальний виграш гравця *A* є максимальним. Це означає, що при найгіршому для гравця *A* варіанті вибору супротивника, він отримає максимальний виграш.

У цьому полягає принцип "мінімакса": "чини так, щоб при якнайгіршій для тебе поведінці супротивника отримати максимальний виграш". Для пошуку такого варіанта рішення матрицю табл. 4.12 подають таким чином: доповнюють стовпцем з мінімальними значеннями елементів за стовпцями та знаходять максимальний з них за рядками; доповнюють рядком з максимальними значеннями елементів за рядками та знаходять мінімальний з них за стовпцями (табл. 4.13).

Таблиця 4.13

Стратегії гравців і значення a_{ij}

Стратегії	B_1	B_2	B_3	B_4	B_5	α_i
A_1	3	4	5	2	3	2
A_2	1	8	4	3	4	1
A_3	10	3	1	7	6	1
A_4	4	5	3	4	8	**3**
β_j	10	8	**5**	7	8	

Обережна стратегія A_4 гравця A забезпечує йому гарантований виграш і полягає у виборі найбільшого з якнайменших значень α (менше значення $\alpha = 3$ він отримати не може). Цей виграш називається нижньою ціною гри або максиміном**.**

Розумний супротивник B бажає віддати менше, але повинен розраховувати на розумну поведінку гравця A. Він повинен вибрати таку стратегію, при якій β приймає якнайменше значення ($\beta = 5$, більш ніж 5 він віддати не зможе). Ця стратегія називається верхньою ціною гри або мінімаксом.

Ці стратегії гравця A і B витікають з принципу мінімакса, і називаються мінімаксними.

Поки супротивники дотримуються цих стратегій, виграш буде рівний α = 3. Якщо супротивники в припущенні майбутніх дій партнера міняють стратегії, говорять, що стратегії нестійкі відносно інформації про поведінку іншої сторони або не володіють властивістю рівноваги.

Наприклад, гравець A дізнався про те, що гравець B вибрав стратегію B_3 (з $a_{33} = 1$), у відповідь він вибере A_1 (з $a_{13} = 5$). Але гравець B, дізнавшись про це, вибере стратегію B_4, тоді виграш гравця A замість 3 стане рівним 2.

У прикладі (табл. 4.14) нижня ціна гри дорівнює верхній ціні гри $\alpha = \beta = v = 6$.

Таблиця 4.14

Стратегії гравців і значення a_{ij}

Стратегії	B_1	B_2	B_3	B_4	α_i
A_1	2	4	7	5	2
A_2	7	**6**	8	7	**6**
A_3	5	3	4	1	1
β_j	7	**6**	8	7	

У разі, коли нижня ціна гри α дорівнює верхній ціні гри β, мінімаксні стратегії гравців є стійкими і рівними ціні гри: $\alpha = \beta = v$.

Поки гравці дотримуються мінімаксних стратегій, виграш дорівнює 6. Якщо гравець A дізнався про стратегію B_2 гравця B і робить спробу змінити стратегію A_2, це тільки погіршить його становище. Те ж відноситься і до гравця B. У цьому випадку пара стратегій A_2, B_2 має властивість рівноваги, а виграш, що досягається в цьому випадку називається "сідловою точкою".

Термін "**сідлова точка**" з'явився з геометрії, де він означає точку на поверхні, де одночасно досягається мінімум за однією координатою і максимум за іншою.

Для матриці з сідловою точкою характерно те, що елемент, мінімальний у своєму рядку є максимальним у своєму стовпці.

Стратегії A_i, B_j (A_2, B_2 у табл. 4.14), при яких досягається виграш "сідлова точка", називаються оптимальними чистими стратегіями, а їх сукупність – рішенням гри. Сама гра називається грою в чистих стратегіях. Для двох гравців A і B такий результат є якнайкращим з можливих. У прикладі табл. 4.14 гравець A виграє 6, гравець B програє 6 (але не більше).

Наявність "сідлової точки" швидше не правило, а виключення. Наприклад, наведена далі матриця не має сідлової точки:

$$\begin{bmatrix} 3 & 2 & 1 \\ 1 & 3 & 4 \end{bmatrix}.$$

Існує обмежена кількість ігор, які завжди мають "сідлову точку", значить, розв'язуються в чистих стратегіях.

Це ігри з повною інформацією, де кожний гравець знає всю передісторію гри, результати всіх ходів (особистих і випадкових). Прикладами таких ігор є: шашки, шахи "хрестики і нулі".

Бувають матриці з декількома сідловими точками. Наприклад, така матриця має чотири сідлові точки.

$$\begin{bmatrix} 1 & 2 & 5 & 1 \\ 1 & 4 & 8 & 1 \\ -3 & 7 & 1 & 0 \end{bmatrix}.$$

Це значення "1" у першій та другій стрічках, у першому та четвертому стовпчиках. У матриці, що складається з однакових чисел, всі числа є сідловими точками.

У кожній грі з повною інформацією існує пара оптимальних стратегій, що дає стійкий виграш, який дорівнює ціні гри v.

На відміну від ігор з чистою стратегією в іграх зі змішаною стратегією гра повторюється множину разів, перед кожним ходом гравець кидає жереб і вибирає випавшу стратегію. Змішані стратегії гравців *A* і *B* позначають таким чином:

$$Sa = (p_1, p_2, ..., p_m),\ Sb = (q_1, q_2, ..., q_n), \qquad (4.24)$$

де $p_1, p_2, ..., p_m$ – вірогідності застосування гравцем A стратегій $A_1, A_2, ..., A_m$;

$q_1, q_2, ..., q_n$ – вірогідності застосування гравцем B стратегій $B_1, B_2, ..., B_n$.

У першому і другому випадку вірогідності в сумі дорівнюють одиниці.

Основна теорема теорії ігор свідчить: будь-яка кінцева гра двох осіб з нульовою сумою має, принаймні, одне рішення – пару оптимальних стратегій, у загальному випадку змішаних (Sa^*, Sb^*) і відповідну ціну *v*. Пара оптимальних стратегій (Sa^*, Sb^*), які створюють рішення гри, має таку властивість: якщо один з гравців дотримується своєї оптимальної стратегії, то іншому не вигідно відступати від своєї. Ця пара стратегій утворює становище рівноваги: один гравець прагне обернути виграш у максимум, інший – у мінімум.

При розумній поведінці обох встановлюється рівновага і стійкий виграш. Якщо $v > 0$, то гра вигідна для гравця A, якщо $v < 0$ – для його супротивника. При $v = 0$, гра справедлива і однаково вигідна для обох учасників гри.

4.12.3. Методи рішення кінцевих ігор

Перед рішенням гри $m \times n$ її спрощують, позбуваючись від зайвих стратегій.

Стратегія A_i гравця *A* називається домінуючою над стратегією A_k, якщо в рядку A_i знаходяться виграші, не менші, ніж у рядку A_k і хоча б один з них більше, ніж у відповідній клітинці рядка A_k. Якщо всі виграші

рядка A_i рівні відповідним виграшам рядка A_k, то стратегія A_i називається дублюючою стратегію A_k. Аналогічно визначаються домінуючі і дублюючі стратегії гравця B.

Наприклад, нехай гра 5 х 5 задана матрицею гри 5 х 5.

Матриця гри 5 х 5

Стратегії	B_1	B_2	B_3	B_4	B_5
A_1	4	7	2	3	4
A_2	3	5	6	8	9
A_3	4	4	2	2	8
A_4	3	6	1	2	4
A_5	3	5	6	8	9

Стратегія A_5 дублює A_2, її необхідно видалити. Стратегія A_1 домінує над A_4. Стратегію A_4 видаляють. Результат – матриця гри 3 х 5.

Матриця гри 3 х 5

Стратегії	B_1	B_2	B_3	B_4	B_5
A_1	4	7	2	3	4
A_2	3	5	6	8	9
A_3	4	4	2	2	8

Щодо гравця B, то розглядаються варіанти домінування стратегій з погляду його критерію: "віддавати поменше". Тому стратегія B_3, домінує над B_4, і B_5, а B_1 – над B_2. Відкидають стовпці: B_2, B_4, B_5. Результатом є матриця.

Матриця гри 3 х 2

Стратегії	B_1	B_3
A_1	4	2
A_2	3	6
A_3	4	2

У матриці гри 3 х 2 A_3 дублює A_1. Остаточно отримана матриця гри 2 х 2.

Матриця гри 2 х 2

Стратегії	B_1	B_3	α
A_1	4	2	2
A_2	3	6	**3**
β	4	6	

Ця гра не має "сідлової точки", виграшем є нижня ціна гри, яка дорівнює 3.

Загальне правило рішення кінцевої гри полягає в такому: хай є гра $m \times n$, яка не має сідлової точки з матрицею a_{ij} (табл. 4.11). Хай усі виграші позитивні (цього завжди можна добитися, додаючи до всіх членів матриці велике число M).

Ціна гри збільшиться на M, а рішення не зміниться.

Ціна гри в цьому випадку теж позитивна $v > 0$.

Необхідно знайти рішення гри, тобто дві оптимальні змішані стратегії $S_a = (p_1, p_2, ..., p_m)$, $S_b = (q_1, q_2, ..., q_n)$, які надають кожній стороні максимально можливий для неї середній виграш (мінімальний програш).

Знайдемо спочатку S_a Відомо, що якщо гравець A застосовує свою оптимальну стратегію, то гравцю B немає сенсу відступати від своєї оптимальної стратегії.

Якщо гравець A використовує оптимальні стратегії S_a, а гравець стане використовувати чисті стратегії $B_1, B_2, \ldots, B_n$, то виграш гравця A буде не менше ніж v:

$$\begin{aligned} a_{11}\ p_1 + a_{12}\ p_2 + \ldots + a_{m1}\ p_m &\geq v, \\ a_{12}\ p_1 + a_{22}\ p_2 + \ldots + a_{m2}\ p_m &\geq v, \\ a_{1n}\ p_1 + a_{2n}\ p_2 + \ldots + a_{mn}\ p_m &\geq v. \end{aligned} \qquad (4.25)$$

Розділивши члени нерівності на v і обравши позначення: $x_i = p_i / v$, отримаємо:

$$\begin{aligned} a_{11}\ x_1 + a_{12}\ x_2 + \ldots + a_{m1}\ x_m &\geq 1, \\ a_{12}\ x_1 + a_{22}\ x_2 + \ldots + a_{m2}\ x_m &\geq 1, \\ a_{1n}\ x_1 + a_{2n}\ x_2 + \ldots + a_{mn}\ x_m &\geq 1. \end{aligned} \qquad (4.26)$$

Внаслідок того, що $p_1 + p_2 + ... + p_m = 1$, сума змінних x_i дорівнює:

$$x_1 + x_2 + ... + x_m = 1/v. \quad (4.27)$$

Значення виграшу v повинне отримати максимальне значення, тому $1/v$ повинне стати мінімальним.

Завдання рішення гри звелося до завдання мінімізації лінійної функції змінних x_i при лінійних обмеженнях – нерівностях.

$$F = x_1 + x_2 + ... + x_m \rightarrow min. \quad (4.28)$$

Завдання рішення гри $m \times n$ звелося до завдання лінійного програмування з обмеженнями нерівностями і змінними.

Знаючи x_i і $1/v$, можна знайти $p_1, p_2, ..., p_m$ і знайти S_a^*.

Оптимальна стратегія гравця B знаходиться аналогічно, з тією різницею, що він прагне мінімізувати виграш, обернувши в максимум $1/v$ і в обмеженнях фігурує знак менше або дорівнює.

Пара завдань лінійного програмування, за якою знаходять оптимальні стратегії *(Sa*,Sb*)*, є парою подвійних задач лінійного програмування, які дають однакове значення змінних x_i і v.

Далі наведений спрощений приклад, підтверджуючий безпосередній зв'язок між теорією ігор і задачею лінійного програмування.

Хай гравець *A* – дистриб'ютор нової продукції на незнайомому для нього ринку, гравець *B* – покупець.

Гравець *A* зацікавлений у реалізації більшої кількості продукції, але на цьому ринку поводиться обережно. Гравець *B*, не бажаючи втрачати гроші на придбання незнайомої продукції, теж поводиться обережно. Обидва керуються принципом мінімакса.

Гра задана матрицею 3 х 3. Елементи матриці – прибуток від реалізації продукції (виграш гравця A, який відповідає стратегіям гравців).

Матриця гри 3 х 3

Стратегії	B_1	B_2	B_3
A_1	20	40	70
A_2	70	60	80
A_3	50	30	40

У такій матриці наведені значення нижньої і верхньої ціни гри.

Матриця гри 3 х 3 із нижньою і верхньою ціною гри

Стратегії	B_1	B_2	B_3	α_i
A_1	20	40	70	20
A_2	70	60	80	**60**
A_3	50	30	40	30
β_j	70	**60**	80	

Це гра з сідловою точкою, де $\alpha_i = \beta_j = 60$.

Пошук цього рішення можна виконати таким чином. З погляду гравця *B* необхідно максимізувати функцію вигляду:

$$x_1 + x_2 + x_3 \rightarrow max, \qquad (4.29)$$

при обмеженнях:

$$20x_1 + 40x_2 + 70x_3 \leq 1,$$
$$70x_1 + 60x_2 + 80x_3 \leq 1,$$
$$50x_1 + 30x_2 + 40x_3 \leq 1,$$
$$x_i > 0.$$

Результат вирішення завдання лінійного програмування в середовищі MS Excel наведений на рис. 4.6.

x1	x2	x3
0	0,016666667	0
Функція мети		0,0167
Обмеження 1		0,6667
Обмеження 2		1
Обмеження 3		0,5

Рис. 4.6. **Результат вирішення завдання лінійного програмування**

Змішана стратегія в цьому випадку перетворилася на чисту. Ціна гри дорівнює v = 1/ 0,016666667 = 60, що відповідає рішенню, яке вже отримане.

Вирішивши подвійне завдання лінійного програмування, отримавши рішення для гравця *A*, можна переконатися, що гра має сідлову точку,

тобто верхня ціна гри дорівнює нижній ціні гри 60. Наведене завдання є прикладом можливості вирішення гри із застосуванням методів лінійного програмування.

Для будь-якого завдання лінійного програмування може бути побудоване еквівалентне йому завдання теорії ігор [36]. Існують наближені чисельні методи вирішення ігор, які застосовують при вирішенні завдань лінійного програмування. Наприклад, метод ітерацій (метод Брауна – Робінсона) [36; 405; 409].

У цьому розділі був наведений короткий огляд антагоністичних ігор і методів вирішення матричних ігор.

На практиці строго антагоністичні конфлікти, де сторони дотримуються принципу мінімакса, зустрічаються вкрай рідко. Прикладом може бути варіант гри, коли несумлінний продавець бажає реалізувати якомога більше товарів низької якості, а покупці прагнуть купити якомога менше цих товарів.

Як основа для безпосереднього прийняття рішень теорія ігор застосовується украй рідко. Але рекомендації моделей ігрового конфлікту корисні в плані обліку дій супротивника (опонента) і можуть бути корисними спільно з іншими підходами при прийнятті рішень.

4.13. Моделі теорії статистичних рішень

Наведено класичні критерії прийняття рішень в іграх з природою в умовах повної невизначеності: Лапласа, Вальда, Севіджа, Гурвіца та приклади їх використання для вирішення завдання вибору раціональної кількості устаткування в умовах стохастичної невизначеності.

Показано, що рішення, отримані за різними методами не дають однакових результатів, що підтверджує головну тезу теорії прийняття рішень про те, що не існує абсолютно кращого рішення.

Теорія статистичних рішень близька за ідеєю до теорії ігор. Від теорії ігор вона відрізняється тим, що невизначена ситуація не має конфліктного забарвлення. Ніхто нікому не протидіє. У цьому випадку невизначеність пов’язана не з діями "супротивника", а з об’єктивною дійсністю, яку в теорії статистичних рішень називають "природою". "Природа" представляється як якась незацікавлена інстанція, поведінка якої невідома.

Теорію статистичних рішень може тлумачити як теорію пошуку оптимальної недетермінованої поведінки в умовах невизначеності.

Сучасна концепція статистичного рішення, висунута А. Вальдом, і вважає поведінку оптимальною, якщо вона мінімізує ризик у послідовних експериментах, тобто математичне очікування збитків статистичного експерименту [36; 405; 409].

Як зазначалося в розділі 4.11, у завданнях теорії статистичних рішень теж розглядаються платіжні матриці (для дискретного випадку), або платіжна функція (в безперервному випадку).

Значення в платіжній матриці, або в платіжній функції залежать від 2-х чинників: стан природи, варіанти рішень ОПР.

У матриці платежів розглядаються m можливих стратегій: $A_1, A_2, ..., A_m$. У стовпцях – стратегії природи: $П_1, П_2, ..., П_n$, a_{ij} – виграш при кожній парі стратегій. Необхідно вибрати таку стратегію A_i гравця A, яка є найвигіднішою порівняно з іншими.

Коли вірогідність станів природи не піддається оцінці, то для прийняття раціонального рішення роблять спробу знайти не найгірше вирішення. У цьому випадку все залежить від точки зору ОПР на ситуацію, від позиції дослідника, від того, якими бідами загрожує невдалий вибір вирішення. У разі, коли вірогідності p_j існують, але ОПР вони невідомі, розроблені спеціальні критерії прийняття рішень: критерій Лапласа, критерій Вальда, критерій Гурвіца, критерій Севіджа [36; 405; 409]. Далі наведені класичні критерії прийняття рішень в іграх з природою в умовах повної невизначеності.

Як приклад застосування критеріїв розглядається завдання розділу 4.11.4. про ввід до ладу раціональної кількості агрегатів. Відмінністю умов вирішення завдання є відсутність вірогідності вводити до ладу певної кількості агрегатів. Відома матриця значень a_{ij} прибутку підприємства (грн), де кожному з варіантів кількості придбаного устаткування відповідає варіант кількості устаткування, яке можливо ввести в дію.

4.13.1. Класичні критерії прийняття рішень в іграх з природою в умовах повної невизначеності

4.13.1.1. Критерій Лапласа. При використовуванні критерію Лапласа умова невизначеності інтерпретується як припущення про рівну вірогідність появи всіх можливих станів природи. В основі цього критерію

лежить "принцип недостатньої підстави" [36; 405; 409]. У цьому випадку виконується пошук варіанта вирішення, для якого виконується така умова:

$$a = \max_{i=1,\dots,m} \sum_{j=1}^{n} a_{ij}. \qquad (4.30)$$

Матриця прибутку табл. 4.10 (наведена в розділі 4.11.4) доповнена стовпцем для пошуку раціонального вирішення за критерієм Лапласа (табл. 4.15).

Таблиця 4.15

Результат розрахунків для вибору альтернативи за критерієм Лапласа

Рішення (кількість обладнання, яке придбають)	Стан природи (кількість обладнання, яке можливо ввести в дію)				Сумарний прибуток (за рядками)
	0,00	100,00	200,00	300,00	
0	0,00	- 5 000 000,00	- 10 000 000,00	- 15 000 000,00	- 30 000 000,0
100	- 4 000 000,00	3 500 000,00	- 1 500 000,00	- 6 500 000,00	- 8 500 000,00
200	- 8 000 000,00	- 500 000,00	7 000 000,00	2 000 000,00	500 000,00
300	- 12 000 000,00	- 4 500 000,00	3 000 000,00	10 500 000,00	- 3 000 000,00

Оптимальна кількість устаткування, яке придбають, відповідає значенню сумарного прибутку 500 000 грн і дорівнює 200 шт. При цьому прибуток підприємства, згідно з припущенням про рівну вірогідність реакції природи, дорівнює 500 000 · 0,25 = 125 000 грн.

Вирішення співпадає з вирішенням, отриманим методом дерева рішень, тобто оптимальна кількість агрегатів, що придбаються, складає 200 штук. Оскільки при використовуванні критерію Лапласа всі вірогідності рівні, для визначення якнайкращого вирішення можна просто підсумувати значення платежів, які відповідають кожному вирішенню, і вибрати те вирішення, яке матиме максимальну суму (що також відповідає максимальному очікуваному платежу). Хоча в багатьох ситуаціях "рівновірогідний підхід" дає цілком прийнятне рішення, в інших ситуаціях він дає явно неправильні вирішення. Причина цього полягає саме в умові рівної вірогідності станів природи.

Незнання вірогідності станів зовсім не гарантує рівності їх реальних значень. Якщо в якій-небудь ситуації вірогідність прояву одного або декількох станів явно і значно перевершує вірогідність прояву інших станів природи, то рішення, отримане на підставі критерію Лапласа, очевидно, буде далеким від якнайкращого. З цієї причини розроблені інші критерії прийняття рішень в умовах невизначеності, які не спираються на вірогідності станів природи, з них найпопулярнішими є: критерій Вальда; критерій Севіджа; критерій Гурвіца.

4.13.1.2. Критерій Вальда. Згідно з цим критерієм гра ведеться з розумним, причому агресивним, гравцем, що робить усе для того, щоб перешкодити ОПР досягти успіху.

Критерій Вальда забезпечує вибір обережної, песимістичної стратегії або вибір якнайкращої з якнайгірших стратегій.

Оптимальною вважається стратегія, при якій гарантується виграш у будь-якому випадку не менший, ніж "нижня ціна гри з природою". Орієнтир при цьому на гірші умови.

Це "перестраховочний варіант" вирішення [36; 405; 409].

Оціночна функція в умовах крайнього песимізму розраховується таким чином:

$$\alpha = \max_i (\min_j a_{ij}). \qquad (4.31)$$

Для отримання вирішення треба доповнити матрицю прибутку табл. 4.10 стовпцем з якнайменших результатів за рядком і вибрати ті варіанти рішень, які містять максимальне значення в цьому результуючому стовпці.

У таблиці 4.16 наведено результат обчислення для пошуку "обережного" вирішення.

У стовпці з мінімальними значеннями вибирається максимальне - 6 500 000,00 з наступних якнайменших за рядками значень:

(- 15 000 000,00; - 6 500 000,00; - 8 000 000,00; - 12 000 000,00), якому відповідає кількість устаткування, рівна 100 шт.

Це "обережне рішення" "зменшило" кількість устаткування, що придбалося згідно з критерієм Лапласа.

4.13.1.3. Критерій Севіджа. Суть критерію полягає в мінімізації ризику. Цей критерій використовує матрицю ризиків. У цьому випадку

вибирають ту стратегію, при якій в якнайгірших умовах величина ризику приймає якнайменше значення [36; 405; 409]. Інакше кажучи, цей критерій рекомендує в умовах невизначеності вибирати ту стратегію, при якій величина ризику приймає якнайменше значення в найсприятливішій ситуації (коли ризик максимальний).

$$r = \min_i (\max_j r_{ij}). \qquad (4.32)$$

Таблиця 4.16

Результат розрахунків для вибору альтернативи за критерієм Вальда

Кількість обладнання	Стан природи (кількість обладнання, яке можливо ввести в дію)				
	0,00	100,00	200,00	300,00	min
0	0,00	- 5 000 000,00	- 10 000 000,00	- 15 000 000,00	- 15 000 000,00
100	- 4 000 000,00	3 500 000,00	- 1 500 000,00	- 6 500 000,00	- 6 500 000,00
200	- 8 000 000,00	- 500 000,00	7 000 000,00	2 000 000,00	- 8 000 000,00
300	-12 000 000,00	- 4 500 000,00	3 000 000,00	10 500 000,00	- 12 000 000,00

При цьому складається матриця R втрат з елементами r_{ij}, які відображають збитки від помилкового вибору i-го вирішення в j-му стані (табл. 4.17).

Для цього в матриці табл. 4.16 знаходять максимальні елементи в кожному стовпчику. Вектор цих значень: (0, 3 500 000, 7 000 000, 10 500 000).

Потім з цих елементів віднімають елементи в стовпцях матриці табл. 4.16. Матриця втрат R виглядає таким чином (табл. 4.17).

Таблиця 4.17

Результат розрахунків для вибору альтернативи за критерієм Севіджа

Рішення (кількість обладнання, яке придбають)	Стан природи (кількість обладнання, яке можливо ввести в дію)				
	0	100	200	300	max
0	0	8 500 000	17 000 000	25 500 000	25 500 000
100	4 000 000	0	8 500 000	17 000 000	17 000 000
200	8 000 000	4 000 000	0	8 500 000	8 500 000
300	12 000 000	8 000 000	4 000 000	0	12 000 000

У кожному рядку R знаходять максимальний елемент *i*, потім, у векторі максимальних елементів знаходять мінімальне значення.

У даному випадку це (8 500 000).

Йому відповідає кількість агрегатів 200 шт.

4.13.1.4. Критерій Гурвіца. Критерій Гурвіца пропонує деякий компроміс між зайвим оптимізмом і зайвим песимізмом [36; 405; 409]. Тобто встановлює баланс між випадками крайнього песимізму і крайнього оптимізму шляхом введення деякого вагового коефіцієнта песимізму α.

Критерій рекомендує при виборі вирішення не керуватися ні крайнім песимізмом ("завжди розраховуй на гірше"), ні крайнім оптимізмом ("можливо повезе"). Згідно з цим критерієм стратегія вибирається з умови:

$$H = \max_i \left[\alpha \min_j a_{ij} + (1 - \alpha) \max_j a_{ij}\right], \qquad (4.33)$$

де α – *1* коефіцієнт песимізму ($0<\alpha<1$).

При $\alpha = 1$ критерій Гурвіца перетворюється на критерій Вальда, при $\alpha = 0$ – у критерій "крайнього оптимізму", що рекомендує вибрати ту стратегію, при якій найбільший виграш у рядку максимальний. Коефіцієнт α вибирається з суб'єктивних міркувань – чим небезпечніше ситуація, і чим більше ОПР хоче "підстрахуватися", тим менше його схильність до ризику, і тим ближче до одиниці вибирається значення α.

У табл. 4.18 введено два додаткові стовпці з мінімальними і максимальними значеннями за стовпцями (рядками), а в табл. 4.19 наведені обчислені значення H при різних коефіцієнтах α.

Згідно з критерієм Гурвіца при $\alpha = 0{,}5$ (при рівноімовірних шансах на успіх і невдачу) при закупівлі 200 агрегатів слідує чекати мінімальні збитки в 500 000 грн.

При завищеному оптимізмі (при $\alpha = 0{,}1$) придбання 300 агрегатів дозволить отримати 8 250 000 грн прибутку, при заниженому оптимізмі (при $\alpha = 0{,}9$) придбання 100 агрегатів дозволить сподіватися на мінімальні втрати прибутку (5 500 000 грн).

Таблиця 4.18

Результат проміжних розрахунків для вибору альтернативи за критерієм Гурвіца

Рішення (кількість обладнання, яке прид-бають)	Стан природи (кількість обладнання, яке можливо ввести в дію)				Min	Max
	0	100	200	300		
0	0	- 5 000 000	- 10 000 000	-15 000 000	- 15 000 000	0
100	- 4 000 000	3 500 000	- 1 500 000	-6 500 000	- 6 500 000	3 500 000
200	- 8 000 000	- 500 000	7 000 000	2 000 000	- 80 000 000	7 000 000
300	- 12 000 000	- 4 500 000	3 000 000	10 500 000	- 120 000 000	10 500 000

Таблиця 4.19

Значення *H* при різних коефіцієнтах песимізму за критерієм Гурвіца

α / Кіль-кість облад-нання	α = 0,1	α = 0,2	α = 0,3	α = 0,4	α = 0,5	α = 0,8	α = 0,9
0	- 1 500 000	- 3 000 000	- 4 500 000	- 6 000 000	- 7 500 000	- 12 000 000	- 13 500 000
100	2 500 000	1 500 000	500 000	- 500 000	- 1 500 000	- 4 500 000	- 5 500 000
200	5 500 000	4 000 000	2 500 000	1 000 000	- 500 000	- 5 000 000	- 6 500 000
300	8 250 000	6 000 000	3 750 000	1 500 000	- 750 000	- 7 500 000	- 9 750 000

Таким чином, відсутність інформації про вірогідність настання тієї або іншої події загрожує невизначеністю в результатах рішення ОПР. Різні критерії прийняття рішень в умовах повної невизначеності часто дають різні рішення. У табл. 4.20 наведені рішення, отримані для завдання про вибір оптимального плану придбання обладнання (дані наведено в табл. 4.10), за критеріями: Лапласа, Вальда, Севіджа, Гурвіца.

Таблиця 4.20

Результат рішення завдання
про вибір оптимального плану придбання обладнання,
на підставі критеріїв: Лапласа, Вальда, Севіджа, Гурвіца

Критерій	Кількість агрегатів
Лапласа	200
Вальда	100
Севіджа	200
Гурвіца	200, при значенні коефіцієнта песимізму α=0,5 100, при значенні коефіцієнта песимізму α=0,9

Остаточне рішення про кількість устаткування, що необхідно придбати, залишається за експертами і ОПР.

4.14. Психолінгвістичні аспекти прийняття рішень

Наведено головні принципи, які покладено в основу теорії нечітких множин у прийнятті рішень. Наведено завдання прийняття рішень з вибору альтернатив, що не домінуються, у разі чіткого опису альтернатив, вибору альтернатив у разі декількох відношень переваги.

Наведено вирішення завдання вибору альтернативи з найбільшим ступенем недомінованості на підставі методу прийняття рішень при нечіткому відношенні переваги на безлічі чітко заданих альтернатив.

4.14.1. Елементи теорії нечітких множин у прийнятті рішень

Прийняття рішень в умовах повної невизначеності має істотний аспект, пов’язаний з таким:

нечітким баченням мети вибору;

нечіткими оцінками альтернатив;

нечіткими оцінками критеріїв;

нечіткими оцінками відношення переваги альтернатив.

У цьому випадку говорять про "невизначеність бажань і мети", коли ОПР не в змозі вибрати єдиний критерій і мета не ясна.

У цьому випадку розглядають клас "відповідних рішень" в рамках теорії нечітких множин. Засновник теорії нечітких множин Л. Заде ще в 1965 році передбачив широке прикладне значення своєї теорії, написавши з цього приводу таке: "Фактично нечіткість може бути ключом до розуміння здатності людини справлятися з завданнями, які дуже складні для вирішення на ЕОМ" [5; 17; 22; 59; 103; 169; 208; 344; 388].

В основі його теорії лежить очевидний факт – суб'єктивне уявлення про мету завжди нечіткі, всі оцінки суб'єкта і обмеження нечіткі, і часто позбавлені кількісних характеристик.

Таким чином, з'явилася лінгвістична змінна – змінна, що описує об'єкт дослідження в словесній формі.

Наприклад, стиль управління описується змінними: "ефективний", "неефективний", "малоефективний", не "дуже ефективний" і так далі, які не мають аналогів у мові традиційної математики. Основна ідея апарату, розробленого Заде, по можливості звузити безліч допустимих альтернатив, звівши їх до безлічі альтернатив, що не домінуються, або Парето-альтернатив [148].

Усі ці ідеї слідують природному ходу людського мислення при аналізі складної ситуації. Апарат теорії нечітких множин знайшов розвиток у роботах багатьох дослідників і сьогодні містить безліч різноманітних підходів до методів прийняття рішень на основі нечіткої інформації. Далі розглядаються деякі елементи теорії нечітких множин, які можуть бути корисні при прийнятті рішень.

В основі поняття нечітка множина лежить уявлення про те, що елементи цієї множини, які мають загальну властивість, можуть володіти нею різною мірою і, відповідно належати цій множині з різним ступенем.

Тобто вислів, що елемент x належить даній множині є недостатнім, необхідно вказати, з яким ступенем він належить цій множині. Нехай X – деяка множина (в звичайному значенні) елементів. Надалі розглядаються підмножини цієї множини.

Нечіткою множиною C у X називають сукупність пар вигляду:

$$(x, \mu_C(x)), \tag{4.34}$$

де $x \in X$, а μ_C – функція $x \to [0,1]$, яку називають функцією приналежності нечіткої множини C.

4.14.2. Нечіткі відношення

Звичайне відношення R на множині X – підмножина декартового добутку $X \times X$, де всі пари елементів $x,y \in X$ і пов'язані співвідношенням R, що позначається: xRy або $(x,y) \in R$.

Нечітке відношення R на множині X – нечітка підмножина декартового добутку $X \times X$, що характеризується функцією приналежності

$$\mu_R : X \times X \to [0,1]. \tag{4.35}$$

Значення $\mu_R(x,y)$ цієї функції – суб'єктивна міра або ступінь виконання відношення xRy.

Множина рівня α нечіткого відношення R на X визначається таким чином:

$$R_\alpha = \{(x,y) \mid (x,y) \in X \times X, \quad \mu_R(x,y) \geq \alpha\}. \tag{4.36}$$

Множина рівня α нечіткого відношення R на X є звичайним відношенням на X, яке зв'язує всі пари (x,y), для яких ступінь виконання відношення R не менше, ніж α.

Матрицю множини рівня α, отримують заміною в матриці нечіткого відношення R, одиницями – всі елементи, які не є меншими числа α, та нулями – всю решту елементів.

Нехай матриця нечіткого відношення R на множині $X = \{x_1, x_2, ..., x_4\}$ має вигляд:

x	x_1	x_2	x_3	x_4
x_1	1	0,5	0	0,2
x_2	0,3	1	1	0,4
x_3	0	0,6	0,5	0,1
x_4	1	0,7	0,3	0

Тоді матриця звичайного відношення, яка є множиною рівня 0,5 нечіткого відношення R, має такий вигляд:

x	x_1	x_2	x_3	x_4
x_1	1	1	0	0
x_2	0	1	1	0
x_3	0	1	1	0
x_4	1	1	0	0

4.14.3. Нечітке відношення переваги на множині альтернатив

При прийнятті рішень розрізняють нечіткі відношення строгої переваги, нестрогої переваги (н.в.н.п.), байдужості, квазіеквівалентності [103; 169; 409]. Розглядається варіант відношення строгої і нестрогої переваги.

Хай X – задана множина альтернатив, R – нечітке відношення переваги.

Нечітким відношенням R строгої переваги на X називають будь-яке задане на цій множині нечітке відношення, функція приналежності якого приймає значення:

$$\mu_R^S(x,y) = \{ \begin{matrix} \mu_R(x,y) - \mu_R(y,x) & \text{в разі } \mu_R(x,y) \geq \mu_R(y,x), \\ 0 & \text{в разі } \mu_R(x,y) \leq \mu_R(y,x) \end{matrix} \}, \quad (4.37)$$

де $y \in X$.

Нечітким відношенням R нестрогої переваги на X називають будь-яке задане на цій множині нечітке рефлексивне відношення.

Функція приналежності відношення нестрогої переваги R: $\mu_R : X \times X \to [0,1]$ володіє властивістю рефлексії: $\mu_R(x,x) = 1$ при будь-кому $x \in X$. Рефлексія відображає той факт, що будь-яка альтернатива не гірше самої себе. Значення $\mu_R(x,x)$ є ступенем виконання переваги "x не гірше ніж y".

4.14.4. Вибір альтернатив, що не домінуються, у разі чіткого опису альтернатив

Нехай X – безліч чітко описаних альтернатив та нечітке відношення нестрогої переваги з μ_R і відповідне йому відношення строгої переваги з μ_R^S.

Необхідно знайти підмножину альтернатив, що не домінуються, множини (X, μ_R).

Нечітка підмножина альтернатив, що не домінуються, множини (X, μ_R) описується функцією приналежності:

$$\mu_R^{н.д.}(x) = 1 \quad \sup_{y \in X} \mu_R^S(y, x), \quad x \in X. \tag{4.38}$$

Далі наведено приклад вибору альтернативи, що не домінується, у разі чіткого опису альтернатив.

У кінцевій множині $X = \{x_1, x_2, ..., x_4\}$ задано R – н.в.п. вигляду:

X	x_1	x_2	x_3	x_4
x_1	1	0,2	0,3	0,1
x_2	0,5	1	0,2	0,6
x_3	0,1	0,6	1	0,3
x_4	0,6	0,1	0,5	1

Відношення R дозволяє побудувати R^* нечітке відношення строгої переваги за формулою (4.14).

Елементи відношення R^* отримані таким чином:

$$R_{11}^* = R_{11} - R_{11} = 0 ; \; R_{12}^* = 0 ;$$

$$R_{13}^* = R_{13} - R_{31} = 0,3 \quad 0,1 = 0,2 ;$$

$$R_{14}^* = R_{41} - R_{14} = 0,6 \quad 0,1 = 0,5 ;$$

$$R_{21}^* = R_{21} - R_{12} = 0,5 \quad 0,2 = 0,3 ;$$

……

$$R_{34}^* = 0 ; \; R_{43}^* = R_{43} - R_{34} = 0,5 \quad 0,3 = 0,2;$$

$$R_{44}^* = 1 - 1 = 0.$$

X	x_1	x_2	x_3	x_4
x_1	0	0	0,2	0
x_2	0,3	0	0	0,5
x_3	0	0,4	0	0
x_4	0,5	0	0,2	0

Звідси функція приналежності підмножини альтернатив, що не домінуються, обчислюється за формулою (4.15) та має вигляд:

x_1	x_2	x_3	x_4
0,5	0,6	0,8	0,5

Найбільший ступінь недомінованості, який дорівнює 0,8, має альтернатива x_3. Її вибір вважається раціональним у рамках цього підходу.

4.14.5. Вибір альтернатив у разі декількох відношень переваги

Нехай задано декілька альтернатив X і кожна характеризується декількома ознаками з номерами: $j = 1,2,...,m$. Інформація про попарне порівняння альтернатив за кожною ознакою j представлена у вигляді відношення переваги R_j. Таким чином, існують m відношень переваги на множині X.

Необхідно зробити раціональний вибір альтернатив з множини $(X, R_1, R_2, ..., R_m)$. Якщо відношення R_j розрізняються за важливістю, використовують коефіцієнти відносної важливості відношень λ_j. Послідовність рішення полягає в такому.

1. Отримати нечітке відношення Q_1 – як перетин вхідних відношень R_j:

$$\mu_{Q1}(x,y) = min\{\mu_1(x,y),...,\mu_m(x,y)\}.$$

2. Знайти нечітку підмножину альтернатив, що не домінуються, у множині (X, μ_{Q1}):

$$\mu_{Q1}^{н.д.}(x) = 1 \quad \sup_{y \in X}[\mu_{Q1}(y,x) \quad \mu_{Q1}(x,y)].$$

3. Отримати нечітке відношення Q_2 як згортку відношень R_j:

$$\mu_{Q2}(x,y) = \sum_{j=1}^{m} \lambda_j \mu_j(x,y).$$

4. Знайти нечітку підмножину альтернатив, що не домінуються, у множині (X, μ_{Q2}):

$$\mu_{Q2}^{н.д.}(x) = 1 \quad \sup_{y \in X}[\mu_{Q2}(y,x) \quad \mu_{Q2}(x,y)].$$

5. Знайти перетин множин: $\mu_{Q1}^{н.д.}$ та $\mu_{Q2}^{н.д.}$:

$$\mu^{н.д.}(x) = min\{\mu_{Q1}^{н.д.}(x), \mu_{Q2}^{н.д.}(x)\}.$$

6. Раціональним вважається вибір альтернатив із множини:

$$X^{н.д.} = \{x \mid x \in X, \mu^{н.д.}(x) = \sup_{x^* \in X} \mu^{н.д.}(x^*)\}.$$

Далі наведено приклад вибору альтернативи, виходячи з заданих трьох однаково важливих відношень переваги: R_1, R_2, R_3.

Дані: множина альтернатив $X = \{x_1, x_2, x_3\}$ та на X задані три однаково важливих відношення переваги: R_1, R_2, R_3.

Знайти альтернативу з найбільшим ступенем недомінованості.

Для простоти розглядаються чіткі відношення. Алгоритм обчислень залишається тим же у разі нечітких відношень, коли функція приналежності задана на інтервалі [0,1]:

X	x_1	x_2	x_3
x_1	1	1	0
x_2	1	1	0
x_3	0	0	1

X	x_1	x_2	x_3
x_1	1	1	1
x_2	0	1	1
x_3	0	0	1

X	x_1	x_2	x_3
x_1	1	1	0
x_2	1	1	0
x_3	1	0	1

1. Будують відношення нестрогої переваги: Q_1 з $\mu_{Q1}(xi, xj)$:

1	1	0
0	1	0
0	0	1

2. Будують Q_2 відношення строгої переваги з $\mu_{Q2}(xi, xj)$, яке відповідає Q_1:

0	1	0
0	0	0
0	0	0

3. Знаходять множину μ_{Q2} альтернатив, що не домінуються, у множині X, μ_{Q2}:

x_1	x_2	x_3
1	0	1

4. Будують відношення Q_3 з $\mu_{Q3}(xi, xj)$ як згортку відношень за такою формулою (це відношення нестрогої переваги):

$$Q_3 = 1/3(\mu_1(x_i, x_j) + \mu_2(x_i, x_j) + \mu_3(x_i, x_j)).$$

X	x_1	x_2	x_3
x_1	1	1	1/3
x_2	2/3	1	1/3
x_3	1/3	0	1

5. Будують відношення Q_4 з $\mu_{Q4}(xi, xj)$ як відношення строгої переваги, на підставі відношення Q_3:

X	x_1	x_2	x_3
x_1	0	1/3	0
x_2	0	0	1/3
x_3	0	0	0

6. Знаходять підмножину μ_{Q4} альтернатив, що не домінуються, у множині X, μ_{Q4}:

x_1	x_2	x_3
1	2/3	2/3

7. Знаходять результуючу множину альтернатив, що не домінуються, як перетин множин μ_{Q2} і μ_{Q4}:

x_1	x_2	x_3
1	0	2/3

Раціональним вважається вибір альтернативи x_1, яка має максимальний ступінь недомінованості.

4.15.6. Завдання вибору альтернативи з найбільшим ступенем недомінованості на підставі методу прийняття рішень при нечіткому відношенні переваги на безлічі чітко заданих альтернатив

Множина альтернатив X складається з п'яти елементів:

$\{X_1, X_2, X_3, X_4, X_5\}$ – п'ять міст України: Харків, Луганськ, Донецьк, Полтава, Київ. Нечітке відношення нестрогої переваги альтернатив з $\mu_R(x_i, x_j)$ наведено далі. Воно відображає оцінку експертом результатів парного порівняння рівня забруднення атмосферного повітря в різних містах України. Тобто, стан повітря в м. Донецьк в 0,7 разів кращий ніж в м. Луганськ та таке саме для інших порівнянь.

Міста	Харків	Луганськ	Донецьк	Полтава	Київ
Донецьк	1	0,7	0,8	0,5	0,5
Полтава	0	1	0,3	0	0,2
Харків	0	0,7	1	0	0,2
Луганськ	0,6	0,1	0,9	1	0,6
Київ	0	0	0	0	1

Знайти альтернативу з найбільшим ступенем недомінованості на підставі методу прийняття рішень при нечіткому відношенні переваги на безлічі чітко заданих альтернатив.

Будуємо нечітке відношення строгої переваги з $\mu_R^S(x_i, x_j)$.

0	0,7	0,8	0	0,5
0	0	0	0	0,2
0	0,4	0	0	0,2
0,1	0,1	0,9	0	0,6
0	0	0	0	0

Функція приналежності нечіткої множини альтернатив, що не домінуються, має такі значення:

Харків	Луганськ	Донецьк	Полтава	Київ
0,9	0,3	0,1	1	0,4

Альтернатива x_4 (місто Полтава) домінує над усіма іншими.

Отже, наведений метод дозволяє визначити альтернативу з найбільшим ступенем недомінованості. Місто Полтава за оцінкою експертів та в рамках певного методу дослідження має менший рівень забруднення повітря у зрівнянні з наведеними містами.

Отже, методи теорії корисності, теорії прийняття рішень в умовах визначеності, стохастичної невизначеності, повної невизначеності, багатокритеріальних методів, методів нечіткої інформації не надають незаперечних рекомендацій щодо остаточного рішення з будь-якої складної проблеми.

Проте математичні методи дозволяють виконати послідовний чисельний аналіз ситуації з різних точок зору. Вибір критеріїв, методів залежить від важливості вирішуваних завдань, від кваліфікації і відповідальності експертів та ОПР.

У процесі прийняття рішення для визначення найвигіднішої стратегії ОПР необхідна інформація про імовірність дій супротивника, про імовірність стану природи тощо. Підвищення рівня інформованості може бути досягнутим при зверненні ОПР до послуг консультаційної служби, здатної скласти добре обґрунтований прогноз розвитку ситуації. Можна розглядати дану дію як свого роду "експеримент", проведення якого, поза сумнівом, вимагає витрати певних засобів. З економічної точки зору експеримент доцільно проводити в тому випадку, якщо витрати на його проведення не перевищують виграш, який можна отримати при більш точному знанні стратегії природи. Реалізація такого експерименту можлива за допомогою імітаційного моделювання.

Розділ 5. Методи та моделі вибору та оцінювання ефективності HRM-систем

Розглянуто функціональність та класи сучасних програмних комплексів для управління персоналом, охарактеризовано український ринок HRM-систем (Human Resource Management). Узагальнено ключові напрями технологічного розвитку HRM-систем та запропоновано критерії вибору програмних комплексів для управління персоналом. Досліджено теоретико-методологічні підходи щодо оцінювання економічної ефективності впровадження HRM-систем та доведено актуальність розробки моделей оцінювання ефективності HRM-систем.

Персонал компанії – це одна з найголовніших рушійних сил, яка забезпечує успішний розвиток бізнесу. Адже успіх будь-якого бізнесу визначається професійною компетентністю персоналу, який сприяє розвитку бізнесу на всіх рівнях – і на керівному, і на виконавському. Тому організаційне вдосконалення і управління персоналом стає однією з найголовніших функцій менеджменту компанії. Актуальність і економічну значущість професійного вирішення цього питання на підприємстві підтверджують розвиток і використання кадрового потенціалу, який стає основним фактором конкурентоспроможності підприємства. Одним з найбільш дієвих способів підвищення ефективності управління персоналом є впровадження автоматизованих комплексних систем управління персоналом – HRM-систем (Human Resource Management – управління людським ресурсом). Особливо гостро постає проблема автоматизації для великих і середніх підприємств, для яких збереження старих управлінських технологій загрожує втратою ефективності управління в умовах ринкової конкуренції.

Перше завдання, яке доводиться вирішувати при переході на нові інформаційні технології – це визначення ключових цілей впровадження ІС, пов’язаних із загальною стратегією бізнесу, а також вибір ІТ-рішення, яке адекватне для цієї стратегії.

Автор розробляє модель оцінювання ефективності систем управління персоналом, тому до кола його інтересів відноситься і проблема вибору подібних систем. Отже, метою роботи є узагальнення критеріїв

вибору програмного продукту (комплексу програмних продуктів) для управління персоналом та дослідження теоретико-методологічних підходів щодо оцінювання економічної ефективності впровадження HRM-систем.

Основна мета програмних продуктів HRM-класу – привернути і утримати цінних для компанії фахівців. Тому вони дозволяють працювати не тільки з кількісними, але і з якісними показниками персоналу.

Серед інших цілей, які досягаються за допомогою HRM-систем, варто виділити такі.

1. Структурування всіх облікових і розрахункових процесів, пов'язаних з персоналом. Це завдання зводиться до усунення подвійного введення даних, об'єднання їх в єдину базу даних з можливістю повного аналізу і генерації звітності, своєчасного і коректного розрахунку і нарахування заробітної плати, податкових відрахувань тощо. Ефект від вирішення таких завдань достатньо очевидний, але його можна досягти і за допомогою звичайних систем автоматизації кадрового обліку і розрахунку зарплати.

2. Усунення і мінімізація негативних наслідків, пов'язаних зі звільненням співробітників. Значущість рішення цього завдання не завжди адекватно оцінюється вітчизняними менеджерами вищої ланки. Очевидно, що компанії мають великі збитки, пов'язані із заміною втраченого співробітника. Враховуючи те, що, за деякими оцінками, витрати, пов'язані з персоналом, складають близько 36 % доходів крупних компаній, текучість кадрів виявляється серйозною проблемою, яка може істотно погіршити показники загальної ефективності організації.

Ключовими властивостями HRM-систем у сучасному бізнесі стають:

здатність зберігати великі об'єми даних, зокрема, у вигляді розподілених баз даних;

оперативно обробляти ці дані за складними алгоритмами;

легко змінювати вказані алгоритми при зміні законодавства;

підтримувати всі нормативні вимоги до вихідних документів;

легко змінювати форми документів при зміні законодавства;

підтримувати різні організаційні структури (наприклад, при плануванні штатного розкладу).

HRM-системи, залежно від реалізації того або іншого рівня автоматизації, можна умовно класифікувати на три види (рис. 5.1) [243; 365].

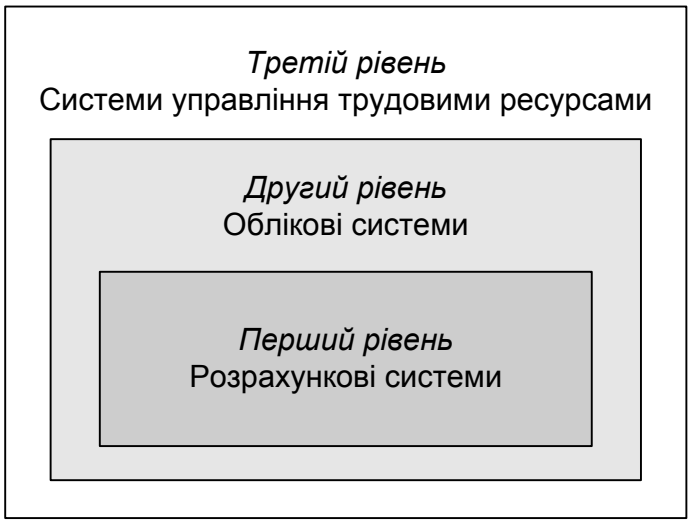


Рис. 5.1. **Три рівні систем автоматизації управління персоналом компанії**

Системи першого рівня направлені виключно на автоматизацію розрахунку заробітної плати. Часто вони є заздалегідь налаштованим "коробочним" продуктом. Але їх низька функціональність і неможливість подальшого налаштування істотно обмежують коло потенційних користувачів.

Системи другого рівня дозволяють розраховувати зарплату, формувати і вести штатний розклад, відображати рух кадрів тощо. Такі системи сьогодні впритул наблизилися до програмних комплексів третього рівня, тому провести чітку грань між ними стає дедалі складніше. Це пов’язано з тим, що, як зазначають багато експертів і гравців ринку, останніми роками замовники проявляють все більший інтерес саме до управлінського функціоналу HRM-систем.

Системи третього рівня – це найбільш комплексні рішення, які дозволяють проводити атестацію співробітників, складати портрети фахівців, розробляти індивідуальні програми їх навчання і службового просування і т. д. Такі системи, як правило, вже не є самостійними, а входять як спеціалізований модуль до систем комплексної автоматизації підприємств (ERP-системи). У той же час існують і окремі HRM-системи третього рівня, що мають можливості інтеграції з популярними ERP-системами. Продукти такого класу дозволяють працювати не тільки з кількісними (зарплата, податкові виплати, надбавки, утримання тощо), але і з якісними показниками персоналу. Якісна функціональність забезпечує автоматизацію таких функцій, як мотивація персоналу, створення "профілів компетентностей співробітників", управління кар’єрою, оцінка персоналу, управління навчанням (підвищенням кваліфікації), дистан-

ційне навчання, аналіз ефективності персоналу, аналіз відповідності співробітника посаді, планування потреби в персоналі і руху персоналу, формування кадрового резерву. Крім того, системи третього рівня забезпечують "самообслуговування персоналу" (віддалений доступ співробітників, у тому числі через Інтернет, до облікових даних про них з можливістю коректування частини даних), а також підтримку HR-порталу в мережі Інтернет, з публікацією і оперативним оновленням даних по вакансіях, новин компанії, реєстрацією резюме, що заповнюються в онлайновому режимі, автоматизованим аналізом цих резюме, відбором потенційних кандидатів на посаду тощо.

Функціональність сучасних HRM-рішень найвищого класу можна умовно об’єднати в такі типові функціональні модулі [88; 351; 360; 365].

Організаційний менеджмент:

1) управління організаційною структурою;
2) штатний розклад;
3) розстановка кадрів.

Кадровий облік:

4) кадровий облік і документообіг;
5) табельний облік;
6) пенсійний (персоніфікований облік);
7) регламентована звітність;
8) зберігання історії.

Управління кадрами:

9) підбір кадрів;
10) планування персоналу;
11) атестація персоналу;
12) ділова оцінка персоналу;
13) управління компетентностями;
14) розвиток кадрового резерву;
15) управління кар’єрою;
16) управління мотивацією;
17) компенсаційний пакет.

Розвиток персоналу:

18) управління навчанням;
19) електронне навчання;
20) управління підвищенням кваліфікації;
21) управління перепідготовкою кадрів.

Фінансово-розрахунковий модуль:

22) розрахунок заробітної плати;

23) інші розрахунки з персоналом;

24) автоматичний розрахунок податків і відрахувань;

25) планування витрат на персонал;

26) глобальна система НДІ;

27) HR-портал;

28) інформаційне самообслуговування;

29) аналітика по персоналу.

У зарубіжних інтегрованих HRM-системах всю сукупність HR-завдань часто розбивають на шість основних функціональних блоків, розподілених за трьома технологічними рівнями (згідно з підходом дослідницької групи Forrester Research) [328]. Цю структуру можна подати таким чином (табл. 5.1).

Таблиця 5.1

Функції сучасних HRM-систем (згідно з Forrester Research)

<table>
<tr><td colspan="5">"Користувальницький" рівень</td></tr>
<tr><td colspan="5">Блок "інформаційного самообслуговування"
Self-service interaction layer</td></tr>
<tr><td>Інтерфейс для персоналу Employee self-service</td><td>Інтерфейс для управлінців Manager self-service</td><td colspan="2">Засоби обміну повідомленнями Employee communications</td><td>Засоби управлінського аналізу і генерації звітності Management reporting and analysis</td></tr>
<tr><td colspan="5">"Стратегічний" рівень</td></tr>
<tr><td colspan="5">Блок управління процесом навчання Learning management processes</td></tr>
<tr><td colspan="2">Управління тренінгами Training administration</td><td colspan="2">Управління змістом курсів Learning content management</td><td>Проведення тренінгів Learning delivery</td></tr>
<tr><td colspan="5">Блок управління процесом найму
Recruitment processes</td></tr>
<tr><td>Пошук і залучення кандидатів Candidate sourcing</td><td>Відстеження претендентів Applicant tracking</td><td>Адаптація найнятого персоналу New-hire onboarding</td><td colspan="2">Управління призначеннями Contingent staffing</td></tr>
<tr><td colspan="5">Блок управління ефективністю і "талантами"
Performance and talent management processes</td></tr>
<tr><td>Управління ефективністю персоналу Employee performance</td><td>Управління кадровим резервом Succession planning</td><td>Управління компетентностями Competency management</td><td>Управління компенсаціями і преміями Compensation and rewards</td><td>Планування і аналіз Planning and analysis</td></tr>
</table>

Занінчення табл. 5.1

<table>
<tr><td colspan="5">"Операційний" рівень</td></tr>
<tr><td colspan="5">Блок обліку праці
Workforce management processes</td></tr>
<tr><td colspan="2">Облік
робочого часу і прогулів
Time and attendance</td><td colspan="2">Планування і прогнозування
Forecasting and scheduling</td><td>Управління
відрядженнями,
відгулами і відпустками</td></tr>
<tr><td colspan="5">Блок обліку кадрових операцій
Transactional HRMS processes</td></tr>
<tr><td>Кадровий облік
і діловодство
Employee records
and personnel
actions</td><td>Управління
заохоченнями
Benefits
administrati-on</td><td>Розрахунковий
контур
Payroll</td><td>Управління
посадами/
штатний розклад
Position
management</td><td>Правове
забезпечення
HR compliance</td></tr>
</table>

В усіх сучасних HRM-системах, представлених на світовому ринку, реалізована функціональність "користувальницького" і "операційного" рівня. Основний же технологічний розвиток спостерігається на "стратегічному" рівні, який включає функції планування і стратегічного управління трудовими ресурсами. Завдання стратегічного рівня реалізовують на даний момент як постачальники комплексних рішень HRM, так і розробники спеціалізованих рішень.

Таким чином, ключовими напрямами технологічного розвитку HRM-систем зараз є автоматизація найму, управління "талантами" і ефективністю персоналу, а також управління навчанням співробітників. Окрім цього, дуже перспективною для HRM-рішень є модель на базі Web-сервісів, яка, окрім інших переваг, надає можливість ефективно реалізувати бізнес-процеси інформаційного самообслуговування співробітників і управлінців.

Розглянемо концепцію інформаційного самообслуговування більш докладно. Ця концепція припускає, що співробітники і керівники можуть самостійно вводити власні персональні дані і управляти безліччю операцій і процесів, які раніше знаходилися у веденні кадрових служб. Це дозволяє знизити матеріальні і трудові витрати на кожну операцію у сфері управління персоналом.

Найбільш ефективним підходом у реалізації функцій інформаційного самообслуговування є підхід на базі інформаційних сервісів. Інформаційні сервіси призначені для процесів, які припускають обробку певної інформації з транзакційних інформаційних систем (отримання різних зві-

тів, аналітичних оцінок і т. д.) або таких повсякденних процедур, як перевірка введеної інформації, заповнення, виправлення або затвердження звітів про виконану роботу, подача заявок на відпустку і їх затвердження тощо.

Функціональність інформаційного самообслуговування пропонується розробниками програмного забезпечення досить рідко і лише комплексних "важких" системах. Однією з найбільш вдалих реалізацій такої функціональності автори вважають автоматизацію зазначених бізнес-процесів у системі SAP.

Програмне рішення SAP [427] використовує технології корпоративних порталів і управління знаннями, які дозволяють перетворити систему управління персоналом з моделі надання послуг у модель обміну знаннями і досвідом та допомагає побудувати ділові відносини, засновані на співпраці і взаємодії. Рішення включає більше 80 передналаштованих, готових до використання сервісів, що персоналізуються.

За допомогою додатка "Інформаційні сервіси для співробітників" (SAP Employee Self-Service, SAP ESS) підприємства можуть надавати персоналу зручні засоби доступу до інформації і додатків, пов’язаних з їх діяльністю на підприємстві.

Наприклад, ці сервіси дають можливість співробітникам:

управляти своїм робочим часом, процесом відряджень, кар’єрою.

створювати, переглядати і змінювати свої персональні дані (наприклад, адресні дані, банківські реквізити, дані про сімейний стан, імена членів сім’ї і осіб, що знаходяться на утриманні, дані про попередніх працедавців);

діставати доступ до своєї персональної інформації, пов’язаної з розрахунком заробітної плати;

діставати доступ і підтримувати в актуальному стані інформацію про компетентності і професійне зростання, результати оцінки і атестацій;

діставати більше можливостей для управління своєю професійною кар’єрою.

Таким чином, з його допомогою співробітники можуть виконувати завдання, які раніше знаходилися у сфері відповідальності інших відділів. Що, у свою чергу, дозволяє оптимізувати документообіг у компанії, вивільнити цінний час фахівців бухгалтерії і відділу кадрів, підвищити точність і актуальність даних про персонал, знизити адміністративні витрати і підвищити якість внутрішньокорпоративних послуг, що на-

даються співробітникам. Крім того, компанія таким чином демонструє високий ступінь довіри своїм співробітникам. Усе це підвищує їх мотивацію, сприяє більш ефективній роботі співробітників і примушує їх відповідальніше відноситися до роботи. У результаті зростає ступінь лояльності співробітників і їх прагнення внести максимальний внесок до розвитку компанії.

Додаток "Інформаційні сервіси для керівників" (SAP Manager Self-Service, SAP MSS) надає інформацію і інструменти, за допомогою яких керівники підприємства мають можливість ефективніше вирішувати управлінські завдання. Цей додаток включає переналаштований інформаційний зміст, сервіси і процеси, які допомагають менеджерам самостійно, без безпосереднього звертання до кадрової служби, визначати, підтримувати і стимулювати кращих співробітників, активно брати участь у процесі вибору кандидатів і ухвалювати оптимальні управлінські рішення в області бюджетування і управління персоналом.

Рішення дозволяє персоналізувати представлення інформації на порталі кожного керівника так, щоб він міг швидко і ефективно знайти всю необхідну йому інформацію на своєму віртуальному робочому місці. Використання інформаційних сервісів допомагає керівникам виконувати завдання в області обліку витрат і бюджетування, включаючи операції планування річного бюджету, контролю виконання і регулювання бюджетів, аналізу витрат.

Інформаційні сервіси дозволяють керівникам удосконалити підхід до виконання адміністративних завдань і завдань планування у сфері управління персоналом. Сервіси забезпечують підтримку таких процесів, як:

- підбір і прийом на роботу персоналу;
- щорічна оцінка ефективності діяльності персоналу і планування компенсаційних програм;
- затвердження запитів співробітників (наприклад, заявок на відрядження, на відпустку або на участь в навчальних заходах);
- процеси розрахунку і моніторингу ключових показників ефективності й індикаторів, що сигналізують про стан справних у тій або іншій області, що відноситься до сфери відповідальності менеджера.

На базі інформаційних сервісів у компанії може бути створений інтерактивний центр взаємодії зі співробітниками (Employee communications) – середовище, яке допомагає співробітникам компанії і фахівцям кадрової служби ефективніше взаємодіяти через єдиний інформаційний

центр. Взаємодія може здійснюватися за допомогою різних каналів комунікації. Єдине стандартизоване джерело інформації, в якому постійно накопичується вся необхідна адміністративна інформація про процедури, прийняті в організації, відповідальних виконавців, шляхи вирішення проблем, дозволяє підвищити ефективність взаємодії між працівниками і працедавцем.

Використання сервісів інформаційного самообслуговування є, на думку авторів, одним з пріоритетних технологічних напрямів подальшого розвитку HRM-систем. Але в Україні цей процес гальмується бюрократичними традиціями, що склалися, в рамках яких всі облікові функції концентруються у відділі кадрів, через який проходить і весь відповідний документообіг. Будь-які зміни даних про співробітників повинні супроводжуватися різного роду і форми довідками й іншими підтверджуючими документами, а відомості про робочі показники співробітника, як правило, доступні тільки його керівництву. Крім того, спілкування співробітників у процесі виконання обов’язків, тим більше за допомогою комп’ютерної системи, часто сприймається начальством негативно. У подібних умовах, упровадження систем Employee self-service (ESS), Manager self-service (MSS), Employee communications легко може спровокувати суперечності із прийнятими в організації правилами.

Еталоном за широтою реалізованої HRM-функціональності є наразі системи компаній SAP і Oracle (у них реалізовано 19 блоків "операційного", "користувальницького" і "стратегічного" технологічних рівнів HRM-систем), серед систем, представлених на вітчизняному ринку – система БОСС-Кадровик (реалізовано 18 блоків). 17 блоків з 19 представлено у системах компаній Robertson & Blums, корпорацій "Галактика", "Інек" і IFS1 [88; 243; 192].

У продуктах компаній "Компас", "Моноліт", "Інформконтакт", "Бізнес Технології" і Epicor / Scala розроблені по 16 функціональних блоків. У системах "1С: Зарплата и Управление Персоналом 8" і "АиТ: Управление персоналом" – 15 блоків [243; 360; 416].

Сьогодні на українському ринку HRM-систем представлено продукти як західного (локалізованого під вітчизняні умови), так і вітчизняного та російського походження. Перші переважно входять до складу потужних і "важких" ERP-рішень (SAP R/3, Oracle Application, Microsoft Dynamics AX та ін.). Другі можуть входити до комплексної системи управління підприємством або пропонуватися як окреме рішення. Найвідоміші

з них – рішення на базі систем БОСС-Кадровик, Галактика, 1С, Мегаполис, PersonPro, Атлас Кадри, Парус. Пропоновані на ринку зарубіжні HRM-системи, як правило, вже адаптовані під українське законодавство.

Оскільки, сьогодні на ринку програмного забезпечення представлений широкий вибір IT-рішень для управління різними сферами бізнесу, то особливої актуальності набувають питання зваженого вибору ІС, які, окрім іншого, включають такі складні питання, як: формулювання вимог до ІС, формулювання критеріїв порівняння ІС, вибір та практичне застосування методів та моделей вибору ІС, оцінка ефективності інвестицій в автоматизацію.

Розглянемо зазначені питання стосовно порівняння та вибору HRM-систем.

Серед основних причин для впровадження підприємствами сучасної HRM-системи відокремлюють такі [88; 243]:

- велика чисельність персоналу. Це призводить до перевантаження фахівців кадрової служби через необхідність ведення відповідної документації по всіх співробітниках з оформленням вручну всіх необхідних паперів, а також через великий об’єм розрахунків, пов’язаних з нарахуванням заробітної плати, визначенням податкових виплат тощо. Як правило, із зростанням чисельності персоналу зростає і число помилок у кадровому обліку, знижується достовірність результатів розрахунку зарплати, можуть виникати затримки з її виплатою;
- висока складність розрахункових операцій за заробітною платою. Упровадження HRM-системи дозволяє вести кадрову документацію і підтримувати документообіг в електронному вигляді, що мінімізує ручне введення даних, виключає дублювання облікових записів співробітників, забезпечує їх блокування для звільненого персоналу, а також дає можливість оперативно виконувати розрахунок зарплати і всіх пов’язаних з ним нарахувань і утримань;
- актуальність завдань управління людським капіталом.

Крім того, передумовами для впровадження HRM-систем є [90; 245; 362]:

- виробнича, торгова, проектна або освітня діяльність;
- територіально-розподілена організаційна структура;
- сучасний стиль управління компанією;
- необхідність використовувати висококваліфікованих кадрів;
- висока цінність накопичених фахівцями знань;
- перевищення попиту на фахівців над пропозицією.

Типовий процес вибору HRM-системи для підприємства зазвичай складається з таких етапів:

створення команди для вибору системи;

формулювання вимог до системи;

пошук і первинний відбір систем, що відповідають зазначеним вимогам;

підготовка докладних списків контрольних питань за групами критеріїв та присвоєння їм пріоритетів;

відбір тих доступних систем, які найбільше відповідають встановленим вимогам за затвердженими критеріями;

оцінка остаточного списку систем з точки зору сукупності вимог;

відбір систем для демонстрації роботи, зустрічі з постачальниками, проведення практичних випробувань;

проведення функціонального і навантажувального тестування.

Формулювання вимог до системи та їх оцінювання є етапами, які вирішальним чином впливають на якість остаточного рішення. Розглянемо ці етапи докладніше.

Цілі, завдання, параметри, структура ІС, що розробляється, безпосередньо залежать від інформаційних потреб управлінського персоналу, які ця система повинна задовольнити.

Із зміною бізнес-цілей, зовнішнього середовища і самих ІТ змінюються також інформаційні потреби користувачів ІС.

Тому при розробці ІС або її модернізації необхідно виробити погляд на систему з точки зору розвитку бізнесу підприємства, оскільки багато нововведень бізнесу залежать від того, яка ІС функціонує на підприємстві. І вимоги до ІС необхідно розробляти для бізнесу в цілому, з урахуванням особливостей його організації на цьому підприємстві, а також з урахуванням вимог до стратегії та тактики розвитку бізнесу.

Кінцевою метою впровадження ІС є підвищення ефективності роботи підприємства. Ця мета досягається завдяки підвищенню ефективності системи управління бізнесом за рахунок автоматизації бізнес-процесів та бізнес-функцій.

Сучасна ІС для бізнесу повинна задовольняти основні вимоги, що наведені на рис. 5.2.

Вимога розвиненої функціональності означає, що ІС повинна мати достатньо широкий набір автоматизованих функцій управління бізнесом та бізнес-процесів, які за рахунок інтеграції з інформаційно-телекомуніка-

ційною інфраструктурою системи та функцій між собою забезпечують високий рівень інформаційної керованості бізнесом.

Функціональні компоненти ІС повинні охоплювати автоматизацією усі аспекти бізнес-діяльності, усі області основних, допоміжних, управлінських бізнес-процесів. Повнофункціональна ІС – це мультипредметна ІС з широкою функціональністю, яка комплексно автоматизує підтримку та реалізацію усього спектру бізнес-процесів ведення бізнесу та управління ним. Така ІС орієнтована на автоматизацію різних предметних областей у середині системи. Основним завданням ІС є забезпечення можливості координації при реалізації різних бізнес-процесів у рамках усього підприємства.

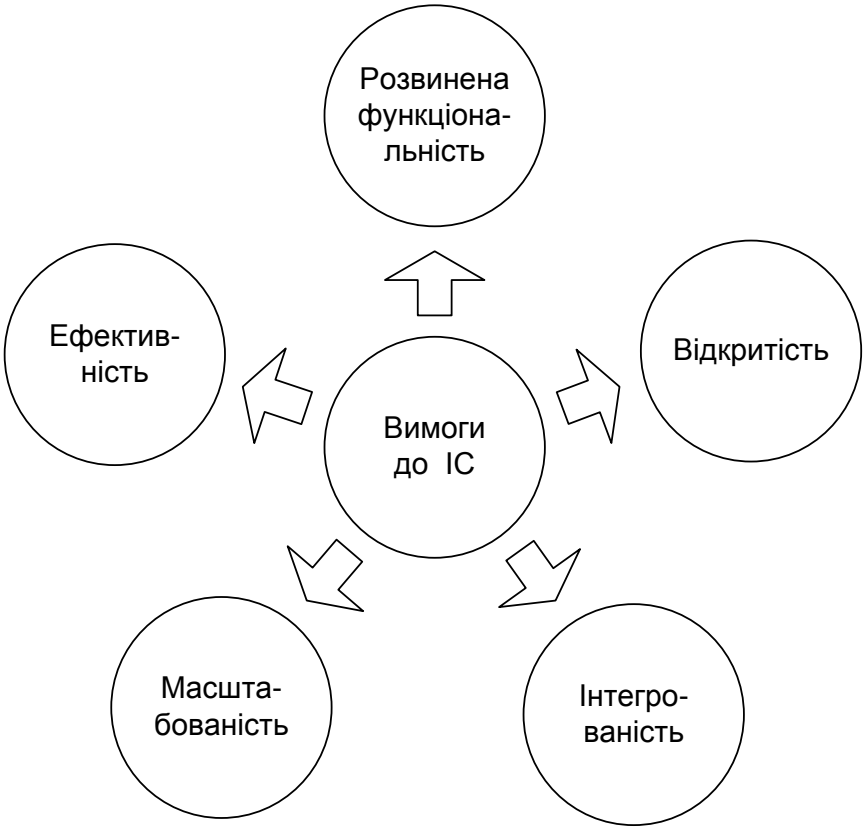


Рис. 5.2. **Вимоги до сучасної ІС**

Повнофункціональна ІС повинна задовольняти інформаційні потреби різних категорій користувачів. Щоб кожен користувач зміг вирішувати свої завдання та відстежувати свій набір показників, необхідно:

визначити склад цих показників;

виділити аналітичні ознаки формування показників та скласти формули для їх розрахунку;

реалізувати механізм формування запитів для вибору із єдиної бази даних інформації, необхідної для розрахунку показників;

реалізувати механізм представлення розрахованих показників у формі, необхідній та найбільш зручній користувачеві.

Вимога відкритості ІС передбачає подальший її розвиток і вдосконалення. Ідеологія побудови ІС повинна забезпечувати можливості додавання нових об'єктів, процесів управління ними, нових бізнес-функцій.

Відкритими вважають інформаційні системи, що мають такі властивості:

розширюваність/масштабованість – можливість додавання нових функцій в ІС або зміни деяких існуючих функцій, при цьому решта функціональних частин ІС мають залишатися незмінними; для реалізації цієї властивості система повинна виконуватися у вигляді каркаса, що містить базові модулі, з можливістю їх доопрацювання;

мобільність/переносимість – можливість перенесення програм і даних при модернізації або заміні апаратних платформ ІС і можливість роботи після цього користувачів без їх перепідготовки;

здатність до взаємодії з іншими ІС;

відповідність стандартам – ІС для підприємств проектуються і розробляються на основі загальноприйнятих міжнародних стандартів;

дружність до користувача – дружні інтерфейси повинні забезпечувати можливість працювати із системою користувача, що не має спеціальної комп'ютерної підготовки.

У зв'язку з необхідністю забезпечити відкритість системи, відразу ж виникає декілька супутніх питань, які слід брати до уваги. Наприклад, чи необхідно окремо докуповувати спеціальне програмне забезпечення, яке використовується для модифікації системи, яким чином впливає модифікація на перехід на нові версії системи, чи зможуть спеціалісти підприємства самостійно супроводжувати та допрацьовувати систему і так далі.

Вимога відкритості реалізується за допомогою принципу модульності побудови ІС.

Принцип модульності побудови ІС передбачає розподіл ІС на ряд компонентів (елементів) за функціональним або об'єктним принципом. Ці елементи є функціональними програмними модулями.

Модуль об'єднує декілька функціональних ІТ, об'єднаних за принципом завершеності предметної технології, і таких, що мають універсальний характер. Це відносно самостійні прикладні частини системи, що автоматизують одну зі сторін бізнес-діяльності.

Набір модулів у системі варіюється залежно від специфіки підприємства, його спрямованості, масштабу діяльності.

Модулі взаємно інтегровані. Число модулів, а значить, і загальна функціональність системи може нарощуватися в міру необхідності в процесі її розвитку.

В умовах динамічного ринку модульний принцип дозволяє мінімізувати витрати на впровадження ІС та на внесення до її функціональності змін, швидко здійснити процес адаптації ІС до вимог бізнесу, що змінюються.

Крім того, модульний принцип побудови ІС дозволяє замовникові при закупівлі та впровадженні системи починати з набору модулів, що реалізовують базову функціональність, а потім поступово розширювати її.

Розробники, які беруть за основу модульну побудову ІС, закладають у кожен модуль рішення і бізнес-моделі, які узагальнюють передовий світовий досвід управління в конкретній галузі. Ці рішення ґрунтуються на найдосконаліших ІТ. Причому принцип модульності може реалізуватися також у межах модуля.

У сукупності модулі різних додатків створюють потужну ІС з розвиненою функціональністю, здатну задовольнити усі вимоги сучасного підприємства та вирішувати практично будь-які завдання, необхідні для управління бізнесом.

Програмні рішення, що реалізовують функціональність модуля, носять універсальний характер, тобто роботу модуля можна налаштувати з урахуванням галузевої специфіки і специфіки конкретного підприємства, в результаті реалізується необхідна функціональність для цього підприємства. Усередині системи модулі інформаційно пов’язані через єдиний інформаційний простір.

За допомогою принципу модульності вирішується проблема розподілу завдань між учасниками процесу управління, оскільки деякі завдання можуть повністю розв’язуватися на одному робочому місці, а інші для їх вирішення вимагають участі багатьох управлінських працівників.

Модуль може складатися із завдань, які бізнес-орієнтовані і передбачають діловий результат. Результатом рішення таких завдань є аналіз ситуації, що склалася, та ухвалення управлінського рішення.

Вимога інтегрованості означає, що ІС побудована на загальносистемних принципах і охоплює автоматизацією усю сукупність бізнес-орієнтованих завдань. Питання автоматизації в системі вирішені комп-

лексно з урахуванням інформаційних і функціональних зв'язків компонентів системи.

При побудові інтегрованої ІС в єдине ціле об'єднуються складові елементи, модулі різних підсистем і навіть систем шляхом їх взаємозв'язки та інформаційної взаємодії. ІС перетворюється на повністю інтегровану систему, в якій кожному окремому модулю в реальному часі доступна уся необхідна інформація, що формується іншими модулями.

Процес інтеграції ІС реалізується шляхом створення єдиного інформаційного простору підприємства. Єдиний інформаційний простір забезпечує включення в управлінський контур усіх учасників бізнес-процесів, незалежно від їх місця розташування, у тому числі віддалених, мобільних, а також контрагентів. Інтеграція модулів (бізнес-додатків) здійснюється за рахунок ведення єдиної БД, сховищ даних, єдиних принципів функціонування і правил використання інформаційно-комунікаційних систем і мереж. За допомогою телекомунікаційних засобів реалізується технологія обміну електронними даними.

Інтегрована ІС повинна покривати автоматизацією усі бізнес-процеси як усередині підприємства, так і в зовнішньому його контурі. При цьому мають бути інтегровані в єдину систему бізнес-процеси front-офісу, back-офісу, middle-офісу.

Вимога масштабованості передбачає зберігання працездатності ІС при необмеженому збільшенні числа одночасно обслуговуваних користувачів. Тобто збільшення числа користувачів ІС не призведе до радикальної її перебудови. Реалізація цієї вимоги стає можливою завдяки реалізації вимоги відкритості системи. Масштабованість, розширюваність використання проектних рішень ІС вимагає лише збільшення потужності апаратного забезпечення (серверів, робочих станцій тощо).

Вимога ефективності означає, що впроваджувана ІС повинна забезпечити повернення інвестицій, вкладених в неї. Підприємство, впроваджуючи ІС, чекає підвищення ефективності бізнес-діяльності від використовуваних ІТ.

Кінцевий успіх будь-якої ІС визначається не лише якістю, розвитком технологій, але і отримуваною економічною вигодою. Важливо, щоб інвестиції в сучасні ІТ самоокуповувалися та при цьому сприяли підвищенню прибутковості бізнесу.

Але розрахувати ефективність інвестицій в автоматизацію управління бізнесом досить складно. Це пов'язано з тим, що багато переваг,

що отримуються бізнесом від ІС, не можуть бути враховані в грошовому вираженні. Тому оцінка ефективності ІС не ґрунтується на чисто грошовому підході. Ця оцінка має бути результатом, отриманим на підставі п’яти складових: вартість, час, якість, гнучкість, зручність користувачів.

При цьому повинен враховуватися рівень узагальнення для економічних переваг від ІС: окремий користувач, група користувачів, управлінський бізнес-процес, підприємство в цілому.

Вартість має велике значення на усіх рівнях. Пряма економія коштів може бути отримана шляхом впровадження електронного документообігу, що виключає дублювання документів, повторне введення їх в систему. Але для впровадження електронного документообігу потрібна реорганізація бізнес-процесів як внутрішніх, так і зовнішніх. Тому велика потенційна економія навряд чи проявиться при впровадженні ІС.

Що стосується часу, то користувачі ІС завдяки автоматизації їх роботи можуть використовувати свій час більш продуктивно, тобто витрати часу окупаються. При цьому підвищується швидкість ухвалення рішень, а отже, ефективність бізнес-діяльності. Бізнес-процеси виконуються швидше.

Завдяки забезпеченню доступу до різноманітної інформації покращується якість ухвалення управлінських рішень. Створення єдиної бази даних системи сприяє поліпшенню якості роботи в цілому.

Підвищується гнучкість роботи в цілому і гнучкість міжособових стосунків. Завдяки електронним телекомунікаціям збільшується ступінь мобільності стосунків між співробітниками, покращується координація їх дій. Співробітники можуть працювати в будь-якому місці, в будь-який час і мають можливість зв’язуватися з іншими за своїм бажанням.

ІС робить роботу співробітників привабливішою і зручнішою, сприяє їх індивідуальному розвитку.

ІС стає невід’ємною частиною роботи підприємства та надає допомогу у виробленні ефективних рішень щодо управління бізнесом. Зрештою впровадження ІТ та ІС сприяє отриманню додаткових конкурентних переваг на ринку та отриманню прибутку.

Основний результат від функціонування розвинутої ІС на підприємстві полягає у впровадженні стратегії розвитку бізнесу та комплексу заходів, заснованих на застосуванні нових управлінських та інформаційних технологій, за допомогою яких управлінський персонал

отримує та використовує детальну, достовірну, актуальну інформацію і знання про внутрішнє і зовнішнє середовище.

Найчастіше дискусії користувачів та розробників програмного забезпечення для підприємств точаться навколо проблеми вибору ERP-систем. На думку авторів, більшість критеріїв вибору ERP є придатними і для оцінювання та порівняння HRM-систем. До таких критеріїв відносяться [88; 127; 345; 347; 351; 367; 373; 404; 408]:

функціональна повнота;

функціональна та лінгвістична локалізація;

захист інформації та надійність системи;

можливість роботи в розподіленому режимі;

наявність стандартизованих інструментальних засобів адаптації та супроводу;

інтеграція з раніше впровадженими системами та іншими програмними продуктами, котрі використовуються на підприємстві;

агрегування інформації на рівні підприємства, окремих функціональних завдань;

наявність спеціальних засобів аналізу стану елементів системи в процесі її експлуатації;

вартість програмного забезпечення;

вартість робіт з адаптації та впровадження системи;

середні терміни адаптації та впровадження системи;

рівень професійної кваліфікації спеціалістів фірми-розробника (або інтегратора) і наявність у них досвіду впровадження подібних систем;

ділова репутація фірми-розробника та її досвід роботи;

можливість роботи з декількома найбільш широко розповсюдженими операційними системами і СУБД.

Серед специфічних критеріїв, що стосуються вибору саме HRM-систем, найважливішими автори вважають такі:

відповідність системи вимогам підприємства щодо HRM-функціональності, в тому числі підтримка оперативного розрахунку заробітної плати великої кількості співробітників, можливість системи самостійно проводити розрахункові операції високої складності, рішення сучасних завдань з управління кадровим потенціалом, підтримка процесів підбору персоналу, оцінки компетентностей, планування кар’єрного розвитку, постановки цілей і розрахунку показників персоналу, управління навчанням, винагородою персоналу, планування витрат на персонал тощо;

резерв функціональності, що забезпечує можливості для зміни і розвитку підходів до управління персоналом протягом найближчих 5 – 10 років;

надання можливості здійснювати інформаційне самообслуговування персоналу;

відповідність системи вимогам вітчизняного трудового та податкового законодавства;

підтримка організаційної структури підприємства;

можливість отримання кадрових вихідних форм будь-якого виду, в будь-якому обсязі і в будь-якому розрізі;

можливість вести паралельно два види обліку – управлінський і регламентований;

можливість вести в єдиній інформаційній базі облік від імені декількох організацій – юридичних осіб, які з погляду організації бізнесу складають єдине підприємство (корпорацію);

можливість формувати корпоративну консолідовану звітність;

наявність механізмів інтеграції з HR-порталом;

потужність і швидка доступність засобів бізнес-аналізу. моделювання та прогнозування змін та їх взаємного впливу один на одного;

можливість оцінити окупність HRM-системи в прогнозовані терміни;

відсутність надмірної складності при впровадженні системи, відпрацьована методологія впровадження.

Найбільш складним для оцінки видається критерій функціональної повноти. З одного боку, вимоги до функціональності системи можуть визначатися на основі знань з предметної області, специфіки того чи іншого бізнесу, з іншого – однозначну формалізацію зазначених вимог можуть здійснити тільки фахівці з HRM-систем, які знають всі тонкощі автоматизації різних бізнес-процесів. Саме тому для роботи з вибору системи необхідно залучати сторонніх консультантів – компанії, що мають досвід упровадження декількох систем. Важливим фактором також виступає досвід сполучення різних систем між собою і системного інтегрування.

Для середнього підприємства (групи підприємств) з метою оцінки функціональної повноти тієї чи іншої системи потрібно від 100 до кількох тисяч критеріїв. При цьому критерії доцільно об’єднувати в групи (підсистеми), що дозволить в подальшому виділити етапи впровадження ІС та оцінити ефект на кожному з етапів.

Прийняття рішення про впровадження системи управління персоналом починається з вибору найсуттєвіших з перелічених критеріїв, які далі будуть використовуватися для порівняння систем. У процесі визначення і обґрунтування критеріїв необхідно враховувати такі основні вимоги:

критерії повинні бути між собою узгодженими і не суперечити один одному;

склад показників повинен бути мінімально достатнім і повним, відповідати поставленим цілям;

значення критеріїв повинні бути реальними і досяжними.

Серед можливих причин помилок у процесі вибору ІС найбільш розповсюдженими є такі:

неправильний вибір як самої системи, так і її постачальника; особливо, якщо система має декількох постачальників;

відсутність розуміння цілей впровадження проекту, в результаті вибирається система, нездібна підтримати стратегію підприємства;

відсутність взаєморозуміння між керівництвом та ІТ-підрозділом підприємства; це призводить до того, що рішення з питань, пов’язаних з інформаційними технологіями, готуються на рівні ІТ-підрозділу, яке не враховує вимоги бізнесу або, навпаки, керівництво самостійно обирає ІС, не враховуючи того, що систему не вдасться впровадити з технічних причин (наприклад, через несумісність з програмними та технічними засобами, що вже використовуються на підприємстві).

Розглянемо методи та моделі оцінки віддачі від впровадження HRM-систем. Експерти стверджують, що економічний ефект від автоматизації процесів управління персоналом виявляється при чисельності персоналу від 1 000 осіб. Це не означає, що на підприємствах з меншою чисельністю персоналу впровадження HRM-системи буде невиправданим, в цьому випадку період її окупності буде довшим.

На початковому етапі розрахунки ефективності носять орієнтовний характер. Проте вони дають можливість визначити, скільки приблизно засобів дозволить заощадити впровадження системи.

1. Універсальні підходи (рис. 5.3), які використовуються для оцінки будь-яких ІТ-проектів [184; 348].

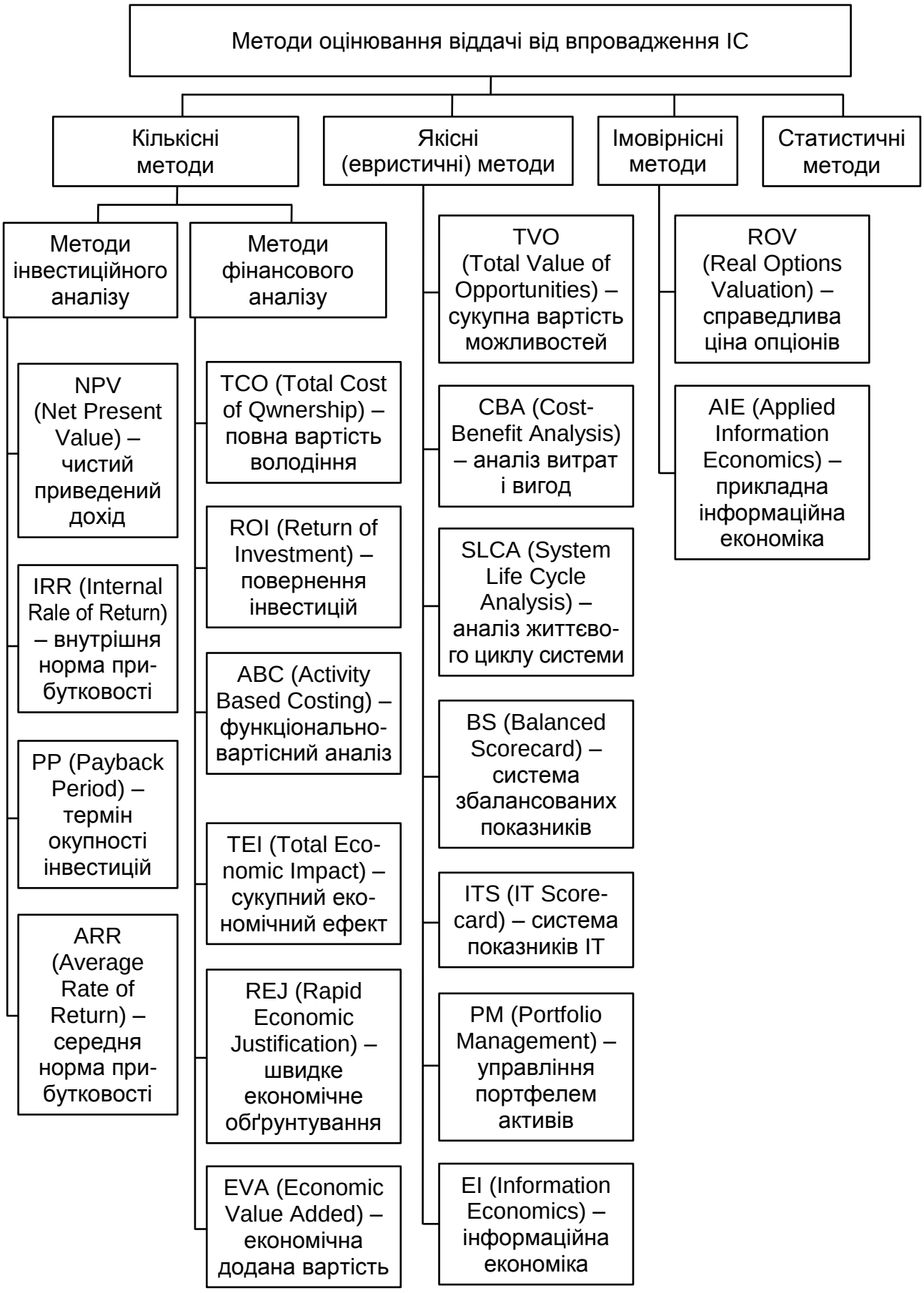


Рис. 5.3. **Універсальні підходи до оцінювання ефективності ІС**

Серед усього різноманіття підходів найбільш затребуваними на практиці виявляються методи ROI (Return on Investment), TCO (Total Cost of Ownership) та статистичний метод. Розглянемо зазначені методи докладніше.

Ефективність впровадження ІС найчастіше оцінюється віддачею від інвестицій (ROI – Return on Investment). При цьому в загальному випадку враховуються такі показники:

загальна вартість проекту, включаючи програмне забезпечення, апаратні засоби, вартість зовнішнього обслуговування і витрат на зарплату;

час упровадження, крім якого треба враховувати і час, який потрібно, щоб окупити впровадження;

час повернення інвестицій;

загальна сума витрат підприємства на впровадження інформаційної системи, в яку входять вартість програмного забезпечення, апаратних засобів, послуг, зарплати, витрат після впровадження.

Розрахувати ефективність інвестицій в автоматизацію достатньо важко. Для цього, по-перше, необхідно скласти бюджет проекту автоматизації. Підприємство може використовувати для впровадження КІС тільки вільні фінансові ресурси, причому, як правило, не всі. Тому спочатку складають бюджет, а потім обирають конкретну систему. На першому етапі зазвичай неможливо скласти детальний бюджет, але, як мінімум, у бюджеті потрібно розділити засоби на впровадження програмного забезпечення та на експлуатацію.

Зауважимо, що вкрай важливо знати загальну вартість системи, а не просто ціну програмного забезпечення. Тому використовують поняття сукупної вартості володіння системою (ТСО – Total Cost of Ownership). ТСО включає не лише ціну придбання системи (точніше, вартість ліцензій для заданого числа робочих місць), а і вартість запуску її в експлуатацію і підтримки в робочому стані, придбання технічних засобів, навчання персоналу і багато іншого.

Витрати на підтримку і обслуговування КІС після впровадження називають прихованими витратами. За статистикою приховані витрати складають 200 – 500 % від початкової вартості проекту.

Статистичний метод визначає економічний ефект на основі середньогалузевих позитивних результатів від впровадження ІС на підпри-

ємствах аналогічної галузі. Так, наприклад, орієнтиром щодо впровадження HRM-систем можуть бути такі ефекти [88; 243]:

підвищення якості доступної інформації на 91 %;

зниження адміністративного навантаження на відділ HR на 83 %;

підвищення швидкості отримання і розповсюдження інформації на 81 %;

підвищення рівня "гнучкості" інформації (що дозволяє використовувати її в процесі бізнес-планування) на 59 %;

підвищення якості HR-сервісів на 56 %;

підвищення ефективності процесів розрахунку HR-показників та засобів вимірювання зростання продуктивності на 55 %;

підвищення ефективності ведення HR-звітності на 42 %;

підвищення продуктивності праці на 39 %;

скорочення експлуатаційних витрат на 35 %;

підвищення ефективності управління робочим часом персоналу на 26 %;

скорочення штату співробітників HR-служби на 8 %.

Зрозуміло, що такі розрахунки носять орієнтовний характер, тому при оцінюванні великих та дорогих систем статистичний метод може використовуватися лише на початковому етапі.

Як правило, компанії не використовують лише один метод оцінювання економічного ефекту від IT-проекту. Досвід показує, що в різних ситуаціях ближче до істини виявляються різні методи. Часто компанії використовують відразу чотири методи – два фінансових і два нефінансових. Саме на підставі такого оцінювання економічної ефективності вже можна прийняти оптимальне рішення, запускати IT-проект, чи ні, а також визначитися, який з IT-проектів компанії більш вигідний. Однак вартість процедури оцінювання в такому разі стає занадто великою.

2. Оцінювання віддачі від впровадження HRM-систем через оцінювання динаміки показників ефективності HR-служби.

Оцінювання персоналу та HR-служби – це складна управлінська проблема. На практиці застосовується безліч методик, способів оцінки, які дають різні за рівнем об’єктивності результати. Оцінка персоналу дозволяє виявити і перевірити: виконання посадових обов’язків співробітниками; особливості поведінки, сильні і слабкі сторони кожного співробітника, переважні ділянки роботи для кожного, передумови підвищення продуктивності праці, виявити ефективність діяльності співробіт-

ника та рівень його компетентності, конкретизувати посадові обов'язки, співставити індивідуальні результати із стандартними вимогами за рівнями і специфікою посад, намітити перспективи кар'єрного зростання окремого співробітника, визначити програму навчання співробітників необхідним навичкам. Необхідно зазначити, що в теоретичному і методичному аспектах система оцінювання персоналу розроблена недостатньо. Між тим, у більшості компаній, які працюють на ринку, гостро постає питання грамотного і системного управління персоналом. Достатньо великі кошти вкладаються у підбір, оцінку і розвиток персоналу, оскільки від якості цих процесів залежить успіх бізнесу. Ці витрати безпосередньо пов'язані з тим результатом, який компанія очікує отримати від кандидата, і тими ризиками, які можуть виникнути в разі прийняття на роботу некваліфікованої людини. У цих умовах важлива роль в оптимізації процесів підбору, оцінки, розвитку персоналу та в зменшенні витрат на зазначені процеси належить автоматизованим системам управління.

Розглянемо найбільш часто використовувані методи оцінювання ефективності HR-служби [127; 385].

Експертна оцінка. Експертну оцінку співробітники служби персоналу можуть провести самостійно. Для цього необхідно опитати керівників суміжних підрозділів і з'ясувати, як вони оцінюють діяльність HR-служби в цілому, а також роботу окремих напрямів: якість і швидкість підбору, якість проведених програм навчання тощо. Таке опитування доцільно проводити регулярно раз на півроку або рік. Отримавши і проаналізувавши дані, важливо зробити правильний висновок і підвищити якість надаваних послуг. Перевага такої оцінки полягає в простоті її реалізації і невисокій вартості проекту, а недоліком є неминучий суб'єктивізм в оцінках. Показник повернення на інвестиції в персонал (ROI) розраховується за формулою:

$$ROI = (Дохід – Витрати) / Витрати \cdot 100\ \%.$$

Такий спосіб оцінки є досить трудомістким. У розрахунках необхідно враховувати не тільки вартість конкретного заходу, але також і непрямі витрати, пов'язані з його проведенням, але найбільш складним є підрахунок доходу від проведеного заходу в галузі управління персоналом.

Метод бенчмаркінгу. При використанні підходу HR-Benchmarking показники діяльності HR-служби порівнюються з аналогичними даними інших компаній, що працюють на ринку. Зовнішні консультанти запрошують в компаніях-учасницях такого проекту необхідні дані про якісні та кількісні показники. Після обробки даних компаніям надається узагальнена по галузі статистика, яку потрібно порівняти з власними показниками HR-діяльності. На пострадянському просторі застосування методу бенчмаркінгу ще недостатньо поширене. Це пов'язано з небажанням компаній надавати конфіденційні дані і недовірою до організаторів таких проектів.

Методика Джека Філіпса. У західних компаніях при розрахунку повернення інвестицій в HR-службу часто використовують методику Джека Філіпса, який запропонував п'ять формул визначення ефективності служби персоналу:

оцінка інвестицій в HR-підрозділ = витрати кадрових питань /операційні витрати,

оцінка інвестицій в HR-підрозділ = витрати кадрових питань /кількість працівників,

показник відсутності на робочому місці = прогули + кількість співробітників, що звільнилися несподівано,

показник задоволеності = числу задоволених своєю роботою співробітників, вираженого у відсотках (визначається методом анкетування).

Крім того, визначається критерій, що відбиває рівень єдності і злагоди в організації. Підраховується на основі статистичних даних про продуктивність та оцінках ефективності праці.

На думку консультантів, методика Філіпса успішно працює в компаніях, де добре поставлений регулярний менеджмент, що в Україні зустрічається досить рідко.

Показники економічної ефективності діяльності служби персоналу.

1. Дохід людського капіталу (Human Capital Revenue Factor), основний показник продуктивності працівників:

HCRF = Дохід / FTE,

де FTE – Full Time Employe – кількість заповнених ставок.

2. Економічна додана вартість персоналу (Human Economic Value Added), показник роботи менеджменту компанії:

HEVA = (Прибуток без податків – Вартість персоналу) / FTE.

3. Собівартість людського капіталу (Human Capital Cost Factor):

HCCF = Загальні витрати на персонал / Оборот.

4. Додана вартість людського капіталу (Human Capital Value Added), показник показує прибутковість усередненого працівника організації:

HCVA = Дохід – (Витрати – Зарплати і премії) / FTE.

5. ROI людського капіталу (Human Capital Return on Investment):

HCROI = Дохід – (Витрати – Зарплати і премії) / Зарплати і премії.

6. Ринкова вартість людського капіталу (Human Capital Market Value) показник корисний для біржових аналітиків та економістів:

HCMV = (Ринкова вартість ЧК-Балансова вартість) / FTE.

Показники ефективності функцій служби персоналу розраховуються як для всього персоналу в цілому, так і для кожної з груп співробітників (топ-менеджери, лінійні керівники, фахівці, ІТП, робітники) залежно від специфіки діяльності самої компанії та характеристик її організаційної структури. Розрахунки проводяться до та після впровадження засобів автоматизації, різниця між значеннями показників відбиває отримані ефекти від впровадження ІТ.

Усі методи визначення економічної ефективності HRM-систем мають певні недоліки, тому використання одного з методів може як не дати результату взагалі, так і призвести до помилкових управлінських рішень. Таким чином, очевидна необхідність використання комплексу методів. Однак дослідження авторів показали, що ні в світовій, ні в вітчизняній практиці не використовуються спеціалізовані методики оцінювання ефективності HRM-систем. У кращому разі оцінювання здійс-

нюється за універсальними методиками, що певним чином адаптовані до HRM-систем. Між тим, дослідниками проводиться постійна робота з розробки або адаптації універсальних моделей для оцінювання систем інших класів (наприклад, CRM-систем). Незважаючи на те, що методики вибору ERP-систем легко адаптуються для вибору програмного модуля управління персоналом, на думку авторів, специфічна функціональність HRM-систем обумовлює необхідність розробки та використання спеціалізованих моделей оцінювання їх ефективності з урахуванням запропонованих у цій роботі особливих вимог до HRM-систем.

Важливо сказати про ті труднощі, що можуть виникнути в процесі оцінювання показників ефективності HRM-системи.

1. Відсутність на підприємстві детальної системи управлінського обліку. У цій ситуації HR-директору необхідно адаптувати існуючу систему під потреби HR-служби для того, щоб полегшити збір і аналіз необхідної інформації. Адаптація полягає у виділенні і прописанні алгоритмів розрахунків необхідних показників.

2. Невизначеність у зонах відповідальності підрозділів і децентралізація витрат на персонал. Необхідно вирішити дану ситуацію, інакше буде складно рознести витрати між підрозділами. Необхідно домовлятися усередині компанії про те, куди віднести, наприклад, витрати на оплату праці тимчасового персоналу, найнятого на час проведення регіональної маркетингової акції: на витрати HR-бюджету або маркетингового бюджету.

3. Фактор віддаленості результату в часі. Результат багатьох проектів вилучений у часі і, таким чином, не завжди очевидно, коли очікувати ефекту і як "обраховувати" його після часу. Також необхідно враховувати те, що аналіз ведеться в умовах вітчизняного бізнесу, який є нестабільним: швидко змінюються люди, алгоритми та методи управління.

4. Брак інформації про досвід інших компаній. Відсутність таких відомостей ускладнює аналіз розрахованих показників. Наприклад, витративши ряд зусиль і вирахувавши ROI на проект впровадження IC, HR-менеджер стикається з тим, що не може проаналізувати цей показник, тому що в кращому разі володіє інформацією лише про досвід західних компаній, що не зовсім актуально для вітчизняної компанії, що працює в умовах національної економіки.

5. Опір співробітників служби персоналу. Такий опір можливий, коли співробітники HR-служби не розуміють важливості і необхідності

проведеного оцінювання. Директор з персоналу повинен мотивувати співробітників брати участь в оціночних процедурах і переконати підлеглих в їх корисності.

Очевидно, що кількість HRM-систем буде постійно зростати, а отже, проблема аргументованого, зваженого вибору буде ставати дедалі актуальнішою. Уже сьогодні на ринку програмного забезпечення пропонується широкій вибір ІС управління персоналом; пропонуються системи як для великих корпоративних клієнтів, так і малого та середнього бізнесу, який також виявляє активність у питаннях автоматизації. Цей факт, а також відсутність надійних методик порівняльного аналізу ІС обумовлюють складність процесу вибору ІС організаційного управління загалом, та HRM-систем зокрема.

У процесі вибору ІС найчастіше використовують такі критерії: відкритість, гнучкість та адаптивність, розподіленість, інтегрованість, наявність успішних впроваджень на підприємствах цієї галузі, великий вибір функціональних модулів, СУБД, яка лежить в основі КІС, імідж фірми-розробника, сукупна вартість володіння системою. Типовими фінансовими показниками, якими оперує керівник організації, ухвалюючи рішення про впровадження нової інформаційної системи, є показник повернення на інвестиції, сукупна вартість володіння системою, приховані витрати. Розрахувати ефективність інвестицій в автоматизацію достатньо важко, отже, на першому етапі зазвичай складають лише орієнтовний бюджет проекту автоматизації.

Зрозуміло, що кожен метод оцінки віддачі від впровадження HRM-систем має свої переваги і недоліки. Використання відразу декількох методів підвищує точність розрахунку і одночасно збільшує вартість самої процедури, а в кінцевому підсумку і всього інвестиційного проекту, відповідно, зменшує рентабельність. Проте оцінка ефективності інвестицій в ІТ доцільна й інформативна.

Для оцінки віддачі від впровадження HRM-систем доцільно, але, на думку авторів, недостатньо використовувати показники ефективності HR-служби до та після впровадження ІС.

Як і в будь-якому проекті, впровадження HRM-системи має давати бізнесу конкурентну перевагу, що оцінюється в грошовому еквіваленті. Тому методика, використовувана при оцінці ефективності впровадження, обов’язково повинна включати в себе кількісні показники, на базі яких можливо провести розрахунок. Такими показниками можуть стати кіль-

кість операцій і часу, що витрачаються користувачем на виконання того чи іншого бізнес-процесу, кількість помилок при розрахунку заробітної плати, кількість вдалих/невдалих співбесід у розрахунку на одиницю часу, відсоток досягнення співробітниками встановлених показників у роботі, кількість співробітників HR-департаменту тощо. Перед упровадженням рекомендується зробити виміри погоджених показників, і зробити те ж саме після завершення проекту. Різниця між значеннями двох вимірів і дасть базу для аналізу ефективності впровадження HRM-системи.

Розділ 6. Метод стиснення текстової інформації в базах даних на основі блоково-статистичного алгоритму

6.1. Аналіз сучасного стану алгоритмів стиснення інформації

Зазначено, що у зв'язку зі стрімким зростанням обсягів інформаційних ресурсів постійно виникає проблема позбавлення надлишковості даних. Констатується, що одним із шляхів вирішення цієї проблеми є розробка алгоритмів стиснення, які дозволяють підвищити ефективність збереження та передачі даних за допомогою зменшення їх надмірності.

Проведено аналіз сучасного стану алгоритмів стиснення та визначено сфери їх застосування.

Інформаційні ресурси – це продукт інтелектуальної діяльності найбільш кваліфікованої й творчо активної частини працездатного населення. В останній чверті XX століття інформаційні ресурси досягли настільки рекордних обсягів, що були введені поняття "інформаційного вибуху", "інформаційної революції" [354]. Підтвердженням тому є збільшення інформаційного потоку з початку цього століття більш ніж в 30 разів. Таким чином, необхідне винаходження та застосування принципово нових методів і засобів сприйняття, передачі, обробки, зберігання і розповсюдження інформації, здатних оперувати з великими масивами інформації в реальному часі.

Ураховуючи лавиноподібно наростаючі потоки інформації в найрізноманітніших сферах людської діяльності, постає запитання, як і якими засобами можна представити у пам'яті комп'ютера настільки різноманітну і численну інформацію і успішно її використовувати. Найбільш досконалою і прогресивною формою організації інформації і знань – є бази даних і бази знань. Головне їхнє завдання – це забезпечення користувачів необхідною інформацією, тобто можливість давати відповіді на інформаційні запити користувачів до бази даних або бази знань з метою отримання шуканої інформації [273].

Характерною особливістю більшості типів даних є їх надлишковість. Для людини надлишковість даних часто пов'язана з якістю інформації, оскільки надлишковість, як правило, покращує зрозумілість та сприйняття інформації. Однак коли мова йде про зберігання та передачу інформації засобами комп'ютерної техніки, то надлишковість відіграє негативну роль, оскільки вона призводить до зростання вартості зберігання та передачі інформації. Особливо актуальною є ця проблема у випадку необхідності обробки величезних обсягів інформації при незначних об'ємах носіїв даних. У зв'язку з цим постійно виникає проблема позбавлення надлишковості або стиснення даних.

Основний принцип, на якому базується стиснення даних, полягає в економічному описі повідомлення, згідно з яким можливе відновлення початкового його значення з похибкою, яка контролюється [8; 147].

Засновником науки про стиснення інформації прийнято вважати Клода Шеннона. Його теорема про оптимальне кодування показує, до чого потрібно прагнути при кодуванні інформації і на скільки та або інша інформація при цьому стиснеться. Крім того, вченим були проведені дослідження за емпіричним оцінюванням надмірності англійського тексту. Шеннон пропонував людям вгадувати наступну букву і оцінював вірогідність правильного вгадування. На основі ряду досліджень він прийшов до висновку, що кількість інформації в англійському тексті коливається в межах 0.6 – 1.3 біта на символ. Не дивлячись на те, що результати досліджень Шеннона були по-справжньому затребувані лише через десятиліття, важко переоцінити їх значення. Перші алгоритми стиснення були примітивними у зв'язку з тим, що була примітивною обчислювальна техніка. З розвитком потужностей комп'ютерів стали можливими все більш досконалі алгоритми.

Алгоритми стиснення можуть підвищувати ефективність збереження і передачі даних за допомогою зменшення їх надмірності. Алго-

ритм стиснення бере в якості входу текст джерела і виробляє відповідний йому стиснутий текст, в той час як зворотній алгоритм має на вході стиснутий текст і отримує з нього на виході початковий текст джерела. Більшість алгоритмів стиснення розглядають вихідний текст як набір рядків, що складаються з літер алфавіту вихідного тексту.

Питання економного кодування інформації в системах управління базами даних було поставлено в першій половині 1970-х років [312], але воно не втратило актуальності і до цього часу. Багато сучасних дослідників зазначають недостатню теоретичну опрацьованість проблеми і неефективність підтримки стиснення даних у промислових СУБД [289].

Застосування в СУБД економного кодування без втрат інформації призводить до ряду позитивних результатів. Найбільш очевидним ефектом є зменшення фізичного розміру бази даних, журнальних та архівних файлів. Але також часто досягається збільшення швидкості виконання запитів і зниження вимог до обсягу оперативної пам'яті, що відзначається практично у всіх роботах у цій галузі знань. Тому ефективна реалізація підтримки стиснення даних істотно покращує якість СУБД.

Інтерес до завдання стиснення даних у СУБД спочатку був обумовлений прагненням зменшити фізичний обсяг баз даних. Ціна підсистеми вводу-виводу становила основну частину вартості апаратури. Тому при належному інтегруванні в СУБД методів стиснення без втрат даних досягалася значна економія. Невелике збільшення числа використовуваних тактів процесора для кодування-декодування більш ніж компенсувалося зниженням витрат на підсистему введення-виведення. Цей результат застосування стиснення затребуваний і в даний час. Зменшення відносної вартості пристроїв зберігання інформації на кілька порядків супроводжувалося відповідним збільшенням розміру типових баз даних. Тим не менш, у даний час фокус інтересу все більше зміщується на збільшення продуктивності системи управління даними за рахунок використання стиснення.

Слід також зазначити, що економне кодування сприяє криптографічному захисту інформації. Усунення статистичної надмірності підвищує крипостійкість алгоритмів шифрування інформації і часто є попереднім етапом у схемах шифрування даних [321].

Використання стиснення даних у СУБД пов'язано з рішенням безлічі завдань. Будь-яка реалізація економного кодування в СУБД пов'язана з компромісом між ступенем стиснення, необхідним об'ємом

оперативної пам’яті, числом звернень до зовнішньої пам’яті та оперативної пам’яті, обчислювальними затратами.

Для застосування в СУБД потрібні специфічні методи і прийоми економного кодування, оскільки звичайні методи не задовольняють ряд вимог. Практична цінність реалізації досягається тільки при забезпеченні швидкого доступу до довільного запису або елемента даних. Затребувані так звані методи стиснення зі збереженням упорядкованості, що дозволяють виконувати операції порівняння без декодування даних [287; 292].

Проблема реалізації стиснення в СУБД має також такі аспекти, як оптимізація виконання запитів до стиснених даних, ефективне стиснення результатів виконання запитів, економне кодування метаданих, оцінювання доцільності стиснення окремих елементів, вибір алгоритму стиснення і його параметрів з урахуванням типових запитів і характеру даних.

Застосування економного кодування без втрат інформації є більш універсальним рішенням, ніж стиснення з втратами. Прийоми стиснення даних з втратами інформації (в першу чергу, мультимедійних даних) та способи їх використання в СУБД володіють істотною специфікою і потребують окремого розгляду.

Протягом більше двох десятків років реляційні СУБД (РСУБД) підтвердили свою життєздатність та ефективність. Реляційні системи можуть не без успіху замінювати спеціалізовані комплекси, наприклад, системи управління багатовимірними базами даних. Переважний сегмент ринку СУБД зайнятий РСУБД. Тому основна маса досліджень і розробок, які зачіпають питання підтримки економного кодування в СУБД, явним чи неявним чином орієнтовані на реляційні системи (РСУБД). Але багато методів стиснення та супутні прийоми обробки запитів застосовні до баз даних різних типів, наприклад, багатовимірних і об’єктних.

Серед РБД у даний час прийнято виділяти два великі класи [56]:

1. Бази даних для оперативної обробки транзакцій (OLTP) у реальному часі, що забезпечують збереження актуальних даних при роботі інформаційних систем.

2. Сховища даних (data warehouse), в яких накопичується в ретроспективі узгоджена інформація про деякі процеси з метою подальшого її використання в системах підтримки прийняття рішень (СППР) та аналізу (OLAP-системи).

Бази даних для OLTP відрізняються високим ступенем нормалізації даних, що значною мірою зменшує надмірність подання інформації та полегшує підтримку узгодженості. Як правило, промислова БД такого типу містить сотні і тисячі таблиць малого обсягу з невеликою кількістю атрибутів і має складну структуру.

Сховища даних, організовані як РБД, зазвичай мають просту денормалізовану структуру, що забезпечує високу швидкість виконання складних запитів, що вимагають агрегування даних і обчислення зведених характеристик. Типовою схемою сховища даних є так звана "зірка" (star schema), при якій вся збережена фактологічна інформація записується в одну велику таблицю фактів (fact table) [13]. Кожен рядок таблиці фактів відповідає точці в багатовимірному просторі, який визначається вимірами сховища даних. Вимірювання класифікує деякий факт (звичайно це число) і, як правило, має ієрархічну структуру. Типовими вимірами є час і територія. Для кожного виміру в таблиці фактів заводиться стовпець, в якому в закодованому вигляді записуються значення вимірювання для кожного рядка. З метою розшифрування закодованих значень для кожного вимірювання створюється окрема таблиця (dimension table). Таблиці зв’язуються на підставі закодованих значень вимірів так, що таблиця фактів стає центром "зірки", а таблиці вимірів – її променями. У загальному випадку сховище даних має кілька таблиць фактів і, отже, складається з кількох "зірок" [13].

Великі обсяги інформації, та вимоги до скорочення строків її надання споживачам, обумовлюють необхідність використання для її обробки та узагальнення сучасної електронної техніки та спеціальних алгоритмів обробки, серед яких гідне місце належить алгоритмам стиснення.

Методи стиснення даних можна розділити на два типи:

1) методи без спотворення (loseless) – методи стиснення (звані також методами стиснення без втрат) гарантують, що декодовані дані будуть в точності збігатися з вихідними;

2) методи з втратами (lossy) – методи стиснення (звані також методами стиснення з втратами) можуть спотворювати вихідні дані, наприклад за рахунок видалення несуттєвою частини даних, після чого повне відновлення неможливо [292].

Методи стиснення даних без втрат інформації засновані на усуненні надмірності подання інформації. Економне кодування досягається за рахунок подання малоймовірних подій більш довгими словами, чим подій

з високою ймовірністю настання. Якщо ймовірність настання події дорівнює P, то, відповідно до теореми Шеннона про кодування джерела інформації, така подія найвигідніше кодувати словом завдовжки – $log_2 P$ бітів. Методи стиснення даних явно або неявно спираються на цей факт [35; 398].

У результаті процесу економного кодування одиниці вихідних даних (символа, слова, рядка, числа тощо) ставиться у відповідність так зване кодове слово. Кодове слово складається з послідовності цифр, зазвичай двійкових. Сукупність усіх кодових слів утворює код. Якщо довжини всіх кодових слів однакові, то використовується код має фіксовану (постійну) довжину, інакше – змінну. Якщо вихідні дані можуть бути однозначно відновлені за масивом відповідних кодових слів, то кодування не призводить до втрати інформації.

Ефективність стиснення як характеристика скорочення розміру подання інформації щодо початкового визначається ступенем стиснення. Ступінь стиснення приймається рівним відношенню обсягу вихідних даних до обсягу відповідних їм стиснутих даних і вимірюється в разах.

Усі методи стиснення прийнято розділяти на два класи: методи статистичного кодування і методи словникового стиснення [12; 34]. У схемах стиснення часто використовуються допоміжні перетворення, що забезпечують або сприяють виконанню етапу економного кодування.

Статистичне кодування

Методи статистичного кодування явним чином спираються на теорему Шеннона. Такі методи включають в себе два етапи: оцінка ймовірності кодованих елементів (моделювання) і власне кодування. На етапі кодування виконується заміщення елемента s_i з оцінкою ймовірності появи $q(s_i)$ кодовим словом довжиною – $log_2 q(s_i)$ бітів. Цей етап ще інколи називається ентропійним кодуванням. Оцінки $q(s_i)$ можуть бути отримані з безумовних частот зустрічальності елементів, умовних частот, тобто з урахуванням контексту, складнішими способами. Відновлення даних без втрат забезпечується в тому випадку, коли кодер і декодер оперують одними і тими ж оцінками $q(s_i)$ в кожний момент часу.

Завдання кодування елемента з заданою вірогідністю традиційно вирішується за допомогою різновидів: методу Хаффмана і арифметичного стиснення [12].

Алгоритм Хаффмана визначає процедуру побудови коду змінної довжини, середня надмірність якого мінімальна для всіх неблочних кодів, тобто які задають відображення рівно одного вихідного елемента в одне кодове слово. Оскільки слово може бути представлено тільки цілим числом бітів, при кодуванні за Хаффманом здійснюється наближення $q(s_i)$ дробами, рівними ступеням двійки. Тому цей алгоритм незастосовний безпосередньо для економного кодування елементів бінарного алфавіту. Код Хаффмана є префіксним і тому зазвичай представляється у вигляді дерева. Традиційно використовується двопрохідна схема (статистичний алгоритм Хаффмана): при першому перегляді даних підраховується статистика зустрічальності елементів, тобто будується модель даних, на підставі якої формується код; при другому перегляді дані стискаються за допомогою отриманого коду. Оцінки ймовірності $q(s_i)$ при кодуванні незмінні, і код не змінюється. Також існує адаптивний однопрохідний варіант алгоритму, але він володіє суттєво більшою обчислювальною складністю і на практиці не використовується.

Арифметичне стиснення, або арифметичне кодування, дозволяє при кодуванні декількох елементів представляти кожен елемент у середньому дробовим числом бітів. Тому зазвичай арифметичне стиснення забезпечує більший ступінь стиснення, ніж кодування за Хаффманом. Блок кодованих елементів подається дробом, який визначається добутком оцінок ймовірності $q(s_i)$ всіх елементів блоку. Це і визначило назву методу. Чим $q(s_i)$ менше, тим довше дріб, і потрібно більше двійкових символів для його подання. Алгоритм декодування складніший, ніж для методу Хаффмана, але дозволяє відновити вихідні дані без втрат. Арифметичне кодування не вимагає явної перебудови коду при зміні оцінювання ймовірності, тому зазвичай використовується адаптивна однопрохідна схема, що дозволяє природним чином враховувати локальні особливості даних.

Словникове стиснення

Ідея словникового стиснення полягає в заміні послідовностей елементів вихідних даних на ідентифікатори таких фраз деякого словника, які збігаються з послідовністю, що замінюється. Методи словникового стиснення експлуатують факт повторюваності рядків символів. Серед словникових схем найбільше поширення одержали методи Зіва-Лемпеля.

Словникові методи, що входять до цього класу, можна розділити на два сімейства: LZ77 (LZ1) і LZ78 (LZ2). Схеми сімейства LZ77 базуються на однойменному методі, запропонованому в 1977 році в статті "Універсальний алгоритм для послідовного стиснення даних" [216; 341; 342]. У методах цього сімейства роль словника відіграє порція вже оброблених даних. Послідовність зазвичай кодується зазначенням позиції початку еквівалентної фрази в словнику (зсуву) і довжини збігу. Пара <зсув, довжина збігу> в цьому випадку є покажчиком. Якщо елемент, що кодується відсутній в словнику, то він певним чином позначається і подається як є. Такий елемент називається літералом. Зі способу формування словника випливає, що методи сімейства LZ77 є адаптивними.

На практиці схеми типу LZ77 використовуються спільно з алгоритмами статистичного кодування покажчиків і літералів. Наприклад, у методі LZH для економного кодування покажчиків і літералів використовується алгоритм Хаффмана.

У схемах сімейства LZ78 у словник включаються не всі послідовності, які зустрічаються в обробленому масиві даних, а лише "перспективні" з точки зору ймовірності появи в майбутньому. Наприклад, в методі LZ78 нова фраза формується як зчеплення (конкатенація) однієї з фраз S словника, що має найдовший збіг з поточною кодованої послідовністю S', і символу **s**. Символ s є символом, наступним за послідовністю S'=S. На відміну від сімейства LZ77, у словнику не може бути однакових фраз. У найвідомішого представника сімейства LZ78, методі LZW, словник ініціалізується фразами для всіх символів алфавіту кодованих даних. Покажчики фраз кодуються словами фіксованої довжини, що визначається розміром словника. У рамках методу сімейства LZ78 нескладно реалізувати ефективне неадаптивне і напівадаптивне стиснення, при якому словник будується заздалегідь [280; 397].

Словник, який використовується в словникових методах стиснення, можна розглядати як аналог статистичної моделі даних, що застосовується у статистичних методах.

Інші методи стиснення

Поширеним методом стиснення є кодування довжин серій (Run Length Encoding, RLE). Цей метод дозволяє кодувати послідовності однакових елементів. Існує велика кількість різновидів кодування довжин серій. На-

приклад, послідовність ідентичних елементів може подаватися трійкою "прапор використання кодування, довжина серії, повторюваний елемент" [34].

Для кодування цілих чисел з невідомим, але монотонно убуваючим розподілом вірогідностей використовуються так звані універсальні коди. Надмірність універсальних кодів цілих чисел для будь-якого конкретного розподілу і будь-якого кодованого числа n є обмеженою зверху, якщо виконується умова $p(n) \geq p(n+1)$. Універсальними є, наприклад, коди Елайеса [35; 251; 397].

Характеристика сучасних алгоритмів стиснення інформації

Алгоритм LZ77

Цей словниковий алгоритм стиснення є найстарішим серед методів LZ. Опис було опубліковано в 1977 році, але сам алгоритм розроблений не пізніше 1975.

Алгоритм LZ77 є родоначальником цілого сімейства словникових схем – так званих алгоритмів з ковзаючим словником або ковзаючим вікном. Дійсно, в LZ77 як словника використовується блок уже закодованої послідовності. Як правило, у міру виконання обробки положення цього блоку щодо початку послідовності постійно змінюється, словник "ковзає" по вхідному потоку даних.

У 1977 два дослідники з Ізраїлю запропонували абсолютно інший підхід до цієї проблеми. Абрам Лемпель і Якоб Зів висунули ідею формування "словника" загальних послідовностей даних.

Завдяки цьому принципу алгоритми LZ іноді називаються методами стиснення з використанням ковзного вікна. Ковзне вікно можна уявити у вигляді буфера (або більш складної динамічної структури даних), який організований так, щоб запам’ятовувати проаналізовану раніше інформацію і надавати до неї доступ. Таким чином, сам процес стискання згідно з LZ77 нагадує написання програми, команди якої дозволяють звертатися до елементів "ковзаючого вікна", і замість значень стисливою послідовності вставляти посилання на ці значення в "ковзному вікні". Розмір ковзаючого вікна може динамічно змінюватися і зазвичай має розмір кратний 2 кілобайтам. Слід також зазначити, що розмір вікна кодувальника може бути менше або дорівнювати розмірам вікна декодувальника, але не навпаки [342].

Метод кодування згідно з принципом ковзаючого вікна враховує інформацію, яка вже раніше зустрічалося, тобто інформацію, яка вже відома для кодувальника і декодувальника (друге і наступні входження деяких рядків символів у повідомленні замінюються посиланнями на її перше входження).

До недоліків цього методу можна віднести:

- довжина підрядка, яку можна закодувати, обмежена розміром буфера;
- мала ефективність при кодуванні незначного обсягу даних.

Алгоритм Шеннона – Фано

Алгоритм Шеннона – Фано – це один із перших алгоритмів стиснення, який сформулювали американські вчені Шеннон та Фано. Цей метод стиснення має велику схожість з алгоритмом Хаффмана, який з'явився на кілька років пізніше. Алгоритм використовує коди змінної довжини: символ, який часто зустрічається кодується кодом меншої довжини, а той, який рідко зустрічається – кодом більшої довжини. Коди Шеннона – Фано – префіксні, тобто ніяке кодове слово не є префіксом будь-якого іншого. Ця властивість дозволяє однозначно декодувати послідовність кодових слів.

Подібно алгоритму Хаффмана, алгоритм Шеннона – Фано використовує надмірність повідомлення, укладену в неоднорідному розподілі частот символів його алфавіту, тобто замінює коди частіших символів короткими двійковими послідовностями, а коди більш рідкісних символів – довшими двійковими послідовностями.

Код Шеннона – Фано будується за допомогою дерева, як і в алгоритмі Хаффмана. Побудова цього дерева починається від кореня. Уся множина кодованих елементів відповідає кореню дерева (вершині першого рівня). Вона розбивається на дві підмножини з приблизно однаковими сумарними ймовірностями. Ці підмножини відповідають двом вершинам другого рівня, які з'єднуються з коренем. Далі кожна з цих підмножин розбивається на дві підмножини з приблизно однаковими сумарними ймовірностями. Їм відповідають вершини третього рівня. Якщо підмножина містить єдиний елемент, то йому відповідає кінцева вершина кодового дерева. Така підмножина розбиттю не підлягає. Подібним чином діємо до тих пір, поки не отримаємо всі кінцеві вершини. Гілки кодового дерева розмічаються символами 1 і 0, як у випадку коду Хаффмана.

Кодування Шеннона – Фано є досить старим методом стиснення, і на сьогоднішній день не становить особливого практичного інтересу. У більшості випадків, довжина послідовності, отримана за цим методом, дорівнює довжині послідовності з використанням кодування Хаффмана. Але на деяких послідовностях можуть сформуватися неоптимальні коди Шеннона – Фано, тому більш ефективним вважається стиснення методом Хаффмана.

Алгоритм Хаффмана

Алгоритм Хаффмана є адаптивним алгоритмом оптимального префіксного кодування алфавіту з мінімальною надмірністю. Був розроблений в 1952 році аспірантом Массачусетського технологічного інституту Девідом Хаффманом при написанні ним курсової роботи. У цей час використовується в багатьох програмах стиснення даних.

Цей метод кодування складається з двох основних етапів:

1. Побудова оптимального кодового дерева.

2. Побудова відображення код-символ на основі побудованого дерева.

Ідея алгоритму полягає в такому: знаючи ймовірності символів у повідомленні, можна описати процедуру побудови кодів змінної довжини, що складаються з цілої кількості бітів. Символам з більшою ймовірністю ставляться у відповідність коротші коди. Як вже вказувалося, коди Хаффмана мають властивість префіксності.

Класичний алгоритм Хаффмана на вході отримує таблицю частот зустрічальності символів у повідомленні. Далі на підставі цієї таблиці будується дерево кодування Хаффмана (Н-дерево) [300].

1. Символи вхідного алфавіту утворюють список вільних вузлів. Кожен лист має вагу, яка може дорівнювати або ймовірності, або кількістю входжень символу в повідомлення, що стискається.

2. Вибираються два вільних вузла дерева з найменшими вагами.

3. Створюється їх батько з вагою, рівною їх сумарній вазі.

4. Батько додається до списку вільних вузлів, а два його нащадки видаляються з цього списку.

5. Одній дузі, котра виходить з батьківського вузла, ставиться у відповідність біт 1, інший – біт 0.

6. Кроки, починаючи з другого, повторюються до тих пір, поки в списку вільних вузлів не залишиться тільки один вільний вузол. Він і буде вважатися коренем дерева.

Класичний алгоритм Хаффмана має ряд істотних недоліків [115]. По-перше, для відновлення вмісту стиснутого повідомлення декодер повинен знати таблицю частот, якою користувався кодер. Отже, довжина стиснутого повідомлення збільшується на довжину таблиці частот, яка повинна надсилатися попереду даних, що може перекреслити всі зусилля зі стиснення повідомлення. Крім того, необхідність наявності повної частотної статистики перед початком власне кодування потребує двох проходів за повідомленням: одного для побудови моделі повідомлення (таблиці частот і Н-дерева), іншого для кодування.

Алгоритм стиснення PPM

PPM (Prediction by Partial Matching – пророкування за частковим співпаданням) – адаптивний статистичний алгоритм стиснення даних без втрат, заснований на контекстному моделюванні і пророкуванні. Модель PPM використовує контекст – безліч символів у стислому потоці, що передують даному, щоб передбачати значення символу на основі статистичних даних. Сама модель PPM лише пророкує значення символу, безпосереднє стиснення здійснюється алгоритмом Хаффмана і арифметичним кодуванням [35].

Довжина контексту, який використовується при прогнозі зазвичай сильно обмежена. Ця довжина позначається n і визначає порядок моделі PPM, що позначається як PPM(n). Необмежені моделі так само існують і позначаються просто PPM*. Якщо пророцтво символу по контексту з n символів не може бути зроблено, то відбувається спроба передбачити його за допомогою n-1 символів. Рекурсивний перехід до моделей з меншим порядком відбувається поки пророкування не відбудеться в одній з моделей, або коли контекст стане нульової довжини (n = 0).

Велике значення для алгоритму PPM має проблема обробки нових символів, ще не зустрічалися у вхідному потоці. Це проблема носить назву "Нульової частоти". Деякі варіанти реалізацій PPM вважають лічильник нового символу рівним фіксованій величині, наприклад, одиниці. Опубліковані дослідження алгоритмів сімейства PPM з’явилися в середині 1980-х років. Програмні реалізації не були популярні до 1990-х років, бо моделі PPM вимагають значну кількість оперативної пам’яті. Сучасні реалізації PPM є кращими серед алгоритмів стиснення без втрат для текстів [215].

Варіанти алгоритму PPM на цей момент широко використовуються і головним чином для компресії надлишкової інформації і текстових даних. Відомі реалізації алгоритму PPM: RAR; 7-Zip; WinZip.

Алгоритм RLE

Алгоритм RLE (Run-length encoding – кодування повторів або довжин серій) – це простий алгоритм стиснення даних, який оперує серіями даних, тобто послідовностями, в яких один і той же символ зустрічається кілька разів підряд. При кодуванні рядок однакових символів, що складають серію, замінюється рядком, який містить сам повторюється символ і кількість його повторів. Алгоритм RLE буде давати кращий ефект стиснення при більшій довжині повторюваної послідовності даних.

Програмні реалізації алгоритмів RLE відрізняються простотою, високою швидкістю роботи, але в середньому забезпечують недостатнє стиснення. Найкращими об'єктами для даного алгоритму є прості графічні файли, в яких великі одноколірні ділянки зображення кодуються довгими послідовностями однакових байтів. Однак це кодування погано підходить для зображень з плавним переходом тонів, таких, як фотографії. Цей метод також може давати помітний виграш на деяких типах файлів баз даних, що мають таблиці з фіксованою довжиною полів. Для текстових даних методи RLE, як правило, неефективні [35; 215].

Методом кодування довжин серій можуть бути стиснуті довільні файли з двійковими даними, оскільки специфікації на формати файлів часто включають в себе повторювані байти в області вирівнювання даних. Проте, сучасні системи стиснення частіше використовують алгоритми на основі LZ77, які є узагальненням методу кодування довжин серій.

Звукові дані, які мають довгі послідовні серії байт (такі, як низькоякісні звукові семпли) можуть бути стиснуті за допомогою RLE.

До позитивних сторін алгоритму можна віднести те, що він не вимагає додаткової пам'яті при роботі, і швидко виконується. Алгоритм застосовується, наприклад, у графічних форматах PCX та TIFF.

У табл. 6.1 наведено стисле порівняння найбільш поширених алгоритмів стиснення даних.

Таблиця 6.1

Порівняльна таблиця алгоритмів стиснення

Алгоритм	Ступінь стиснення	Стиснення без втрат	Кількість проходів	Використання	Класифікація
Хаффман статичний	5 – 6	Так	2	Стиснення текстів, бінарної інформації та ін.	Неблоковий, статистичний
Хаффман адаптивний	4 – 5	Так	1	Стиснення текстів, бінарної інформації та ін.	Неблоковий, статистичний
LZ77	9 – 10	Так	1	Універсальний	Блоковий
LZ88	6 – 7	Так	1	Універсальний, частіше тексти, зображення	Блоковий
PPM	10 – 12	Так	1	Універсальний стиснення даних з великою надлишковістю	Адаптивний, статистичний
RLE	2 – 6	Так	1	Стиснення зображень, аудіо	Блоковий, статистичний

Таким чином, можна зробити висновок, що найбільш ефективним методом стиснення даних є метод PPM, але інші методи також мають право на існування, бо вони дуже часто використовуються в інших алгоритмах в якості додаткового етапу для покращення результату.

6.2. Розробка блоково-статистичного алгоритму стиснення інформації

Констатується, що застосування алгоритмів стиснення у базах даних, особливо для зменшення об'єму текстових полів, має певні особливості і зазвичай базується на алгоритмі Хаффмана.

Запропоновано модифікацію алгоритму Хаффмана – блоково-статистичний алгоритм і теоретично обґрунтовано його ефективність порівняно з класичним алгоритмом.

Особливий інтерес викликає застосування методів стиснення у базах даних для зменшення об'єму текстових полів. По-перше, для таких даних неприпустимо використання алгоритмів безповоротного стиснення, а по-друге, застосування алгоритмів, закладених у широко відомих архіваторах, наприклад, RAR або ZIP, є неефективним з причини того, що стисненню піддаються текстові поля невеликого об'єму і в цьому

випадку отриманий при стисненні результат, з урахуванням даних для декодування, може займати об’єм пам’яті більший, ніж початкові дані [215; 216]. Найбільш часто, в таких випадках, застосовується метод Хаффмана [215; 397].

Код Хаффмана (Huffman code) – це мінімально-надлишковий префіксний код (minimum-redundancy prefix code). Розглянемо більш докладно основні ідеї кодування за Хаффманом та дослідимо ряд важливих властивостей алгоритму.

Основною ідеєю алгоритму Хаффмана є те, що можна кодувати всі символи різним числом біт. Символи, які зустрічаються частіше, будуть закодовані меншим числом біт, ніж ті, які зустрічаються рідше. Отриманий код буде оптимальний або, іншими словами, мінімально-надлишковий [12].

Алгоритм Хаффмана двопрохідний. На першому проході будується частотний словник і генеруються коди. На другому проході відбувається безпосередньо кодування.

За 60 років з дня опублікування код Хаффмана нітрохи не втратив своєї актуальності і значущості. Так, з упевненістю можна сказати, що доводиться стикатися з ним в тій чи іншій формі (справа в тому, що код Хаффмана рідко використовується окремо, частіше працюючи у зв’язці з іншими алгоритмами), практично кожен раз, коли архівуємо файли, дивимося фотографії, фільми, посилаємо факс або слухаємо музику.

Стискаючи файл за алгоритмом Хаффмана перше, що необхідно зробити – це прочитати файл повністю і підрахувати, скільки разів зустрічається кожен символ з розширеного набору ASCII. Якщо врахувати всі 256 символів, то для нас не буде різниці в стисненні текстового і EXE файла.

Після підрахунку частоти входження кожного символу необхідно переглянути таблицю кодів ASCII і сформувати уявне розташування кодів за убуванням їх частоти. Тобто, не міняючи місцезнаходження кожного символу з таблиці в пам’яті, відсортувати таблицю посилань на них. Кожне посилання з останньої таблиці назвемо "вузлом". Надалі (у дереві) будемо пізніше розміщувати покажчики, які будуть вказувати на цей "вузол". Для наочності розглянемо приклад.

Нехає є файл довжиною 100 байт, який складається з 6 різних символів. Розглянемо приклад для частот символів з табл. 6.2.

Таблиця 6.2

Таблиця з частотами символів

Символ	A	B	C	D	E	F
Число входжень	10	20	30	5	25	10

Далі необхідно відсортувати символи за спаданням їх частоти. Результат операції наведений в табл. 6.3.

Таблиця 6.3

Впорядковані частоти символів

Символ	C	E	B	F	A	D
Число входжень	30	25	20	10	10	5

Візьмемо з останньої таблиці два символи з найменшою частотою. У цьому випадку – це D (5) і який-небудь символ з F або A (10), можна взяти будь-який з них наприклад A.

Сформуємо з "вузлів" D і A новий "вузол", частота входження для якого буде дорівнювати сумі частот D і A. Отриманий результат зображений на рис. 6.1.

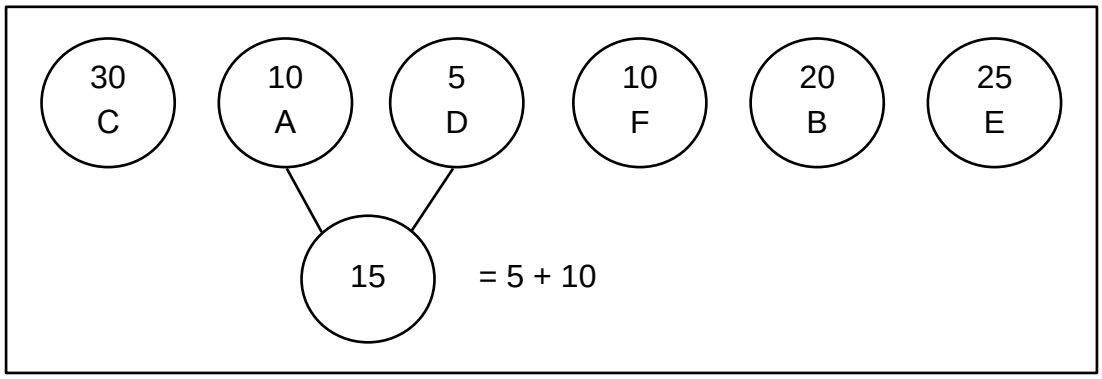


Рис. 6.1. **Результат першого кроку**

Цифра 15 – сума частот символів D і A. Тепер знову шукаємо два символи з найнижчими частотами входження. Виключаючи з перегляду

D і A, і розглядаючи замість них новий "вузол" з сумарною частотою входження 15. Найменша частота тепер у F і нового "вузла". Знову зробимо операцію злиття вузлів. Результат операції зображений на рис. 6.2.

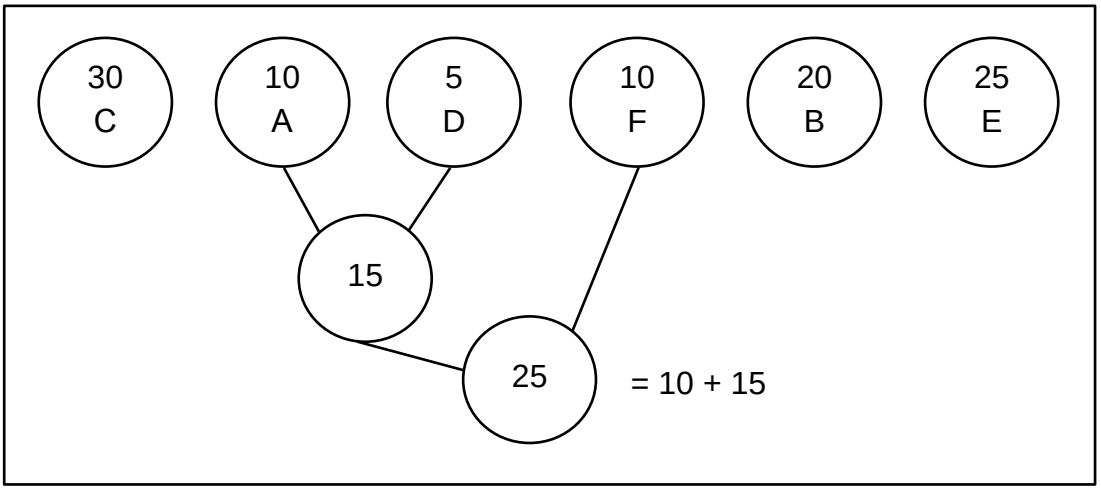


Рис. 6.2. **Результат другого кроку**

Розглядаємо таблицю знову для наступних двох символів (B і E). Алгоритм виконується до тих пір, поки все "дерево" не сформоване, тобто поки все не зведеться до одного вузла. Результат побудови дерева зображений на рис. 6.3.

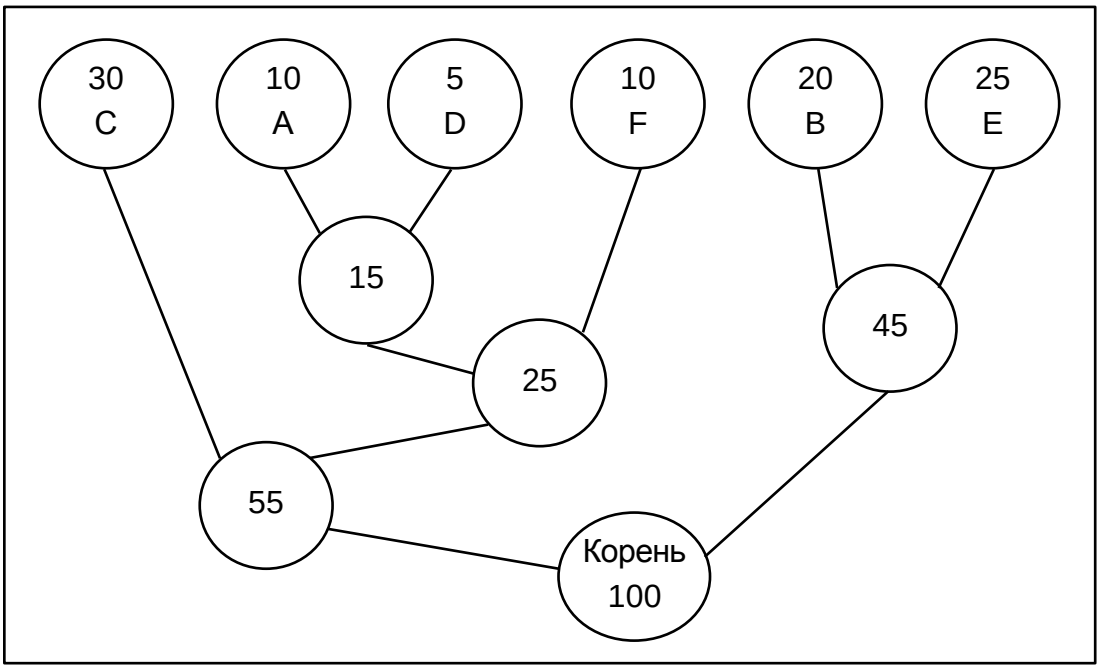


Рис. 6.3. **Результат побудови бінарного дерева**

Тепер, коли дерево створене, можна кодувати файл. Процес кодування завжди починається з кореня. Кодуючи перший символ (лист дерева С), простежуємо вгору по дереву всі повороти гілок і якщо робимо поворот ліворуч, то запам'ятовуємо 0-й біт, і аналогічно 1-й біт для повороту праворуч. Так, для символу С, йдемо ліворуч до 55 (і запам'ятаємо 0), потім знову ліворуч (0) до самого символу. Код Хаффмана для нашого символу С – 00. Для наступного символу (А) виходить – ліворуч, праворуч, ліворуч, ліворуч, що виливається в послідовність 0100. Виконавши сказане для всіх символів, отримаємо такі кодові послідовності:

С = 00 (2 біта);

А = 0100 (4 біта);

D = 0101 (4 біта);

F = 011 (3 біта);

В = 10 (2 біта);

Е = 11 (2 біта).

Кожен символ спочатку подавався 8-ма бітами (один байт), а оскільки число бітів, необхідних для подання кожного символу, було зменшено, то відповідно зменшиться і розмір вихідного файла. Результати стиснення відображені в підсумковій табл. 6.4.

Таблиця 6.4

Результат стиснення символів

Частота	До	Після	Зменшення на
С 30	30·8=240	30·2=60	180
А 10	10·8=80	10·3=30	50
D 5	5·8=40	5·4=20	20
F 10	10·8=80	10·4=40	40
В 20	20·8=160	20·2=40	120
Е 25	25·8=200	25·2=50	150

Початковий розмір файла: 100 байт – 800 біт.

Розмір стисненого файла: 30 байт – 240 біт.

У результаті проведених операцій розмір файла зменшився на 70 відсотків.

Усе це досить добре, але існує негативний момент, який полягає у тому, що для відновлення первісного файла, необхідно мати дерево для декодування, оскільки дерева будуть різні для різних файлів. Отже, необхідно зберігати дерево разом з файлом. Це перетворюється в підсумку у збільшення розмірів вихідного файла [35; 215; 216].

У розглянутому прикладі стиснення в кожному вузлі знаходяться 4 байти покажчика, з цього, повна таблиця для 256 байт буде мати розмір приблизно 1 Кбайт.

Таблиця в даному прикладі має 5 вузлів плюс 6 вершин (де і знаходяться символи), всього 11. У результаті обсяг даних буде складати $4 \cdot 11 = 44$ байти. Якщо ж додати ще невелику кількість байтів для збереження місця вузла і деяку іншу статистику – таблиця буде приблизно мати розмір 50 байтів.

Додавши до 30 байтів стисненої інформації, 50 байтів таблиці отримуємо, що загальна довжина архівного файла зросте до 80 байт. Ураховуючи, що первісна довжина файла в розглянутому прикладі була 100 байт – отримали 20 % стиснення інформації.

Як вже зазначалося, для того, щоб закодоване повідомлення вдалося декодувати, декодеру необхідно мати таке ж кодове дерево (в тій чи іншій формі), яке використовувалося при кодуванні. Тому разом з закодованими даними зазвичай зберігається й відповідне кодове дерево. Звісно, що чим компактніше воно буде, тим краще.

Вирішити це завдання можна декількома способами. Найочевидніше рішення – зберегти дерево в явному вигляді (тобто як упорядковану безліч вузлів і покажчиків того чи іншого виду). Це мабуть найнемарнотратніший і найнеефективніший спосіб. На практиці він не використовується [35; 215; 216].

Можна зберегти список частот символів (тобто частотний словник). З його допомогою декодер без зусиль зможе реконструювати кодове дерево. Хоча цей спосіб і менш марнотратний ніж попередній, він не є найкращим.

Нарешті, можна використовувати одне із властивостей канонічних кодів [354]. Канонічні коди цілком визначаються своїми довжинами. Іншими словами, все що необхідно декодеру – це список довжин кодів

символів. Враховуючи, що в середньому довжину одного коду для N-символьного алфавіту можна закодувати $[log_2(log_2 N)]$ бітами, отримаємо дуже ефективний алгоритм [371].

Припустимо, що розмір алфавіту N = 256, і необхідно піддати стисненню звичайний текстовий файл (ASCII). Швидше за все у файлі не зустрінуться усі N символів нашого алфавіту в такому файлі. Покладемо тоді довжину коду відсутніх символів рівною нулю. У цьому випадку список довжин кодів, що зберігається, буде містити досить велике число нулів (довжин кодів відсутніх символів) згрупованих разом. Кожну таку групу можна стиснути за допомогою так званого групового кодування – RLE (Run – Length – Encoding). Цей алгоритм надзвичайно простий. Замість послідовності з M однакових елементів що йдуть підряд, будемо зберігати перший елемент цієї послідовності і число його повторень, тобто (M-1). Приклад: RLE ("AAAABBBCDDDDDDD") = = A3 B2 C0 D6.

Більш того, цей метод можна дещо розширити, оскільки можна застосувати алгоритм RLE не тільки до груп нульових довжин, а й до всіх інших. Такий спосіб передачі кодового дерева є загальноприйнятим і застосовується в більшості сучасних реалізацій.

Алгоритм класичного кодування за Хаффманом наведений на рис. 6.4. Виникає питання, чи не можна зменшити середню довжину коду, розбивши увесь вхідний алфавіт на дві або більше груп і провівши кодування за Хаффманом для кожної з них окремо? Звісно в цьому випадку у вхідному алфавіті з’являються нові символи, що характеризують перехід до тієї або іншої групи, але довжина коду у кожній окремій групі може бути зменшена. Був проведений експеримент, який для вхідного алфавіту з 80 символів визначив середню довжину коду символу для алгоритму Хаффмана, при розподілі частот символів, що підкоряються закону Ципфа [325].

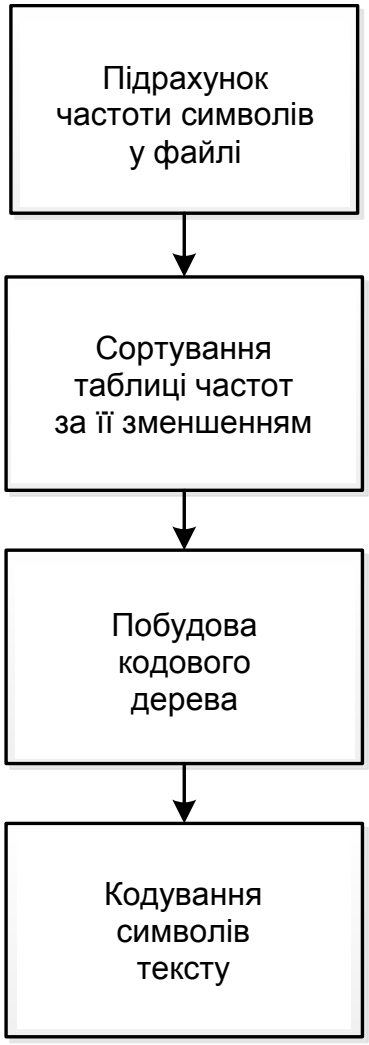


Рис. 6.4. **Блок схема класичного алгоритму Хаффмана**

Далі початковий алфавіт був розбитий на дві рівні за кількістю символів групи. Сумарна імовірність символів у кожній групі при цьому склала: $P_1 = 0{,}862$ і $P_2 = 0{,}138$. Вірогідність переходів з групи в групу при цьому дорівнює $P_{12} = P_{21} = P_1 \cdot P_2 = 0{,}119$. Далі символи в кожній групі були окремо піддані стисненню за методом Хаффмана. Блок-схема модифікованого алгоритму, назвемо його блоково-статистичним алгоритмом стиснення (БСАС), зображена на рис. 6.5.

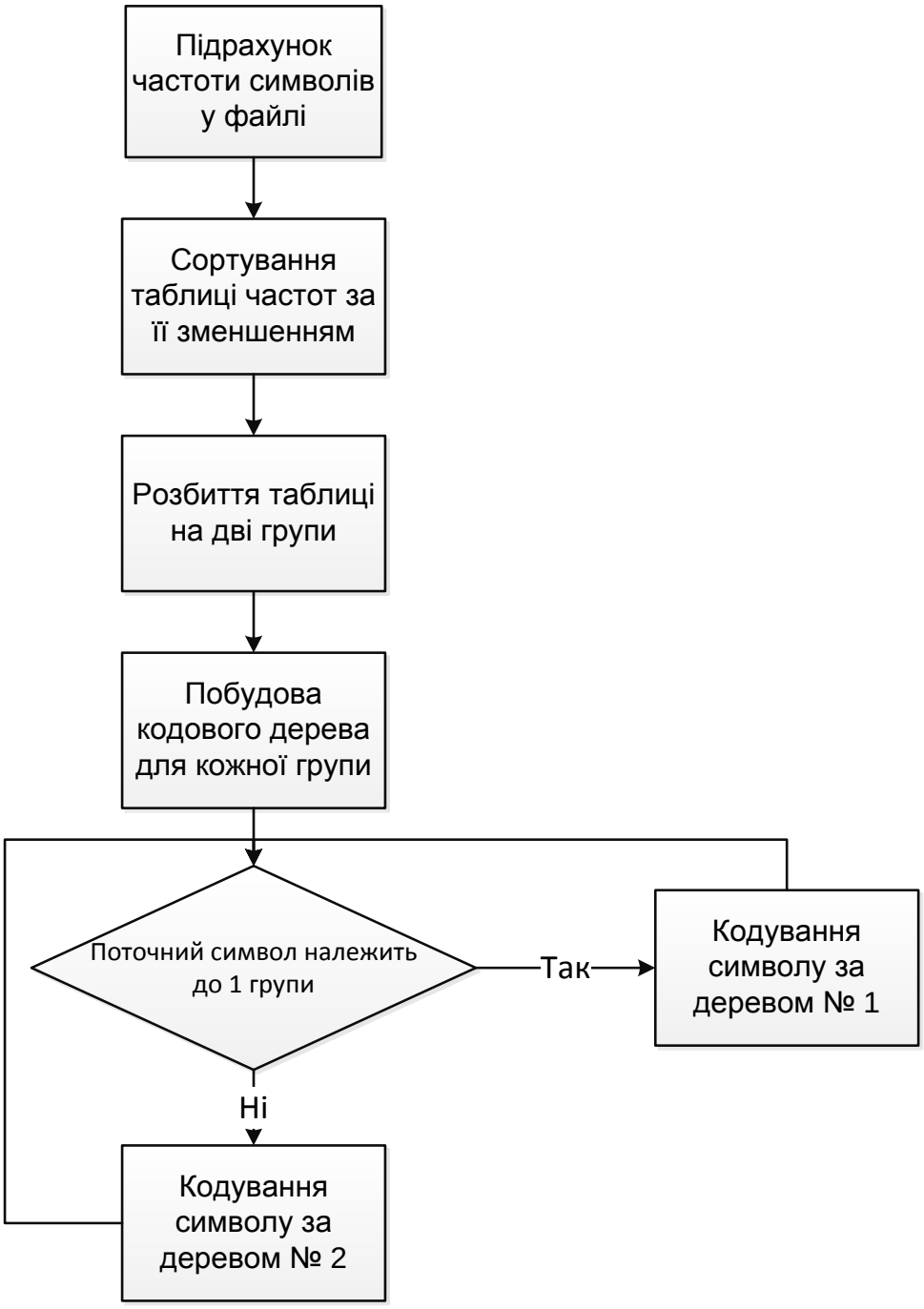


Рис. 6.5. **Блок-схема модифікованого алгоритму**

Результати теоретичних розрахунків наведені в табл. 6.5.

Таблиця 6.5

Результати розрахунку середньої довжини коду

Для усього тексту	Для блоку № 1 (P_1=0,862)	Для блоку № 2 (P_2=0,138)
4,91	4,36	3,49
	Середня довжина = 4,24	

Однак для підтвердження ефективності запропонованого алгоритму необхідно було провести певні експерименти. Для цього була розроблена спеціальна програма на мові C#, яка отримує на вхід текстовий файл, проводить кодування за класичним алгоритмом Хаффмана (будує кодове дерево та кодує кожен символ) та за його модифікацією (розбиває таблицю символів та їх частот на дві групи, будує кодове дерево для кожної з них та кодує символи за допомогою них), підраховує розмір стиснених даних за оригінальним алгоритмом та модифікацією [237].

Основними складовими програми є класи CalcTransitions.cs, SizeComparisonManager.cs, StatisticsCalculation.cs, HuffmanTree.cs та Node.cs.

Клас CalcTransitions.cs використовується для підрахунку кількості переключень між двома кодовими деревами в процесі кодування вхідного тексту.

Клас SizeComparisonManager.cs підраховує розмір даних, що були стиснуті за допомогою оригінального та модифікованого алгоритмів.

Клас StatisticsCalculation.cs використовується для підрахунку, побудови таблиці частот символів, та її сортування.

Клас HuffmanTree.cs використовується в якості представлення бінарного дерева та для кодування символів.

Клас Node.cs є об’єктом, котрий є вузлом дерева.

Діаграма основних класів наведена на рис. 6.6.

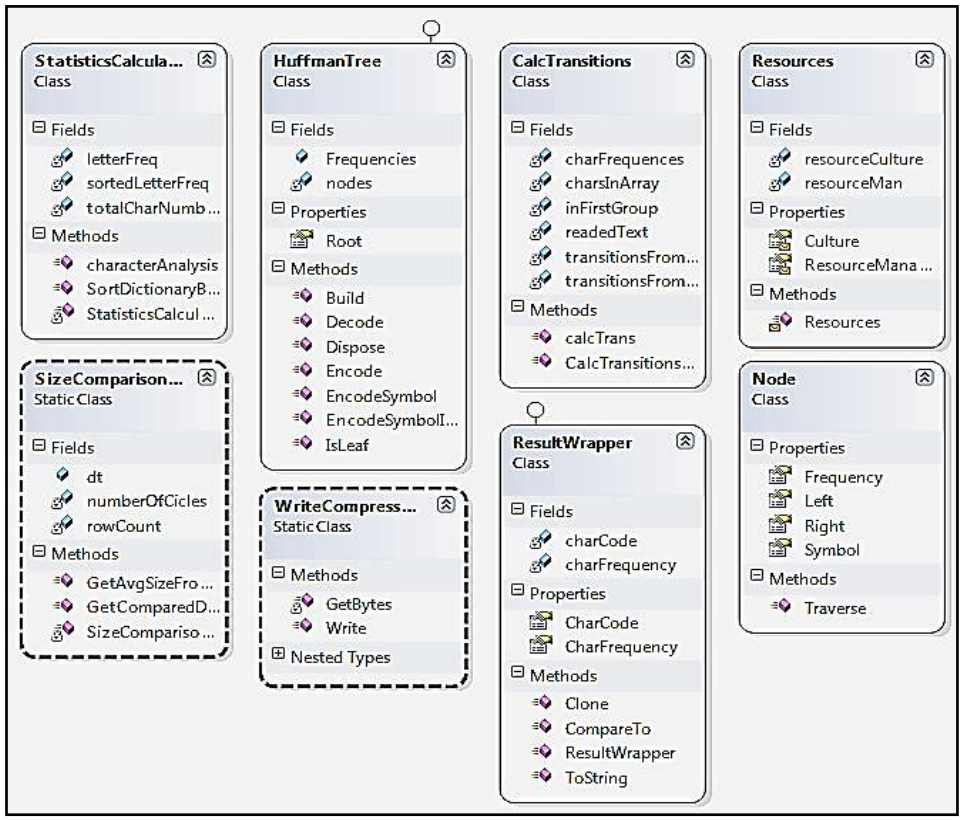


Рис. 6.6. **Діаграма основних класів розробленої програми**

6.3. Експериментальне дослідження ефективності блоково-статистичного алгоритму стиснення інформації

Проведено експериментальне дослідження ефективності блоково-статистичного алгоритму стиснення інформації.

На основі даних різного об'єму, що підкоряються різноманітним законам розподілу частоти зустрічальності символів, проведено порівняльний аналіз запропонованого блоково-статистичного алгоритму та класичного алгоритму Хаффмана. Стверджується, що ефективність стиснення запропонованого блоково-статистичного методу вище за класичний алгоритм, та досягає свого максимуму при розподілі вхідного алфавіту на дві рівні за сумарною частотою символів групи.

При дослідженні технічних систем можуть використовуватися теоретичні та емпіричні методи досліджень. Кожен з цих напрямів має відносну самостійність, свої переваги і недоліки. Іншими словами, теоретичні та експериментальні дослідження доповнюють один одного і є складовими елементами процесу пізнання навколишнього світу.

Як правило, результати експериментальних досліджень потребують певної математичної обробки. У цей час процедура обробки експериментальних даних досить добре формалізована і досліднику необхідно тільки її правильно використовувати. Коло питань, що вирішуються при обробці результатів експерименту, не таке вже й велике. Це питання підбору емпіричних формул і оцінювання їх параметрів, питання оцінки істинних значень вимірюваних величин та точності вимірювань, питання дослідження кореляційних залежностей та деякі інші.

Метою будь-якого експерименту є визначення якісної та кількісної міри зв'язку між досліджуваними параметрами або оцінювання чисельного значення якого-небудь параметра.

У випадку оцінки ефективності застосування блоково-статистичного методу метою є порівняння ступеня стиснення класичного алгоритму Хаффмана та блоково-статистичного на різних вхідних даних, для яких розподіл частот зустрічаємості символів підкоряється різним законам.

У деяких випадках вид залежності між змінними величинами відомий за результатами теоретичних досліджень. Як правило, формули, які виражають ці залежності, містять деякі параметри, значення яких і необхідно визначити.

Для отримання оптимального результату були проведені експерименти з розбиттям таблиці частот символів на групи різні за розміра-

ми. На першому кроці до першої групи були віднесені 5 % символів, котрі містяться в вхідному тексті, до другої – 95 %. На кожному наступному кроці кількість символів для першої групи збільшувалась на 5 %, а для другої – зменшувалась на 5 %.

Моделювання було проведено за допомогою розробленої програми.

Для проведення експериментів використовувалися дані п’яти типів.

На першому етапі були використані згенеровані дані, в яких символи розташовані за спаданням їх частоти, а самі частоти підкоряються закону Ципфа.

На другому етапі були використані згенеровані дані, в яких розподіл символів також підкоряється закону Ципфа, але розташовані вони були у довільному порядку.

На третьому етапі були використані згенеровані дані, в яких частота символів підкоряється нормальному закону розподілення.

На четвертому етапі були використані згенеровані дані, в яких частота символів підкоряється експоненціальному закону розподілення.

П’ятий етап експерименту включав дослідження ефективності модифікації алгоритму порівняно з класичним на даних, котрі були отримані з реальних баз даних.

6.3.1. Порядок проведення експерименту

Для проведення експерименту необхідно запустити програму (рис. 6.7) та вибрати файл для стиснення.

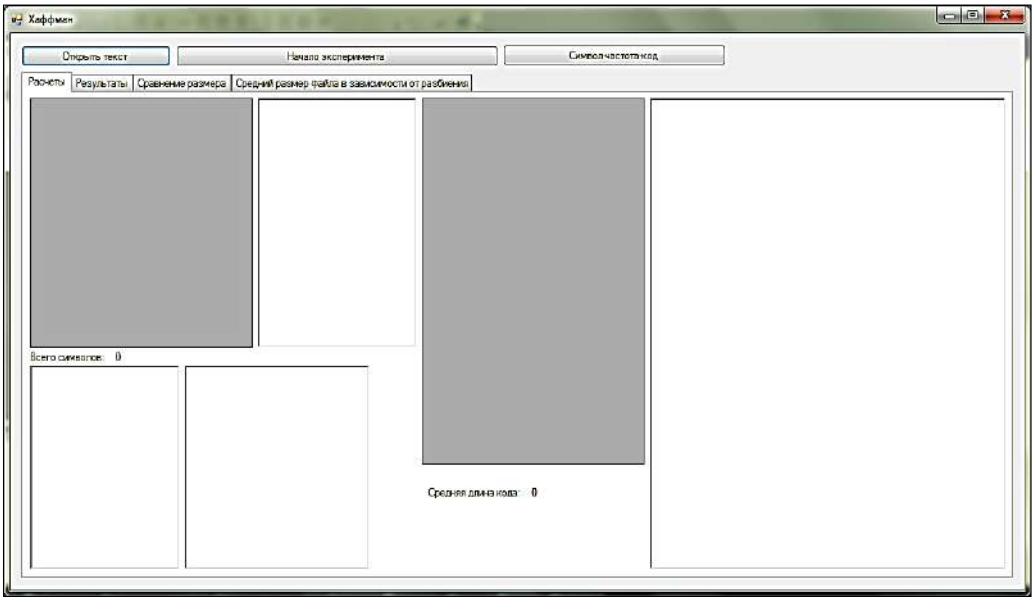


Рис. 6.7. **Графічний інтерфейс розробленого додатка**

Для відкриття файла з даними необхідно натиснути на кнопку "Открыть текст". Після цього з’явиться вікно вибору файла, яке зображено на рис. 6.8.

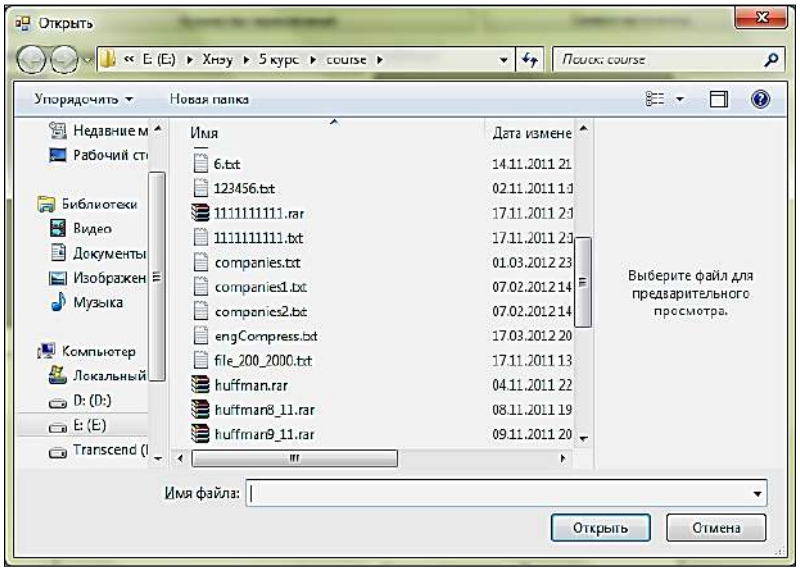


Рис. 6.8. **Вікно вибору файла**

Після того, як користувач підтвердить вибір файла, програма автоматично підрахує кількість різних символів та їх частоту у файлі. Результати підрахунку зображені на рис. 6.9.

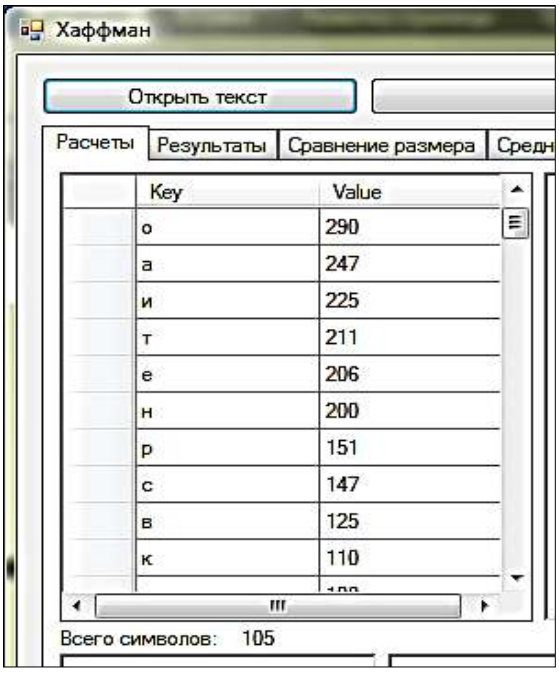


Рис. 6.9. **Підрахована кількість та частота символів**

Наступним кроком є стиснення даних. Для цього необхідно натиснути на кнопку "Начало эксперимента". У ході стиснення даних будуть проведені різноманітні розрахунки для визначення оптимального алгоритму. Розрахунок кодів символів залежно від розбиття на інтервали наведений на рис. 6.10.

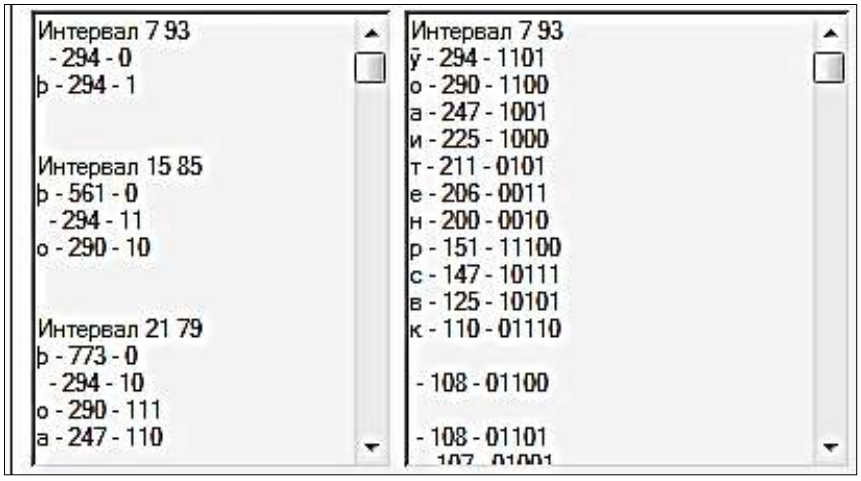


Рис. 6.10. **Підрахунок кодів символів залежно від розбиття на групи**

На вкладці "Результаты" буде побудована порівняльна таблиця середньої довжини коду (рис. 6.11).

Расчеты | Результаты | Сравнение размера | Средний размер файла в зависимости от разбиения

Средня длина кода по хаффману	Количество переключений	Средня длина кода	Средня длина кода I	Средня длина кода II	Размер группы I	Размер группы II	Коэффициент
5,29163429163429	1122	5,57031857031857	1,51004366812227	5,15320479416363	15	85	0,949969777281815
5,29163429163429	1547	5,6977466977467	1,85286783042394	5,00184016824395	21	79	0,928724032910587
5,29163429163429	1884	5,75006475006475	2,05705705705706	4,82812917000267	27	73	0,920273861537769
5,29163429163429	2054	5,78736078736079	2,29468177855275	4,71720519193593	32	68	0,914343253524278
5,29163429163429	2298	5,86713286713287	2,4626239511823	4,57902176986146	38	62	0,901911446607513
5,29163429163429	2086	5,78632478632479	2,73969072164948	4,6115753636645	43	57	0,914506960297211
5,29163429163429	2008	5,75472675472675	2,91654879773692	4,59421243012167	47	53	0,919528331608083
5,29163429163429	1922	5,71147371147371	3,06105047748977	4,58681164503683	51	49	0,926491928169781
5,29163429163429	1602	5,56073556073556	3,35118057864982	4,63884364820847	57	43	0,951606893339544
5,29163429163429	1714	5,64180264180264	3,52516010978957	4,45296167247387	62	38	0,937933250700087
5,29163429163429	1530	5,58637658637659	3,74159292035398	4,44027986006996	67	33	0,947239093142937
5,29163429163429	588	5,44392644392644	1	5,29163429163429	7	93	0,972025310433417
5,29163429163429	1246	5,4988344988345	3,96402456858731	4,54857819905213	72	28	0,962319250153078
5,29163429163429	1070	5,44807044807045	4,12665134979897	4,60041407867495	76	24	0,971285951984787
5,29163429163429	754	5,32452732452732	4,36619318181818	4,73881278538813	81	19	0,993822356260337
5,29163429163429	620	5,33929033929034	4,59270433351618	4,63473053892216	86	14	0,991074460344409
5,29163429163429	462	5,33022533022533	4,81201602136182	4,42733564013841	91	9	0,992759961127308

Рис. 6.11. **Порівняльна таблиця середньої довжини коду**

На вкладці "Средний размер" буде сформована порівняльна таблиця розмірів отриманих файлів. У ній відображено розмір стиснутих даних для класичного і модифікованого алгоритмів та коефіцієнт, що показує ефективність розробленої модифікації (рис. 6.12).

Расчеты | Результаты | Сравнение размера | Средний размер файла в зависимости от разбиения

Размер первой группы в символах	Сжатие по Хаффману (байт)	Сжатие по Модификации Хаффмана (байт)	Коэффициент	Длина строки	Сам текст
7	20	18	1,11	31	Символ 7, магазин автозапчастей
7	22	21	1,05	31	Магазин автозапчастей, ООО ЛАКЦ
7	21	20	1,05	35	Акерманн, производственная компания
7	21	20	1,05	30	Автокомплекс, ИП Абрамкин С.Е.
7	12	11	1,09	17	АМС, автотехцентр
7	18	18	1	23	Motor Domus, автосервис
7	15	15	1	22	Svs-Моторс, автосервис
7	12	11	1,09	17	АМС, автотехцентр
7	11	11	1	18	Дельта, автосервис
7	22	21	1,05	31	Автотехпомощь, служба техпомощи
7	20	20	1	27	Shop77.ru, интернет-магазин
7	25	24	1,04	35	Люберецкая автошкола, ДОСААФ России
7	25	24	1,04	35	Люберецкая автошкола, ДОСААФ России
7	21	20	1,05	29	Екко, бюро судебных экспертиз
7	18	17	1,06	27	Модус-А, оценочная компания
7	26	25	1,04	35	Rent Moskow, агентство недвижимости

Рис. 6.12. **Порівняльна таблиця розмірів отриманих файлів**

6.3.2. Результати експерименту оцінки блоково-статистичного алгоритму

Для перевірки ефективності розробленого алгоритму були виконані експерименти зі стиснення різних наборів вхідних даних.

Для впорядкованих даних незалежно від їх довжини та алфавіту простежується картина, яка зображена на рис. 6.13.

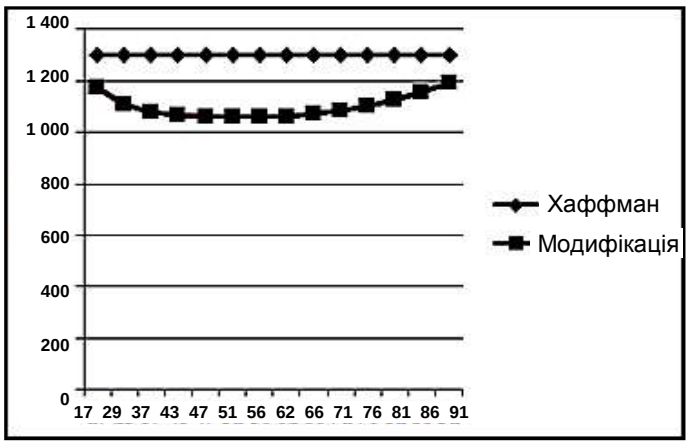


Рис. 6.13. **Стиснення впорядкованих даних**

Для даних, символи тексту яких розташовані у довільному порядку найбільший коефіцієнт досягається при розбитті групи символів на дві рівні частини. За віссю ординат відображений розмір стиснутих даних, за віссю абсцис – розмір першої групи символів (у відсотках). Це наглядно демонструється на рис. 6.14 – 6.16 для рядків із різною довжиною.

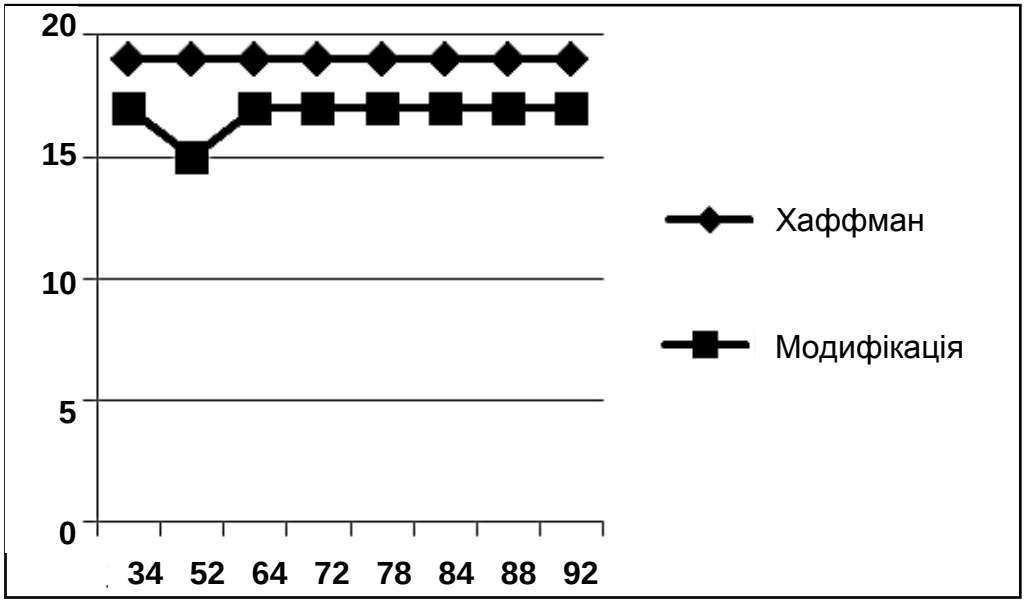


Рис. 6.14. **Стиснення короткого рядка (9 байтів за Хаффманом)**

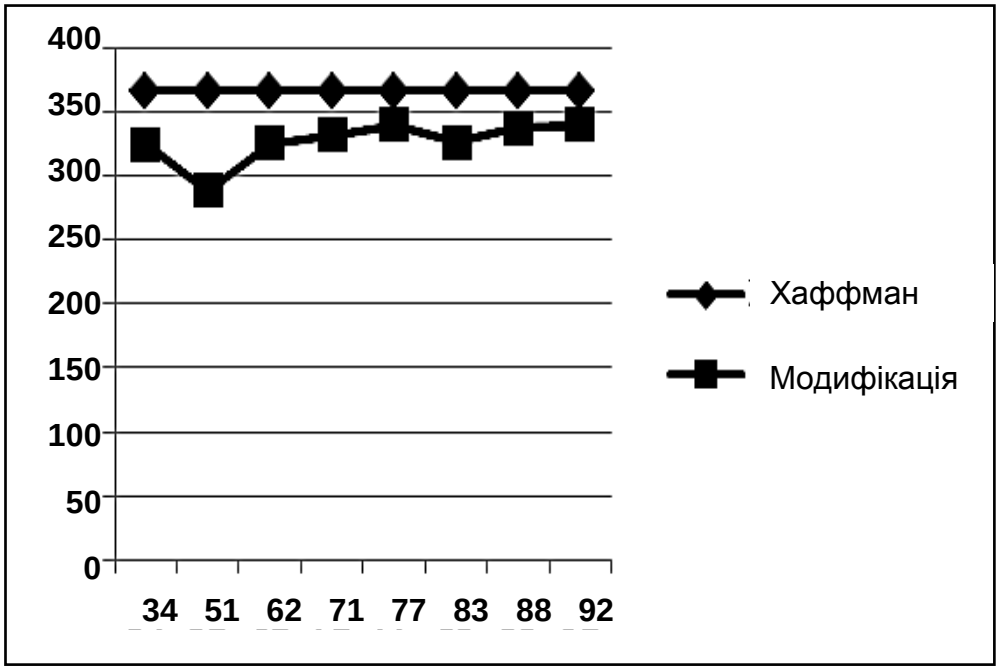


Рис. 6.15. **Стиснення середнього рядка (370 байтів за Хаффманом)**

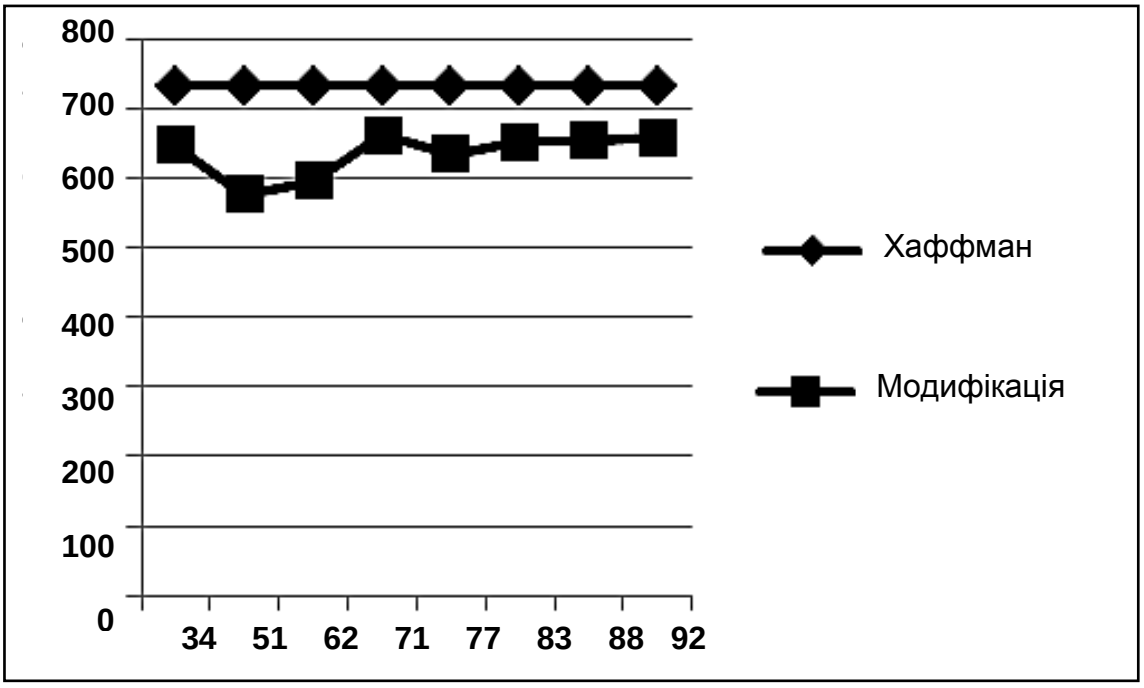


Рис. 6.16. **Стиснення довгого рядка (730 байтів за Хаффманом)**

Для вхідних текстів, у яких кількість різних символів більше 50, спостерігається закономірність, яка зображена на рис. 6.17.

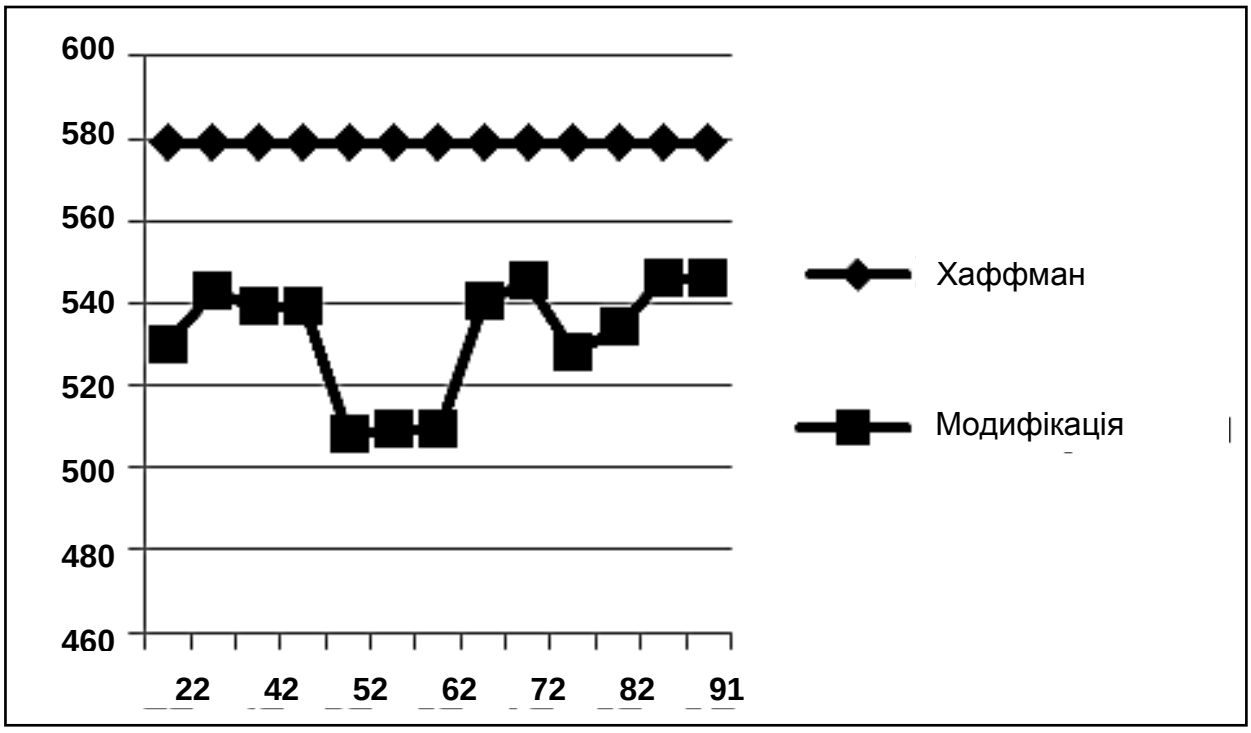


Рис. 6.17. **Стиснення даних, у яких кількість символів більше 50**

Для даних, частота символів котрих підкорюється нормальному закону, спостерігається закономірність, яка зображена на рис. 6.18 – 6.20.

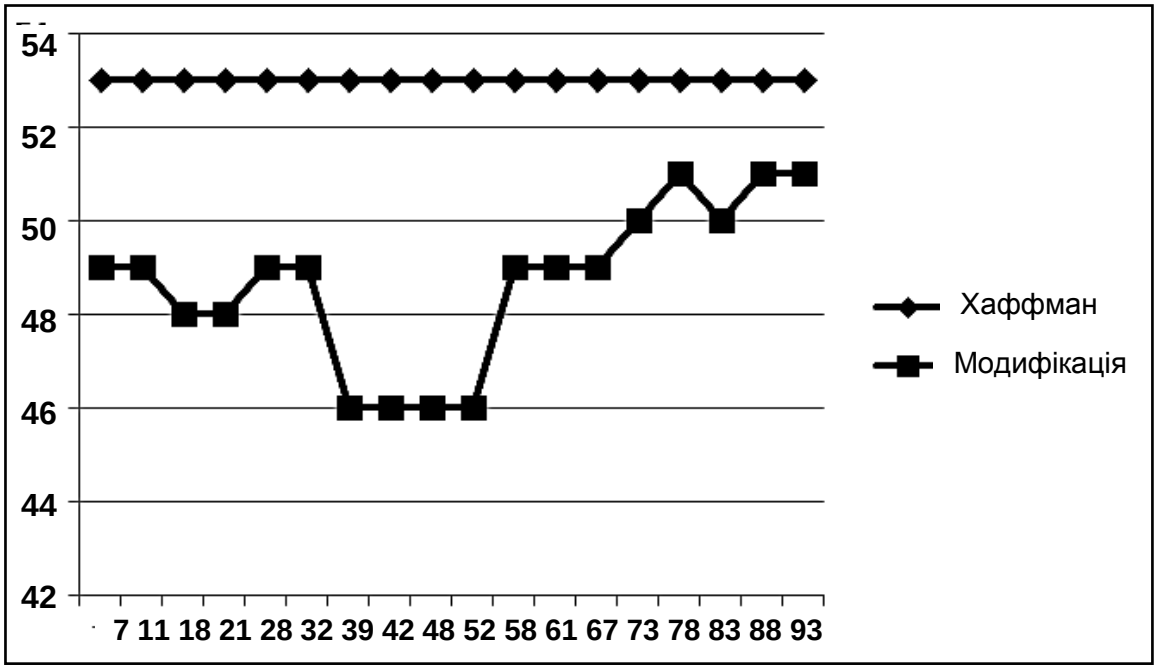


Рис. 6.18. **Стиснення даних, в яких частота символів розподілена за нормальним законом та їх довжина менше 100 символів**

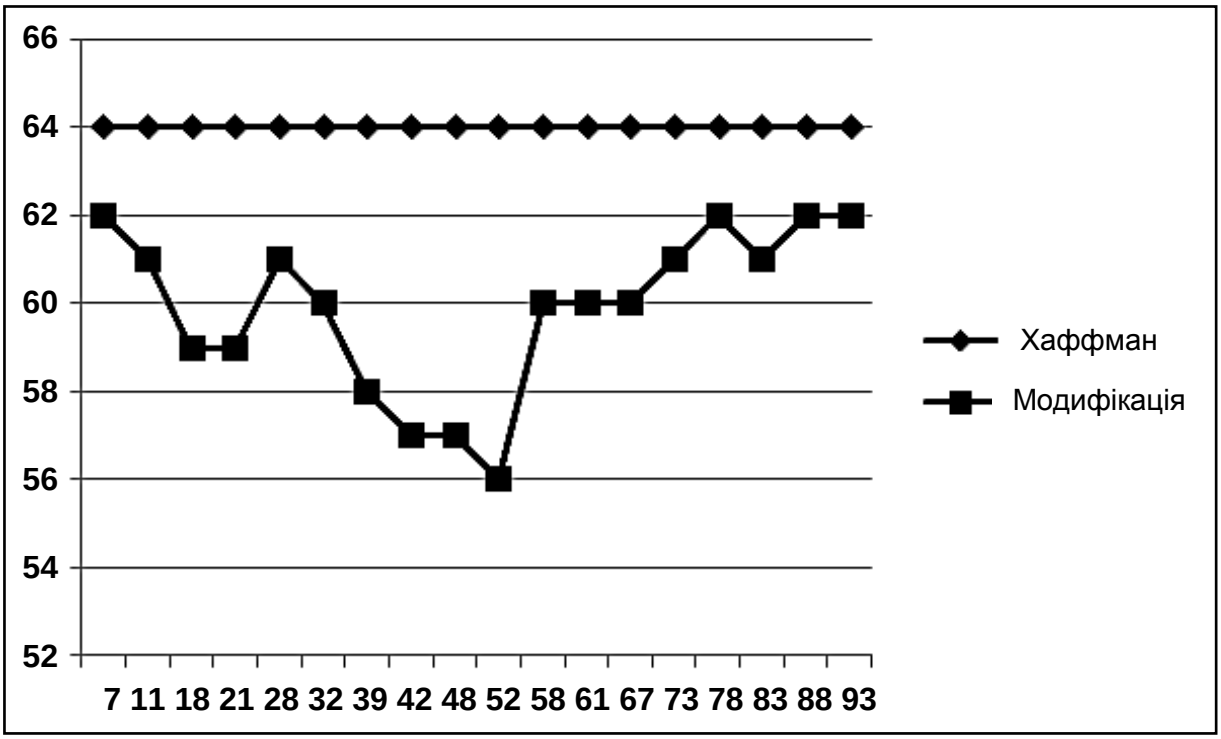


Рис. 6.19. **Стиснення даних, в яких частота символів розподілена за нормальним законом та їх довжина в інтервалі 100 – 200 символів**

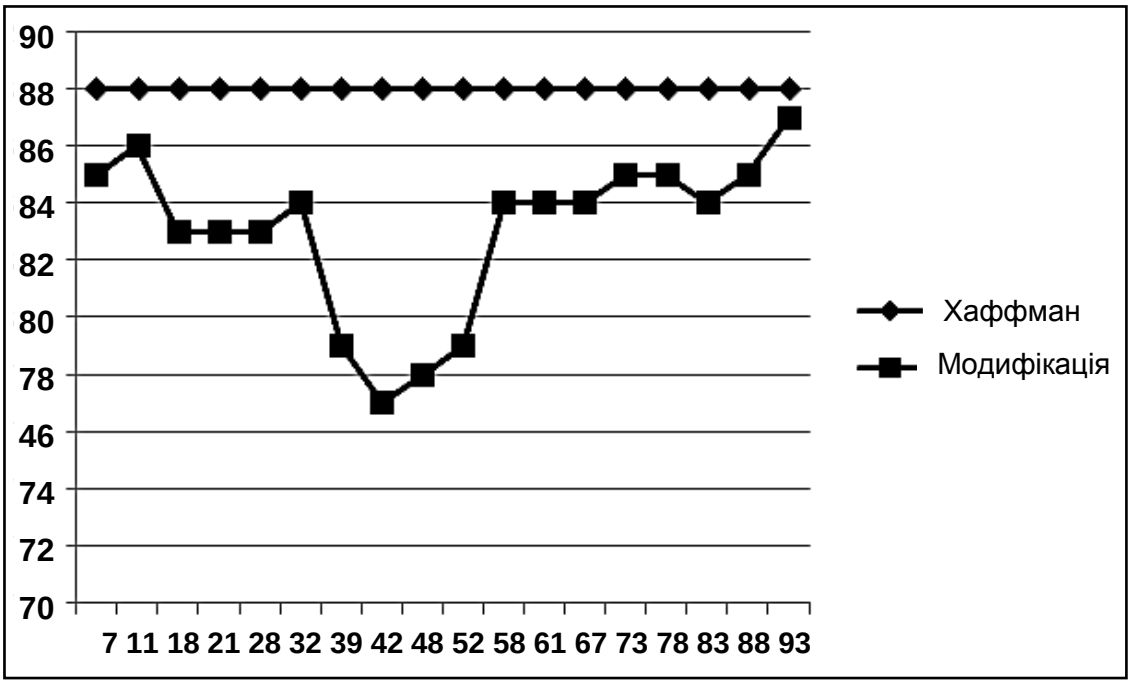


Рис. 6.20. **Стиснення даних, в яких частота символів розподілена за нормальним законом та їх довжина більше 200 символів**

Для даних, котрі розподілені за експоненціальним законом, простежується картина, яка зображена на рис. 6.21 – 6.23.

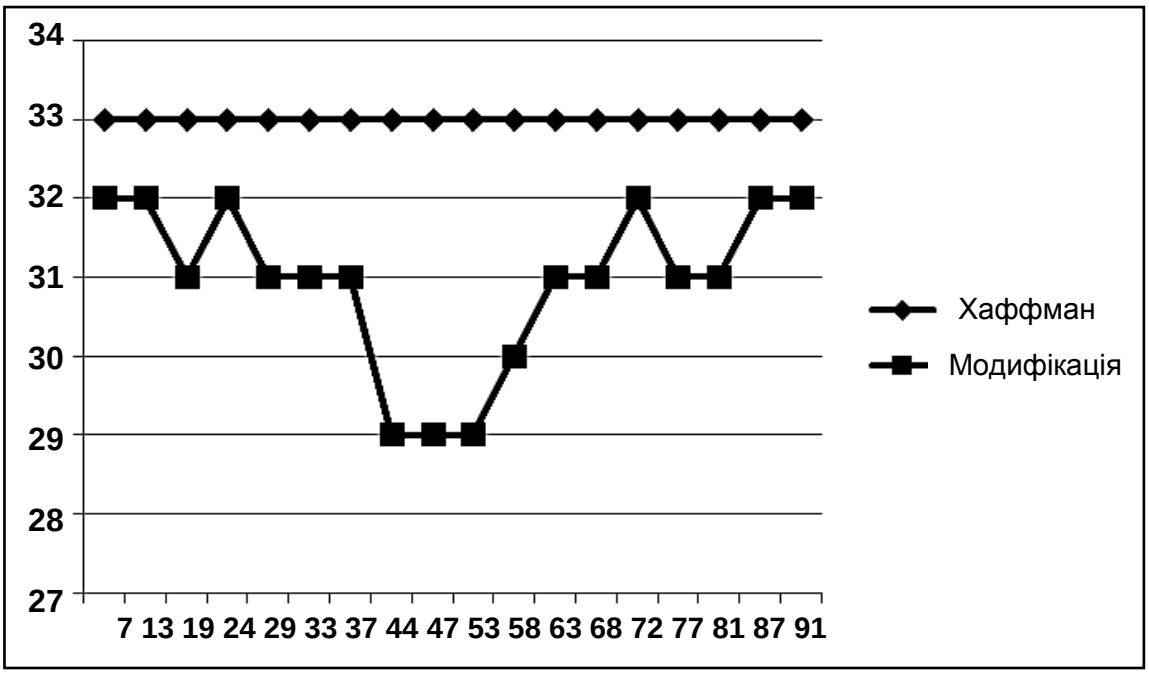


Рис. 6.21. **Стиснення даних, в яких частота символів розподілена за експоненціальним законом та їх довжина менше 100 символів**

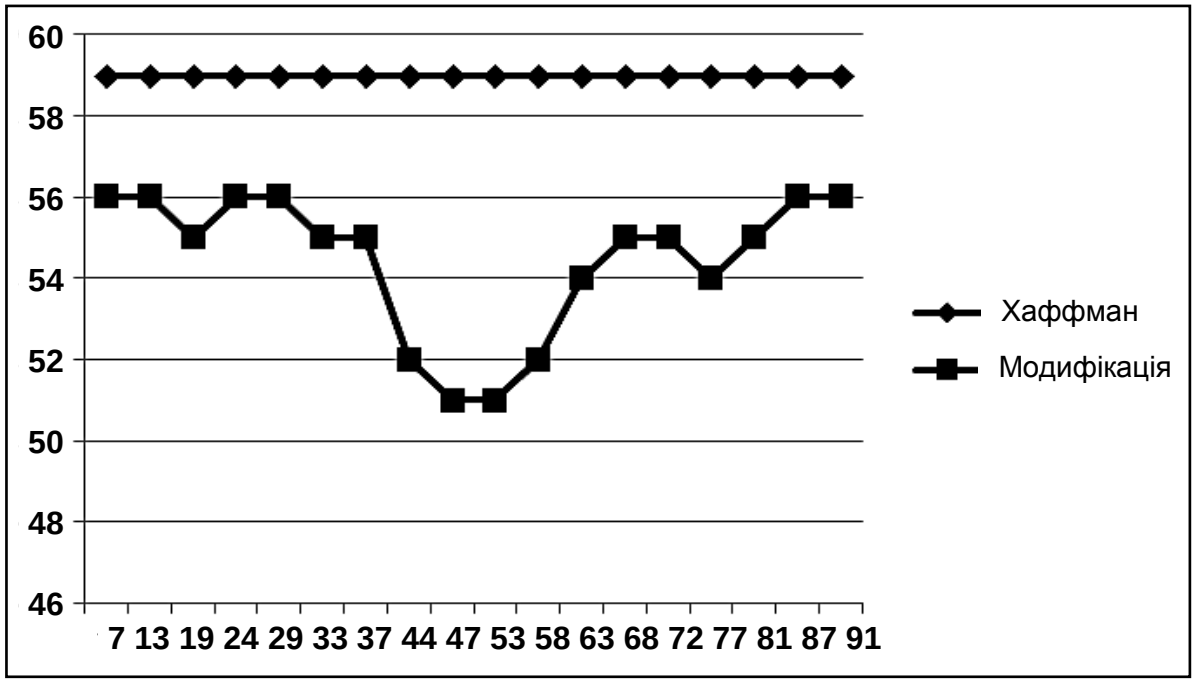


Рис. 6.22. **Стиснення даних, в яких частота символів розподілена за експоненціальним законом та їх довжина в інтервалі 100 – 200 символів**

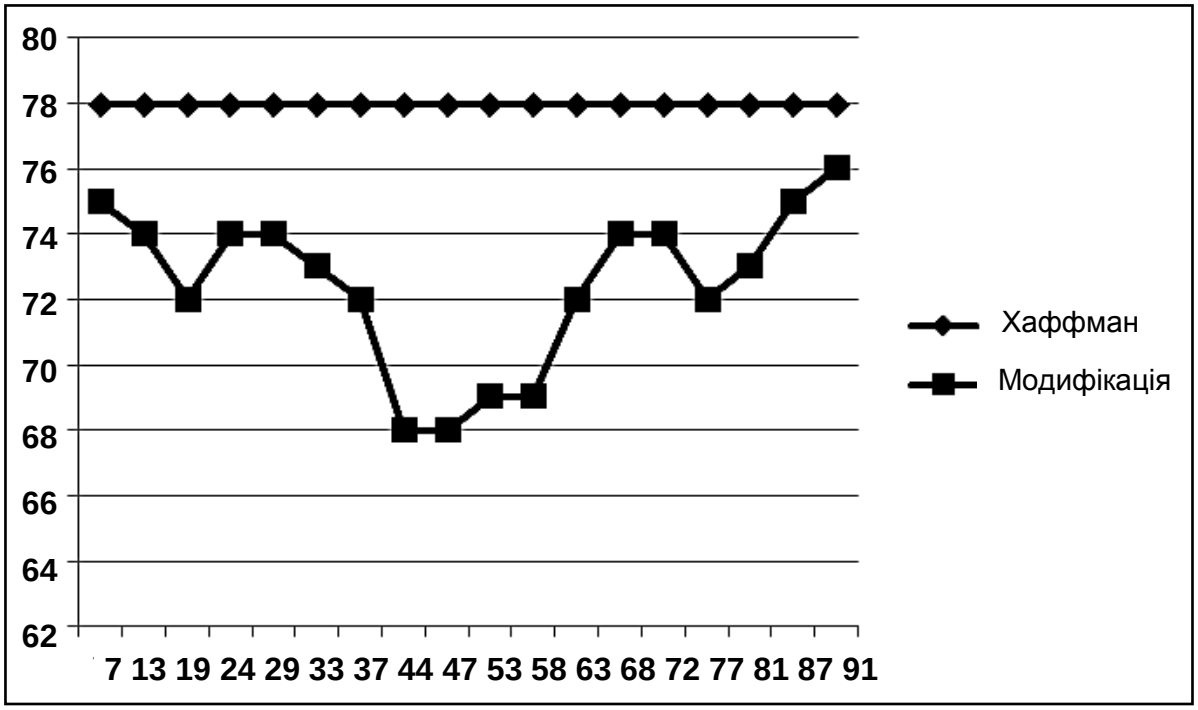


Рис. 6.23. **Стиснення даних, в яких частота символів розподілена за експоненціальним законом та їх довжина більше 200 символів**

Для реальних даних простежується картина, яка зображена на рис. 6.24.

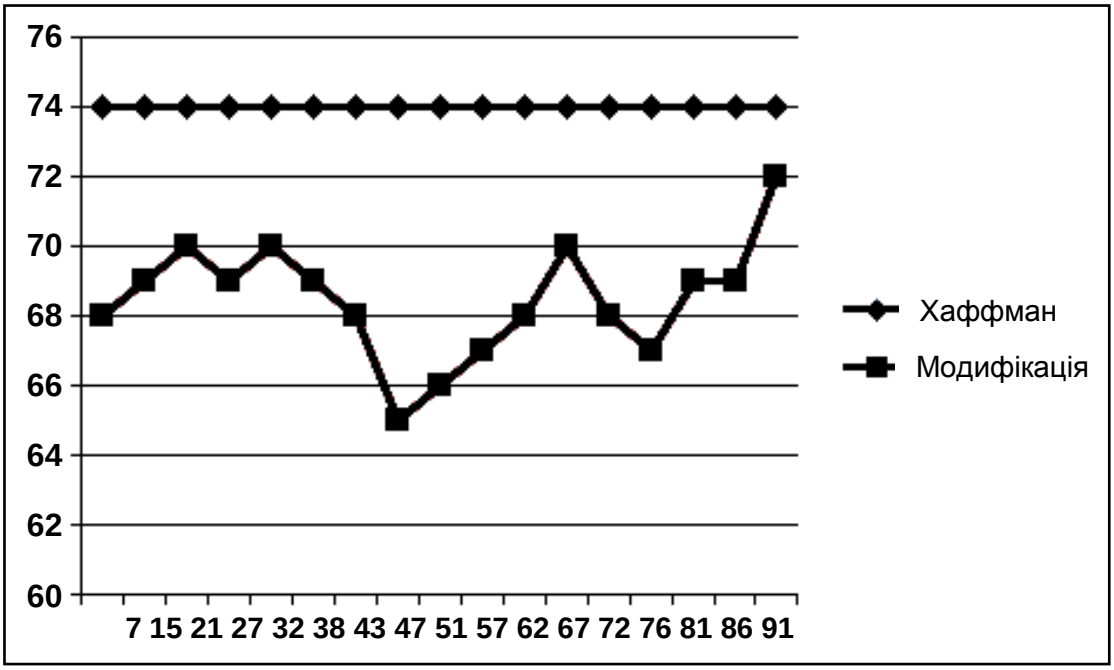


Рис. 6.24. **Стиснення реальних даних**

6.3.3. Аналіз ефективності блоково-статистичного алгоритму

Базуючись на результатах проведених досліджень першого експерименту можна зробити висновок, що розроблена модифікація алгоритму Хаффмана є більш ефективною порівняно з класичним алгоритмом. Для даних, довжина яких приблизно дорівнює 50 символам, ефективність досягає 30 % порівняно з класичним алгоритмом. У середньому ефективність досягає 23 %. Для цього типу даних доцільно розділяти символи тексту на дві групи, котрі також, приблизно рівні за обсягом.

Для даних, у яких символи розподілені за законом Ципфа та розташовані у довільному порядку, модифікований алгоритм найбільш ефективний для даних, довжина котрих приблизно дорівнює 50. На цих даних ефективність алгоритму на 13 % вище порівняно з кодом Хаффмана. Також для цього типу даних доцільно розділяти символи тексту на дві групи, приблизно рівні за обсягом. На рис. 6.25 зображений графік, котрий демонструє перевагу модифікації при стисненні тексту, що відрізняється довжиною.

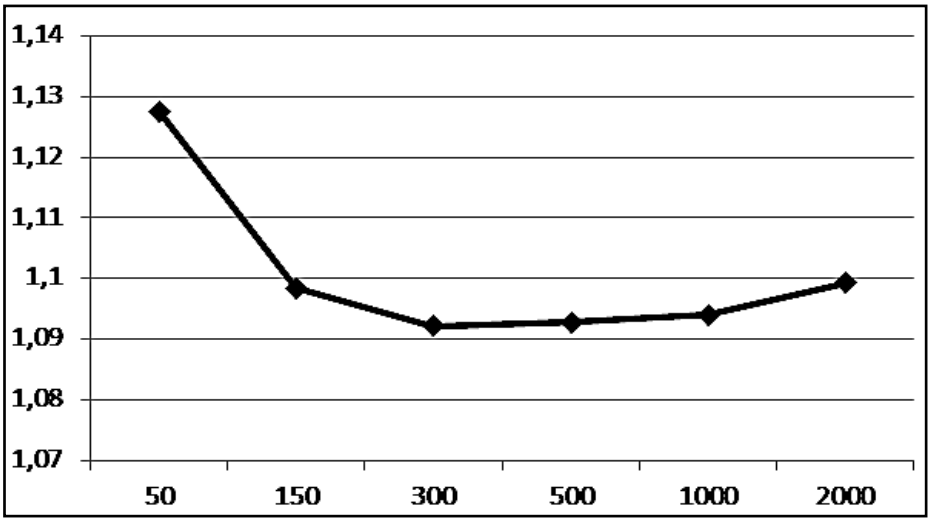


Рис. 6.25. **Ефективність стиснення для даних, у яких символи розподілені за законом Ципфа та розташовані у довільному порядку**

Для даних, у котрих частота символів підкорюється нормальному закону, ефективність розробленої модифікації знаходиться в межах 3 – 13 %. Як і в попередніх експериментах максимальна ефективність отримана при розбитті групи символів на дві рівні за обсягом групи. Результати експерименту зображені на рис. 6.26.

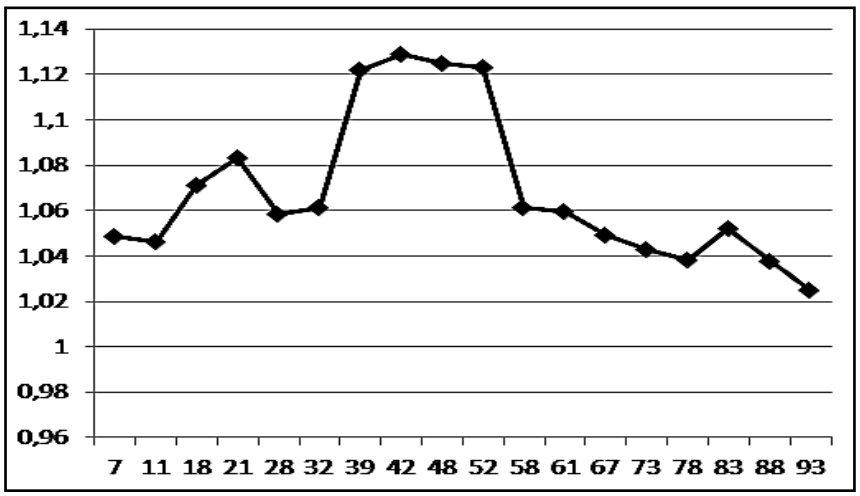


Рис. 6.26. **Ефективність стиснення даних, у яких частота символів підкорюється нормальному закону**

Для даних, у котрих частота символів підкорюється експоненціальному закону, ефективність розробленої модифікації знаходиться в межах 4 – 14 %. Як і в попередніх експериментах максимальна ефективність отримана при розбитті групи символів на дві рівні за обсягом групи. Результати експерименту зображені на рис. 6.27.

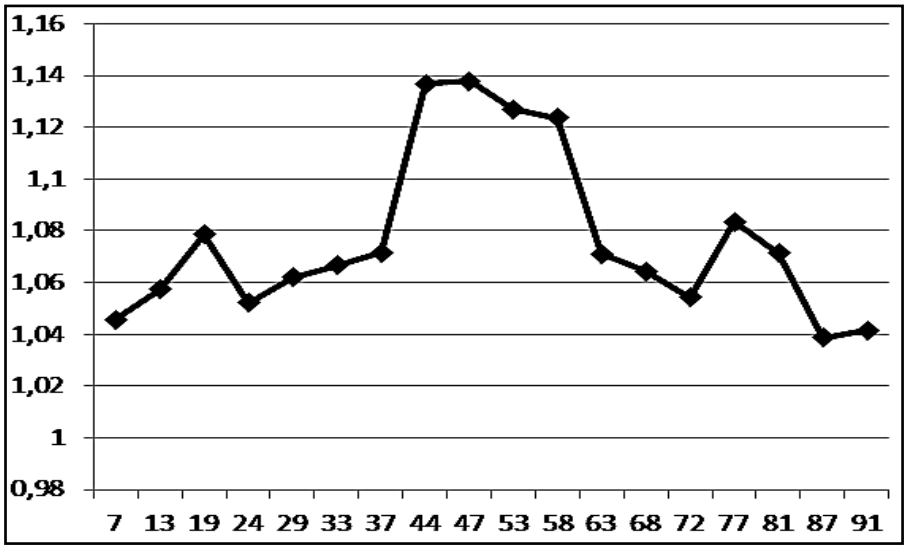


Рис. 6.27. **Ефективність стиснення даних, у яких частота символів підкорюється експоненціальному закону**

Тестування для реальних даних проводилося для двох наборів даних.

Перший набір містив рядки тексту з символів кирилиці довжиною від 10 до 80. Ефективність розробленої модифікації досягає приблизно 13 %. Цей показник правильний для даних, котрі суттєво відрізняються довжиною. Найбільший коефіцієнт стиснення отриманий при розділенні символів тексту на дві рівні групи. На рис. 6.28 зображені узагальнені дані, що характеризують залежність розміру стиснутих даних від розміру двох груп символів (за частотою). За віссю ординат відображене середнє значення довжини рядка після стиснення, за віссю абсцис – розмір першої групи символів.

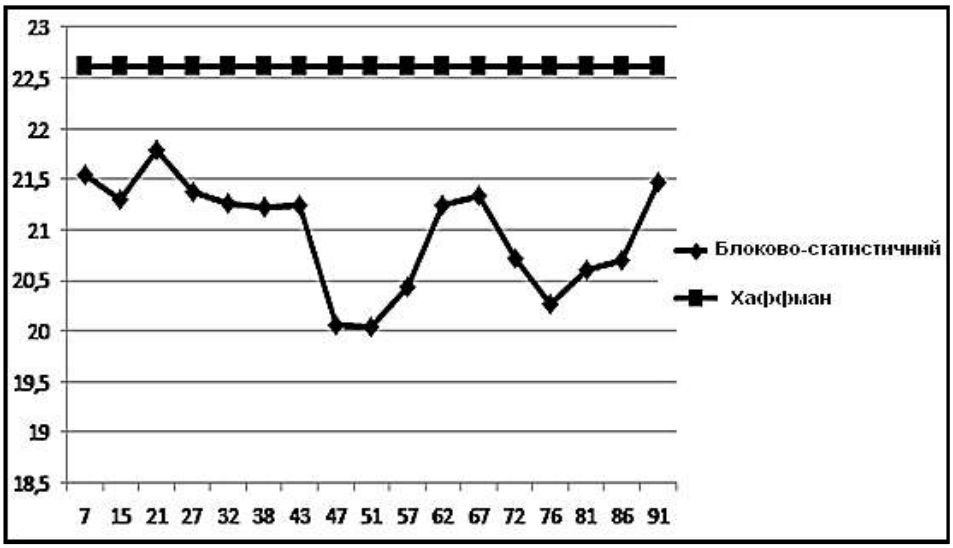


Рис. 6.28. **Залежність об’єму стиснутих даних від кількості символів у групах порівняно з алгоритмом Хаффмана**

На рис. 6.29 зображений графік, котрий демонструє перевагу модифікації при стисненні реальних даних.

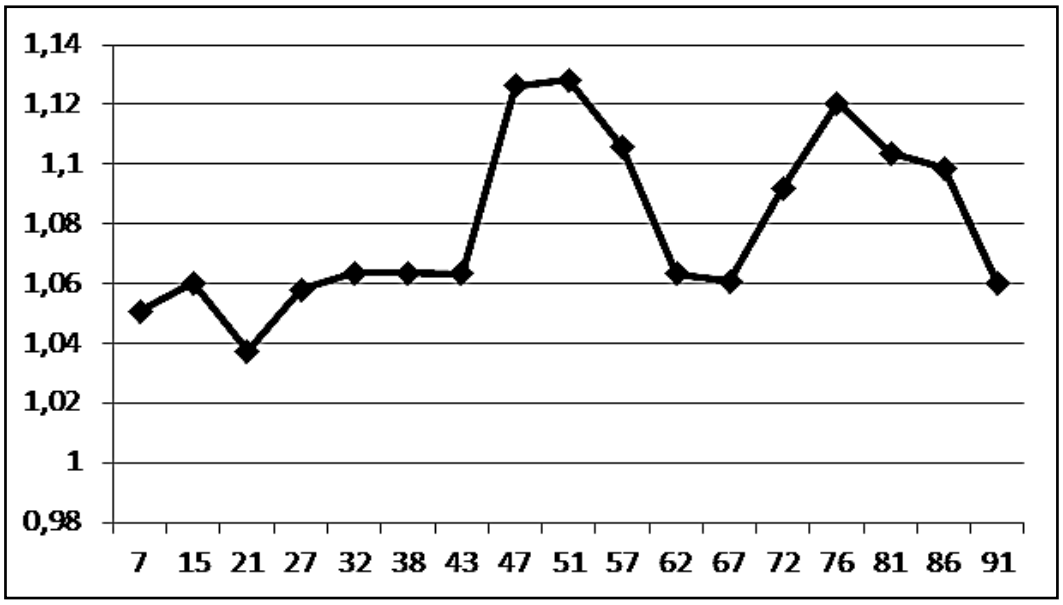


Рис. 6.29. **Ефективність стиснення реальних даних**

Другий набір реальних даних містив текст змішаного характеру, тобто включав символи як кирилиці, так і латиниці. Довжина рядка коливалась від 10 до 170 символів. Отримані результати для другого набору теж свідчать про більшу ефективність блоково-статистичного методу. В середньому коефіцієнт стиснення дорівнює 11 %. Графік, котрий демонструє перевагу модифікації при стисненні другого набору реальних даних зображений на рис. 6.30.

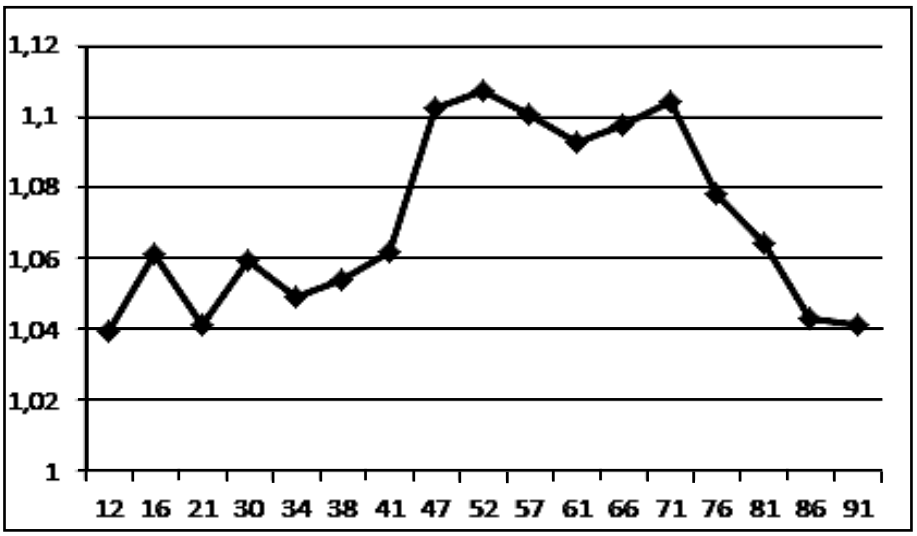


Рис. 6.30. **Ефективність стиснення реальних даних**

У результаті проведених досліджень були проаналізовані сучасні методи стиснення інформації. Особлива увага була приділена класичному алгоритму Хаффмана як найбільш придатному для використання у базах даних для стиснення текстових полів невеликої довжини. Була сформульована пропозиція щодо модифікації алгоритму Хаффмана (блоково-статистичний алгоритм) для отримання більшої ефективності при стисненні даних. З метою оцінки ефективності запропонованого алгоритму було проведено ряд експериментів для визначення ступеня стиснення класичного та модифікованого алгоритмів для вхідних даних різних типів.

Базуючись на результатах проведених досліджень можна зробити висновок, що розроблена модифікація алгоритму Хаффмана є більш ефективною порівняно з класичним алгоритмом. Для різних даних, ефективність знаходиться в проміжку від 11 до 29 % порівняно з класичним алгоритмом. Найбільш ефективне стиснення відбувається для впорядкованих даних розміром близько 50 символів. Для впорядкованих даних показник ефективності коливається від 9 до 13 %. Максимальна ефективність отримується також при довжині даних близько 50 символів. Дані, в яких частоти символів розподілені за нормальним та експоненціальними законами розподілення, мають коефіцієнт стиснення, що дорівнює 3 – 13 % порівняно з оригінальним алгоритмом. Для реальних даних стиснення в середньому було на 11 – 12 % більш ефективне порівняно з класичним алгоритмом. Для всіх типів текстових даних доцільно розділяти символи тексту на дві групи, приблизно рівні за обсягом.

Розроблена модифікація підтвердила свою ефективність для різних типів текстових даних і заслуговує на подальше вивчення.

Розділ 7. Моделювання роботи комунікаційної мережі

7.1. Аналіз проблематики, постановка завдань та методи й моделі їх вирішення

Розглянуто функціонування сучасних мереж передачі даних з точки зору подання інформації, її маршрутизації і комутації. Проведено аналіз основних мережних протоколів з точки зору доцільності їх корпоративного використання, технології передачі даних, конкретного обладнання та його конфігурації.

Функціонування сучасних обчислювальних мереж базується на методах пакетної передачі та комутації, які використовують єдину ідею подання будь-якого виду інформації. Це можуть бути дані, зображення, звук, службові та управляючі повідомлення та інше, у вигляді цифрової послідовності та подальшого розподілення цієї послідовності на пакети, що містять усю необхідну інформацію для їх ідентифікації та маршрутизації. За допомогою такого підходу всі види інформації можна транслювати через єдиний інформаційний канал, використовуючи різні шляхи та засоби, а також застосовувати універсальні системи комутації [284; 285; 313; 337].

Управління сучасною організацією, яка має відділення або філії в різних кінцях міста, країни або світу, неможливе без застосування сучасних інформаційних технологій, перш за все – побудови відповідної мережі, яка дозволить ефективно працювати будь-якій кількості працівників одночасно. Ці рішення базуються на моделюванні обчислювальних мереж. Обчислювальні мережі поділяють на розподілені мережі WAN (Глобальна Комп'ютерна Мережа) та локальні мережі LAN (Локальна Обчислювальна Мережа).

WAN – це технологія побудови мереж, яка забезпечує передачу інформації на значні відстані з використанням комутуючих та виділених ліній, спеціальних каналів зв'язку та засобами мережі Інтернет. Ці мережі проектуються і будуються для вирішення великої кількості завдань щодо передачі інформації між віддаленими офісами, філіями й окремими периферійними пристроями. Переваги протоколів, які застосовуються в WAN мережах, полягають у тому, що в одній мережі можна передавати одночасно всі види інформації: дані, голос, факс, відео [311; 323].

У сучасних умовах розвитку бізнесу для підприємства стає необхідним пошук рішень, здатних оптимізувати роботу співробітників, зробити її більш продуктивною. Виникає потреба в побудові локальної мережі передачі даних LAN.

LAN – це мережі, які проектуються і будуються для високошвидкісного обміну даними між користувачами та доступу до загальних ресурсів компанії в межах однієї або групи будівель [294; 295; 297; 320]. Унаслідок того, що перед організаціями або підприємствами виникають різні функціональні завдання, а також вони мають різні фінансові можливості і початкові умови, для розробки рішення необхідно застосовувати зважений інтегральний підхід з урахуванням усіх складових [333]. В умо-

вах наявності безмежних обчислювальних ресурсів та безмежної пропускної спроможності каналів, проектування подібних комунікаційних мереж стає лише технічним завданням. Проблеми з'являються тоді, коли названі ресурси стають обмеженими [298; 302; 316; 327]. Варто звернути увагу на деякі проблеми, пов'язані зі здійсненням телефонних переговорів з використанням мереж із пакетною передачею та комутацією в умовах обмежених ресурсів. Ці проблеми є багатоплановими та охоплюють широке коло питань наукового, технічного та економічного характерів [308; 330; 334].

Основне завдання IP-телефонії полягає в забезпеченні природного мовного спілкування двох або декількох осіб, що є абонентами однієї або різних комунікаційних мереж, за допомогою мережі зв'язку з комутацією пакетів [332]. Взагалі в більшості обчислювальних мереж, й перш за все – в мережі Інтернет, для формування пакетів використовується протокол IP (Internet Protocol). Отже, телефонію засобами Інтернет та Інтранет мереж доцільно називати IP-телефонією [278; 336]. Інтернет-провайдери та телефонні оператори активно розроширяють ринок IP-телефонії.

У корпоративному секторі IP-телефонія поки що не дуже поширена, як на ринку операторських рішень. Стосовно корпоративного ринку IP-телефонію можна умовно розділити на магістральну і локальну.

У LAN-телефонії головним стримуючим фактором є передусім кінцевий пристрій. Коли єдиним варіантом клієнтського пристрою є мультимедійний комп'ютер, сприймати рішення як корпоративне не має сенсу. На сьогоднішній день існують сучасні IP-телефони, які можуть працювати в автономному режимі деякий час.

На корпоративному ринку попит на IP-телефонії зростає також завдяки тому, що мережне обладнання набуло рис засновницької автоматизованої телефонної мережі. В першу чергу, це стосується проблеми живлення IP-телефонів, що працюють у мережному оточенні.

Особової уваги заслуговують рішення компанії Cisco Systems, яка оперативно модернізувала мережне обладнання, щоб воно могло забезпечувати живлення абонентських пристроїв. Для цього компанією випускаються, по-перше, спеціальні інтерфейсні модулі, здатні подавати живлення по дротам локальної мережі, по-друге, що встановлюються в слот розширення, а також зовнішні блоки живлення постійного струму [9; 145; 303; 307; 338]. Варто зазначити, що "електричні" інтерфейсні модулі можуть працювати також зі звичайним мережним устаткуванням,

оскільки мають функцію автоматичного визначення типу підключеного до порту пристрою – живлення подається тільки після того, як кінцевий пристрій його запитав.

Під корпоративною мережею розуміють територіально розподілену мережу, яка об'єднує офіси, підрозділи та інші структури, які можуть знаходитися на значній відстані один від одного – в різних містах, а іноді і країнах. Дуже часто при створенні корпоративної телефонної системи, що охоплює кілька філій компанії, розрізнені телефонні станції потрібно об'єднати в загальну мережу. При цьому важливо не тільки забезпечити звичайне встановлення з'єднань між абонентами, а й надати їм доступ до додаткових сервісів. Використання IP-телефонії може стати рішенням даного завдання. Реалізація такої системи зв'язку на підприємстві забезпечить співробітників регіональних філій можливістю оперативного обміну інформацією, обговорення поточних питань та прийняття спільних рішень без проведення особистих зустрічей і нарад, при одночасному скороченні витрат на телекомунікації [84; 92; 95; 96].

Вартість є головною перевагою IP-телефонії для корпоративного користувача перед традиційними телефонними системами зв'язку. Тут можна виділити декілька положень:

• дійсна економія на міжміських та міжнародних телефонних розмовах;

• швидка окупність капітальних витрат, що пов'язано, перш за все, з поступовим зниженням ціни на обладнання для IP-телефонії і появою програмного забезпечення, яке значно дешевше, ніж аналогічне ПО для звичайних аналогових телефонних станцій;

• скорочення витрат на адміністрування. Немає необхідності мати роздільний персонал для адміністрування телефонної та комп'ютерної мереж. Крім того, завдяки концентрації всіх інтелектуальних ресурсів у центральному офісі, обслуговуючий персонал у віддалених офісах не потрібен взагалі.

Перевагою IP-телефонії є різноманітність сервісів, їх налаштування відповідно до потреб конкретного користувача. Можливість інтеграції IP-телефонії з існуючими мережами телефонного зв'язку дозволить модернізувати телекомунікаційну систему підприємства із найменшими витратами. Серед нових сервісів, недоступних користувачам АТС, найбільші додатки, що користуються попитом, пов'язані з інтеграцією телефонних сервісів з існуючими інформаційними системами замовника:

каталогами, базами даних клієнтів. Для корпоративних користувачів цікаві також інтерактивні додатки VoIP-систем, зокрема, розсилки інформаційних повідомлень, курсів валют, котирувань тощо [41; 231; 256; 258; 261].

З точки зору масштабованості використання IP-телефонія також має свої переваги. Оскільки з'єднання на базі протоколу IP може починатися і закінчуватися в будь-якій точці мережі від абонента до магістралі, IP-телефонію в мережі можна вводити ділянка за ділянкою. У той же час для IP-телефонії характерна певна модульна кількість і потужність різних вузлів, яку можна нарощувати практично незалежно, відповідно до поточних потреб [45].

Кінцевий користувач IP-телефонії не тільки збереже наявні переваги телефонної мережі загального користування, а й отримає нові, а саме:

• IP-телефонія одночасно підтримує голос і дані, задовольняючи вимоги конвергенції. Клієнти отримають додаткові переваги від економії в розвитку, можливі за рахунок використання єдиної мережі;

• мобільність користувача. Звичний апаратний телефон може бути легко перенесений при зміні співробітником робочого місця – зникає необхідність виробляти перекомутацію телефонних дротів;

• наявність доступу до будь-яких нових послуг. Таким чином, рішення задачі розгортання телекомунікаційної мережі підприємства на базі IP-телефонії, чи то побудова абсолютно нової телефонної мережі або модернізація вже існуючої, є досить актуальною, оскільки пропонує величезний ряд переваг, без яких стабільна, організована і конкурентоспроможна робота корпорації в справжніх умовах не є можливою.

Ефективність і надійність роботи мережного комплексу, чи то корпоративна мережа підприємства або робочої групи, територіально-розподілена телекомунікаційна інфраструктура або система доступу віддалених користувачів, багато в чому визначається правильністю вибору і застосування тієї чи іншої технології передачі даних, конкретного обладнання та його конфігурації [44; 46].

Основною проблемою під час створення корпоративної мережі є проведення організаційно-технічних заходів. Існує декілька варіантів організації телефонних комунікацій на базі мережі Інтернет, що дозволяють виділити основні характерні функціональні елементи IP-телефонії [220].

Технологія VoIP (Voice over Internet Protocol) реалізує завдання та рішення, які за допомогою технології PSTN (Public Switched Telephone Network) побудувати буде важче або дорожче. Наприклад: можливість передавати більше одного телефонного дзвінка в рамках високошвидкісного телефонного підключення. VoIP використовується в якості простого засобу для залучення додаткової телефонної лінії вдома або в офісі. Властивості, такі, як конференція, переадресація дзвінка, автоматичний перенабір, визначення номера, що дзвонить, надаються безкоштовно або майже безкоштовно, тоді як в традиційних телекомунікаційних компаніях – це зазвичай платні послуги. Безпечні дзвінки зі стандартизованим протоколом [10; 272].

Більшість труднощів для включення безпечних телефонних з'єднань за традиційними телефонними лініями, такі як відцифровування сигналу, передача цифрового сигналу вже вирішені в рамках технології VoIP. Необхідно лише провести шифрування сигналу і його ідентифікацію для існуючого потоку даних, незалежно від місця розташування. Потрібно тільки Інтернет-з'єднання для підключення до провайдера VoIP. Оператори центру дзвінків за допомогою VoIP-телефонів можуть працювати з будь-якого офісу, де є в наявності ефективне швидке і стабільне Інтернет-підключення. Доступна інтеграція з іншими через Інтернет, включаючи відеодзвінок, обмін повідомленнями і даними під час розмови, аудіоконференції, управління адресною книгою та отримання інформації про те, чи доступні для дзвінка інші абоненти. Додаткові телефонні властивості – такі, як маршрутизація дзвінка, спливаючі вікна, альтернативний GSM-роумінг та впровадження IVR – легше і дешевше впровадити та інтегрувати. Той факт, що телефонний дзвінок знаходиться в тій же самій мережі передачі даних, що і персональний комп'ютер користувача, відкриває шлях до багатьох нових можливостей [24; 212].

Сумісність мобільних номерів MNP (Mobile number portability) також робить свій вплив на IP-телефонію, тобто на комерційне застосування VoIP. Голосовий дзвінок, який прийшов по каналу VoIP, маршрутизується на мобільний телефон традиційного мобільного оператора, також досягає мети призначення, яка у випадку з мобільним телефоном виражається в тому, що сигнал повинен досягти порту.

Сумісність мобільних номерів – це сервіс, який дозволяє його користувачам зберегти існуючий телефонний номер при переході від одного мобільного оператора до іншого.

Система з мінімальною вартістю маршрутизації дзвінка LCR (Least Cost Routing system). Виклики в IP-телефонії вважають системою з мінімальною вартістю маршрутизації дзвінка LCR, яка заснована на тому, що здійснюється перевірка пункту призначення кожного телефонного дзвінка, як тільки він зроблений всередині мережі, що дає споживачеві найнижчу ціну. За умови сумісності з GSM-номерами, яка зараз широко поширена, провайдери систем з мінімальною вартістю маршрутизації дзвінка LCR, більше не можуть покладатися на використання префікса номера, для того щоб визначити, як перенаправити дзвінок. Замість цього їм потрібно знати фактичну назву мережі мобільного оператора для кожного дзвінка, щоб здійснити його маршрутизацію [156; 161].

Отже, VoIP-рішення також необхідні для того, щоб керувати сумісністю мобільних номерів MNP при маршрутизації голосового дзвінка. Перевірки сумісності мобільних номерів MNP потрібні для того, щоб гарантувати, що якість послуги буде відповідати необхідному рівню. При проведенні перевірки сумісності мобільних номерів перед тим, як здійснюється маршрутизація дзвінка, і тим самим гарантувати, що голосовий дзвінок справді потрапить за призначенням, VoIP-компанії дають своїм клієнтам гарантію, що вони знайдуть провайдера послуг IP-телефонії. Компанія-оператор надає послугу Інтернет-пейджера – Voice Network Query (система передачі голосових повідомлень). Ця послуга дає можливість як традиційним операторам голосового зв’язку, так і VoIP-операторам відправляти в GSM-мережу запит, спрямований на те, щоб знайти домашню мережу для перенесеного номера [53; 144; 254].

Дзвінки за номерами екстрених викликів. Через властивості, притаманні технології IP, важко визначити місцезнаходження користувача. Дзвінки за номерами екстрених викликів не можна легко маршрутизувати на центр прийому дзвінків. Іноді VoIP-системи можуть маршрутизувати екстрені внутрішньомережеві дзвінки на неекстрені телефонні лінії в потрібному підрозділі [98].

Протоколи забезпечують реєстрацію IP-шлюзу, терміналу або IP-телефону на сервері або гейткипері провайдера, виклик або переадресацію виклику, встановлення голосового або відеоз’єднання, передачу імені або номера абонента. В даний час широке поширення одержали такі VoIP-протоколи:

- SIP – протокол сеансового встановлення зв’язку, що забезпечує передачу голосу, відео, повідомлень систем миттєвого обміну повідом-

лень і довільного навантаження. Для сигналізації зазвичай використовується порт 5060 UDP. Підтримується контроль присутності;

- H.323 – протокол, більш прив'язаний до систем традиційної телефонії, чим SIP, сигналізація по порту 1720 TCP, і 1719 TCP для реєстрації терміналів на гейткипера;
- IAX2 – через 4569 UDP-порт і сигналізація, і медіатрафік;
- MGCP (Media Gateway Control Protocol) – протокол управління медіашлюзом;
- Megaco/H.248 – протокол управління медіашлюзом, розвиток MGCP;
- SIGTRAN – протокол тунелювання PSTN сигналізації ОКС-7 через IP на програмний комутатор (SoftSwitch);
- SCTP (Stream Control Transmission Protocol) – протокол для організації гарантованої доставки пакетів у IP-мережах;
- SCCP (Skinny Call Control Protocol) – закритий протокол управління терміналами (IP-телефонами і медіашлюзи) в продуктах компанії Cisco;
- Unistim – закритий протокол передачі сигнального трафіку в продуктах компанії Nortel [206].

Для передачі голосу по IP-мережі, людський голос відцифровується за допомогою імпульсно-кодової модуляції, стискається, кодується і розбивається на пакети. На приймаючій стороні, відбувається зворотна процедура – дані вилучаються із пакетів, декодуються і перетворюються назад в аналоговий сигнал.

Кодек вносить додаткову затримку порядку 15 – 45 мс, що виникає з таких причин: використання буфера для накопичення сигналу і обліку статистики подальших відліків – алгоритмічна затримка; математичні перетворення, що виконуються над мовним сигналом, вимагають процесорного часу – обчислювальна затримка.

Дану затримку необхідно враховувати при розрахунку крізних затримок. Крім того, складні алгоритми кодування/декодування вимагають більш серйозних витрат обчислювальних ресурсів системи [14; 32; 262; 270].

Проведений в різних дослідницьких групах аналіз якості передачі мовних даних через Інтернет показує, що основним джерелом виникнення спотворень, зниження якості і розбірливості синтезованої мови є

переривання потоку мовних даних, викликане втратами пакетів при передачі по мережі зв'язку або перевищенням допустимого часу доставки пакета з мовними даними. Це вимагає рішення задачі оптимізації затримок у мережі і створення алгоритмів компресії мови, стійких до втрат пакетів.

Більшість споживачів VoIP-рішень ще не підтримують криптографічне шифрування, незважаючи на те, що наявність безпечного телефонного з'єднання набагато простіше впровадити в рамках VoIP-технології, ніж у традиційних телефонних лініях [18; 164].

Існує кілька ресурсів з відкритим кодом, що виконують аналіз трафіку VoIP-розмов. Невисокий рівень безпеки надається в рамках патентованих аудіокодеків, які не можна знайти в списках джерел з відкритим кодом. Проте, така безпека через незрозумілість не зарекомендувала себе як ефективний засіб в інших областях. Деякі вендори використовують також стиснення, щоб перехоплення інформації було важче виконати. Є думка, що безпека мережі вимагає проведення повного криптографічного шифрування і аутентифікації, які не доступні широкому споживачеві. Однак за деякими параметрами IP-телефонія виграє у традиційної в плані безпеки [181; 182].

Рішення Voice VPN (яке є поєднанням технології VoIP і Virtual Private Network) надає можливість створення безпечного голосового з'єднання для VoIP-мереж всередині компанії, шляхом застосування IPSec шифрування до оцифрованого потоку голосових даних [271].

Так само можна виконати багаторівневе шифрування і повну анонімність всього VoIP трафіку за допомогою мережі I2P, програму-маршрутизатор для роботи, яку можна встановити на ПК, смартфон, нетбук, ноутбук та ін. Така мережа є повністю децентралізованим, анонімним середовищем передачі даних, де кожен пакет даних піддається чотирирівневому шифруванню з використанням різних алгоритмів шифрування з максимальними розмірами ключа. Мережа I2P використовує тунельну передачу даних, де вхідний і вихідний трафіки йдуть через різні тунелі, кожен з яких зашифрований різними ключами, при цьому тунелі періодично перебудовуються зі зміною ключів шифрування. Все це призводить до неможливості прослухати і проаналізувати потік, що проходить третьою стороною. При цьому на потокову передачу тунелювання і шифрування не позначається, тому що використовується спеціально створена для потокових служб бібліотека, з цього дані при-

ходять строго в заданому порядку, без втрат і дублювань [271]. Підтримка послуги визначення ідентифікатора абонента Caller ID у різних провайдерів може відрізнятися. Коли дзвінок йде на номер місцевої мережі від якогось VoIP-провайдера, послуга визначення caller ID не підтримується.

У деяких випадках VoIP-провайдери можуть дозволити людині, що дзвонить, імітувати якийсь не належний йому caller ID, потенційно даючи можливість демонструвати такий ID, який фактично не є номером абонента. Комерційне VoIP-обладнання та програмне забезпечення зазвичай легко дає можливість змінювати інформацію caller ID. Незважаючи на те, що ця послуга може забезпечити величезну свободу дій, вона також дає можливість для зловживань [60; 265].

Взагалі VoIP з'єднання має цілий ряд параметрів, загальноприйнятих як точні показники оцінки якості з'єднання. Крім того, більшість існуючих операторів IP-телефонії при наданні послуг дозволяють навіть вибирати вузол, через який пройде дзвінок, не тільки керуючись ціною, а й додатковим статистичними параметрами, що характеризують якість зв'язку: ASR – відношення кількості обслужених дзвінків до числа спроб зателефонувати у відсотках. Характеризує найкращий дозвін, ACD – середня тривалість дзвінків через вузол на даний напрямок, відсоток дзвінків, що відбулися з тривалістю менше 30 секунд – характеризує найбільш стійкий зв'язок під час розмови.

Іноді операторами зв'язку для оцінки напряму застосовуються й інші статистичні параметри: затримка після набору PDD, відсоток втрати пакетів QoS, максимальне наростання викликів у секунду CPS.

Отже, виходячи з цього, проблеми якості зв'язку можна вирішити, здійснивши оцінку основним характеристикам: рівню спотворення голосу; частоті пропажі голосових пакетів; часу затримки між проголошенням фрази першого абонента і моментом, коли вона буде почута другим абонентом [232]. Ефективність і надійність роботи мережного комплексу як корпоративної мережі підприємства, так і робочої групи, територіально-розподілена телекомунікаційна інфраструктура або система доступу віддалених користувачів, багато в чому визначається правильністю вибору і застосування тієї чи іншої технології передачі даних, конкретного обладнання та його конфігурації.

Одне з найбільш складних питань, яке виникає перед керівником підприємства або організації – це інформаційна система, здатна вирі-

шити існуючі та майбутні цілі та завдання компанії, а також відповідати потребам кожного співробітника відповідно до його посадових обов'язків. Перед початком розробки конкретного рішення необхідно провести обстеження об'єкта. До поняття обстеження входить повний цикл робіт, до яких належать:

• передпроектне обстеження, яке дозволяє виявити основні потреби для створення комунікаційної мережі;

• розробка архітектури корпоративної інформаційної системи та при необхідності її моделювання, дозволяє схематично показати, яким чином буде виконуватись підключення усіх вузлів комунікаційної мережі;

• вибір продуктів, необхідних для її створення, під час створення комунікаційної мережі використовуються апаратні та програмні засоби, які відповідають основним потребам.

7.2. Вирішення задачі моделювання комунікаційної мережі на основі системи ASTERISK

За допомогою методу аналізу ієрархій проведено порівняння за найбільш важливими технічними та експлуатаційними параметрами основних апаратно-програмних комунікаційних систем для забезпечення функціонування корпоративної мережі обміну інформацією. Практичні розрахунки за створеною моделлю визначили доцільність використання комплексу Asterisk.

Зазвичай задачу прийняття технічних рішень прийнято ділити на такі етапи: формування цілей вибору, покупка виробів і вибір напряму проектування організації виробництва; формування альтернатив, тобто складання списку об'єктів, які передбачається порівнювати між собою, щоб зробити вибір; формування системи критеріїв; формування вирішальних правил, за допомогою яких проводяться парні порівняння; розстановка і синтез пріоритетів; визначення зважених показників якості з урахуванням напряму вибору.

Метод аналізу ієрархій – математична процедура ієрархічного уявлення критеріїв, що визначають суть проблеми. Метод полягає в розподілі проблеми на все більш прості складові частини і подальшого відпрацювання послідовності суджень по парним порівнянням об'єктів

вибору. В результаті знаходження відносної ступеня взаємодії елементів у системі, сформульовані судження отримують кількісні оцінки.

Метод аналізу ієрархій включає: процедури синтезу безлічі суджень, отримання пріоритетності критеріїв, знаходження альтернативних рішень. Завдання вирішується на основі поетапного встановлення пріоритетів. На першому етапі виявляються найбільш важливі елементи проблеми. На другому етапі перебуває найкращий спосіб оцінки параметрів. Далі виробляється спосіб застосування рішення.

Цей процес багаторазово повторюють, уточнюють, переглядають до тих пір, поки не з'явиться впевненість у тому, що охоплені всі важливі характеристики, що визначають вирішення проблеми вибору. Передбачається, що інтуїція і суб'єктивні судження є основним вихідним матеріалом, на підставі якого виходить уявлення про перевагу одного елемента над іншим [62; 116].

Принцип ідентичності та композиції передбачає структурування проблеми у вигляді ієрархії. У найбільш простому вигляді ієрархія будується з вершини через проміжні рівні до самого низького рівня, яким зазвичай є перелік альтернатив. Ієрархія вважається повною, якщо кожен елемент заданого рівня діє як критерій для всіх елементів нижче стоячого рівня. В іншому випадку ієрархія – неповна.

Закони ієрархічної безперервності вимагають, щоб елементи нижнього рівня ієрархії були попарно порівнянні за відношенням до елементів наступного рівня.

Після формування системи критеріїв у вигляді ієрархії виникають природні питання установки пріоритетів критеріїв та оцінки альтернатив за цим критерієм з метою виявлення найважливішою з них.

Найбільш доцільно організувати парні порівняння по відношенню до їх впливу, а результати порівнянь представити в формі матриці (табл. 7.1).

Таблиця 7.1

Результати порівнянь

	A_1	A_2	A_3	A_4
A_1	W_1/W_1	W_1/W_2	W_1/W_3	W_1/W_4
A_2	W_2/W_1	W_2/W_2	W_2/W_3	W_2/W_4
A_3	W_3/W_1	W_3/W_2	W_3/W_3	W_3/W_4
A_4	W_4/W_1	W_4/W_2	W_4/W_3	W_4/W_4

=

	A	B	C	D
A	a_{11}	a_{12}	a_{13}	a_{14}
B	a_{21}	a_{22}	a_{23}	a_{24}
C	a_{31}	a_{32}	a_{33}	a_{34}
D	a_{41}	a_{42}	a_{43}	a_{44}

Ця матриця мати властивості зворотно симетричної матриці, тобто: $a_{ij}=1/a_{ij}$, де індекси *i* та *j* відносяться до рядка і стовпця відповідно.

Рядки та стовпці утворюють "вектор" матриці.

Квадратна матриця характеризується власним вектором і власними значеннями, спосіб обчислення цих характеристик визначає спосіб кількісного визначення порівняльної важливості критеріїв [62; 116].

Оскільки a_{11}, a_{12}, ..., a_{ij} невідомі заздалегідь, то попарні порівняння елементів виробляються з використанням суб'єктивних суджень та чисельного оцінювання за шкалою важливості.

Результати порівняння заносяться в матрицю, рядки і стовпці якої утворюють альтернативи порівнюваних між собою елементів.

На основі даних заповненої таблиці формується набір локальних пріоритетів, які виражають відносний вплив критеріїв якості на вибір кращого об'єкта порівняння, для цього організується обчислення власних векторів матриці, а потім нормалізуються результати до одиниці, отримуючи тим самим шуканий вектор пріоритетів, який і розставляє порівнювані об'єкти за значенням [62; 116].

Для обчислення власних векторів існує безліч прийомів. Одним з найкращих є знаходження геометричного середнього.

Це виходить при перемножуванні елементів у кожному рядку і витягом з добутку кореня N-го ступеня, де N – кількість елементів.

Отриманий таким способом стовпець нормалізується діленням кожного числа на суму всіх чисел, що наведено в табл. 7.2.

Таблиця 7.2

Оцінка векторів пріоритетів

	Матриця				Обчислення оцінок компонент власного вектора за рядками	Нормалізація вектора пріоритетів
N	A_1	A_2	A_3	A_4		
A_1	W_1/W_1	W_1/W_2	W_1/W_3	W_1/W_4	$\sqrt[4]{\frac{W_1}{W_1}\cdot\frac{W_1}{W_2}\cdot\frac{W_1}{W_3}\cdot\frac{W_1}{W_4}}=a$	$X_1= a/F$
A_2	W_2/W_1	W_2/W_2	W_2/W_3	W_2/W_4	$\sqrt[4]{\frac{W_2}{W_1}\cdot\frac{W_2}{W_2}\cdot\frac{W_2}{W_3}\cdot\frac{W_2}{W_4}}=b$	$X_2= b/F$
A_3	W_3/W_1	W_3/W_2	W_3/W_3	W_3/W_4	$\sqrt[4]{\frac{W_3}{W_1}\cdot\frac{W_3}{W_2}\cdot\frac{W_3}{W_3}\cdot\frac{W_3}{W_4}}=c$	$X_3= c/F$
A_4	W_4/W_1	W_4/W_2	W_4/W_3	W_4/W_4	$\sqrt[4]{\frac{W_4}{W_1}\cdot\frac{W_4}{W_2}\cdot\frac{W_4}{W_3}\cdot\frac{W_4}{W_4}}=d$	$X_4= d/F$
					$\sqrt[4]{\frac{W_4}{W_1}\cdot\frac{W_4}{W_2}\cdot\frac{W_4}{W_3}\cdot\frac{W_4}{W_4}}=d$	

$F=W(a+b+c+d)$

Процес вибору кращого виробу залежить від способу формування системи критеріїв і обмежень, що накладаються на їх вибір. Критерії можуть бути за значимістю рівнозначні, нерівнозначні, утворювати багаторівневу розгалужену структуру – ієрархії.

У простому випадку критерії можна вважати рівними за своєю значимістю і тоді вибір кращого (прийнятного варіанта) знаходиться згідно з алгоритмом (рис. 7.1). В іншому випадку – виконується інший алгоритм (рис. 7.2).

Якщо критерії є багаторівневою ієрархічною структурою, то в цьому випадку на кожному рівні організується процес ранжування критеріїв даного рівня і знаходження відповідних локальних пріоритетів об'єктів порівняння [62; 116].

Для проведення парних порівнянь об'єктів аналізу використовується шкала відносної важливості, показана в табл. 7.3.

Оцінки починають з лівого верхнього елемента матриці і задаються питання – який з об'єктів важливіший (кращий).

При порівнянні елемента із самим собою відношення дорівнює одиниці. Якщо перший об'єкт важливіше, ніж другий, то використовується ціле число зі шкали, що наведено у табл. 7.3.

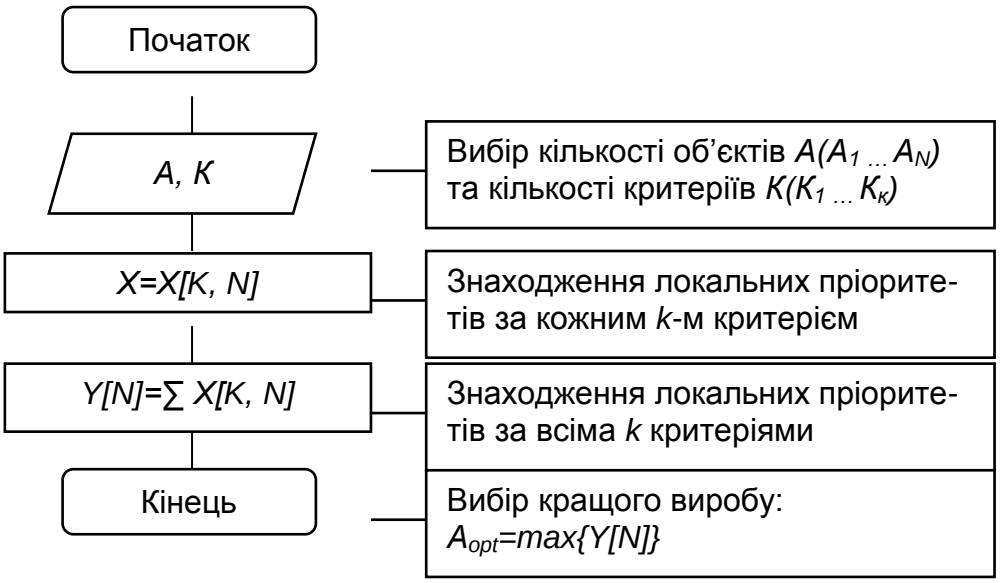


Рис. 7.1. **Вибір за рівнозначними критеріями**

Рис. 7.2. **Вибір за нерівнозначними критеріями**

Зворотні один до одного відносини заносяться в симетричні позиції матриці. Утворюється позитивна зворотно-симетрична матриця, і треба зробити *(N-1)*N/2* суджень, де *N* – загальне число порівнюваних об’єктів.

Таблиця 7.3

Шкала показників відношень

Інтенсивність відношень важності	Визначення	Пояснення
1	Рівна важність	Однаковий внесок двох видів діяльності до мети
3	Помірна перевага одного над іншим	Досвід і судження дають легку перевагу одному виду діяльності над іншим
5	Значна або сильна перевага	
7	Значна перевага	Одному виду діяльності надається сильна перевага, що він стає практично значним
9	Дуже сильна перевага	Очевидна перевага одного виду діяльності над іншими підтверджується найбільш сильно
2; 4; 6; 8;	Проміжні рішення між сусідніми визначеннями	Застосовується у компромісних випадках
Зворотні величини чисел	Якщо при порівнянні одного виду діяльності з іншим отримано одне з зазначених чисел, то при порівнянні другого типу діяльності з першим отримаємо зворотну величину	

Оскільки оцінки, зроблені в результаті суб'єктивних суджень – бали, призначаються самим проектувальником у співвідношенні до його смаків і внутрішніх переконань, то існує необхідність зробити перевірку узгодженості оцінок.

Для цього обчислюється індекс узгодженості, який характеризує порушення цієї узгодженості [62; 116].

В основі такої операції лежить аргумент про те, що всі вимірювання, в яких використовуються прилади, містять похибки вимірювань.

Вони пов'язані насамперед з неточністю вимірювальних приладів та неточностями самих вимірювань.

Ці похибки призводять до неузгодженості результатів. Наприклад, при зважуванні виявилося, що предмет А важче, ніж предмет Б, Б важче за В, а В важче за А. Це можливо, коли ваги А, Б, В близькі, а точність порівняна з різницею їх ваг.

Спосіб оцінки узгодженості такий. Слід підсумувати кожен стовпець суджень S_i:

$$S_i = \sum_{i=1}^{N} a_{ij};\ j = const.$$

Сума першого стовпця збільшується на величину першої компоненти нормалізованого вектора пріоритетів X_i: $Z_i = S_i \cdot X_i$.

Складаються отримані значення: $\lambda_{max} = \sum_{i=1}^{N} Z_i$.

Знаходиться індекс узгодженості за формулою: $\alpha = \frac{\lambda_{max} - N}{N - 1}$.

Для обернено-симетричної матриці завжди $\lambda_{max} \geq N$.

Тепер необхідно порівняти α з тією, яка могла бути отримана при випадковому виборі суджень зі списку 1/9, 1/8, 1/7 ... 1, 2, 3, ..., 9 при формуванні обернено-симетричної матриці.

Середні дані узгодженості для випадкової матриці різного порядку наведені в табл. 7.4.

Таблиця 7.4

Середні дані узгодженості

Розмір матриці *N*	1	2	3	4	5	6	7	8
Узгодженість *γ*	0	0	0,58	0,9	1,12	1,24	1,32	1,41
Розмір матриці *N*	9	10	11	12	13	14	15	16
Узгодженість *γ*	1,45	1,49	1,51	1,54	1,56	1,57	1,59	1,60

Якщо розділити індекс узгодженості α на число γ, що відповідає випадковій узгодженості матриці того ж порядку γ, то отримаємо відношення узгодженості $\beta=\alpha/\gamma$.

На β накладаються умови: $\beta = \begin{cases} \leq 0{,}1 – \text{добре співвідношення}; \\ \leq 0{,}2 – \text{співвідношення, що задовольняє} \\ > 0{,}2 – \text{погане співвідношення}. \end{cases}$

При γ>0,2 треба досліджувати задачу знову і перевірити судження. Критерії порівняння обраних корпоративних систем наведені на рис. 7.3.

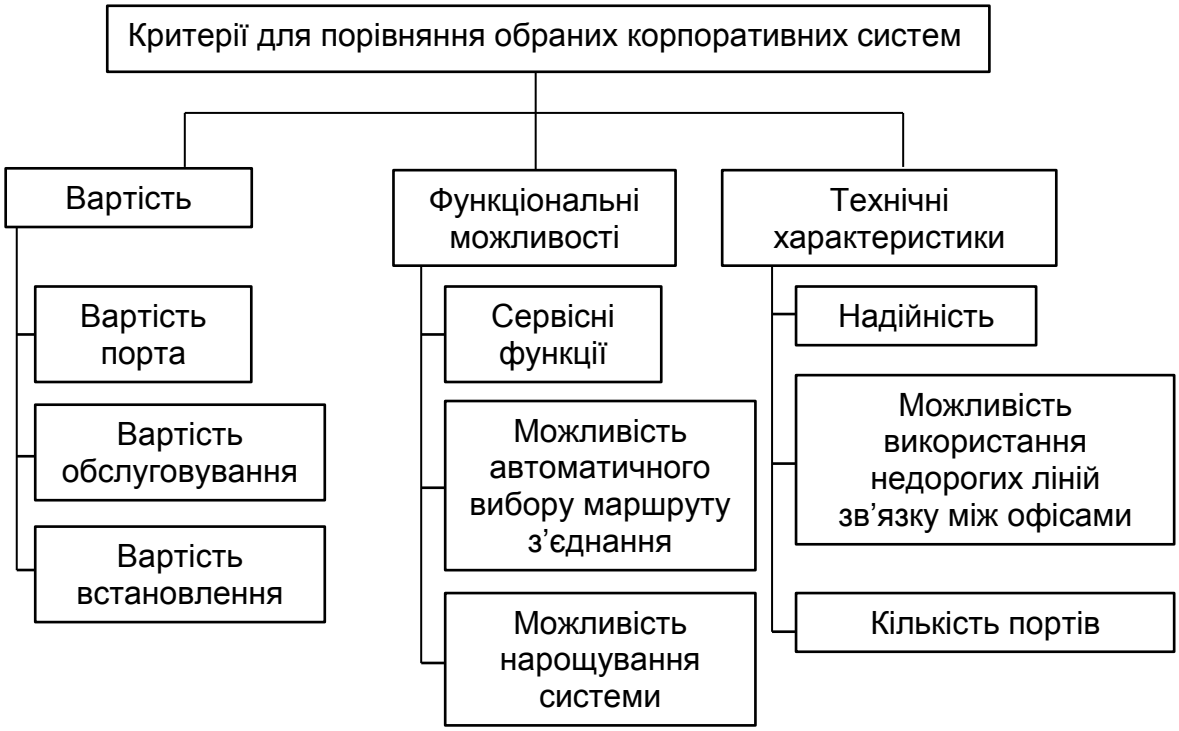


Рис. 7.3. **Критерії порівняння обраних корпоративних систем**

Існує багато готових апаратних систем, які можна підключити до системи Asterisk. Варіанти апаратних систем запропоновані у табл. 7.5. Ці системи обрані у співвідношенні функціональних спроможностей до ціни Asterisk.

Цей програмний комплекс дозволяє поєднати апаратну та програмну складові системи для організації комунікаційної мережі.

Він дозволяє коректно розподіляти дзвінки, вести статистику телефонних розмов, також покращити робочий процес співробітників підприємства та підвищити рівень обслуговування клієнтів [62; 116].

Таблиця 7.5

Моделі систем бізнес телефонії

Модель системи	Ємність портів	Виробник	Вартість, $/порт	Конфігурація	Засіб комутації
2N 400	до 23000	Alcaltel	от 130	Розширюється	Гібридний
YealinkMyPBX V3	до 5	Yealink	от 90	Розширюється	Гібридний
OmniPC X4400	до 50000	Alcaltel	от 150	Розширюється	Гібридний
Tele Vantage	до 264	Artisoft	от 100	Розширюється	Гібридний

Маючи групу, запропоновану з 4-х моделей систем, можна виконати вибір з групи однієї найбільш оптимальної системи з порівнянням варіантів за різними складовими (табл. 7.6 – 7.8).

Таблиця 7.6

Порівняння варіантів за поданням сервісних функцій

	2N 400	YealinkMy	OmniPC	Tele Vantage	$(Па_{ij})^{(1/4)}$	*X(i)=*	*S(i)*x(i)*
2N 400	1.0000	0.3333	0.5	0.3333	0.485	0.11	0.99
YealinkMy	3	1.0000	2	1	1.565	0.351	0.994
OmniPC	2	0.5	1.0000	0.5	0.841	0.188	1.034
Tele Vantage	3	1	2	1.0000	1.565	0.351	0.994
	S1 = 9	*S2* = 2.83	*S3* = 5.5	*S4* = 2.8333	*SU* = 4.45	1	λ_{max} = 4.01
	γ = 0.9	α = 0.004	β = 0.0044				

Таблиця 7.7

Порівняння варіантів за автоматичним вибором маршруту

	2N 400	YealinkMy PBX V3	OmniPC X4400	Tele Vantage	$Па_{ij}^{(1/4)}$	X(i)=	S(i)*x(i)
2N 400	1.0000	0.3333	0.5	0.3333	0.485	0.11	0.99
YealinkMyPBX V3	3	1.0000	2	1	1.565	0.351	0.994
OmniPC X4400	2	0.5	1.0000	0.5	0.841	0.188	1.034
Tele Vantage	3	1	2	1.0000	1.565	0.351	0.994
	S1 = 9	S2 = 2.833	S3 = 5.5	S4 = 2.8333	SU = 4.46	1	λ_{max} = 4.01
	γ = 0.9	α = 0.004	β = 0.0044				

Таблиця 7.8

Порівняння варіантів за можливістю розширення системи

	2N 400	YealinkMyPBX V3	OmniPC X4400	Tele Vantage	$Па_{ij}$^(1/4)	X(i)=	S(i)*x(i)
2N 400	1.0000	0.3333	1	0.25	0.537	0.112	1.008
YealinkMyPBX V3	3	1.0000	3	1	1.732	0.36	0.96
OmniPC X4400	1	0.3333	1.0000	0.25	0.537	0.112	1.008
Tele Vantage	4	1	4	1.0000	2	0.416	1.04
	S1 = 9	S2 = 2.67	S3 = 9	S4 = 2.5	SU = 4.81	1	λ_{max} = 4.02
	γ = 0.9	α =0.0053	β = 0.0059				

Слід визначити пріоритет локальних критеріїв за функціональними спроможностями (табл. 7.9).

Таблиця 7.9

Розрахунок показників пріоритетів локальних критеріїв за функціональними спроможностями

	Сервісні функції	Можливість автоматичного вибору маршруту	Можливість розширення системи	$Па_{ij}$^(1/4)	X(i)	S(i)*x(i)
Сервісні функції	1.0000	0.5	0.333	0.55	0.168	1.006
Можливість автоматичного вибору маршруту	2	1.0000	2	1.587	0.484	0.967
Можливість розширення системи	3	0.5	1.0000	1.145	0.349	1.612
	S1 = 6	S2 = 2	S3 = 3.333	SU = 3.28	1	λ_{max}=3.12
	γ = 0.58	α = 0.067	β = 0.11			

Порівняння варіантів за технічними характеристиками наведено в табл. 7.10 – 7.12.

Таблиця 7.10

Розрахунок коефіцієнта надійності

	2N 400	YealinkMyPBX V3	OmniPC X4400	Tele Vantage	$Па_{ij}$^(1/4)	X(i)=	S(i)*x(i)
2N 400	1.0000	0.5	1	0.3333	0.639	0.144	1.008
YealinkMyPBX V3	2	1.0000	2	1	1.414	0.32	0.96
OmniPC X4400	1	0.5	1.0000	0.3333	0.639	0.144	1.008
Tele Vantage	3	1	3	1.0000	1.732	0.392	1.045
	S1 = 7	S2 = 3	S3 = 7	S4 = 2.6666	SU = 4.42	1	λ_{max} = 4.02
	γ = 0.9	α = 0.007	β = 0.0078				

Таблиця 7.11

Розрахунок коефіцієнта можливості використання недорогих ліній для з'єднання між офісами

	2N 400	YealinkMy PBX V3	OmniPC X4400	Tele Vantage	$Па_{ij}$^(1/4)	X(i)=	S(i)*x(i)
2N 400	1.0000	0.5	1	0.5	0.707	0.165	0.99
YealinkMyPBX V3	2	1.0000	2	2	1.682	0.393	0.9825
OmniPC X4400	1	0.5	1.0000	0.5	0.707	0.165	0.99
Tele Vantage	2	0.5	2	1.0000	1.189	0.277	1.108
	S1 = 6	S2 = 2.5	S3 = 6	S4 = 4	SU= 4.26	1	λ_{max} =4.07
	γ = 0.9	α = 0.024	β = 0.0263				

Таблиця 7.12

Розрахунок показника кількості портів

	2N 400	YealinkMy PBX V3	OmniPC X4400	Tele Vantage	$Па_{ij}$^(1/4)	X(i)=	S(i)*x(i)
2N 400	1.0000	2	0.5	0.2	0.669	0.122	1.037
YealinkMyPBX V3	0.5	1.0000	0.333	0.2	0.427	0.078	0.858
OmniPC X4400	2	3	1.0000	0.2	1.047	0.191	1.305
Tele Vantage	5	5	5	1.0000	3.344	0.609	0.974
	S1 = 8.5	S2 = 11	S3 = 6.833	S4 = 1.6	SU = 5.487	1	λ_{max} = 4.2
	γ = 0.9	α = 0.058	β = 0.064				

Слід визначити пріоритет локальних критеріїв за технічними характеристиками (табл. 7.13).

Таблиця 7.13

Розрахунок показників пріоритетів локальних критеріїв за технічними характеристиками

	Надійність	Можливість використання недорогих ліній зв'язку між офісами	Кількість портів	$Па_{ij}$^(1/4)	X(i)=	S(i)*x(i)
Надійність	1.0000	3	4	2.289	0.625	0.99
Можливість використання недорогих ліній зв'язку між офісами	0.333	1.0000	2	0.874	0.238	1.073
Кількість портів	0.250	0.5000	1.0000	0.5	0.137	0.956
	S1 = 1.583	S2 = 4.5	S3 = 7	SU = 3.66	1	λ_{max} = 3.02
	γ = 0.58	α = 0.009	β = 0.016			

Порівняння за економічним критерієм наведені в табл. 7.14 – 7.16.

Таблиця 7.14

Розрахунок показників вартості порту

	2N 400	YealinkMy PBX V3	OmniPC X4400	Tele Vantage	$Па_{ij}$^(1/4)	X(i)=	S(i)*x(i)
2N 400	1.0000	2	6	9	3.224	0.531	0.944
YealinkMyPBX V3	0.5	1.0000	5	7	2.045	0.337	1.127
OmniPC X4400	0.167	0.2	1.0000	2	0.508	0.083	1.038
Tele Vantage	0.111	0.143	0.5	1.0000	0.298	0.049	0.931
	S1 = 1.778	S2 = 3.34	S3 = 12.5	S4 = 19	SU = 6.075	1	λ_{max} = 4.04
	γ = 0.9	α= 0.013	β = 0.014				

Таблиця 7.15

Розрахунок показників вартості обслуговування

	2N 400	YealinkMy PBX V3	OmniPC X4400	Tele Vantage	$Па_{ij}$^(1/4)	X(i)=	S(i)*x(i)
2N 400	1.0000	0.5	2	5	1.495	0.288	1.066
YealinkMyPBX V3	2	1.0000	3	7	2.546	0.49	0.968
OmniPC X4400	0.5	0.333	1.0000	3	0.841	0.162	1.026
Tele Vantage	0.2	0.143	0.333	1.0000	0.312	0.06	0.96
	S1 = 3.7	S2 = 1.976	S3 = 6.333	S4 = 16	SU = 5.194	1	λ_{max} = 4.02
	γ = 0.9	α = 0.007	β = 0.0074				

Таблиця 7.16

Розрахунок показників вартості установки

	2N 400	YealinkMy PBX V3	OmniPC X4400	Tele Vantage	$Па_{ij}$^(1/4)	X(i)=	S(i)*x(i)
2N 400	1.0000	0.5	0.5	2	0.841	0.189	1.04
YealinkMyPBX V3	2	1.0000	1	3	1.565	0.351	0.994
OmniPC X4400	2	1	1.0000	3	1.565	0.351	0.994
Tele Vantage	0.5	0.333	0.333	1.0000	0.485	0.109	0.981
	S1 = 5.5	S2 = 2.833	S3 = 2.833	S4 = 9	SU= 4.456	1	λ_{max} = 4.009
	γ = 0.9	α = 0.003	β = 0.0033				

Слід визначити пріоритет локальних критеріїв за економічним критерієм (табл. 7.17).

Таблиця 7.17

Розрахунок показників пріоритетів локальних критеріїв за економічним критерієм

	Вартість порту	Вартість обслуговування	Вартість установки	$Па_{ij}$^(1/4)	X(i)=	S(i)*x(i)
Вартість порту	1.0000	6	5	3.107	0.722	0.986
Вартість обслуговування	0.167	1.0000	3	0.794	0.184	1.352
Вартість установки	0.2	0.333	1.0000	0.405	0.094	0.847
	S1 = 1.367	S2 = 7.333	S3 = 9	SU = 4.306	1	λ_{max} = 3.185
	γ = 0.58	α = 0.093	β = 0.16			

Виконаємо порівняння критеріїв за значимістю (табл. 7.18).

Таблиця 7.18

Порівняння критеріїв за значимістю

	Функціональні можливості	Технічні характеристики	Економічний критерій	$Па_{ij}$^(1/4)	X(i)=	S(i)*x(i)
Функціональні можливості	1.0000	0.250	0.5	0.5	0.149	1.046
Технічні характеристики	4	1.0000	0.5	1.26	0.376	1.223
Економічний критерій	2	2	1.0000	1.587	0.474	0.948
	S1 = 7	S2 = 3.250	S3 = 2	SU = 3.347	1	λ_{max} = 3.22
	γ = 0.58	α = 0.109	β= 0.187			

Для обрання оптимальної системи слід виконати необхідні порівняння варіантів за різними складовими вибору (табл. 7.19 – 7.22).

Таблиця 7.19

Результат порівняння варіантів за функціональними можливостями

	Сервісні функції	Можливість автоматичного вибору маршруту	Можливість розширення системи	Всього
2N 400	0.437766	0.437766	0.44788	1.323412
YealinkMyPBX V3	1.408	1.408	1.448	4.264
OmniPC X4400	0.759	0.759	0.44788	1.96588
Tele Vantage	1.408	1.408	1.672	4.488

Таблиця 7.20

Результат порівняння варіантів за технічними характеристиками

	Надійність	Можливість використання недорогих ліній зв'язку між офісами	Кількість портів	Всього
2N 400	0.578536	0.665	0.4953	1.738836
YealinkMyPBX V3	1.288	1.607	0.324403	3.219403
OmniPC X4400	0.578536	0.665	0.7908	2.034336
Tele Vantage	1.576	1.1335	2.564	5.2735

Таблиця 7.21

Результат порівняння варіантів за економічним критерієм

	Вартість порту	Вартість обслуговування	Вартість установки	Всього
2N 400	2.144	1.157	0.758	4.059
YealinkMyPBX V3	1.3605	1.972	1.407	4.7395
OmniPC X4400	0.337077	0.64917	1.407	2.393247
Tele Vantage	0.197632	0.241616	0.437266	0.876514

Таблиця 7.22

Розрахунок загальної суми за критеріями

	Порівняння варіантів за функціональним спроможностям	Порівняння варіантів за технічними характеристиками	Порівняння варіантів за економічним критерієм	Всього
2N 400	1.323412	1.738836	4.059	7.121248
YealinkMyPBX V3	4.264	3.219403	4.7395	12.222903
OmniPC X4400	1.96588	2.034336	2.393247	6.393463
Tele Vantage	4.488	5.2735	0.876514	10.638014

Внаслідок виконання розрахунків з вибору системи бізнес-телефонії методом ієрархій оптимальною є система YealinkMyPBX V3, яка відповідає функціональним потребам та вартості. Метод ієрархії дозволяє використовувати будь-який тип та кількість характеристик під час вибору в даному випадку подібних систем. Але існують деякі недоліки з точки зору вибору системи бізнес-телефонії. Цей метод дозволяє обрати лише якусь конкретну систему, яка вже складається з апаратних модулів, і додати якісь ще необхідні зовнішні модулі за потребою користувача можливості немає. Можна використовувати лише ті модулі, які пропонує виробник, в ході цього з'являється потреба у спеціалісті, який буде виконувати роботу по заміні чи встановленні модулів у систему. Заміна модулів потребує відключення системи, що тягне за собою збої у комунікаційній мережі підприємства, а це в свою чергу тягне втрату довіри клієнтів, якість обслуговування та обмеженість в комунікаціях з точки зору телефонії.

Тому пропонується створення зовнішньо-модульної комунікаційної мережі. Пристрої, що забезпечують телефонну комунікацію, придбаються окремо, не залежно один від одного. В такому випадку якщо якийсь пристрій вийшов з ладу, його можна замінити не перериваючи робочого процесу. Лише в одному випадку зовнішньо-модульна комунікаційна мережа може втратити працездатність, коли вийде з ладу системний блок, але проблему можна легко вирішити, це придбати другий системний блок для підстрахування, але як показує практика, це буває дуже рідко. Придбання другого системного блоку – це набагато дешевше ніж придбати другу готову систему типу YealinkMyPBX V3, до того ж деякі пристрої зовнішньо-модульної комунікаційної мережі можуть працювати автономно, тобто без підключення до системного блоку. А це надає більше шансів не втратити довіру клієнтів, понести менші втрати при обслуговування клієнтів та робочому процесі співробітників.

7.3. Практичне моделювання комунікаційної мережі та його результати

Проведено практичне проектування корпоративної інформаційно-комунікаційної системи на базі комплексу Asterisk з урахуванням вимог замовника до технічних характеристик системи в цілому та її елементів, забезпечення необхідних функціональних можливостей, вартісних вимог та обмежень.

Сучасні комунікаційні мережі потребують гнучких схем організації такого типу мереж. Це пов’язано з тим, що темпи розвитку технологій зростають з кожним днем, отже і постійно вдосконалюється виробництво пристроїв, в тому ж числі і для IP-телефонії. Разом з цим зростають потреби підприємств щодо внесення змін у корпоративні мережі, направлені на покращення якості роботи працівників та якості надання послуг клієнтам. Отже, разом із потребами організацій з’являються потреби в архітектурних змінах комунікаційних мереж підприємств.

Метод ієрархій направлений на оптимальний вибір конкретної системи бізнес-телефонії. У контексті конкретної системи розуміється комплекс готових апаратних засобів, які утворюють єдиний модуль. Цей метод не дозволяє обрати окремі модулі бізнес-телефонії та поєднати їх у одне ціле. Дуже часто з’являється потреба, коли необхідно використовувати лише визначені апаратні модулі, це пояснюється зменшенням витрат на організацію комунікаційної мережі та використання лише потрібних модулів. Іноді буває, що організована комунікаційна мережа підприємства використовується лише на 50 – 60 % відсотків можливостей бізнес-телефонії, але початкові витрати були дещо більше ніж потрібно [62; 116].

Пропонується метод, який дозволяє більш детально та оптимально організувати апаратний комплекс, що відповідає потребам підприємства. Цей метод потребує меншого часу на виконання розрахунків ніж метод ієрархій, цим саме зменшуються витрати вже на початковому етапі розробки комунікаційної мережі.

Завдання прийняття технічних рішень прийнято ділити на етапи.

Вибір напряму проектування комунікаційної мережі підприємства, тобто необхідно виявити функції, які буде виконувати створювана система, також необхідно виявити види пристроїв, що будуть застосовуватись.

Формування альтернатив, тобто складання списку об’єктів, які передбачається порівнювати між собою, щоб зробити вибір. Формування системи критеріїв. Розстановка і синтез пріоритетів. Визначення складу системи внаслідок розрахованих показників.

Метод вибору системи бізнес-телефонії, що пропонується, можна назвати як метод вибору модульних компонентів системи, саме завдяки оптимально розрахованим окремим компонентам можна отримати апаратну систему бізнес-телефонії, що відповідає потребам конкретного підприємства. Метод вибору модульних компонентів – математична проце-

дура лінійного уявлення критеріїв, що визначають суть проблеми. Метод полягає в розподілі проблеми на все більш прості складові частини і подальшого відпрацювання послідовності суджень по парним порівнянням об'єктів вибору. В результаті знаходження відносного ступеня взаємодії елементів у системі, сформульовані судження отримують кількісні оцінки.

Завдання вирішується на основі встановлення пріоритетів кожного із критеріїв. На першому етапі виявляються найбільш важливі елементи проблеми. На другому етапі перебуває найкращий спосіб оцінки параметрів. Передбачається, що інтуїція і суб'єктивні судження є основним вхідним матеріалом, на підставі якого виходить уявлення про перевагу одного елемента над іншим. Далі знаходиться середнє значення оцінки критеріїв за кожним елементом. У результаті обирається той елемент, який має найбільше значення оцінки.

Спочатку необхідно розподілити складову систему на окремі модулі за типами приклад зображено на рисунку 7.4. Кожний тип складається з декількох елементів, які за критеріями приблизно схожі між собою. Кількість елементів обирається спеціалістом. Оцінка за критеріями відбувається за такою шкалою, максимальний показник шкали оцінювання становить кількість елементів у групі. Оцінювання виконується відповідно до змісту критерію, оцінки елементів за одним критерієм можуть бути однаковими. Якщо елемент не відповідає на зміст або не несе ніякого змісту критерію, то він оцінюється в нуль. Після того, як оцінку критеріїв зроблено, розраховується середня оцінка кожного елемента групи, результатом оптимального розрахунку є елемент, який має найвищий показник середньої оцінки у групі.

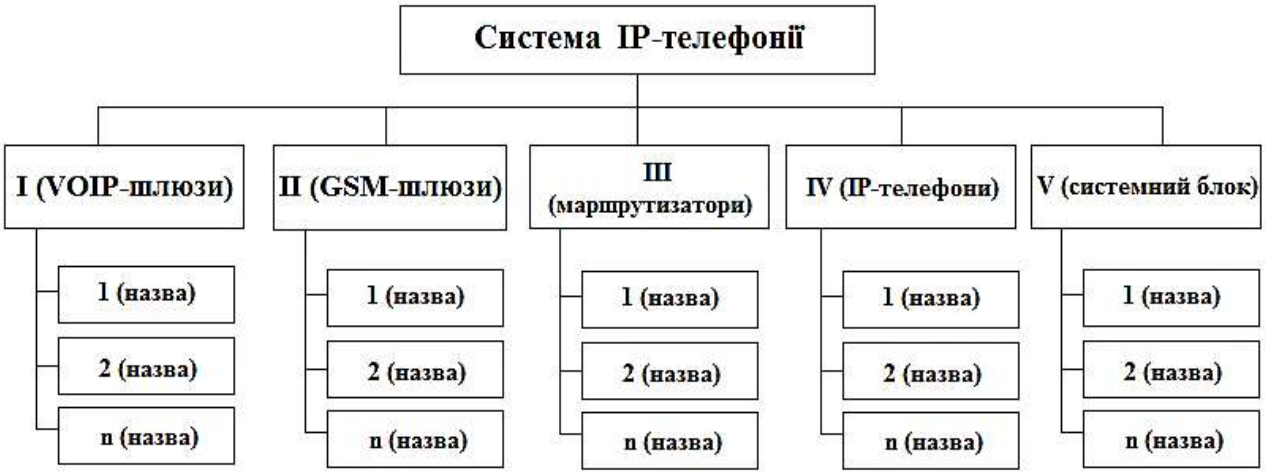


Рис. 7.4. **Розподілення системи на окремі групи модулів**

Для розрахунку вартості системи бізнес-телефонії варто виділити основні критерії, за допомогою яких можна виконувати оцінку модулів:

- складність налаштування (чим складніше налаштовувати, тим більша оцінка);
- наявність портів (якщо всі порти присутні, що необхідні для повноцінної роботи комунікаційної мережі, ставиться максимальна оцінка, якщо відсутній хоча б один потрібний порт, ставиться нуль, інші оцінки ставляться на думку експерта);
- якість зв'язку (якщо якість телефонної розмови ідеальна без перешкод ставиться максимальна оцінка, інші оцінки ставляться на думку експерта);
- можливість розширення (якщо є можливість даний модуль розшири, збільшити його функціональні можливості необхідно поставити оцінку 1, якщо модуль подібних можливостей немає ставиться 0);
- надійність (якщо модуль надійний – ставиться максимальна оцінка, інші оцінки ставляться на думку експерта);
- інтеграція з Asterisk (якщо є можливість, то даний модуль можливо інтегрувати з системою Asterisk необхідно поставити оцінку 1, якщо модуль подібних можливостей немає ставиться 0);
- відносна вартість (якщо цей модуль має низьку ціну порівняно з іншими, то необхідно поставити найбільшу оцінку (яка відповідає кількості модулів у групі), а найдорожчому модулю треба встановити найменшу оцінку, тобто 1, оцінка інших модулів виконується згідно з оцінкою найдорожчого та найдешевшого).

Оптимальним модулем у групі є той, коефіцієнт середньої оцінки якого є найбільшим.

Отримані на виході кожної групи модулі складають оптимальну систему бізнес-телефонії, які мають співвідношення якості до ціни.

Слід розглянути створення комунікативної мережі на основі локальної мережі, яка б могла відповідати таким вимогам:

- співвідношення ціни пристроїв до їх якості;
- наявність мобільних номерів операторів, за допомогою яких можна приймати вхідні дзвінки від клієнтів та робити вихідні дзвінки, використовуючи оператора відповідно набраного номера, можливість підключення ще одного мобільного оператора передбачити;
- наявність двох міських ліній, за допомогою яких можна приймати дзвінки від клієнтів та робити вихідні дзвінки на міські та міжміські номери;

- у відділі маркетингу повинно бути встановлено 2 IP-телефони з внутрішніми номерами 1001 та 1002 та два стаціонарних радіотелефони із номерами 701 та 702;
- у відділах електронної комерції та розробників під Android системи по одному IP-телефону із номерами 1003 та 1004 відповідно;
- у відділі технічної підтримки встановити два IP-телефони з номерами 1005 та 1006 відповідно;
- у відділі розробників встановити один IP-телефон з номером 1007;
- у відділі керівників встановити один IP-телефон з номером 1000;
- передбачити можливість підключення одного внутрішнього номера (1008) із зовнішньої мережі Інтернет;
- для всіх вхідних дзвінків у робочий час з 9.00 до 17.00 програвати голосове привітання та надати можливість клієнту обрати відділ, в який він хоче подзвонити (натиснути 1, щоб потрапити до відділу маркетингу, 2 – до відділу технічної підтримки, 3 – до відділу електронної комерції, 4 – до відділу керівників), якщо клієнт подзвонив у неробочий час або вихідний день програвати голосове повідомлення, яке повідомляє про те, що він подзвонив у не робочий час, та запропонувати залишити голосове повідомлення або залишити свій номер, щоб в робочий час йому передзвонили (голосове повідомлення або номер клієнта повинен бути направлений на електрону пошту технічної підтримки).

Виходячи з поставлених вимог можна виділити, що для організації комунікаційної мережі необхідно придбати такі апаратні засоби: системний блок, 8 – IP-телефонів, 1xGSM шлюз на 4 SIM-картки, VOIP-шлюз для підключення міських телефонних ліній та 2 стаціонарних радіотелефони, маршрутизатор, який дозволить підключитися із зовнішньої мережі Інтернет до системи Asterisk.

Отже, можна виділити 5 груп, на які можна розподілити модулі системи:

- VOIP-шлюз (пристрій, який необхідний для з'єднання 2-х міських та 2-х стаціонарних радіотелефонів);
- GSM-шлюз (пристрій, який необхідний для підключення 4-х мобільних операторів);
- IP-телефон (телефонний апарат, що підключається до локальної мережі);
- системний блок для встановлення системи Asterisk, за допомогою якої виконуватиметься з'єднання усіх модулів мережі .

З використанням описаного методу вибору модульних компонентів слід зробити вибір системи, розрахунки якої наведені в табл. 7.23.

У ході виконання розрахунків із першої групи (VOIP-шлюзи) найвищий коефіцієнт (1,86) отримав модуль D-Link DVG-6004S, який більшею

мірою відповідає потребам, адже недоліком є відсутність можливості розширення його функціональності, тобто, якщо необхідно буде підключити ще один, чи декілька стаціонарних телефонів або міські телефоні лінії – необхідно буде придбати ще один такий пристрій.

Стосовно другої групи найвищий коефіцієнт (1,86) отримав модуль Gudwin 4GSM, недоліком якого є також відсутність можливості розширити функціональність.

У третій групі найвищий коефіцієнт (1,86) отримав модуль MikroTik, який у групі має найвищі показники окрім вартості, але співвідношення його ціни до якості цілком дійсне.

У четвертій групі найвищий коефіцієнт (1,86) отримав модуль Lynk-Sys SPA901, ціна цього пристрою дещо дорожча за його можливості порівняно з D-Link DPH-150SH, велика різниця – це відсутність дисплею, який відображає номер людини, яка дзвонить, але в якості зв'язку він значно краще ніж у порівнюваній моделі.

У п'ятій групі всі модулі отримали показник (1,86), але оскільки основним завданням є створення бюджетної комунікаційної системи, тому варто обрати модуль Intel Core3 500GB 4GB, бо заявлені вимоги цілком підходять під його технічні характеристики.

У середньому система Asterisk використовує 1-2 Гб оперативної пам'яті, а виходячи з того, що для збереження голосових повідомлень потрібно місце на жорстокому диску, то 500 Гб цілком достатньо. Якщо одночасно в неробочий час телефонують 5 клієнтів, а пропускна здатність АТС дорівнює 5 (3 мобільних оператори та 2 міські телефонні лінії) і вони усі одночасно залишають голосове повідомлення протягом (14 годин * 5 днів), бо це є неробочий час, коли система виконує запис голосових повідомлень, а також протягом 2-х вихідних днів, а це ще 48 годин, отримаємо 118 годин за тиждень, а це 7 080 хвилин.

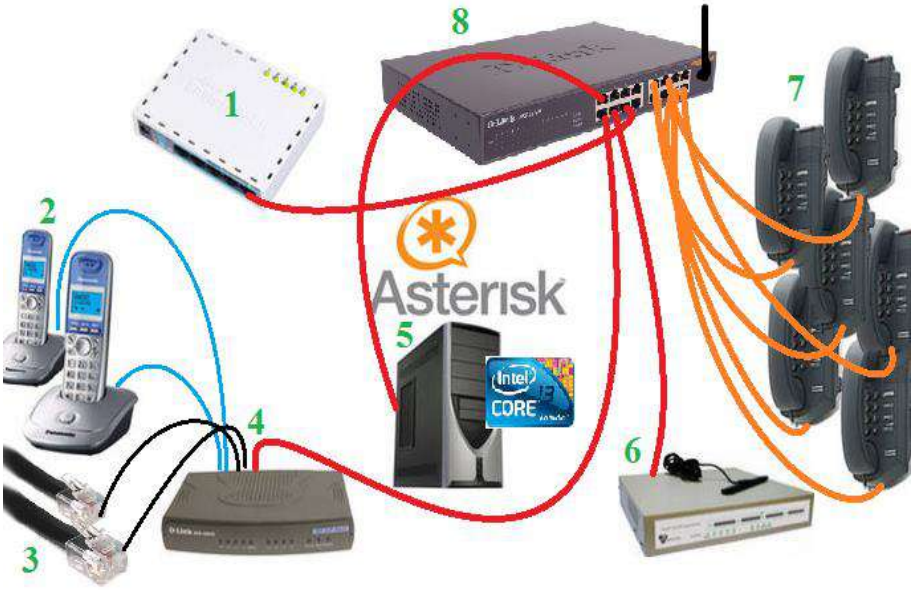
Якщо ці хвилини розподілити на кожного із 5 клієнтів, що телефонують, можна отримати 35 400 хвилин запису, бо кожен може наговорити по 7 080 хвилин. Для того, щоб зберегти 35 400 хвилин записів із голосовими повідомленнями, потрібно приблизно 354 Гб місця на жорстокому диску, оскільки в середньому 1 хвилина голосового запису складає 1 Мб пам'яті на жорстокому диску. Отже, обраний системний блок із характеристиками цілком відповідає поставленим вимогам. На виході методу, за допомогою якого зроблено вибір системи, отримано приблизно вартість АТС (15 734,00 грн), яка відповідає поставленим вимогам, а також отримано перелік конкретних модулів, що входять до складу цієї системи, та відповідають співвідношенню ціни до якості.

Таблиця 7.23

Результат розрахунків для обраної системи

Група №	Назва модулю	Складність налашту-вання	Наявність портів	Якість зв'язку	Можливість розширення	Надій-ність	Інтеграція з Asterisk	Відносна вартість	Коефі-цієнт	Вартість, грн	Кількість
I (VOIP-шлюзи)	D-Link DVG-6004S	3	3	2	0	2	1	2	1,86	1 300	1
	Cisco SB SPA8000	2	0	3	1	3	1	1	1,57	2 090	1
	D-Link DVG-N5402SP	2	2	2	0	2	1	3	1,71	863	1
II (GSM-шлюзи)	GoIP 4GSM	2	3	2	0	2	1	2	1,71	6 000	1
	Gudwin 4GSM	3	3	1	0	2	1	3	1,86	5 600	1
	AddPAC 4GSM	2	3	3	1	3	1	1	2,00	8 000	1
III (маршру-тизатори)	MikroTIK	3	3	3	0	3	0	1	1,86	750	1
	D-Link DIR-300	2	3	2	0	2	0	2	1,57	300	1
	TP-Link	1	3	1	0	1	0	3	1,29	240	1
IV (IP-телефони)	D-Link DPH-150SH	1	3	2	0	2	1	3	1,71	460	8
	LynkSys SPA921	2	2	3	0	3	1	1	1,71	791	8
	LynkSys SPA901	2	2	3	0	3	1	2	1,86	573	8
V(Систем-ний блок)	Intel Core3 1TB 4GB	1	3	3	1	2	1	2	1,86	4 200	1
	Intel Core3 500GB 4GB	1	3	3	1	1	1	3	1,86	3 500	1
	Intel Core7 1TB 8GB	1	3	3	1	3	1	1	1,86	4 800	1
Всього									9,29	15 734	

Даний метод не тільки показує склад елементів та собівартість системи, також він дозволяє побудувати концептуально готову комунікаційну мережу з усіма необхідними пристроями (рис. 7.5), порівняно з цим метод ієрархії, на жаль, не надає такої можливості.



1. Маршрутизатор MikroTilk (5×LAN)
2. Стаціонарні радіотелефоні
3. Міські телефонні лінії
4. VOIP-шлюз D-Link (5×LAN, 2×FXO, 2×FXS)
5. Системний блок (Intel Core i3, 500Gb HDD, 4Gb RAM, 1×LAN)
6. GSM-шлюз (Gudwin 4×GSM, 1×LAN)
7. IP-телефон (LinkSys SPA-90, 11×LAN)
8. Комутатор (16×LAN, Wi-Fi)

Рис. 7.5. **Концептуальна схема комунікаційної мережі**

Система Asterisk побудована на базі операційної системи CentOS, що з ряду Unix-подібних систем. Доступ до налаштувань системи надається за допомогою web-інтерфейсу, оскільки сама система CentOS не має графічного інтерфейсу, необхідно використовувати другий комп'ютер з операційною системою, яка надає графічний інтерфейс.

Порядок налаштування системи Asterisk відбуватиметься за такою схемою: реєстрація внутрішніх номерів працівників; підключення IP-телефонів; підключення міських телефонних ліній; підключення GSM-шлюзу; написання плану дзвінків.

Виходячи з потреб, необхідно додати проміжок внутрішніх номерів від 1000 до 1007, до яких будуть підключені IP-телефони та два номери 701 та 702, до яких будуть підключені стаціонарні радіотелефони. Налаштування виконуються у розділі "PBX", пункт меню "Extensions" web-інтерфейсу пакета Elastix (рис. 7.6).

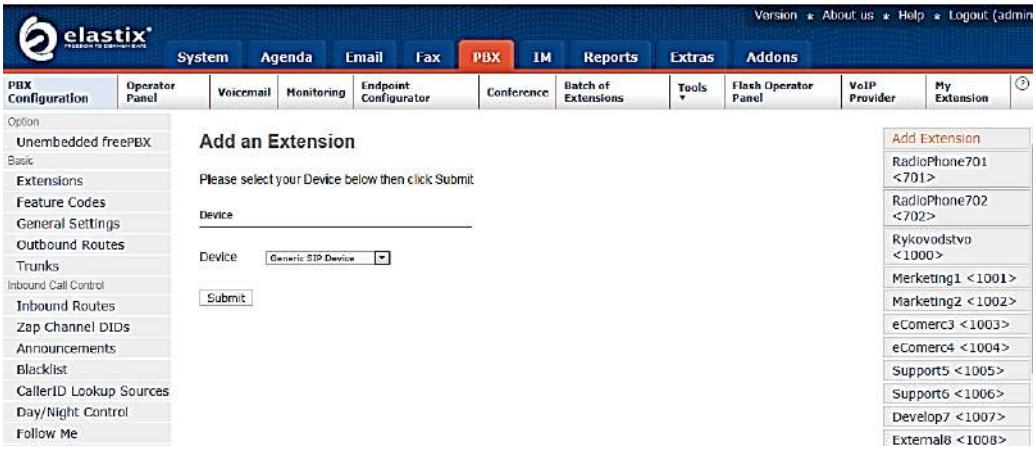


Рис. 7.6. **Внутрішні телефонні номери працівників**

Під час додавання внутрішнього номера існують особливі параметри (рис. 7.7), а саме:

- secret (пароль), який повинен бути надійним, щоб інший працівник не мав можливості зареєструватися в системі під цим номером;
- dtmfmode (тип режиму набору клавіш), в сучасній телефонії використовується тональний набір клавіш (rfc2833);
- context (контекст), вказується назва правила дозвону, за яким буде діяти вихідний дзвінок;
- host (хост), дозволяє реєструватися у системі під цим номером будь-якому пристрою (якщо стоїть значення "dynamic") та тільки конкретному пристрою, IP-адреса якого буде відповідати заданому значенню (наприклад: 192.168.1.72);
- type (тип), дозволяє або забороняє виконувати дзвінки за двома напрямами (вхідні та вихідні), якщо стоїть значення "friend", то дзвінки можуть відбуватися у двох напрямах, якщо поставити значення "user", в такому випадку цей номер зможе приймати тільки вхідні дзвінки.

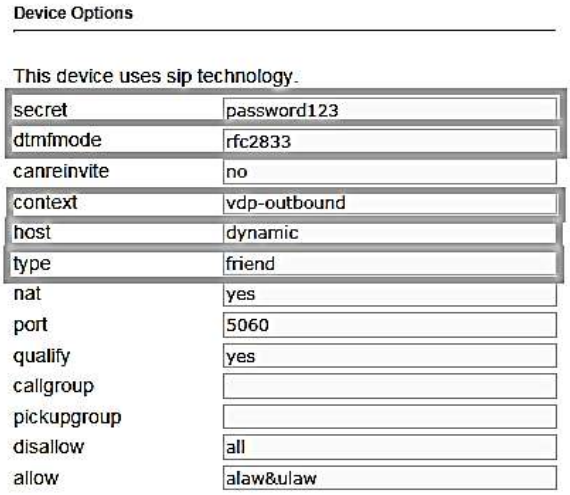


Рис. 7.7. **Параметри налаштування внутрішнього номера**

У вимогах до завдання сказано, що клієнт, який зателефонував у неробочий час або вихідний день, повинен мати можливість залишити голосове повідомлення, яке потім повинно бути надіслане на адресу електронної пошти відділу технічної підтримки. Для цього необхідно активувати голосову пошту, щоб клієнти мали можливість залишати голосові повідомлення. Налаштування голосової пошти виконується в тому ж місці, де загальні налаштування внутрішнього номера, але необхідно звернути увагу на інші параметри (рис. 7.8):

- status (статус), саме цей параметр дозволяє активувати голосову пошту;
- mail Address (адреса електронної пошти), параметр дозволяє відправляти усі голосові повідомлення, що надходять до АТС, на вказану адресу електронної пошти;
- Email Attachment (вкладення до електронної пошти), цей параметр дозволяє відправляти безпосередньо голосове повідомлення у звуковому файлі на вказану електронну адресу.

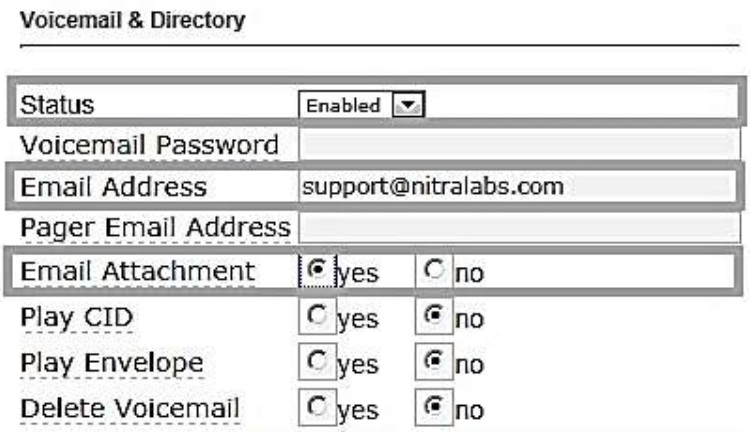


Рис. 7.8. **Параметри налаштування відправлення голосових повідомлень до електронної пошти**

На підставі доданих внутрішніх номерів працівників можна зареєструвати IP-телефони. Для цього необхідно приєднати кожен телефонний апарат до локальної комп'ютерної мережі за допомогою дротів.

Кожен IP-телефон має IP-адресу, що роздається DHCP-сервером локальної мережі, а також web-інтерфейс, за допомогою якого можна виконати налаштування щодо реєстрації телефонного апарату в системі Asterisk за відповідним внутрішнім номером працівника.

Щоб зареєструвати телефонний апарат необхідно виконати деякі налаштування, а саме вказати IP-адресу комп'ютера (рис. 7.9), на якому встановлено Asterisk (IP-адреса: 192.168.1.73), та вказати внутрішній номер (наприклад: 1000) і пароль (наприклад: password1000), за якими буде відбуватися реєстрація в системі (рис. 7.10) [16; 94; 191].

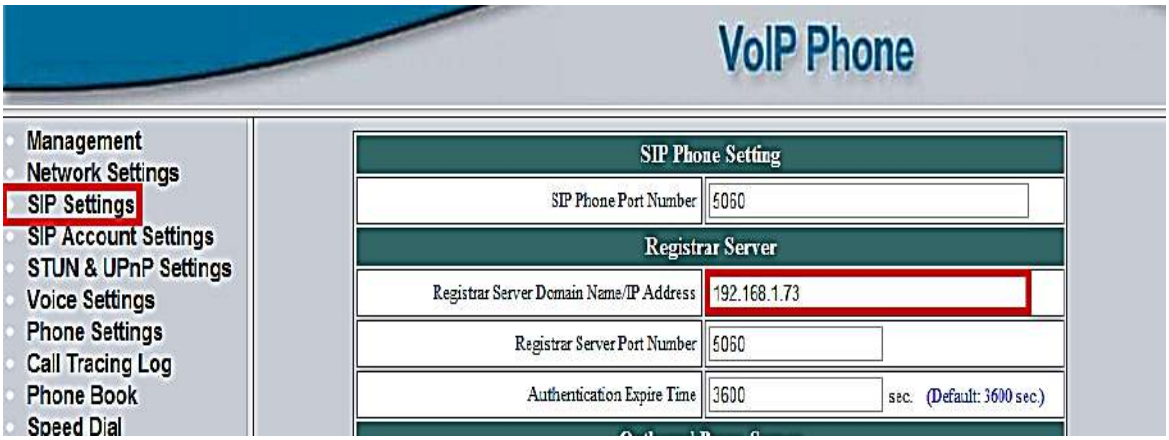


Рис. 7.9. **Налаштування IP-адреси системи Asterisk**

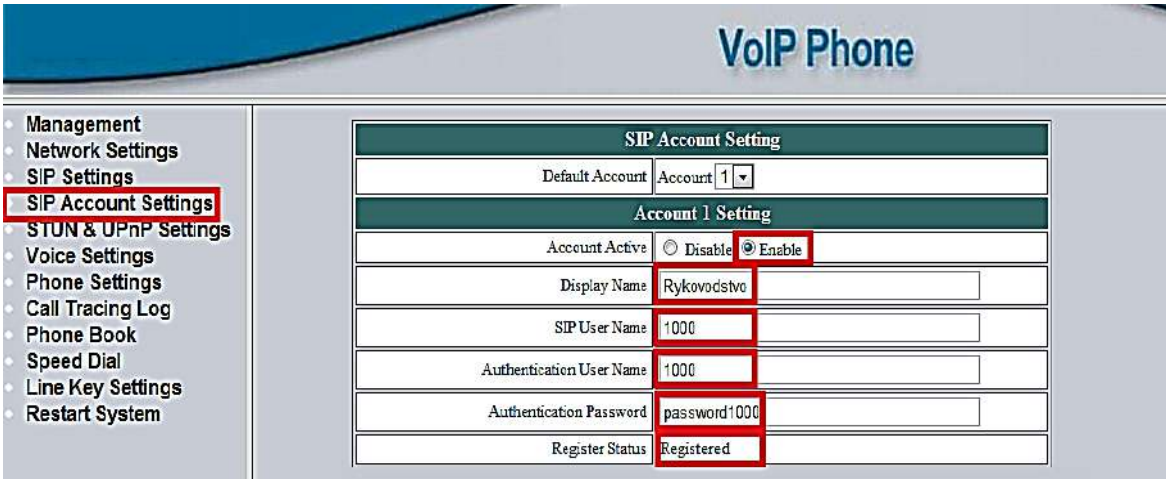


Рис. 7.10. **Налаштування параметрів реєстрації IP-телефону**

У разі успішної реєстрації в системі Asterisk, параметр Register Status (статус реєстрації) у телефоні буде зі значенням "Registered". Подібні налаштування повинні бути виконані для усіх телефонних апаратів, але із відповідними параметрами логіну та паролю [16; 94; 191].

Попередні два етапи дозволяють створити комунікаційну мережу, для спілкування працівників всередині організації. Для того, щоб працівник одного відділу мав можливість поспілкуватися з працівником іншого

відділу, він повинен на телефоні набрати внутрішній номер потрібного працівника та дочекатися відповіді. Адже до офісу ТОВ "Нітралабс" заведено дві міські телефонні лінії, які необхідно підключити до системи Asterisk для того щоб надати можливість працівникам спілкуватися із зовнішнім світом, а не тільки в середині організації. У випадку приєднання аналогових телефонних ліній необхідно використовувати VOIP-шлюз D-Link DVG-6004S, за допомогою якого сигнали аналогової лінії засобами апаратно-програмного комплексу перекодовуватимуться у сигнали для передачі їх локальною комп'ютерною мережею до системи Asterisk. Отже, два дроти необхідно приєднати до 2-х роз'ємів типу FXO (Foreign Exchange Office) – це роз'єм, до якого приєднується аналогова телефонна лінія на шлюзі.

Також за вимогами сказано, що необхідно підключити два стаціонарні радіотелефони, саме вони повинні бути підключені до двох роз'ємів типу FXS (Foreign Exchange Station) – це роз'єм, який надає можливість підключити абонента до аналоговой телефонної лінії. Для реєстрації телефонних апаратів та телефонних ліній, що підключені до VOIP-шлюзу, необхідно виконати налаштування, що зазначені на рис. 7.11, а саме вказати відповідні внутрішні номери телефонів (701 та 702), міські телефонні лінії також повинні мати внутрішні телефонні номери (81 та 82) та відповідні їм значення логіну та паролю, також необхідно вказати IP-адресу комп'ютера, на якому встановлено Asterisk, для того, щоб зареєструвати порти VOIP-шлюзу у системі [16; 94; 191].

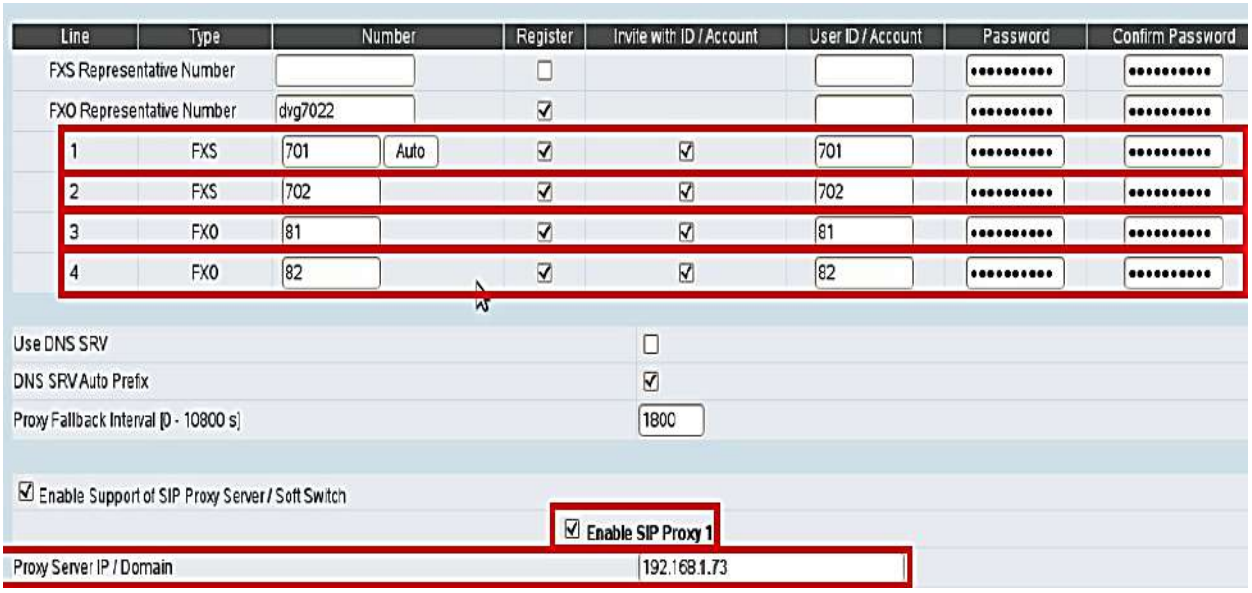


Рис. 7.11. **Налаштування портів VOIP-шлюзу**

Однією особливістю VOIP-шлюзу D-Link DVG-6004S є те, що вхідний дзвінок не може бути перенаправлений одразу ж до системи Asterisk, тому необхідно встановити деякі параметри щодо донабору внутрішнього номера, завдяки чому телефонний дзвінок буде перенаправлено на АТС (рис. 7.12).

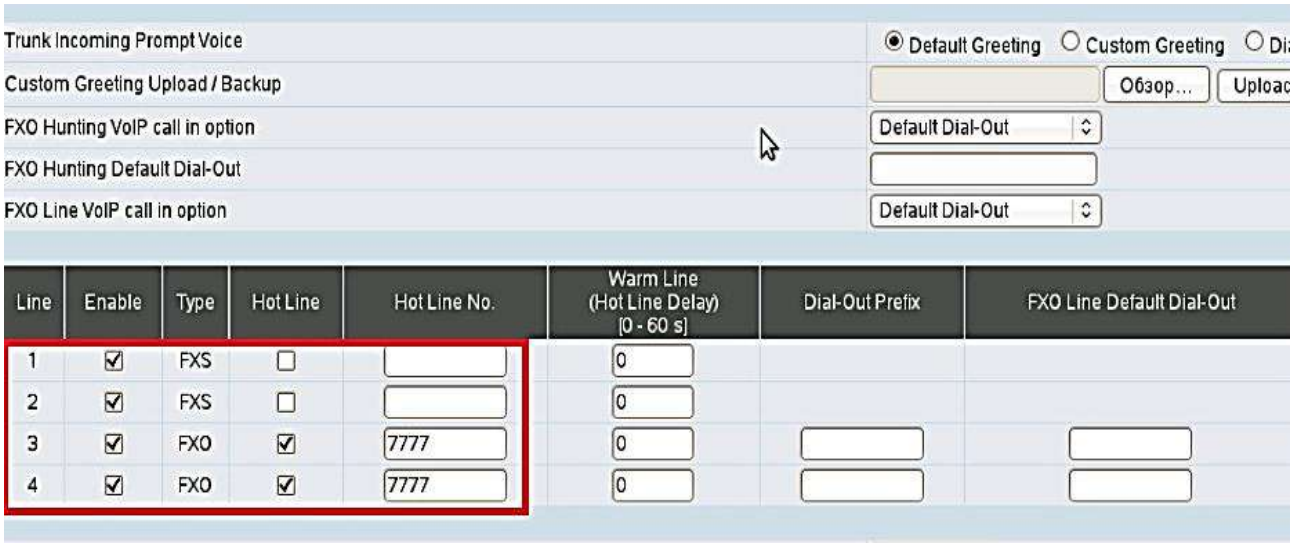


Рис. 7.12. **Налаштування донабору внутрішнього номера**

Інші налаштування VOIP-шлюзу треба залиши за замовчуванням, оскільки вони орієнтовані на досвідних спеціалістів.

Система Asterisk повинна приймати вхідні та робити вихідні дзвінки з міських ліній, а для того, щоб VOIP-шлюз зареєстрував FXO порти в системі, необхідно зробити trunk (магістральний канал) з'єднання – це канал, який з'єднує Asterisk та FXO порти VOIP-шлюзу. Параметри магістрального каналу можна поділити на чотири групи: загальні налаштування (вказується назва транку, його активність, максимальна кількість каналів), правила для вихідних дзвінків (вказується маска, якій повинні відповідати набрані номери), налаштування параметрів для вихідних дзвінків (вказуються параметри налаштування, які дозволяють VOIP-шлюзу приєднатися до Asterisk) та налаштування вхідних дзвінків (вказуються налаштування, які дозволяють керувати вхідними дзвінками з міських телефонних ліній). Налаштування виконуються у розділі "PBX", пункт меню "Trunks" web-інтерфейсу пакета Elastix (рис. 7.13) [16; 94; 191].

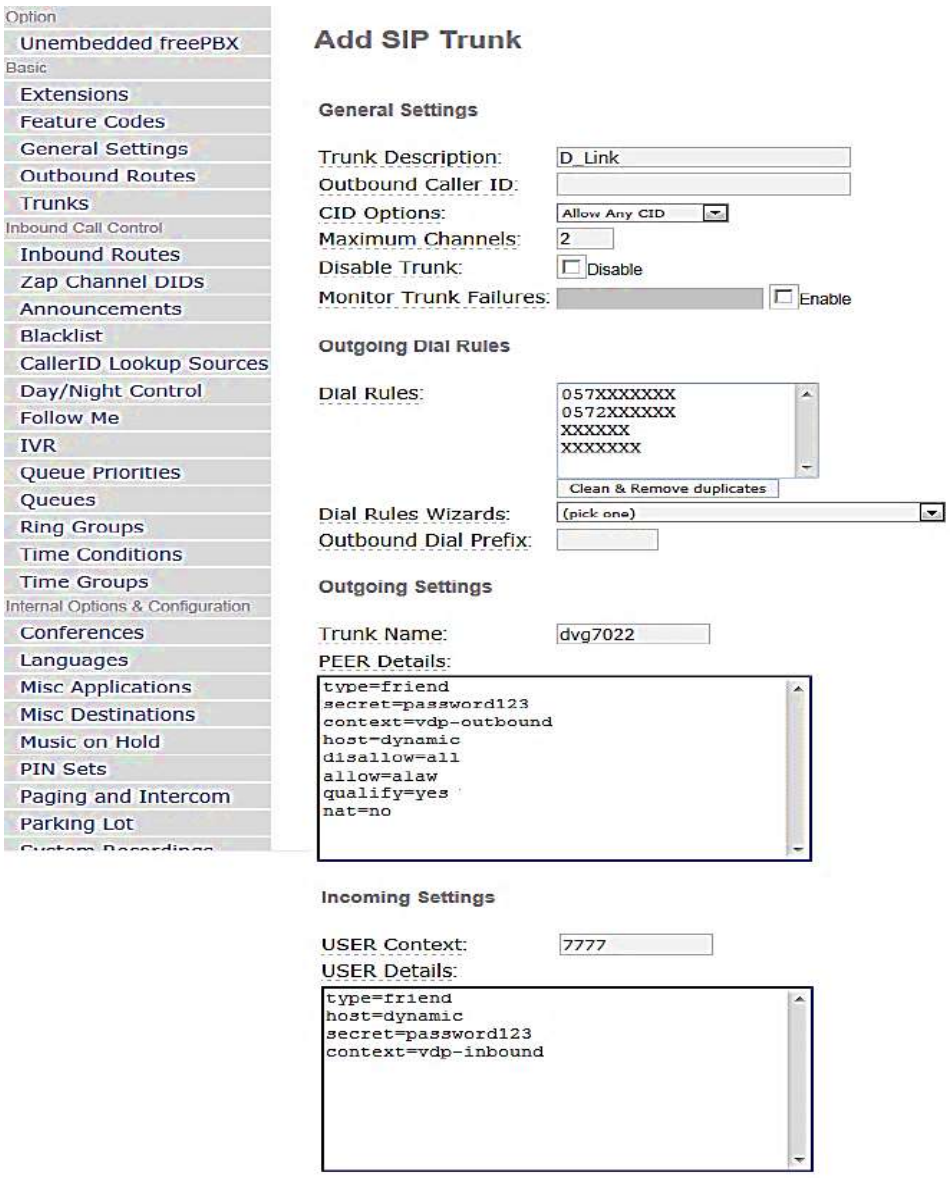


Рис. 7.13. **Налаштування магістрального каналу VOIP-шлюзу**

Комунікаційна мережа на даному етапі надає змогу не тільки спілкуватися в середині мережі, а ще й телефонувати у зовнішній світ та приймати вхідні дзвінки з двох міських телефонних ліній.

Для того, щоб зменшити витрати на телефонні розмови відповідно до вимог завдання необхідно приєднати до системи Asterisk GSM-шлюз, який дозволяє телефонувати на мобільні номери операторів та приймати вхідні дзвінки відповідно. GSM-шлюз має IP-адресу локальної мережі та web-інтерфейс, який дозволяє виконувати налаштування. Принцип налаштування GSM-шлюзу збоку АТС аналогічний, як і для VOIP-шлюзу, шляхом створення магістрального каналу, але для кожного порту, до якого підключено мобільного оператора, він створюється окремо, різниця

полягає тільки в назві транку, логіну та паролю. Параметри магістрального каналу можна поділити на чотири групи: загальні налаштування (вказується назва транку, його активність, максимальна кількість каналів), правила для вихідних дзвінків (вказується маска, якій повинні відповідати набрані номери), налаштування параметрів для вихідних дзвінків (вказуються параметри налаштування, які дозволяють GSM-шлюзу приєднатися до Asterisk) та налаштування вхідних дзвінків (вказуються налаштування, які дозволяють керувати вхідними дзвінками з ліній мобільних операторів). Налаштування виконуються у розділі "PBX", пункт меню "Trunks" web-інтерфейсу пакета Elastix (рис. 7.14).

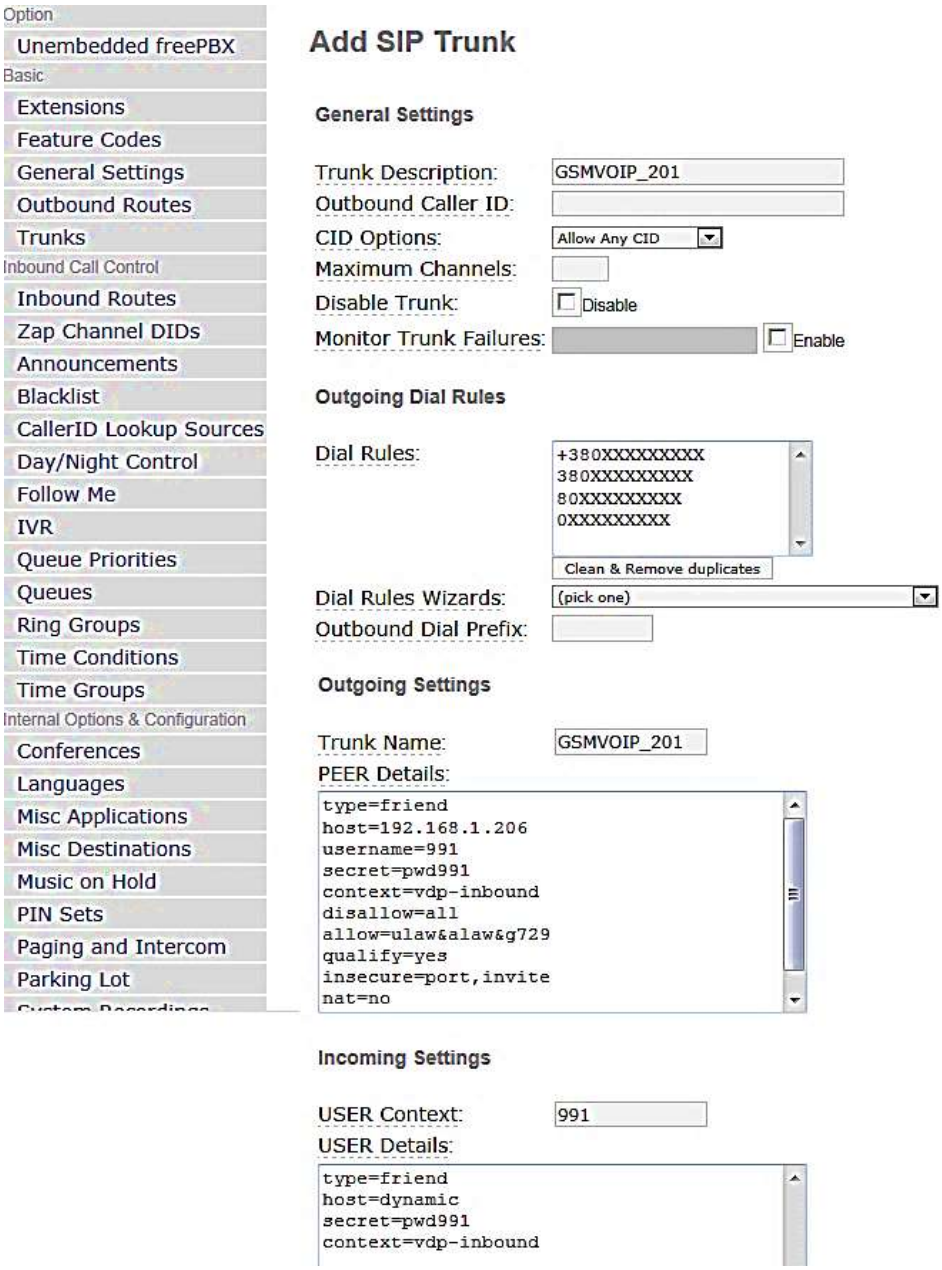


Рис. 7.14. **Налаштування магістрального каналу GSM-шлюзу**

Реєстрація GSM-шлюзу в системі Asterisk виконується на основі вказаних параметрів логіну, паролю та номеру каналу, налаштування для кожного каналу виконуються окремо. Аналогічно VOIP-шлюзу GSM-шлюз має IP-адресу локальної мережі та web-інтерфейс для налаштувань (рис. 7.15).

Рис. 7.15. **Налаштування параметрів реєстрації GSM-шлюзу**

З точки зору апаратної частини АТС цілком працездатна та відповідає усім технічним вимогам завдання, але без заданих правил система не може коректно розподіляти вхідні та вихідні дзвінки, а це сприяє збільшенню витрат на телефонні розмови. Отже, важливим етапом під час налаштування комунікаційної мережі є створення коректних правил, що відповідають вимогам та сприяють зменшенню витрат на телефонні розмови. Для побудови правил, тобто плану дзвінків використовується програмний засіб "Visual Dial Plan", який дозволяє у графічному режимі створити план обробки вхідних та вихідних дзвінків, а на виході отримати скомпільований код, який автоматично завантажується до файлів конфігурацій Asterisk. Це комерційний програмний засіб, який має аналоги, але різниця в тому, що аналогічні засоби вже вбудовані у корпоративні системи.

Згідно з вимогами завдання для всіх вхідних дзвінків у робочий час з 9.00 до 17.00 програвати голосове привітання та надати можливість клієнту обрати відділ, в який він хоче подзвонити (натиснути 1, щоб потрапити до відділу маркетингу, 2 – до відділу технічної підтримки, 3 – до відділу електронної комерції, 4 – до відділу керівників), якщо клієнт

подзвонив у неробочий час або вихідний день, то програвати голосове повідомлення, яке повідомляє про те, що він подзвонив у неробочий час, та запропонувати залишити голосове повідомлення або залишити свій номер, щоб в робочий час йому передзвонили (голосове повідомлення або номер клієнта повинен бути направлений на електрону пошту технічної підтримки) (рис. 7.16).

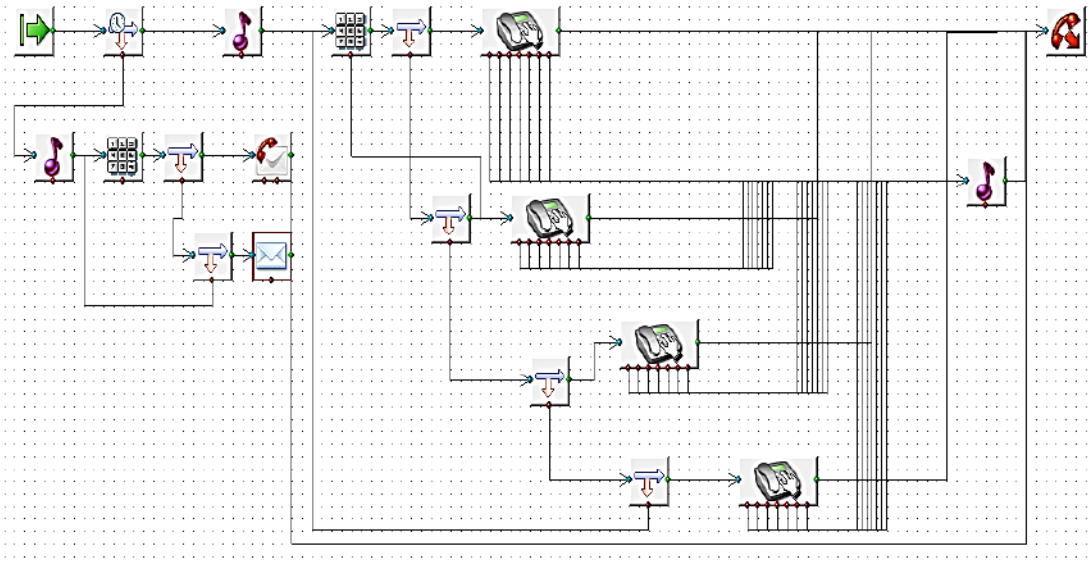


Рис. 7.16. **План обробки вхідних дзвінків**

Вихідні дзвінки розподіляються відповідно до набраного номера, тобто якщо працівник телефонує на номер мобільного оператора МТС, то вихідний дзвінок виконується через картку оператора МТС, що встановлено в GSM-шлюзі, а якщо працівник телефонує на міські телефони, то дзвінок виконується через міські аналогові лінії, інші дзвінки розподіляються відповідно до інших операторів (рис. 7.17).

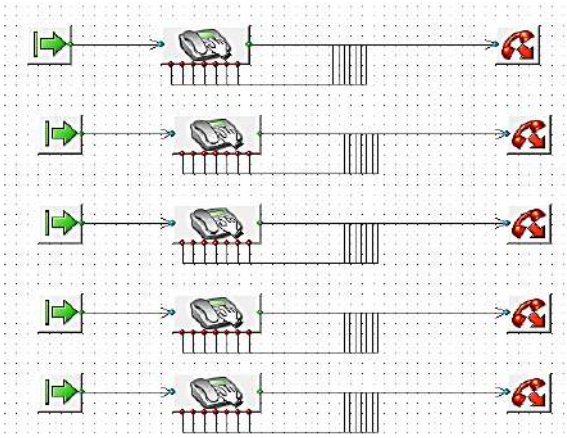


Рис. 7.17. **План обробки вихідних дзвінків**

Комунікаційна мережа побудована завдяки оптимально підібраній апаратній частині та оптимально налаштованій системі Asterisk, яка цілком відповідає вимогам завдання. Основна мета комунікаційної мережі полягає в зменшенні витрат на телефоні розмови шляхом розподілення дзвінків на відповідні номери міських та мобільних операторів, підвищення якості обслуговування клієнтів та якості робочого процесу працівників. Окрім розподілення телефонних дзвінків та поєднання апаратної частини система Asterisk дозволяє контролювати дзвінки шляхом перегляду статистики за кожним дзвінком, що дає змогу переглянути, який працівник і якого числа телефонував, на який номер, скільки хвилин тривала розмова.

Також є можливість переглянути статистику наговореного часу вхідних або вихідних дзвінків за якийсь період, кількість цих дзвінків у розрізі за кожним внутрішнім номером, можливо відстежити номери, за якими найбільш часто телефонують працівники (рис. 7.18).

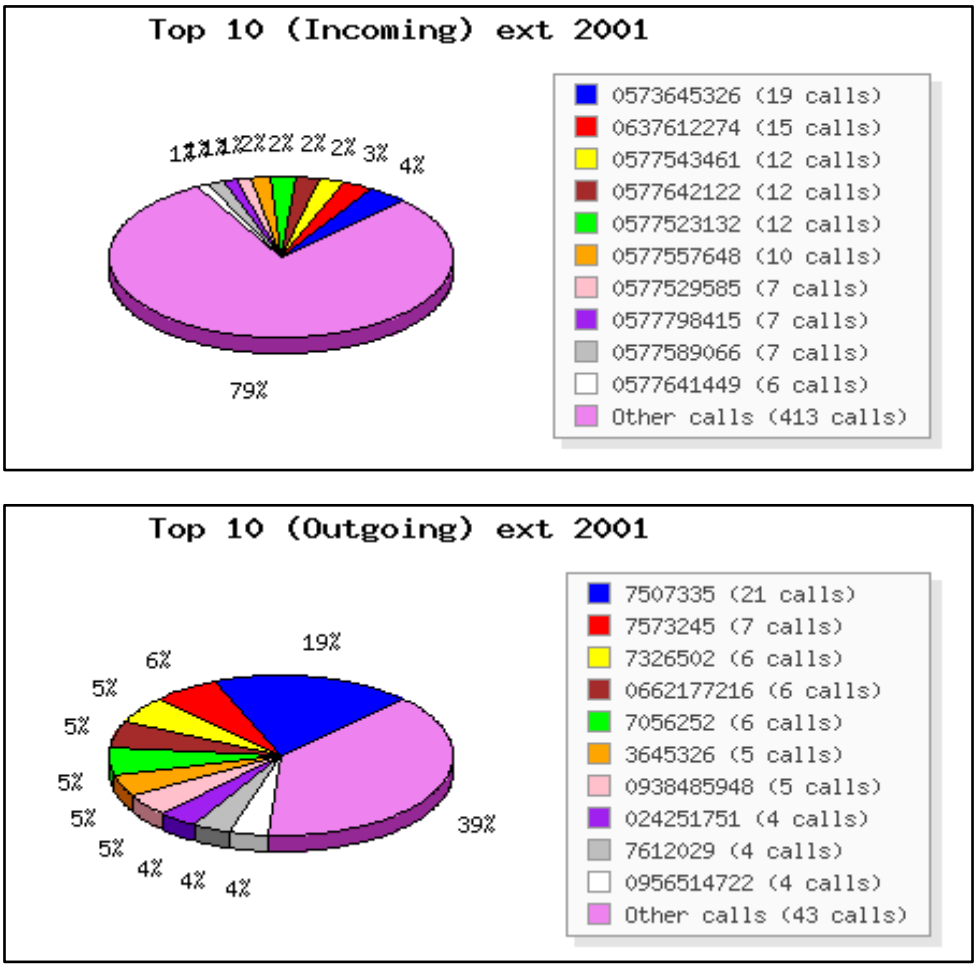


Рис. 7.18. **Статистика дзвінків за кожним внутрішнім номером та частішими номерами, за якими телефонують**

Можливість контролювати телефонні дзвінки в режимі онлайн надає змогу підвищити якість обслуговування клієнтів та підвищити контроль працівників. До контролю телефонних дзвінків у режимі онлайн входить: можливість негайної відповіді на телефонний дзвінок; перевести телефонну розмову на номер іншого працівника, голосову пошту або мобільний номер телефону за потребою; прослуховувати телефонну розмову; прослуховувати у режимі підказки – це коли в момент розмови з клієнтом інший працівник може підказати щось працівнику, який веде розмову з клієнтом, а в той час клієнт не буде чути того, хто підказує; також існує можливість відхилити дзвінок або вести запис розмови у разі, якщо це є необхідним. Але основна можливість контролю – це перегляд поточного стану внутрішнього номера співробітника, тобто він може спілкуватися за телефоном, якщо це так, то можна побачити, вхідний чи вихідний це дзвінок, який номер телефонує та час, який триває розмова. Усі можливості надає програмне забезпечення FOP2 (Flash Operator Panel 2) – панель оператора (рис. 7.19), яка має умовно-безкоштовну ліцензію, тобто безкоштовно можливо її використовувати лише на 15 внутрішніх телефонних номерів. До системи Asterisk панель оператора встановлюється окремо [189; 190; 192; 195].

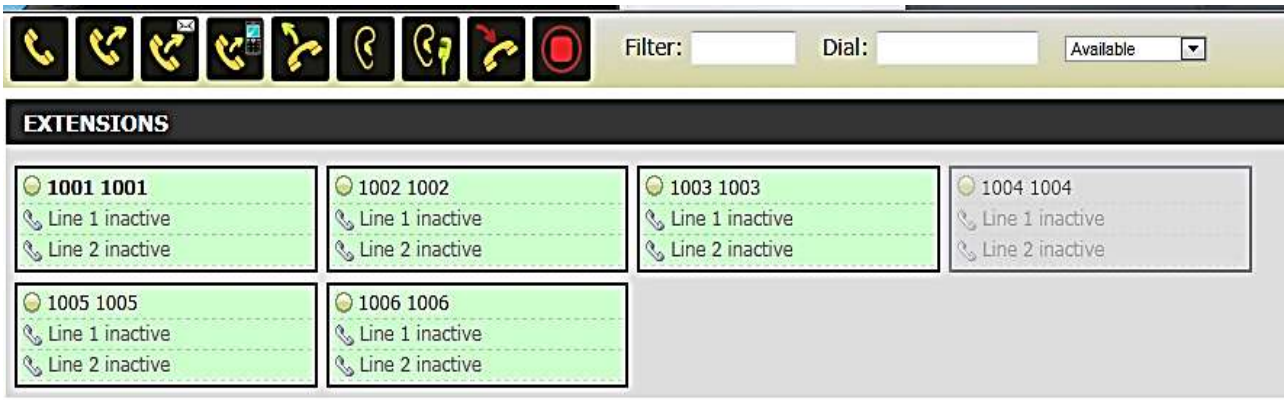


Рис. 7.19. **Панель оператора**

Запропонований метод вибору модульних компонентів системи дозволяє знайти оптимальне рішення апаратної частини комунікаційної мережі в співвідношенні ціни до якості, потребує значно меншого часу та ресурсів на прорахування показників, ніж метод ієрархій, також за допомогою цього методу можна визначити апаратну складову комунікаційної мережі за окремими модулями, на виході отримаємо приблизну вартість апаратної складової, що є дешевше, ніж придбати запропоноване готове

апаратне рішення, яке містить зайві модулі або ремонт чи додавання нових модулів може потребувати спеціаліста цієї системи. Система Asterisk дозволяє поєднати окремі апаратні модулі в єдину цілу комунікаційну систему та оптимально налаштувати розподілення телефонних дзвінків між цими модулями. Дуже великий плюс має система контролю працівників, яку можна поділити на два типи – це статистика телефонних розмов та контроль стану працівника в режимі онлайн. Порівняно з аналогами такий апаратно-програмний комплекс засобів для комунікаційної мережі є більш вигідним, тому що він спрямований на зменшення загальних витрат, покращення якості обслуговування клієнтів, покращення процесу роботи та контролю працівників, він є гнучким, можна в будь-який момент розширити можливості системи з точки зору апаратної та програмної складової.

Розділ 8. Моделювання взаємодії споживачів і виробників транспортних послуг

8.1. Розробка моделі розподілу клієнтів за центрами транспортного сервісу

Наведено постановку завдання розподілу споживачів по підприємствах, які пропонують транспортні послуги з вантажних перевезень на конкурентному транспортному ринку.

Запропоновано математичну модель вирішення задачі з урахуванням параметрів обслуговування, виробничих можливостей надавачів транспортних послуг та вимог клієнтів.

Модель дозволяє визначити раціональний розподіл надання послуг центрами транспортного сервісу для споживачів.

Наведено метод розв'язання, граничні умови та обмеження, цільову функцію.

В умовах сучасного конкурентного ринку транспортного обслуговування виникає завдання оптимізації взаємодії замовника (споживача) та виробника (виконавця) транспортних послуг. При визначенні стратегії обслуговування споживачів можна розглядати дві моделі сервісу [151; 152].

У першій споживач транспортних послуг керується лише власними інтересами. Він має інформацію про тарифи на транспортні послуги, що надаються центрами транспортного сервісу (надавачами окремих транспортних послуг).

У результаті обробки інформації про ціни та тарифи будується матриця витрат. Стовпчиками її є центри транспортного сервісу, а рядками – типи послуг. У клітинках міститься вартість виконання окремих операцій транспортного сервісу.

Шляхом аналізу матриці витрат можна визначити центри транспортного сервісу, при зверненні до яких забезпечується мінімум витрат на транспортне обслуговування.

Друга модель відбиває більш складну ситуацію, коли в регіоні діяльності крім кількох центрів транспортного сервісу розташовані і діють кілька *(i = 1, .., n)* фірм, що належать одній корпорації (компанії) та взаємодіють з замовниками. Якщо в регіоні знаходяться *(j = 1,.., m)* замовників, і необхідно взаємодіяти з усіма ними, то загальне число прямих контактів складе $n \cdot m$.

При використанні наявних *(k = 1, .., kn)* центрів транспортного сервісу кількість контактів складе (максимально) $n \cdot kn$ або менше, тобто зменшиться (як мінімум) на $n \cdot m - n \cdot kn$.

Визначити доцільність залучення посередників (тобто центрів транспортного сервісу) можна таким чином.

Варто припустити, що y_{ij} – кількість безпосередніх контактів *i*-го споживача з *j*-м виробником транспортних послуг, – витрати на один контакт; x_{ik} – кількість сервісних послуг *i*-го споживача, що надається *k*-м центром сервісу; c_{ik} – ціна однієї послуги.

Тоді умовою доцільності централізації транспортного сервісу для компанії в цілому є:

$$\sum_{i=1}^{n} \sum_{k=1}^{kn} x_{ik} \cdot c_{ik} \le \sum_{i=1}^{n} \sum_{j=1}^{m} y_{ij} \cdot K_{ij} . \qquad (8.1)$$

Умова виконується, зокрема, якщо $c_{ik} \le K_{ij}$.

Тобто для споживача обслуговування за участю центрів транспортного сервісу є ефективним, якщо безпосередній контакт коштуватиме для нього дорожче, ніж звернення за послугами в центр транспортного сервісу.

Для *k*-го центру транспортного сервісу доцільно надавати транспортні послуги, якщо він отримає прибуток:

$$\Delta П_k \geq \sum_{i=1}^{n} x_{ik} \cdot c_{ik} - c_k , \tag{8.2}$$

де c_k – його власні витрати з надання послуг.

Слід побудувати модель розподілу сервісних послуг *rn* типів між *kn* центрами транспортного сервісу для *n* клієнтів при необхідності мінімізувати сумарні витрати *(R)* на обслуговування:

$$R = min \sum_{i=1}^{n} \sum_{k=1}^{kn} \sum_{r=1}^{rn} x_{ikr} \cdot c_{ikr} , \tag{8.3}$$

де x_{ikr} та c_{ikr} – відповідно кількість та вартість замовлень на послуги *r*-го типу, що надійшли від *i*-го клієнта (розподілені до виконання) для *k*-го центру транспортного сервісу.

При цьому повинні бути виконані такі додаткові умови:

$$x_{ikr} \geq 0 ; \tag{8.4}$$

$$\sum_{i=1}^{n} x_{ikr} \leq q_{ik} ; \tag{8.5}$$

$$\sum_{k=1}^{kn} x_{ikr} = p_{ir} . \tag{8.6}$$

Наведені умови забезпечують відповідність продуктивності q_{ik} для *k*-го центру транспортного сервісу потрібному загальному обсягу послуг при виконанні цим центром послуг *r*-го виду для всіх клієнтів разом (2.5), та враховують необхідність виконання запланованого обсягу p_{ir} послуг *r*-го виду для *i*-го клієнта по всіх центрах, що його обслуговують, разом (2.6).

До послуг, що надають центри транспортного сервісу, входять вантажні, складські, комісіювання, доставка вантажів іншими видами транспорту (залізничним, водним, авіаційним), збір та обробка інформації про

рух вантажів тощо. Якшо послуга потребує витрат часу, в систему обмежень включають умову виконання у визначений термін:

$$t_{ij} \le T_{ij}, \tag{8.7}$$

де T_{ij} – час доставки вантажів з пункту i в пункт j за умовами угоди;

t_{ij} – фактичний час доставки.

Останній складається з часу руху вантажу з i-го пункту в центр транспортного сервісу k, часу сервісних операцій, що виконуються з вантажем у центрі транспортного сервісу, часу руху вантажу з центру транспортного сервісу до пункту призначення j. За наведеною умовою перевіряються t_{ij} , до яких входять операції, що потребують затрат часу і впливають на терміни доставки.

Розглянуті задачі відносяться до задач лінійного програмування з оптимізацією за критеріями мінімізації витрат (для споживачів послуг, замовників) або максимізації прибутку (для обслуговуючих центрів).

Множина розв'язань таких задач є випуклою, тому для пошуку розподілу слід використати один з методів оптимізації.

Головною вимогою є ефективна програмна реалізація методу.

В практичних умовах, коли ситуація на транспортному ринку постійно змінюється, необхідне розв'язання задачі розподілу в режимі реального часу, лише тоді можливо оперативно реагувати на зміни кон'юнктури транспортному ринку, оптимізувати завантаження центрів транспортних послуг.

Також стане можливим подальший післяоптимізаційний аналіз задачі.

При розробці комп'ютерної програми ставилися такі вимоги:

- простий інтерфейс, виконаний у стилі Windows-додатків;
- мінімальні вимоги до апаратного, програмного забезпечення;
- відкритість архітектури програми, тобто можливість модернізації та розвитку її в разі потреби з мінімальними зусиллями;
- сумісність по даних зі стандартними програмами (текстовими процесорами, базами даних, електронними таблицями);
- використання у розрахунковому блоці оптимізації однієї зі стандартних програм з перевіреними засобами оптимізації. З урахуванням

цих вимог розглядалося декілька інструментальних пакетів для програмування, які б забезпечили:

- створення сучасного, простого, зручного інтерфейсу;
- сумісність з програмними продуктами Microsoft як на рівні вхідних та вихідних даних, так і на рівні мови програмування;
- достатні засоби і можливості з точки зору програмування;
- обмежені потреби з апаратної і програмної підтримки.

На рис. 8.1 і 8.2 подано схему дій користувача та потоків даних.

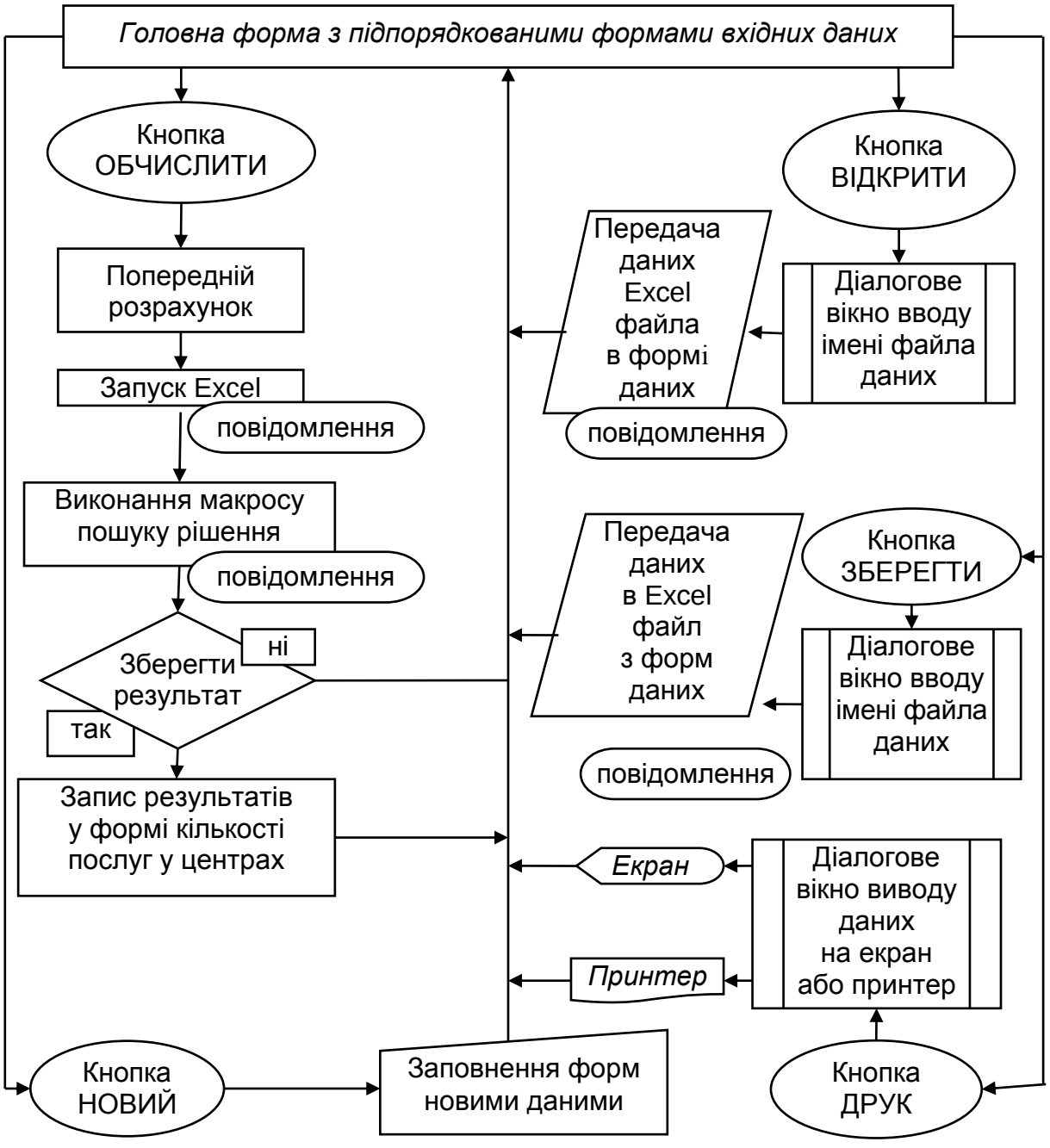


Рис. 8.1. **Схема можливих дій користувача програми**

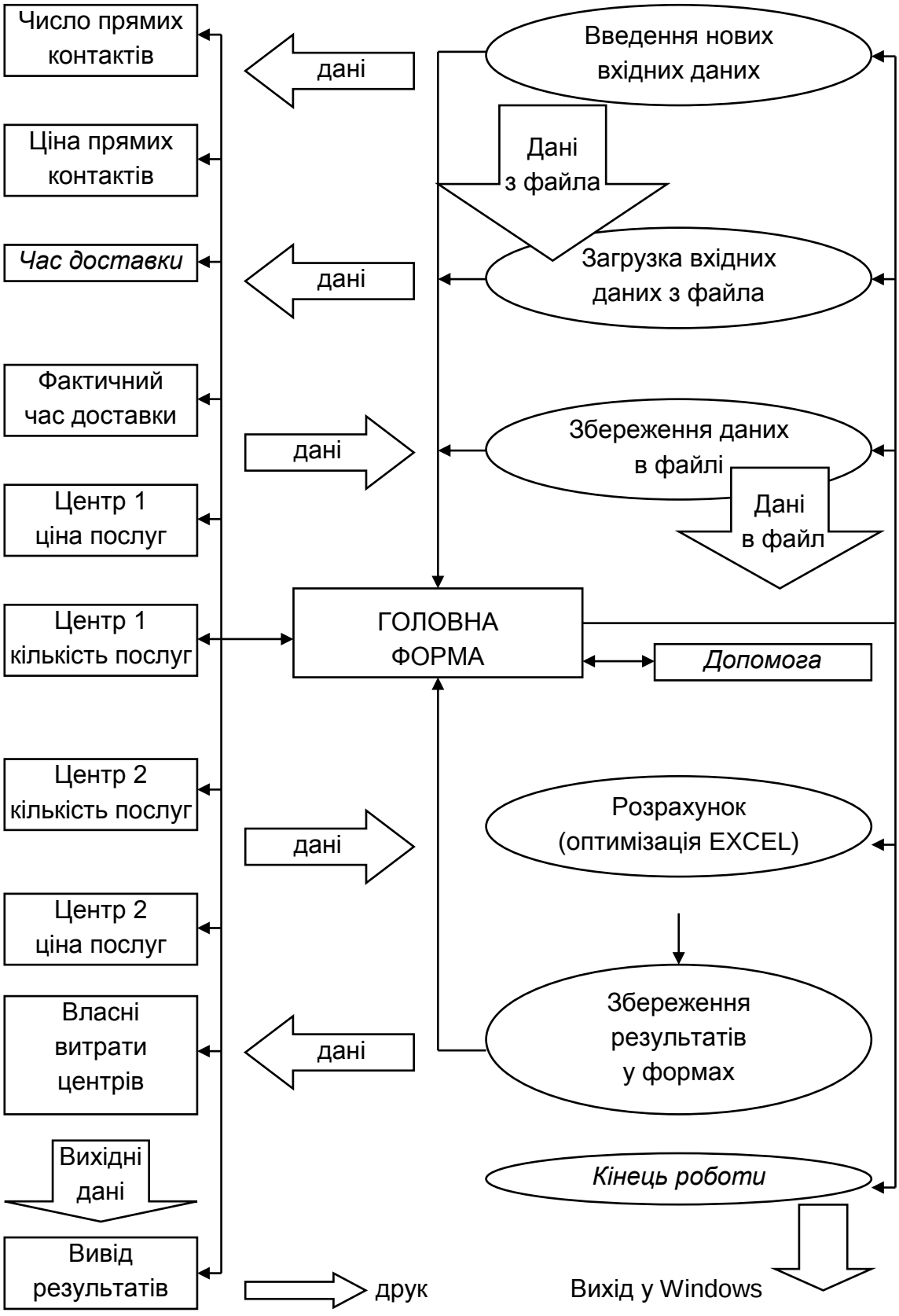


Рис. 8.2. **Схема переміщення потоків даних**

Для блоку оптимізації (пошуку розв'язання системи рівнянь з відповідними граничними умовами) розроблено спеціальний макрос з вико-

ристанням бібліотеки Solver пакета MS Excel. Вхідні дані при зверненні користувача до відповідної команди інтерфейсу автоматично передаються до Excel. Виконується макрос пошуку рішення. Після його завершення результати розрахунків автоматично повертаються до відповідних форм інтерфейсу додатка.

Для забезпечення надійності роботи додатка звернення до Excel, його виклик та завершення організовані програмним способом без участі користувача. Робочі листи, де знаходяться дані та макроси, парольно захищені і користувачем змінені бути не можуть. Елементи інтерфейсу, вікна вводу захищені від помилок користувача шляхом перевірки даних при вводі та обчисленнях.

Перевірка програми на практичних задачах розподілу транспортних послуг показала придатність до використання.

8.2. Розробка моделей для сегментації, класифікації, структуризації на ринку транспортних послуг

Розглянуто питання визначення структури транспортного ринку як з точки зору підприємств, так і з точки зору споживачів послуг. Обґрунтовано застосування сегментації, класифікації, структуризації для ринку транспортного обслуговування. Вперше запропоновано метод класифікації за ентропією.

Значне місце у покращенні рівня організації, планування та управління для всіх рівнів та складових частин транспортного обслуговування займають питання вибору, розробки, програмної реалізації методів та алгоритмів структуризації, класифікації, сегментації на транспортному ринку.

Методи класифікації в теоретичному вигляді широко представлені в літературі. Так, класичне визначення сегментації ринків наведене в [43]. Визначені та розглянуті основні критерії сегментації (географічні, демографічні, соціально-економічні, психографічні, поведінкові тощо).

Для продукції та послуг виробничо-технічного призначення використовуються такі ознаки, як тип організації, розміри закупівель, напрями використання продукції тощо. Сегментація проводиться за одним, або послідовно за кількома критеріями. Важливим є правильне визначення критеріїв сегментації і послідовності їх застосування.

Слід зазначити, що методи сегментації для ринку транспортних послуг на практиці використовуються недостатньо. В той же час, при вивченні взаємодії споживачів та виробників на транспортному ринку, постійно виникають задачі класифікації, розподілу об'єктів або явищ на групи за сукупністю ознак, що характеризують ці об'єкти. Є велика кількість методів та підходів до розв'язання таких задач у загальному вигляді [227].

Однак практичне їх застосування викликає труднощі. Класичні математичні постановки є складними для безпосереднього використання особами, що приймають рішення.

Стандартні програми (MathCad, MatLab, Statistica тощо) для комп'ютерного розв'язання цих задач, є громіздкими, складними у використанні для непідготовленого користувача, потребують значного рівня технічного (апаратного) забезпечення. Відсутні адаптовані постановки задач структуризації, класифікації, сегментації для транспортного ринку. Існуючі методи та алгоритми розпорошені по програмних продуктах, що ускладнює їх практичне застосування.

Водночас, значна кількість публікацій підтверджує актуальність розробки засобів класифікації для задач і суб'єктів транспортного обслуговування. Аналіз практичного стану справ підтверджує відсутність прийнятного програмного забезпечення для практичного вирішення задач структуризації, класифікації, сегментації на транспортному ринку. Існуючі математичні методи, підходи та алгоритми недостатньо адаптовані для безпосереднього використання суб'єктами транспортного ринку.

Тому необхідно визначити прийнятні методи та алгоритми для вирішення цих задач, створити відповідне програмне забезпечення. Воно має бути простим, надійним, зручним у використанні, невибагливим щодо технічних вимог до обчислювальної техніки та рівня підготовки користувачів. Для дослідження та подальшого застосування було обрано [67]: кластерний, дискримінантний аналіз, одно- та багатопараметричну класифікацію на основі нечітких множин, класифікацію за ентропією.

Програму було створено для користувачів, що мають лише елементарні навички роботи на обчислювальній техніці. Інтерфейс забезпечує зручність роботи в усіх режимах. Є система підказок, база вхідних даних; блоки роботи з файлами, допоміжної і довідкової інформації, формування, виводу вихідних даних, настроювання параметрів роботи.

Модульний принцип побудови і функціонування дозволяє незалежне використання окремих компонентів системи. Складом і формою вихідних даних можна керувати за допомогою механізму приєднаних форм.

Слід навести особливості застосування і програмної реалізації пропонованих методів [68; 69]. Кластерний аналіз призначений для розподілу об’єктів на однорідні групи. Основою є матриця "об’єкти-ознаки" вигляду:

$$X_{ij} = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1m} \\ x_{21} & x_{22} & \cdots & x_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ x_{n1} & x_{n2} & \cdots & x_{nm} \end{bmatrix}. \qquad (8.8)$$

Тут X_{ij} є значенням *j*-ї ознаки для *i*-го об’єкта. Подібність об’єктів O_k та O_l визначається відстанню між ними $S_{kl}(O_k,O_l)$. Менша відстань означає більшу схожість об’єктів.

У програмі реалізовано розрахунки за відстанями основних стандартних видів: Евклідової; зваженої Евклідової; Хемінгової ("відстані міських кварталів"). Користувач може обрати побудову ізоморфного розподілу (за подібністю структури об’єктів) або ізотонічного розподілу (за подібністю рівнів ознак об’єктів). Для розбиття на кластери використано метод шарів. При цьому можливе використання таких відстаней між кластерами: за принципом "найближчого сусіда", за принципом "далекого сусіда", за "центрами тяжіння" кластерів, за принципом "середнього зв’язку".

Дискримінантний аналіз застосовується при визначенні приналежності нового об’єкта до однієї з наявних груп об’єктів, що задаються "навчаючими" вибірками. Можливе розв’язання задачі при наявності двох та *k* груп. Алгоритм дискримінантного аналізу, як і кластерного, ґрунтується на обчисленні відстані між об’єктом, який класифікується, та центрами заданих класів. Для дискримінантного аналізу (на відміну від кластерного) необхідні навчаючі виборки, де згруповані об’єкти, вже віднесені до певних груп. При розрахунках визначається приналежність нового об’єкта до однієї з наявних груп.

Постановка задачі і послідовність розрахунків такі. Задані дві (або більше) групи об’єктів (навчальні вибірки). Для них задані матриці "об’єкти-властивості":

$$x_{ij} = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1m} \\ x_{21} & x_{22} & \cdots & x_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ x_{n1} & x_{n2} & \cdots & x_{nm} \end{bmatrix}, \qquad (8.9)$$

де x_{ij} – значення j-го властивості і-го об’єкта.

Розглядається новий об’єкт із заданими значеннями властивостей. Треба встановити, до якої групи він відноситься. Для випадку двох класів 1-й клас визначається вибіркою *X* об’ємом *n1,* 2-й клас – вибіркою *Y* об’ємом *n2*. Порядок обчислень такий.

Розраховується середнє значення за кожною змінною для кожної вибірки (класу):

$$\bar{x}_j = \frac{1}{n_1}\sum_{i=1}^{n_1} x_{ij}\ ,\ \bar{y}_j = \frac{1}{n_2}\sum_{i=1}^{n_2} y_{ij}\ . \qquad (8.10)$$

Обчислюються оцінки коваріаційних матриць для кожного класу *Sx* і *Sy* :

$$S_{kj}(x) = \frac{1}{n_1}\sum_{i=1}^{n_1}(x_{ij} - \bar{x}_j)(x_{ik} - \bar{x}_k)\ , \qquad (8.11)$$

$$S_{kj}(y) = \frac{1}{n_2}\sum_{i=1}^{n_2}(y_{ij} - \bar{y}_j)(y_{ik} - \bar{y}_k)\ . \qquad (8.12)$$

Визначається незміщена оцінка об’єднаної коваріаційної матриці:

$$S = \frac{1}{n_1 + n_2 - 2}(n_1 S_x + n_2 S_y)\ . \qquad (8.13)$$

Обчислюється матриця S^{-1}, зворотня до матриці *S.*

Знаходяться вектори оцінок коефіцієнтів дискримінантної функції: $A = S^{-1}(\bar{X} - \bar{Y})$ та оцінки векторів дискримінантних функцій для початкових змінних: *Ux = X·A* і *Ux = X·A.*

Далі розраховуються середні значення оцінок дискримінантних функцій:

$$\bar{u}_x = \frac{1}{n_1}\sum_{i=1}^{n_1} u_{xi}\ ,\ \bar{u}_y = \frac{1}{n_2}\sum_{i=1}^{n_2} u_{yi}\ , \qquad (8.14)$$

а також дискримінантної константи:

$$C = 1/2\,(\bar{u}_x + \bar{u}_y)\ . \qquad (8.15)$$

Обчислюються оцінки дискримінантної функції для об'єкта Z, що класифікується:

$$u_Z = \sum_{i=1}^{p} a_i \cdot z_i \cdot \tag{8.16}$$

Якщо отримане значення $u_Z \geq C$, то новий об'єкт належить до класу X, інакше – до класу Y.

Класифікація за значеннями ентропії здійснюється таким чином. Розглядаються N об'єктів, кожний з яких має M ознак. Спочатку визначаються середні значення кожної ознаки за всіма об'єктами.

Далі для кожної i-ї ознаки розраховується ентропія, що є оцінкою дисперсії:

$$H_i = \left(\frac{n(i+)}{N} log_2 \frac{n(i+)}{N} + \frac{n(i-)}{N} log_2 \frac{n(i-)}{N} \right), \tag{8.17}$$

де $n_i(+)$ та $n_i(-)$ відповідно кількість позитивних (більших за середнє) та негативних (менших за середнє) значень ознаки.

Далі проводиться розподілення значень для комбінацій кожної пари ознак і розраховується загальна ентропія H_{ij} для розподілу двох ознак (формула для H_{ij} аналогічна наведеній для H_i).

Частка загальної дисперсії h_{ij} відбиває зв'язок між значеннями ентропій при двомірній номінальній змінній: $h_{ij} = H_i + H_j - H_{ij}$. Інформативність кожної ознаки обчислюється, як:

$$J_i = \frac{\sum_{j \neq i}^{m} h_{ij}}{\sum_{j \neq i}^{m} H_{ij}} \cdot \tag{8.18}$$

Ознака, що має максимальне значення J_i, є найбільш інформативною щодо інших.

За максимальним значенням J_i об'єкти розділяються на два класи: де рівень ознаки вище середнього, і де цей рівень нижче.

Наступним етапом є перевірка однорідності груп, що утворилися внаслідок розподілу. Для цього розраховується імовірність помилки класифікації:

$$P(\varepsilon) = \frac{m * N - \sum_{j}^{mT} \sum_{k} r_j(k)}{m * N}, \qquad (8.19)$$

де m – кількість ознак;

T – кількість типів;

$r_j(k)$ – кількість найчастіших оцінок у k – му типі $(j=1,\ldots,m)$.

Однорідність розраховується як $1-P(\varepsilon)$. Прийнятний її рівень, як правило, повинен бути не меншим 80 %. Якщо групи однорідні, то процес припиняється. Інакше групування продовжується, доки всі групи, що утворилися, не будуть однорідними.

8.3. Розробка теоретико-ігрової моделі для вибору структури парку рухомого складу

Подано модель на основі теорії ігор для визначення структури парку транспортних засобів при плануванні діяльності перевізників в умовах транспортного ринку. Вона враховує ризики, протидію конкурентів, невизначеності різного походження.

В умовах невизначености транспортного ринку, наявності та взаємодії на ньому різних факторів, тенденцій, процесів виникає необхідність побудови моделей, що ґрунтуються на відповідних економіко-математичних методах, зокрема теорії ігор [155].

Як сторони гри, можуть розглядатися види транспорту, споживачі, посередники, виробники транспортних послуг, їх взаємодія між собою та з іншими чинниками ринку (попитом, пропозицією, умовами перевезень, надання послуг тощо). З урахуванням особливостей конкретних задач використовуються моделі кооперативних ігор (при партнерстві, співробітництві учасників), безкоаліційних (інтереси сторін не є протилежними, але партнерство відсутнє), антагоністичних (конкурентні відносин), багатокрокових, ігор з безкінченною кількістю гравців [74].

При розв'язанні використовуються матричні алгоритми, диференційні рівняння, нелінійне, лінійне програмування [221].

Недоліком загальних ігрових моделей (для матричних ігор) є те, що в них використовуються умовні показники, котрі не відбражають реальних обставин, а лише математично ілюструють процедуру розв'язання платіжних матриць. Не вивчаються питання практичної побудови та розрахунку платіжних функцій.

Слід розглянути модель для аналізу та прийняття рішення щодо визначення структури парку (кількості та типажу транспортних засобів), яка забезпечила б необхідний рівень гарантованого прибутку (не нижче розрахованої величини) в умовах невизначеності (коливань у певних межах) майбутніх обсягів перевезень [226].

При побудові платіжної функції варто розглянути три моделі автомобілів різної вантажопідйомності (означимо їх, як A, B, C) та прогнозовану денну потребу у перевезеннях вантажів. Розрахунок техніко-економічних характеристик перевезень для конкретних моделей можно провести за методикою, наведеною в [225].

Структура парку транспортних засобів є прийнятною, якщо вона забезпечує певний рівень рентабельності перевезень. В умовах невизначеності майбутніх їх обсягів доцільно виконати таку послідовність дій. Спочатку визначити рентабельність при використанні кожної з моделей автомобілей та виключити з подальшого розгляду ті, котрі не дають прибутку.

Для моделей, що залишилися, розрахувати виграші при різних станах ринку, за результатами скласти матрицю виграшів. Знайти стратегію (розв'язання матриці), яка забезпечує гарантований показник (не нижче розрахованої межі), відповідний склад парку транспортних засобів (кількість автомобілів кожної моделі).

Виграші по суті є прибутками (збитками), які можуть бути отримані при різних стратегіях (структурах парку) та станах ринку (попиту на перевезення), що визначаються як умовами навколишнього середовища, так і діями конкурентів.

Розрахунок виграшів слід виконати для ситуацій, котрі задані матрицею платежів, наведеною у табл. 8.1. Її стовбці відбивають можливі стани ринку транспортних послуг, а строки – можливі стратегії реалізації.

Значення рентабельності задано в умовних грошових одиницях, методика її розрахунку наведена в [225]. У випадках від'ємного значення

відповідний елемент матриці слід прийняти равним нулю. Слід розглянути три стани ринку, три стратегії дій на ньому, та проаналізувати кожну стратегію.

Таблиця 8.1

Матриця виграшів (у дужках наведено числові значення)

Модель автомобіля (вантажопідйомність)	Стан ринку (очікувана потреба в перевезеннях, т/день)		
	Нижня межа Q_1 (469 т.)	Середній стан Q_2 (550 т.)	Верхня межа Q_3 (632 т.)
1. A (5 т.)	$П_{11}$ (40 од.)	$П_{12}$ (10 од.)	$П_{13}$ (30 од.)
2. B (6 т.)	$П_{21}$ (30 од.)	$П_{22}$ (50 од.)	$П_{23}$ (20 од.)
3. C (8 т.)	$П_{31}$ (0 од.)	$П_{32}$ (60 од.)	$П_{33}$ (80 од.)

Стратегія № 1 ефективна, коли потреба в перевезеннях становить Q_1. Тоді буде отримано весь очікуваний прибуток, а втрат не буде. Якщо при цій стратегії буде більша потреба в перевезеннях, близька до Q_2, то утвориться упущений зиск (недоотриманий прибуток). Щоб не втратити його (не віддати замовників) слід збільшити провізну спроможність, що потребує додаткових витрат. При зростанні попиту до Q_3 також виникає упущений зиск, необхідні додаткові витрати.

Стратегія № 2 найкраща при потребі в перевезеннях Q_2, тоді весь очікуваний прибуток буде отримано без втрат. Якщо потреба в перевезеннях наблизиться до Q_3, знадобляться додаткові витрати. Навпаки, при попиті Q_1 виникають втрати через утримання не забезпечених роботою ресурсів.

Стратегія № 3 застосовується при максимальній потребі в перевезеннях Q_3 (щоб отримати весь можливий прибуток). Але в інших випадках (середній рівень Q_2 або нижня межа Q_1) виникнуть прямі збитки за рахунок зайвих витрат.

При розрахунках $П_{ij}$ враховуються капіталовкладення в матеріальну базу, втрати від утримання надлишкових ресурсів, обов'язкові відрахування тощо [225].

Слід знайти кращу структуру парку транспортних засобів, що забезпечує гарантований максимальний прибуток при будь-якій з можливих

ситуацій. Для цього в матриці виграшів варто проаналізувати кожну стратегію, знайти відповідний мінімально можливий виграш, далі з мінімальних значень обрати максимальне. Стратегія, що відповідає цьому значенню, є шуканою, бо задовільняє поставлені вимоги.

У формалізованому записі:

$$H_ц = max_i\,[min_j\,(П_{i,j})]\,, \qquad (8.20)$$

де $H_ц$ – нижня оцінка виграшу, менше котрої при використанні стратегії i він бути не може при будь-якому j стані ринку.

Існує вплив на стратегії з боку конкурентів, спрямований на зменшення виграшу, оскількі з їх точки зору всі виграші автотранспортних підприємств є їх програшами (втратами). Конкуренти спрямовуватимуть ринок у стан з меншими виграшами для автотранспортних підприємств. Для цього вони можуть проаналізувати матрицю очікуваних виграшів (якщо розрахунок її можуть провести, але інформація про обрану автотранспортними підприємствами стратегію їм невідома), знайти по кожному стану ринку максимально можливий виграш, та обрати і підтримувати стан, коли автотранспортне підприємство отримає лише мінімальний виграш (забезпечить конкурентам максимально можливий гарантований програш, вище якого виграш автотранспортного підприємства не зросте).

Ці міркування зводяться до формули:

$$B_ц = min_j\,[max_i\,(П_{i,j})]\,, \qquad (8.21)$$

де $B_ц$ – верхня оцінка виграшу (що може отримати автотранспортне підприємство) з позиції конкурентів, у разі використання ними своїх найкращих стратегій.

Якщо $H_ц$=$B_ц$, існує точка рівноваги V ($V = H_ц = B_ц$) при використанні відповідних стратегій з матриці виграшів. При цьому ризик неотримання гарантованого виграшу нульовий. Для його отримання парк має бути одномарочним. Якщо ж $H_ц \neq B_ц$, треба шукати точку рівноваги V в змішаних стратегіях, що складаються з використання чистих стратегій в певній кількості P_i , тобто структура парку складається з різних моделей, доля їх в загальній кількості дорівнює величині P_i. Визначення точки рівноваги V

(при різних нижній та верхній оцінках) і оптимальної змішаної стратегії дає розв'язання задачі пошуку мінімуму цільової функції лінійного виду:

$$F(X) = X_1 + X_2 + X_3 \qquad (8.22)$$

при обмеженнях:

$$\begin{gathered}(\Pi_{11} \cdot X_1 + \Pi_{21} \cdot X_2 + \Pi_{31} \cdot X_3) \geq 1.0; \\ (\Pi_{12} \cdot X_1 + \Pi_{22} \cdot X_2 + \Pi_{32} \cdot X_3) \geq 1.0; \\ (\Pi_{13} \cdot X_1 + \Pi_{23} \cdot X_2 + \Pi_{33} \cdot X_3) \geq 1.0; \\ X_i > 0, \quad i = 1, 2, 3,\end{gathered} \qquad (8.23)$$

де X_i – змінна, отримана з вихідної змінної P_i за формулою $X_i = P_i / V$, $i = 1,2,3.$

Розв'язання задачі слід виконати симплекс-методом. Результатом будуть чисельні значення функції $F(X)$ та змінних X_i. Далі варто знайти шукані P_i та V :

$$V = 1/F(X); \quad P_i = X_i \cdot V, \quad i = 1, 2, 3. \qquad (8.24)$$

Кількість рухомого складу моделі i визначається за формулою:

$$A_{спі} = Q_{нв} \cdot P_i / W_{Qi}\,, \qquad (8.25)$$

де $Q_{нв}$ – найбільш ймовірна денна потреба в перевезеннях, т.;

W_{Qi} – середня денна перевізна спроможність однієї одиниці i-ї моделі рухомого складу (методика її визначення наведена в [225]).

Значення $Q_{нв}$ дає розв'язання задачі визначення кращої стратегії конкурентів (стану ринку). Для цього шукаємо максимум цільової функції:

$$F(Y) = Y_1 + Y_2 + Y_3 \qquad (8.26)$$

при обмеженнях:

$$\begin{gathered}(\Pi_{11} \cdot Y_1 + \Pi_{12} \cdot Y_2 + \Pi_{13} \cdot Y_3) \leq 1.0; \\ (\Pi_{21} \cdot Y1 + \Pi_{22} \cdot Y_2 + \Pi_{23} \cdot Y_3) \leq 1.0; \\ (\Pi_{31} \cdot Y_1 + \Pi_{32} \cdot Y_2 + \Pi_{33} \cdot Y_3) \leq 1.0; \\ Y_j > 0, \quad j = 1, 2, 3,\end{gathered} \qquad (8.27)$$

де Y_j – змінна, отримана з вихідної змінної E_i за формулою $Y_j = E_j / V$, $j = 1,2,3;$

$\Pi_{i,j}$ – елементи матриці виграшів.

Розв'язавши задачу, отримуємо $F(Y)$ та Y_j, при цьому $F(X) = F(Y) = V$. Використавши зворотні перетворення $E_j = Y_j / V$, слід знайти E_1, E_2, E_3 та розрахувати величину найбільш ймовірного попиту на перевезення:

$$Q_{нв} = Q_1 \cdot E_1 + Q_2 \cdot E_2 + Q_3 \cdot E_3. \quad (8.28)$$

Слід розглянути матрицю виграшів (табл. 2.1) для автомобілей вантажопід'ємністю q_1, q_2, q_3. Варто визначити кількість кожної моделі для отримання певної суми виграшу при будь-якому стані ринку. Необхідно розглянути задачу вибору оптимальної структури парку в вигляді пошуку мінімуму цільової функції лінійного вигляду:

$$F(X) = X_1 + X_2 + X_3 \quad (8.29)$$

при обмеженнях:

$$\begin{aligned} 40 \cdot X_1 + 30 \cdot X_2 + 0 \cdot X_3 &\geq 1.0; \\ 10 \cdot X_1 + 50 \cdot X_2 + 60 \cdot X_3 &\geq 1.0; \\ 30 \cdot X_1 + 20 \cdot X_2 + 80 \cdot X_3 &\geq 1.0, \end{aligned} \quad (8.30)$$

де X_1, X_2, X_3 відображають використання автомобілів вантажопідйомністю q_1, q_2, q_3.

Розв'язання дає оптимальні значення: $F(X) = 0.0317$, $X_1 = 0.0155$, $X_2 = 0.0127$, $X_3 = 0.0035$. Після зворотнього перетворення змінних отримуємо: $V = 1/F(X) = 1/0.032 = 31.56$; $P_1 = X_1 \cdot V = 0.015 \cdot 31.56 = 0.49$; $P_2 = X_2 \cdot V = 0.0127 \cdot 31.56 = 0.4$; $P_3 = X_3 \cdot V = 0.0085 \cdot 31.56 = 0.11$.

Слід перевірити умову правильності обчислення частоти використання стратегій: $P_1+P_2+P_3=1.0$. Умова виконується $(0.49+0.40+0.11=1.0)$. Таким чином, виграш гарантовано складає 31.56, якщо 49 % обсягу вантажу перевозити автомобілями вантажопідйомністю q_1, 40 % – q_2, та 11 % – q_3.

Варто знайти найбільш ймовірний обсяг перевезень. Для цього треба визначити оптимальні стани ринку, тобто максимум цільової функції:

$$F(Y) = Y_1 + Y_2 + Y_3 \quad (8.31)$$

при обмеженнях:

$$\begin{aligned} 40 \cdot Y_1 + 10 \cdot Y_2 + 30 \cdot Y_3 &\leq 1.0; \\ 30 \cdot Y_1 + 50 \cdot Y_2 + 20 \cdot Y_3 &\leq 1.0; \\ 0 \cdot Y_1 + 60 \cdot Y_2 + 80 \cdot Y_3 &\leq 1.0, \end{aligned} \quad (8.32)$$

де Y_1, Y_2, Y_3 – перетворені змінні, що відібражають стани ринку Q_1, Q_2, Q_3. Розв'язання дає: $F(Y)=0.0317$, $Y_1=0.0176$, $Y_2=0.0063$, $Y_3=0.0077$.

Після зворотнього перетворення змінних: *V = 1/F(Y) = 1/0.0317 = 31.56; E1 = Y_1·V = 0.018·31.6 = 0.56; E2 = Y_2·V = 0.006·31.6 = 0.2; E3 = Y_3·V = = 0.008·31.6 = 0.24.*

Умова правильності обчислення частоти використання стратегій $E_1+E_2+E_3 = 1.0$ виконується (*0.56+0.2+0.24=1.0*). Тому найбільш ймовірний обсяг перевезень $Q_{нв} = 469·0.56 + 550·0.2 + 632·0.24 = 523$ т.

Приймемо денні перевізні спроможності для автомобілів А, В та С відповідно 20, 23.5 та 29 т. Визначимо їх кількість, що гарантує виграш не менше 31.5, на основі перевізної спроможності моделей окремо та середньозваженої (*0.49·20 + 0.40·23.5 + 0.11·29 = 22.39* т.). У першому випадку кількість автомобілів:

$$A\ (5m) = 523 \cdot 0.49 / 20 = 12.81 \cong 13;$$
$$Б\ (6m) = 523 \cdot 0.40 / 23.5 = 8.90 \cong 9;$$
$$C\ (8m) = 523 \cdot 0.11 / 29 = 1.98 \cong 3.$$

Загальна потреба складає 24 одиниці (*13+9+2*). У другому випадку:

$$A\ (5m) = 523 \cdot 0.49 / 22.39 = 11.45 \cong 12;$$
$$Б\ (6m) = 523 \cdot 0.40 / 22.39 = 9.34 \cong 10;$$
$$C\ (8m) = 523 \cdot 0.11 / 22.39 = 2.57 \cong 3.$$

Загальна потреба складе 25 одиниць (12+10+3). Тому слід використовувати перевізну спроможність кожної моделі окремо.

8.4. Принципи побудови інтерфейсів користувача та обробки помилок вводу даних для транспортних задач

Отримали розвиток принципи та вимоги до розробки, проектування програмного забезпечення для систем підтримки прийняття рішень у галузі транспортного обслуговування. Доведено необхідність першочергового забезпечення достовірності вводу даних, обробки помилок, підвищення швидкодії програмного забезпечення. Наведено відповідні засоби та рекомендації. Запропоновано принципи проектування форм і інтерфейсів.

Умови, що склалися на ринку транспортного сервісу, вимагають як від споживачів, так і від виробників транспортних послуг використання сучасних інформаційних технологій, засобів обчислювальної техніки для оперативного управління, прийняття обґрунтованих рішень. Виникають завдання, вирішення яких в режимі реального часу можливе тільки при використанні відповідних комп'ютерних систем [70; 122; 150; 153; 154]. Існує значна кількість таких систем, проте часто вони мають істотні недоліки (складність у модернізації, використанні, адаптації до рішення конкретних завдань, громіздкість).

Для невеликих автотранспортних підприємств вживання складних систем значної вартості недоцільне з економічних і технічних причин. Тому розробка комплексних комп'ютерних систем управління для них залишається актуальною. Необхідні системи підтримки прийняття рішень, здатні отримувати, аналізувати великі обсяги даних, вилучати з них інформацію, належним чином подавати її користувачу для прийняття ним рішення. Комп'ютеризація обліку, збору, аналізу, обробки інформації, прийняття рішень має метою мінімізацію витрат операторів транспортних послуг при якісному виконанні технічних і економічних умов транспортного обслуговування.

Для цього необхідна не лише розробка обґрунтованих і коректних статистичних і економіко-математичних методів, моделей і алгоритмів, збір і аналіз реальних даних для формування на їх основі відповідних баз даних, але й використання сучасних інформаційних технологій та обчислювальної техніки для оперативного управління і прийняття рішень.

Ця задача реалізується за допомогою стандартних, або самостійно розроблених програмних продуктів і як окрема, і у складі складних інтегрованих спеціалізованих додатків (програмного забезпечення).

Основним їх недоліком є або надмірно загальний характер, або навпаки – тісна прив'язка до конкретних моделей і умов. Тому перенесення і перенастроювання таких програмних продуктів на інший об'єкт стикається із технічними, часовими, фінансовими труднощами і витратами. Часто більш доцільно і вигідно створити нову розробку, ніж переробляти і пристосовувати стару, межі модернізації котрої обмежені.

Тоді розробка програми з "чистого аркушу" є найбільш прийнятною. Тому при створенні програмного забезпечення (за викладеними у попередніх розділах моделями і алгоритмами) було необхідно визначити найбільш прийнятні для цього засоби, особливості їх застосування.

При порівнянні програмних продуктів і пакетів для розробки призначених для користувача додатків, їх можливостей і необхідних ресурсів, найбільш доцільним виявляється проектування Windows-додатків у середовищі VBA [149]. Цей вибір визначається таким:

- низькі технічні (апаратні) вимоги до характеристик комп'ютера;
- не вимагається присутності будь-яких інших програмних продуктів, окрім самої операційної системи і MSOffice;
- можливості створення простого інтерфейсу, що дозволяє працювати з програмами без додаткової комп'ютерної підготовки;
- стійкість до збоїв і відмов у роботі завдяки простоті інструментів і засобів, що використовуються;
- швидкість і легкість установки (інсталяції), настроювання для конкретних умов, перевстановлення і відновлення при необхідності;
- використання вхідних та вихідних документів і баз даних у форматах Word, Excel, що забезпечує зручність роботи з ними;
- зручні засоби збереження результатів у вигляді документів MSOffice для подальшої обробки, корегування, аналізу, роздрукування.

Таким чином, система повинна забезпечувати:

- можливість роботи в режимі реального часу, отримання вихідної інформації в простому, чіткому, наочному, зручному для використання особою що приймає рішення вигляді;
- простоту користування (мінімальні вимоги до кваліфікації користувача щодо володіння комп'ютером, математичними методами), зручний і зрозумілий інтерфейс;
- низькі вимоги до апаратного, програмного (у тому числі ліцензійного) забезпечення, простоту встановлення, експлуатації, модернізації;
- можливість використання додаткових блоків для нових підзадач;
- легкість включення (у разі потреби) нових моделей, корегування постановок задач при зміні умов, цілей, особливостей практичної реалізації;
- адаптивність до вимог конкретного користувача;
- методологічну підтримка протягом періоду експлуатації, модернізація (заміна, доповнення блоків, компонентів, оновлення версій тощо).

Досліджуючи шляхи створення функціональних інтерфейсів для задач транспортного обслуговування, слід зазначити, що на першому етапі застосування обчислювальної техніки для управління найбільше поширен-

ня набули програми обробки даних у вигляді електронних таблиць [153]. Вони були ефективні при виконанні розрахунків, але не мали достатніх можливостей для обробки великих масивів даних.

Наступним кроком стала розробка інформаційних систем на мовах програмування високого рівня (Сі, Паскаль). Ці системи забезпечують можливість аналізу великих масивів даних, але потребують значних витрат при розробці, їх важко підтримувати на стадії експлуатації. Вони або дуже предметно-орієнтовані, або надмірно узагальнені.

Спроби зменшити складність розробки програм високого рівня призвели до появи візуального програмування, що спростило розробку додатків, зменшило вартість та зусилля, необхідні для їх створення. Сучасні засоби розробки інформаційних систем об'єднують можливості електронних таблиць і візуальних засобів розробки додатків [149]. Лише вони дозволяють розробляти та підтримувати гнучкі та ефективні інформаційні системи для транспортного сервісу.

Microsoft Excel – перший засіб розробки інформаційних систем, що поєднує в собі переваги електронних таблиць та інструментів візуального програмування. Він містить у собі візуальний засіб розробки додатків та програмування – VBA, що забезпечує доступ з прикладних програм користувача до функцій аналізу данних (які має електронна таблиця), до інших додатків MS Office і навпаки.

Важливо, що Excel – не лише електронна таблиця. Його бібліотеки мають більше ста об'єктів для обробки та аналізу даних. За допомогою VBA можливе об'єднання об'єктів та створення розвинених інформаційних систем.

Об'єкти Excel мають широкі межі застосування та дозволяють створювати гнучкі системи, що відповідають вимогам багатьох користувачів. Excel підтримує механізм OLE, може бути як сервером, так і клієнтом Automation. Це дозволяє інтегрувати його об'єкти до систем, створених на базі інших засобів.

Проектування інформаційних систем потребує попереднього аналізу засобів, що передбачається використати при її розробці, умов супроводу та експлуатації. Для розв'язання задач управління транспортним сервісом (при розробці програм) були застосовані можливості оптимізації (Excel), обробки текстів (Word), створення інтерфейсу користувача (VBA) тощо [153].

При розробці інтерфейсів слід вирішити два питання. Перше – які об'єкти використовувати. Друге – використати обрані об'єкти так, щоб ко-

ристувач легко засвоїв інтерфейс, мав швидкий доступ до інформації, зручність роботи в різних режимах. Існують різні підходи щодо використання меню, діалогових вікон, панелей інструментів, елементів керування на формах тощо. При цьому слід враховувати складність задач, що їх вирішує система, час та ресурси для її створення, навички користувачів, можливості наявної у них обчислювальної техніки.

Наведені результати отримані при розробці програмного забезпечення для задач транспортного обслуговування. Деякі рекомендації та методологичні підходи очевидні, інші менш наявні, їх розуміння досягнуто після набуття досвіду розробки відповідних задач [153].

Доцільно використовувати основну керуючу форму. Це форма, до якої користувач "потрапляє" відразу після відкриття додатка. Вона відображає назву, призначення додатка, дозволяє пересуватися до його різних частин (component parts). Слід розподіляти додаток на чотири – п’ять основних логічних компонентів, і створити для доступу до кожного з них окрему форму. Якщо одна задача розв’язується за допомогою однієї форми, додаток стає зрозумілим, що дозволяє зменшити час, необхідний для навчання користувачів. Навпаки, зосередження кількох різних задач на одній формі заплутує користувача.

Треба розробляти зрозумілі маршрути переміщення по додатку. Користувач не повинен замислюватися, як отримати доступ до потрібної форми або компонентів, інтерфейс повинен бути розроблений так, щоб ця інформація була очевидною. Кращим засобом є розміщення великих кнопок на формах, що дають доступ до різних частин додатка. Необхідна обережність при використанні меню та панелей інструментів для переміщення по додатку, бо вони гірше сприймаються користувачем, ніж об’єкти керування на формі. Користувач може не помітити меню, призначеного для доступу до форми. Зручним є застосовування графіки.

Подання інформації в графічному вигляді дозволяє краще її сприйняти. Наприклад, при створенні додатка щодо даних про продажі, доцільно відобразити дані графічно на діаграмах – це спрощує сприйняття. При створенні додатків, з відображенням числових даних у таблицях, слід використовувати вбудовані автоформати. Бажано уникати безладу на формах, вони повинні містити не більше десяти елементів керування, бо розміщення надмірної кількості елементів керування заплутує користувача.

По можливості краще використовувати об’єкти елементів керування на формах. Якщо на формі є таблиця даних і написана підпрограма, яка

керує цими даними, то доцільно підключити її до елемента керування, що розташований поряд з таблицею даних. Функції елемента керування, якщо він знаходиться поряд з даними, на котрі він діє, стають більш зрозумілими. Використання елемента керування на формі більш зручне, ніж використання меню або діалогового вікна.

Недоцільним є використання елементів керування виключно в діалогових вікнах, що потребує додаткових дій для відображення діалогового вікна. При розташуванні елемента керування безпосередньо на формі цього можна уникнути.

Для багатокрокових процесів доцільне створення "майстра". Розподіл складного процесу на частини і розміщення їх в "майстер" спрощує його виконання.

Розміщення команди, що викликає підпрограму, глибоко в ієрархії меню є дуже незручним (можна її просто не знайти). Водночас, об’єкти елементів керування є більш наочними, легко досяжними. Тому слід використовувати меню користувача тільки тоді, коли застосування об’єктів елементів керування безпосередньо на формах значно перевантажує їх.

Доцільно застосовувати команди "Сервис", "Настройка" ("Tools", "Customize") для розробки панелей команд користувача (меню та панелей інструментів). Їх можна розповсюджувати разом з додатком. Далі під час виконання додатка можна використати код VBA для керування панелями команд.

Необхідно видаляти зайві елементи Excel з додатка, бо їх наявність заплутує користувача. Також треба приховати всі кнопки на панелях інструментів Excel та настроїти заголовки додатка і робочого вікна. Якщо додаток не потребує взаємодії користувача зі стандартними вбудованими можливостями Excel, треба виключити можливості безпосереднього прямого виходу в Excel.

Бажано використовувати обробник подій "Open" об’єкта "Workbook" для завдання установок середовища додатка при запуску і обробник подій "Close" об’єкта "Workbook" для відновлення установок Excel після завершення додатка. Якщо додаток змінює властивості середовища, треба відновити попередні їх значення після завершення його роботи. Це дає можливість після виходу з додатка продовжити роботу з Excel, без впливу установок, що залишилися від додатка.

Підсумовуючи, можна твердити, що спільне використання Excel, Word, Access, VBA дозволяє (з урахуванням пропонованих принципів

побудови інтерфейсів) створювати сучасне програмне забезпечення для прикладних задач [153]. Вдало спроектований інтерфейс при створенні систем інформаційного забезпечення транспортного обслуговування є важливим фактором, що визначає їх ефективність та функціональну придатність.

При створенні прикладного програмного забезпечення важливими є збільшення швидкості обчислень [70]. Вона визначається параметрами процесора, мережного з'єднання, оперативною пам'яттю, дисковим об'ємом. Зі збільшенням складності додатків зростають вимоги до об'єму пам'яті та швидкодії. Виникає потреба в оптимізації за розмірами програмного коду та швидкості виконання обчислень і екранного виводу.

На етапах проектування та створення коду існують різні методи оптимізації. Одні роблять додаток швидким у роботі, інші скорочують його розмір та потрібні апаратні ресурси. Тому слід розглянути і проаналізувати загальні підходи до оптимізації додатків, що створюються для комп'ютерної підтримки задач транспортного обслуговування. Взагалі оптимізація додатків є процесом збільшення ефективності, тобто створенням менших за розміром та (або) більш швидких програм, шляхом вибору відповідних структур даних і алгоритмів. Оптимізація проводиться динамічно, безпосередньо в процесі розробки додатка, а не після її закінчення.

Слід визначити цілі та напрями оптимізації додатків: збільшення реальної швидкості обчислень та інших операцій; швидкодії екранного виводу; покращення суб'єктивної швидкодії (швидкості виконання додатоку з точки зору користувача – що пов'язана з швидкодією відображення, але не завжди з реальною швидкодією); зменшення розміру в оперативній пам'яті та на диску; керування розміром графіки.

Провести оптимізацію за всіма напрямами одночасно неможливо – оптимізація за розміром може зменшити швидкодію і навпаки. Тому методи оптимізації для одного параметра можуть суперечити іншому.

Треба мати на увазі, що оптимізація не завжди доцільна. Іноді результатом збільшення швидкодії або скорочення розміру додатка стає надмірне ускладнення коду, який неможливо підтримувати та відлагоджувати. Також виникають ускладнення при подальшій модернізації додатка, включенні до нього нових підпрограм. Тому при визначенні стратегії оптимізації потрібно визначити об'єкти, місця, межі оптимізації.

Цілі та об'єкти оптимізації вибираються на основі потреб користувача. Так, для програм, що будуть використовуватися замовниками транс-

портних послуг, головною характеристикою є швидкодія, а розмір додатків є важливим при їх розповсюдженні або роботі в мережах, а також на малоресурсних комп'ютерах. Необхідність визначити місця оптимізації викликана тим, що в реальних умовах (часу, вартості розробки) неможлива оптимізація всіх компонентів. Зусилля треба зосередити там, де відносно незначне втручання дає максимальний ефект. Межі оптимізації визначає співвідношення зусиль та результатів. Швидка програма сортування масивів непотрібна, якщо вона оброблятиме лише кілька елементів.

Якщо робота додатка стримується швидкодією дисків або мережі, слід зробити затримки менш подразливими для користувача, запропонувати йому (під час тривалої обробки даних) виконати інші роботи тощо. Швидкодія часто є головним фактором оцінки додатка користувачем. Ряд компонентів, які впливають на швидкодію, часто не можуть бути програмно покращені (швидкодія процесора, апаратні можливості пам'яті, продуктивність мережи). Тому необхідно збільшити швидкодію додатка, або створити враження, що він виконується швидше.

Оптимізація за швидкодією розподіляється на реальну (час фактичного виконання обчислень і програмного коду), швидкодію екранного виводу (час виводу графіки, заповнення екрану), уявну швидкодію (суб'єктивне сприйняття швидкості роботи). Для визначення шляхів оптимізації, які слід використати, треба проаналізувати тип та призначення додатка, співставити ефект з витратами, вибрати елементи, де удосконалення будуть ефективні і відчутні для користувача.

Для вивчення засобів збільшення швидкодії за допомогою тест-програми було протестовано кілька створених додатків, призначених для розв'язання задач транспортного сервісу та вироблено рекомендації [70].

Якщо в програмі відсутні рекурсії, швидкість роботи не буде визначатися швидкістю обробки коду. Більшим є вплив відеосистеми, мережних затримок, дискових операцій. Якщо форма повільно завантажується, причиною може бути велика кількість елементів керування і графіки, а не обробка коду завантаження.

У підпрограмах, що часто викликаються, для збільшення швидкодії треба уникати використання змінних типу Variant; використовувати цілі змінні Long та цілочисельну математику; кешірувати властивості (що часто використовуються) в змінних; заміняти часті виклики процедур на вбудовані процедури; використовувати константи; передавати парамет-

ри за значенням, а не за посиланням; використовувати необов'язкові параметри стандартних типів; колекції об'єктів.

Графічний характер Windows зумовлює вплив швидкодії графічних і інших операцій відображення на загальне сприйняття додатка. Для прискорення екранного виводу треба керуватися таким: встановлювати властивість ClipControls елементів-контейнерів в False; коректно використовувати властивість AutoRedraw; використовувати елементи керування-образи Image замість елементів керування-зображень PictureBox; приховувати елементи керування для уникнення регенерацій зображення; використовувати метод Line замість PSet.

Досвід розробки програм, що були створені для вирішення задач транспортного обслуговування, показав, що суб'єктивне сприйняття швидкодії додатків відрізняється від фактичної швидкості їх виконання. Важливим є швидкість старту, виводу інтерфейсу, роботи в діалоговому режимі. Тому для кращого сприйняття додатків слід зберігати форми прихованими, але завантаженими; попередньо завантажувати та підвантажувати потрібні дані; використовувати індікатори процесу; прискорювати запуск додатка. Реактивність (час запуску) можна скоротити такими прийомами: максимально спростити стартову форму; не завантажувати модулі, що безпосередньо після запуску не потрібні; запустити спочатку невеликий допоміжний додаток, щоб попередньо швидко завантажити DLL-бібліотеки середовища виконання.

Запропоновані засоби дозволяють значно збільшити швидкість обчислень, обробки даних, графічних операцій при розробці інформаційного забезпечення транспортного обслуговування [70].

Розглядаючи доцільність оптимізації та її шляхи, слід співставити потенційний ефект та витрати. Треба також визначити компоненти додатка, де вдосконалення будуть явно ефективні та корисні для користувача. При моделюванні конкурентного середовища транспортного сервісу, а також управління автотранспортним підприємством, виникають задачі, комплексне розв'язання яких можливе лише при використанні відповідних комп'ютерних технологій. Як інструментальний засіб доцільно використовувати сучасне інтегроване середовище розробки додатків Net.

Зараз активно розробляються прикладні програми для розв'язання різноманітних локальних задач транспортного обслуговування. Так, у роботі [100] наведені алгоритм та графічний інтерфейс модуля складання графіку спільної роботи автомобілів у логістичній системі. Програма

(з фрагментами інтерфейсів) по розрахунку значень критеріїв ефективності роботи автомобілів у логістичній системі наведена в праці [49].

Важливим аспектом розробки програм та інтерфейсів є забезпечення коректності даних, що вводяться. Необхідна розробка загальних підходів, методів перевірки вхідних даних при комп'ютерній реалізації цих задач, комплексний розгляд питань створення та експлуатації стійкого (з точки зору вхідних даних, їх обмежень та взаємодії) програмного забезпечення при створенні інформаційних систем транспортного обслуговування [154].

Перевірка введення до того, як дані надійдуть до програми для обчислень забезпечує якість даних, що зберігаються в базах або використовуються при розрахунках. Виключається можливість помилок, непередбачених дій програм, викликаних некоректними даними. Ретельний контроль введення робить інтерфейси програм "дружніми" по відношенню до користувача, прискорює введення даних.

При розробці прикладних програм для транспортного обслуговування були розглянуті питання перевірки достовірності введення: перевірка достовірності даних на рівні поля та форм; прискорення введення з клавіатури шляхом фільтрації даних; використання шаблонів для підказок при вводі даних; обмеження вибору користувача списками можливих значень; обробка поля форми, яке потребує обов'язкового введення; перевірка достовірності введення даних в залежні поля форми [154].

Після визначення принципів перевірки введення доцільно розробити нестандартні елементи керування (custom controls) для контролю введення. Їх можна використовувати для контролю введення при подальшій розробці програм. Взагалі перевірка достовірності введення є процесом перевірки введених користувачем даних до їх передачі в програму. Перевірка достовірності є проактивним процесом (носить попередній характер) і відбувається під час введення даних. Слід відрізняти перевірку достовірності введення від виявлення помилок введення. Останнє є післядією (реактивним процесом) і відбувається вже після введення даних. Перевірка достовірності введення потрібна саме для попередження помилок введення.

Добре організований контроль введення виключає виникнення помилок введення та знимає необхідність створення додаткових засобів обробки помилок введення всередені програми. Перевірка достовірності введення може бути водночас підказкою з введення припустимих значень. Прикладом цього є список значень для поля введення.

Якщо користувач має обмежену кількість варіантів заповнення поля, це зменшує можливість виникнення помилок. Засоби перевірки достовірності введення можуть редагувати вхідні дані, не потребуючи від користувача їх виправлення. Якщо необхідні великі літери, програма повинна автоматично їх перетворювати. Вона не повинна чекати, доки користувач набере текст у різних регістрах, а потім інформувати про помилку, вимагати повторення, виправлення введення. Важливою є перевірка введення даних на рівні форми в цілому. Процедури контролю введення повинні забезпечити заповнення припустимими даними всіх обов'язкових полів форми. Якщо є кілька таких полів, треба забезпечити попередню спільну перевірку їх змісту до передачі даних у програму.

Залежні поля також треба перевіряти. Ці поля не є обов'язковими, вони використовуються у випадку, коли користувач повинен ввести додаткові дані. Так, якщо користувач вказує на формі, що необхідне додаткове замовлення транспортних засобів (крім власних), то перевірка достовірності введення повинна гарантувати, що у полях джерела додаткових транспортних засобів будуть введені необхідні значення.

Іншим прикладом необхідності перевірки достовірності введення в залежні поля є випадок, коли значення (введене в одне поле) потребує, щоб значення в іншому полі знаходились в певному диапазоні.

Наприклад, якщо вартість перевищує певну суму, треба задати максимальну граничну знижку. Тоді обидва поля треба спільно перевіряти перед тим, як користувач збереже запис у базі вхідних даних.

Таким чином, перевірка достовірності введення даних не є простою перевіркою припустимості даних, що введені у поле. Вона є набором засобів для забезпечення програми якісними за змістом, взаємоузгодженими даними. Тому при проектуванні форм для введення даних попередньо розробляється повний список правил перевірки достовірності введення, а також відпрацьовується відповідне програмне забезпечення. Незважаючи на те, що кожна форма для введення даних є унікальною, при розробці засобів контролю введення треба керуватися загальними принципами.

Практично всі поля введення даних вимагають, в тій чи іншій формі, забезпечення перевірки достовірності введення. Тому перед проектуванням та створенням форми в цілому необхідно скласти список всіх необхідних для неї полів введення та розглянути для кожного з полів та їх разом питання: чи є поле обов'язковим; які символи є припустимими

(неприпустимими); якщо поле є числовим, чи існує діапазон його значень; чи існує для цього поля список припустимих значень; чи є поле залежним.

Треба обмежити натискання клавіш тільки припустимими. Якщо поле повинне бути числовим, необхідно виключити можливість введення літер. Якщо не повинно бути пробілів, відповідну клавішу треба заборонити. Можна обмежити варіанти введення за допомогою списку припустимих значень, щоб була лише можливість вибрати варіант з переліку або натиснути кнопки-перемикачі. Програма повинна інформувати користувача про обмеження діапазонів введення (якщо для поля визначені граничні значення, треба попередити користувача).

Треба виділяти на формі обов'язкові поля (шляхом відзначення певним символом, зміною кольору фону тощо). Якщо введення у поле викликає необхідність заповнення інших полів, слід згрупувати залежні поля разом, а також заблокувати введення до залежних полів, доки не введені дані в головне поле.

Перший рівень перевірки достовірності введення – рівень полів. На цьому рівні можна забезпечити введення припустимих символів, даних у необхідному форматі, припустимих значень (на основі переліку їх можливих варіантів).

Одним з засобів є фільтрація вводу з клавіатури за допомогою клавішних фільтрів. При цьому натискання клавіш перехоплюються до того, як відповідні символи з'являться на екрані, крім того відбувається фільтрація неприпустимих символів. Натискання небажаних клавіш може супроводжуватися сигналом. Можна перетворювати неприпустимі клавіші на припустимі, або їх ігнорувати, не відображаючи у полях вводу.

На формах можуть бути застосовані поля зі спеціальним форматом введення. Тоді треба створювати спеціальні елементи керування Masked-Edit controls, здатні відповідним чином форматувати та відображати дані.

Поширеним засобом перевірки достовірності введення на рівні полів є застосування списку припустимих значень, що містить всі можливі значення для поля введення та відображається у вигляді списку Drop-down listbox control.

Використання списків припустимих значень потребує значного обсягу програмування, але гарантує безпомилкове введення даних. Пере-

лік припустимих значень можна завантажити до списку на початку програми в процедурі FormLoad або динамічно – під час роботи програми.

Контроль введення на рівні форми є важливою частиною перевірки достовірності введення. Ряд помилок можна виявити на рівні полів, але деякі перевірки достовірності введення можна виконати тільки на рівні форми. Якщо контроль на рівні полів відбувається при натисканні клавіш (змін "фокусу вводу"), то контроль на рівні форми виконується після натискання користувачем клавіші Enter (командних кнопок), тобто після заповнення всіх полів форми, але до передачі даних у програму.

Перевірка достовірності введення на рівні форми включає перевірку залежних, незалежних та обов’язкових полів. Звичайно така перевірка проводиться на рівні полів. Але доцільно виконувати її саме на рівні форми. Якщо вводяться значення, що виходять за межи діапазону, фокус введення треба повернути у поле з невірними даними для їх виправлення.

Встановлення фокусу вводу треба виконувати поза подіями GotFocus, LostFocus інших елементів керування. Користувач може обминути поле, тому розміщення процедур перевірки незалежних полів на рівні подій окремих елементів створює можливість невиконання контролю. Форми можуть мати поля, що підлягають обов’язковому заповненню. Перевірка їх також здійснюється на рівні форми. При цьому треба перевіряти довжини строк у текстових полях, виключити введення пробілів, їх сприйняття як даних. Якщо наявність даних в одному полі обумовлює необхідність введення даних в інші поля, треба забезпечити контроль залежних полів.

Наведені принципи контролю введення враховують основні випадки, що виникають при проектуванні форм [154]. При створенні спеціалізованих засобів контролю введення слід одночасно виконувати повну перевірку введення як на рівні окремих полів, так і на рівні форми (або кількох взаємопов’язаних форм) проекту. Необхідне створення набору спеціалізованих елементів керування, що мають відповідні методи для перевірки достовірності введення з урахуванням взаємовідповідності даних у задачах транспортного сервісу. Надалі такі елементи керування можна використовувати при розробці інформаційних систем різного призначення.

Розділ 9. Моделювання інформаційного впливу соціальних мереж на лояльність клієнтів

9.1. Проблеми і перспективи впливу соціальних мереж на лояльність клієнтів

Зазначено, що основна мета сучасної маркетингової стратегії направлена на формування сприятливих взаємовідносин з клієнтами. Показано кореляцію економічної лояльності з реальною поведінкою клієнтів.

Стратегія управління взаємовідносинами з клієнтами побудована на моделі взаємодії, в якій центральне місце в бізнесі займає клієнт, а основними напрямами діяльності є заходи з підтримки маркетингу, продажів та обслуговування клієнтів. Інформаційні технології дають нову платформу для поширення взаємовідносин з клієнтами. Такою платформою є соціальні мережі.

Основна мета сучасних маркетингових досліджень направлена на формування сприятливих взаємовідносин з клієнтами. В процесі еволюції бізнес-діяльності формування відносин з клієнтами пройшло ряд етапів. У 50-60-ті роки XX сторіччя формула відносин між клієнтом та бізнесменом була такою: витрати виробництва складалися з бажаним прибутком та таким чином встановлювалися ціни на продукти. Тобто умови диктували виробники і, відповідно, цей період називався періодом ринку виробника. З 70-х років згадане співвідношення змінилось на визначення прибутку, як різниця між ціною та витратами на виробництво. З цього періоду почалося становлення ринку споживача. В цих умовах успіх виробника залежить від швидкості його реакції на запити споживача, явні і передбачувані. У відповідь на зміну ринку стали з'являтися різні системи менеджменту, і в 80-ті роки утвердився ринок споживача. Ринки наповнилися продукцією. Почала з'являтися конкуренція. Постійні зміни у організації виробництва, товарному різновиді, тощо – це був нормальний стан сучасної компанії. В зв'язку з новими змінами необхідні були гнучкість та висока швидкість реакції на зміни. З 2000-х років почалася інтеграція бізнес-процесів підприємств у рамках холдингу або вертикально-інтегрованої компаній, тобто на перший план вийшло процесно-орієнтоване партнерство.

У наші часи маркетинг передбачає широке використання найвигідніших ринкових можливостей [30; 130]. Він залежить від виробництва і забезпечує випуск виробниками лише тих товарів, які можуть бути реалізовані. Звідси випливає важливість маркетингу як процесу, що пов'язує виробника зі споживачем через торгівлю і забезпечує зворотні зв'язки між ними. Маркетинг — це управлінська діяльність, що вивчає всі види діяльності, пов'язані із спрямуванням потоку товарів і послуг від виробника через систему реалізації (у визначених умовах) до кінцевого споживача. Маркетинг охоплює всі аспекти діяльності організації. Усі його функції направлені на одну загальну мету – підвищення лояльності клієнтів. Лояльність (англ. loyalty – вірність) – характеристика клієнта, покупця, яка визначає його прихильність певному продавцю, бренду тощо [250].

Істотний внесок у вивчення ефекту лояльності вніс Фредерик Райхельд (президент міжнародної консалтингової фірми Baind and Company). Він зібрав матеріал щодо проведення маркетингових досліджень, здійснюваних різними компаніями на предмет установленнями ступеня задоволеності споживачів.

Лояльність – це якість, що властива для користувача цінності (товару, послуги), який щоразу повертається до свого джерела й передає це джерело в спадщину [204]. Іншими словами лояльність – це відданість своєму джерелу цінностей. Лояльний покупець не міняє джерело цінностей і рекомендує його своєму оточенню.

Під лояльністю також мається на увазі деяке образно позитивне відношення споживачів у відношенні усього, що стосується діяльності організації, а саме продуктів і послуг, вироблених, проданих або наданих організацією, її персоналу, іміджу, торговельних марок, логотипу. Саме наявність цієї лояльності, тобто сприятливого відносини споживачів до даної компанії, продукту і є основою для стабільного обсягу продажів. Що у свою чергу є стратегічним показником успішності компанії.

Ступінь лояльності клієнта характеризується його прихильністю до певної марки продукту й виміряється зазвичай числом повторних покупок продукту. Вищою формою лояльності споживачів є фанатичне шанування бренда – продукту, якому споживачі надають перевагу і придбають не керуючись засадами "ціна-якість". Лояльними можна назвати тих споживачів, які досить довго (порівняно зі строком функціонування товару) залишаються з компанією й роблять при цьому повторні покупки [266].

Однією з основ лояльності є позитивний досвід споживача у процесі покупки або споживання даного товару або послуги.

Постійні клієнти – це в основному ті, хто роблять повторні покупки однієї й тої ж марки. Багато фахівців розглядають цей фактор (здійснення повторних покупок) як ключовий в розвитку компанії. Взагалі, чим довше споживач спілкується з компанією, тим більше він для неї цінний. Таких споживачів можна образно називати довгостроковими споживачами. Вони купують більше, менше вимагають до себе уваги в плані сервісу й часу для обслуговуючого персоналу, менш чутливі до зміни цін, а також сприяють залученню нових клієнтів. Довгострокові споживачі настільки цінні, що в деяких сферах бізнесу збільшення числа довгострокових споживачів усього на 5 % у загальній структурі клієнтів приводить до збільшення прибутків на 100 % [199]. Традиційно лояльність розглядають у трьох аспектах: лояльність споживачів, співробітників, інвесторів. Для детального аналізу лояльності клієнтів доцільно виокремити певні типи лояльності: транзакційна, перпенційна, комплексна [374]. У табл. 9.1 наведені характеристики цих типів.

Таблиця 9.1

Характеристики лояльності клієнтів

Транзакційна лояльність	Перцепційна лояльність	Комплексна лояльність		
		істинна лояльність	хибна лояльність	латентна лояльність
Розглядає зміни в поведінці клієнтів за допомогою показників повторної покупки, частки конкретної торгової марки у загальних обсягах покупок	Акцентує увагу на таких аспектах, як суб'єктивні думки споживачів та їх оцінки (задоволеність, довіра)	Споживач задоволений виробами і купує їх регулярно, не чутливий до дій конкурентів	Споживач не задоволений. Він здійснює покупку виробів конкретної організації у зв'язку з сезонними або накопичувальними знижками, або ж у зв'язку з тимчасовою недоступністю виробів марки, яка йому більше подобається	Споживач високо оцінює конкретну організацію, але не має можливості часто купувати її, проте всякий раз, коли в нього з'являється можливість, він здійснює купівлю виробів цієї марки

Крім того, лояльність характеризується впливом таких факторів: особисті комунікації, раціональні фактори, функціональні фактори, іміджеві фактори.

Особисті комунікації – довгострокові зв'язки між співробітниками підприємств, суб'єктів торгового маркетингу, дозволяють оперативніше й ефективніше вирішувати різні питання, а також полегшують пошук компромісу при виникненні спірних ситуацій. З іншого боку, занадто велике значення особистих комунікацій позбавляє гнучкості і перешкоджає приймати раціональні рішення.

Раціональні фактори – якість самого товару. Найбільш значимий фактор – співвідношення ціни і якості. Посередники віддають пріоритет збуту великим партіям стандартних товарів відповідної якості за середньоринковими цінами.

Другий за значимістю фактор – це асортимент. Якщо він недостатньо широкий, посередник рано чи пізно зробить вибір на користь постачальника, що пропонує максимально широкий діапазон товарів.

Функціональні фактори – це умови оплати, доставки та просування товарів, додаткові послуги. На досить розвинутому ринку компанії пропонують приблизно однаковий пакет умов, тому контрагенти намагаються оперувати іншими факторами, такими, як набір додаткових послуг, оперативність вирішення тактичних питань, компетентність персоналу.

Іміджеві чинники – частка ринку, репутація бренда, компетентність персоналу, стабільність і надійність підприємства. Фактори стабільності і надійності підприємства, його репутація не потребують коментарів, оскільки саме вони служать гарантією подальшого просування товару на ринку і своєчасної оплати послуг посередника.

Крім того, імідж підприємства-виробника має дуже велике значення для іміджу підприємства-посередника. До категорії іміджевих можна віднести проведення різних корпоративних заходів для контрагентів, які справляють незабутнє враження на партнерів і вносять значний внесок у зміцнення лояльності.

Ступінь задоволеності клієнта є фактором емоційної лояльності. На перший погляд здається, що емоційна не піддається вимірюванню та управлінню. Однак на практиці емоції клієнтів можна не тільки вимірювати, але і направляти в потрібну для компанії сторону. Так чи інакше, компанії завжди намагалися зрозуміти, що відчувають клієнти по відношенню до них.

Але проблемою є те, що позитивно відповідаючи на питання про ступінь задоволеності продуктами або роботою компанії, високо оцінюючи свою готовність обрати цю компанію ще раз або повторно здійснити покупку, на ділі клієнти часто демонстрували протилежну поведінку – негативну економічну лояльність. Тобто, просто, покидали компанію. Виникала парадоксальна ситуація: задоволений з точки зору вимірювання клієнт перестає купувати.

Після багатьох років досліджень, кількох тисяч опитаних клієнтів і десятків тисяч заданих питань Фредом Райхельдом було знайдено рішення. Ним виявився питання про те, з якою ймовірністю клієнт порекомендує "свою" компанію знайомим або друзям. Відповіді показали статистично найсильнішу кореляцію з реальною поведінкою клієнта по відношенню до компанії з точки зору його економічної лояльності (рис. 9.1) [199].

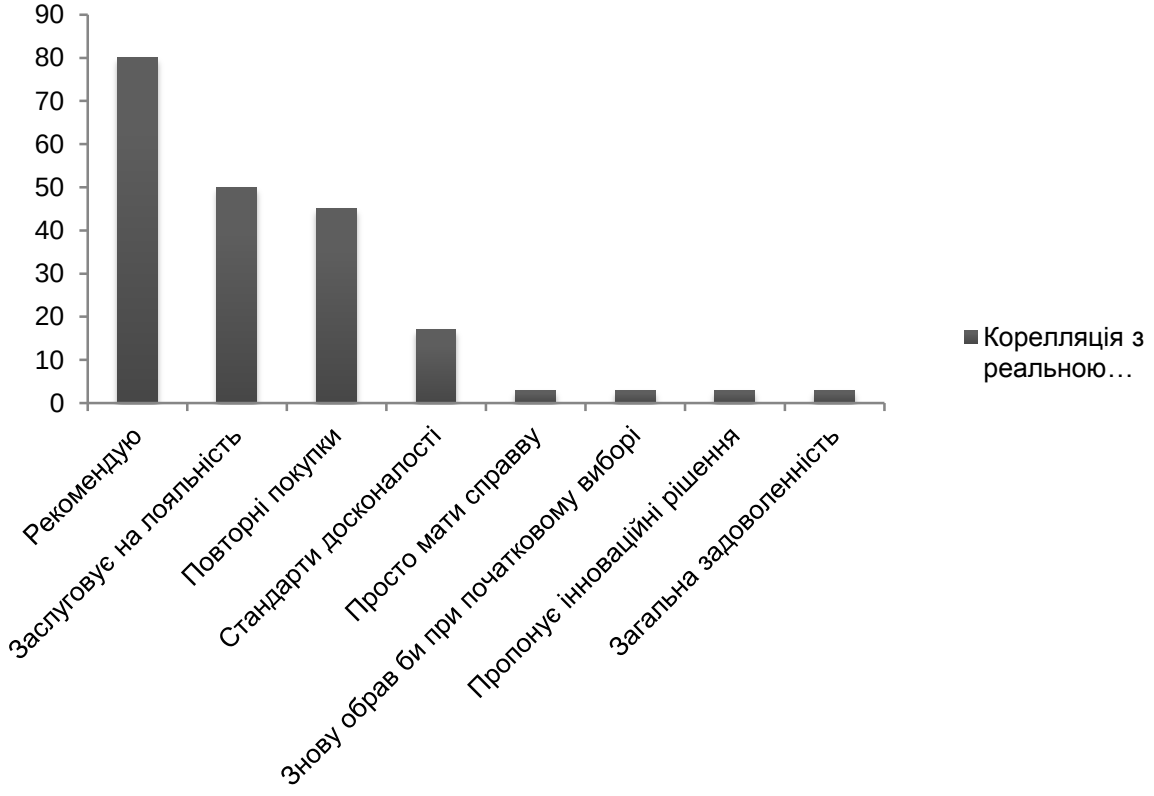


Рис. 9.1. **Кореляція економічної лояльності з реальною поведінкою клієнта**

Частина найбільш лояльних до компанії клієнтів готова прийняти на себе особисті репутаційні ризики і позитивно рекомендувати дану компанію на ринку (клієнти – промоутери). Друга частина клієнтів, як правило, задоволена тим, як працює компанія, але не готова брати на себе

репутаційні ризики і рекомендувати її (пасивні клієнти). І, нарешті, третя частина клієнтів – це клієнти, які отримали негативний досвід спілкування з компанією і дають їй "контррекомендації" на ринку (клієнти – детрактори).

Крім того, проведені дослідження показали, що для встановлення зв'язку "лояльність – прибуток", необхідний системний підхід, який дасть компанії можливість побудувати бізнес-модель, засновану на лояльності клієнтів (рис. 9.2).

Сьогодні існують різноманітні методи управління відносинами з клієнтами, але зараз найбільш популярним є підвищення їх лояльності за допомогою соціальних мереж.

Рис. 9.2. **Модель бізнесу, заснована на лояльності клієнтів**

Управління взаємовідносинами з клієнтами (CRM, Customer Relationship Management) стало зараз одним з найбільш модних термінів. CRM – це технологія, націлена на завоювання, задоволення і збереження платоспроможних клієнтів. CRM є стратегією, яка може бути обрана в якості напряму розвитку бізнесу практично будь-якою компанією за таких умов [400]:

стратегія CRM застосовна там, де є конкуренція і її рівень досить високий;

стратегія CRM потрібна, якщо є зацікавленість у зростанні бізнесу;

стратегія CRM вимагає певного масштабу. Тільки середній і великий обсяг бізнесу окупить інвестицій в IT та бізнес-процеси;

стратегія CRM може бути застосовна тільки на основі сучасних IT-технологій.

Іноді тим же терміном називають технологію, яка забезпечує досягнення обраної CRM стратегії і навіть програмні системи, розроблені для підтримки цих технологій. Стратегія CRM розвивалася з розвитком ринку. Етапи її еволюції наведені на рис. 9.3 [400].

Рис. 9.3. **Етапи еволюції CRM**

Метою стратегії є вибудовування міцних і тривалих відносин із клієнтами. Такі відносини повинні бути вигідні обом сторонам – і для самої компанії, і для її клієнтів [246; 247].

Безликий символ – "клієнт" стає справжнім тільки в тому випадку, якщо це конкретна персона. Якщо ж в якості клієнта виступає компанія, то справа ведеться з різними людьми, що виконують різні ролі і мають, взагалі кажучи, різні, часто протилежні інтереси. Найбільш важливими є такі ролі усередині компанії-клієнта: Покупець – той, хто може купити або купує товари чи послуги; платник – той, хто оплатив придбання товарів і

послуг; користувач – той, хто використовує куплені у вас товари та послуги; клієнт – той, хто має якесь відношення до вашої компанії (сюди включені і всі попередні ролі).

CRM можна описати у вигляді протяжного в часі циклу відносин із клієнтом (рис. 9.4).

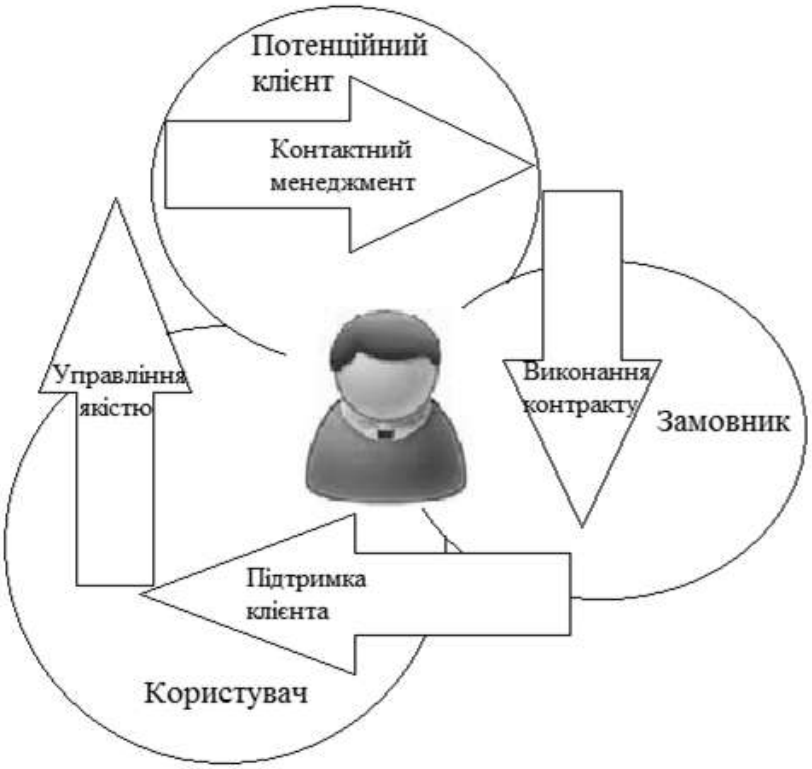


Рис. 9.4. **Цикл відносин з клієнтом**

Клієнта треба залучити. Сюди відноситься період від першого контакту до юридичного оформлення угоди.

Клієнта треба задовольнити, забезпечивши позначеними в договорі товарами або послугами. Це в період виконання контракту.

Клієнта не можна кидати після завершення робіт. Починається період підтримки клієнта. На цей етап слід віднести вивчення бажань і потреб клієнта. Одна з ідей CRM полягає в тому, щоб не тільки і не стільки чекати ініціативи від клієнта, скільки спробувати намацати те, що, можливо, приверне його увагу і дозволить знову перейти до першого етапу – продаж йому нових товарів і послуг. Клієнта треба вмовити на наступний контракт. Клієнт повинен не просто залишитися задоволений виконанням договору, але, з одного боку, прийти до рішення про укладення нової угоди, а з іншого – бути впевненим з тому, що постачальник знову опиниться на висоті.

Таким чином, відносини з клієнтом є спіраль, що розкручується, на кожному витку якої розширюється віяло надання клієнту товарів і послуг, зміцнюються і затверджуються ділові контакти, підвищується якість обслуговування клієнта.

Сучасні інформаційні технології дають нову платформу для поширення взаємовідносин з клієнтами. Це соціальні мережі, що будуються на просторах Інтернету [211; 222; 389].

Онлайновий соціальний граф – це всесвітня павутина людей – система зв'язків між людьми, які користуються сайтами соціальних мереж на зразок Facebook, Linkedin, Hoover's Connect тощо [174; 324]. Соціальний граф для людей означає те ж саме, що WWW для сторінок, з'єднаних гіперпосиланнями: засіб організації, фільтрації та асоціації. Після того, як Інтернетом були з'єднані всі комп'ютери, сайти і сторінки, прийшов час для наступної цифрової революції – з'єднання людей. Метадані веб-сторінок, такі, як їх заголовки, ключові слова і система зв'язків з іншими сторінками, були найважливішим інструментом, що дозволив нам знаходити інформацію в Інтернеті й оперувати нею. Аналогічно метадані соціального графа, що описують конкретних людей – місце їх роботи, вид діяльності, інтереси, коло друзів, дозволяють управляти безліччю взаємин з величезною кількістю людей у соціальних мережах.

Соціальна мережа (англ. social network) – соціальна структура, що складається з групи вузлів, якими є соціальні об'єкти (люди або організації), і зв'язків між ними [399]. Термін "соціальна мережа" був введений задовго до появи Інтернету і власне сучасних Інтернет-мереж, ще в 1954 році соціологом "Манчестерської школи" Джеймсом Барнсом.

Сучасне поняття соціальної мережі означає певне коло знайомих людини, де є сама людина – центр соціальної мережі, її знайомі – гілки цієї соціальної мережі і відносини між цими людьми – зв'язки. Якщо розглядати соціальну мережу більш глибоко, то можна виявити, що зв'язки діляться за типами: односторонні і двосторонні; мережі друзів, колег, однокласників, однокурсників. У другій половині XX століття соціальні мережі стали активно розвиватися, спочатку вони стали популярними на заході, трохи пізніше прийшли і до нас. Потім це звичайне професійне поняття соціологів перетворилося на модну концепцію, одну з центральних у веб 2.0. Соціальні мережі, піддаються умовної класифікації, тобто поділу за певними ознаками (табл. 9.2) [211; 248; 324].

Таблиця 9.2

Класифікація соціальних мереж

Ознака класифікації	Вид соціальної мережі
Тип	1. Для пошуку людей (Одноклассники.ру). 2. Для розваги (ВКонтакте). 3. Для роботи і бізнесу (МойКруг). 4. Для збору новин (news2.ru). 5. Для збору закладок (БобрДобр). 6. Для відео (YouTube). 7. Для аудіо (Last.fm). 8. Для фото (FiXX.RU). 9. Нішеві соціальні мережі (Хабрахабр, drugme, geni та інші)
Відкритість	1. Відкриті (FaceBook). 2. Змішані (ПРО2). 3. Закриті (PlayboyU.com)
Географічне охоплення	1. Світові (MySpace). 2. В межах країни (Connect.com.ua). 3. В межах регіону
Рівень розвитку	1. Web 1.0. 2. Web 2.0. 3. Web 3.0

Усі соціальні мережі поділяються за типом. Є мережі для пошуку юдей: однокласників, однокурсників, колег та інших людей. Є бізнес-мережі, для пошуку роботи, партнерів, професійного спілкування та інших ділових питань. Деякі мережі призначені для відео, деякі для аудіо і конкретно музики, а деякі для фото. Є й нішеві мережі, які можуть не потрапляти під перераховані категорії.

Також умовно мережі можна розділити за географічною орієнтацією: світові або для конкретної країни. Крім того, в різних мережах порізному ставляться до політики відкритості інформації. Більшість мереж на даний момент відкриті, але є і закриті, куди люди потрапляють тільки на запрошення.

Закриті мережі тільки починають з’являтися, але вже можна чекати їх популярність через кілька років – людям, природно, подобається все заборонене і важкодоступне.

За рівнем розвитку соціальні мережі можна поділити на веб 1.0 – перші соціальні мережі з базовим функціоналом, веб 2.0 – сучасні соціальні мережі з широким функціоналом для спілкування та веб 3.0 – соціальні мережі майбутнього, які вирішують конкретні проблеми та підвищують лояльність існуючих та потенційних клієнтів .

Розумінню структури і можливостей соціальних мереж сприяє їх класифікація з позицій домінування та комунікативності. В роботі [50] якій запропоновано 4 типи мережних структур (рис. 9.5).

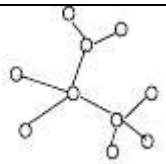
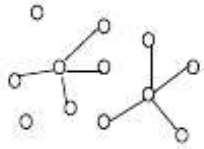
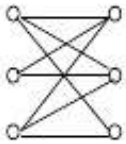
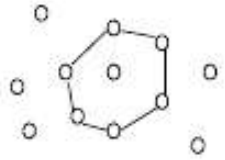
		Комунікативність (зв'язність)	
		висока	низька
Домінування	високе		
	низьке		

Рис. 9.5. **Типи мережних структур**

Висока домінантність і висока комунікативність притаманні "супутниковій" структурі, де ресурси переміщуються від центру до периферії.

У системі з високим ступенем домінування більшість зв'язків будуть з'єднувати "центри" і "кліки", тобто найбільш активні актори мережі.

У системі з високою зв'язаністю і низькою домінантністю загальне число зв'язків розподілено відносно рівномірно таким чином, що потоки спрямовані від одного фрагмента системи до іншого.

Ця структура добре моделює гіпертекстову комунікацію, де не передбачається контролю центру над периферією.

Система з низькою комунікативністю і високою домінантністю зосереджує зв'язки в певних ареалах співтовариства і позначає його декомпозицію. Такого роду "ідеальні типи" мереж дозволяють типологізувати різні види комунікації.

Система з низькою комунікативністю і низькою домінантністю властива дифузним, слабоінтегрованим популяціям.

Не зважаючи на різноманіття соціальних мереж, всі вони мають спільну властивість, що є суттєвою для бізнесу – це можливість зв'язків з широким колом клієнтів.

Перевагою участі бізнесу підприємств у спілкуванні з клієнтами на просторах соціальних мереж є велика їх кількість у WWW.

Сучасні технології змінили саме розуміння спілкування. Якщо раніше компанії відділялися і навіть в деякому сенсі нехтували соціальними

мережами і взагалі Інтернетом, то зараз вони розробляють свої подібні Інтернет-проекти.

Перевагами соціальних мереж є можливість з їх допомогою налагоджувати взаємовідносини з клієнтами, а також здійснювати їх моніторинг. Це новий вид управління, який здійснюється за допомогою Social CRM (SCRM – social customer relationship management).

У багатьох сенсах традиційні системи CRM були важливими попередниками сьогоднішніх сайтів соціальних мереж. На найпростішому рівні CRM є базою контактів.

Це інструмент "однонаправленого" соціального нетворкінгу, що дозволяє бізнесу бачити профілі своїх клієнтів, фіксувати інформацію про хід угоди, оцінювати ефективність роботи, спілкуватися з контактними особами і ділитися інформацією всередині своєї компанії з менеджерами продажів і іншими співробітниками [324].

Головна відмінність сайтів соціальних мереж полягає в тому, що вони пропонують двонаправлену видимість і взаємодію.

Це перетворює динаміку продажів у щось більше, ніж партнерство "з непарним числом партнерів" (табл. 9.3).

Таблиця 9.3

Порівняльна характеристика CRM та сайтів соціальних мереж

Характеристика	CRM	Сайти соціальних мереж
Встановлення нових зв’язків	Покупка маркетингового списку, сканування візиток та бейджиків з конференцій, розміщення на сайті форми "Зв’яжіться з нами"	Зв’язок може бути ініційовано будь-якою стороною, але рішення про контактування повинно бути взаємним
Показ контакту/особистої інформації	Записи акаунту	Сторінка профілю
Доступність даних, оновлення, оповіщення	Команді з продажів, менеджеру з продажів	За замовченням – друзям та їх мережі, але налаштування приватності можуть бути змінені
Механізми комунікацій	Шаблони електронної пошти, оповіщення	Повідомлення, замітки
Оновлення даних	Торговими представниками або адміністраторам системи	Підхід "знизу вгору": кожен сам відповідає за оновлення інформації про себе

Бурхливий розвиток соціальних CRM викликаний в першу чергу тими можливостями, які надають соціальні мережі для залучення клієнтів. Основні переваги соціальних мереж перед традиційними CRM полягають в такому [246; 247]:

наявність інформації про потенційних клієнтів у соціальних мережах. Соціальна мережа вже наповнена інформацією про потенційних клієнтів. З великою ймовірністю істотна частина клієнтів, інформацію про які в CRM треба буде вносити, у соціальній мережі вже присутня. Наприклад у соціальній мережі "ВКонтакті" в березні 2012 року щоденна аудиторія перевищувала 29 мільйонів осіб, у соціальній мережі Facebook понад 900 мільйонів користувачів. Таким чином, кожен житель планети, який присутній в соціальній мережі, вже врахований в ній з усією контактною інформацією, уподобаннями, друзями тощо. Це не означає, що автоматично можна отримати всю інформацію про користувача соціальної мережі. Однак сучасні пошукові інструменти дозволяють вирішити ці завдання, які досить розвинені в тих же соціальних мережах. Наприклад, за e-mail можна автоматично відстежити всі контакти користувача, які вже зареєстровані у мережі. І це набагато простіше і швидше, ніж заповнити базу клієнтів у CRM;

наявність необхідних комунікаційних інструментів для роботи з клієнтами всередині соціальної мережі. У соціальних мережах не потрібна спеціальна поштова програма для відправки повідомлень. Інструменти листування користувачів мережі вбудовані в саму мережу;

гарантована доставка повідомлення до отримувача. Одержувач точно побачить повідомлення з мережі, воно не буде піддано і затримано спам-фільтрами, оскільки зв’язки в мережі дружні, а блокувати повідомлення друзів недоречно;

простота доступу до інформації. Якщо вам потрібно подивитися історію листування з конкретною людиною – просто зайдіть на його картку і дивіться. Приховувати інформацію від друзів також немає сенсу;

швидкість поширення інформації. Плануєте провести маркетинговий захід – напишіть інформацію про нього в соціальній мережі, запросіть друзів його відвідати, отримаєте список тих, хто відгукнувся. І все це буквально в кілька кліків, значно простіше, ніж у традиційних CRM-систем. Щоб поширити відомості про компанію, продукт, нову маркетингову ініціативу тощо досить просто помістити інформацію в мережі і запросити друзів її переглянути. З’явилися компанії, у яких немає корпоративного сайта, але є кілька сторінок на Facebook;

низька вартість. Тут соціальним мережам точно немає конкурентів. Реєстрація та більшість можливостей безкоштовні. Порівняйте з вартістю будь-якої, навіть найдешевшої CRM-системи. Інтерфейс інтуїтивно простий і зрозумілий, причому не потрібно платити спеціалізованій компанії за впровадження. Але ще більш важливо, що взагалі не треба дбати і нести витрати на супровід даної інформаційної системи. Очевидно, що її обслуговують фахівці досить високого рівня, і сервери, які за вартістю, швидше за все, значно перевищують річний оборот компанії малого бізнесу;

технологічна надійність. Соціальна мережа доступна 24 години на добу 7 днів на тиждень, має інтерфейси всіма поширеними мовами, працювати з нею можна практично з будь-якого пристрою, що підключений до Інтернету і має браузер. Звичайно, жодна соціальна мережа, принаймні, безкоштовна, не гарантує, що ваші дані ніколи не загубляться, не буде збоїв, хакери не пошкодять вашу інформацію, але, як показує практика, інцидентів такого типу майже не трапляється.

І при інших рівних надійність CRM-системи, за якою наглядає невеликий IT-відділ або просто системний адміністратор, швидше за все, буде нижче, ніж у будь-якій соціальній мережі;

низькі витрати на підтримку інформації про клієнтів в актуальному стані. У разі використання CRM-системи потрібно витрачати на це як мінімум час співробітників.

У разі соціальної мережі користувачі оновлюють інформацію самостійно або, принаймні, мають можливість її самостійно оновити, якщо ви їх попросите; широке охоплення молодіжної аудиторії.

А це клас потенційних співробітників, які знайомі з роботою в соціальних мережах і, швидше за все, будуть зацікавлені продовжувати займатися улюбленою справою та ще й отримувати за це зарплату.

Тому очевидним напрямом розвитку CRM-систем є їх інтеграція з соціальними мережами, тобто через SCRM. Згідно зі звітом Gartner, 80 % зростання CRM ринку в 2010 році було обумовлено саме розвитком соціальних CRM-технологій. Згідно з висновками експертів, обсяг інвестицій в цей сектор у наступному році досягне 1 мільярда доларів [424].

Social CRM є інструментом, який сприяє кращій, більш ефективній взаємодії з клієнтом і використовує колективний розум більш широкого клієнтського співтовариства з передбачуваним поліпшенням контакту між організацією та її потенційними і реальними клієнтами.

Мета Social CRM полягає в побудові більш близьких відносин з клієнтами і прив'язки їх до компанії шляхом створення громадської екосистеми, для кращого розуміння, чого хочуть і як вони взаємодіють з різними точками дотику компанії, наприклад, продажу, обслуговування клієнтів і т. д.

Організація Chess Media Group відобразила наочну картину еволюції CRM у SCRM [247; 439]. SCRM – це наступний крок до взаємодії з клієнтами. Еволюція відбувається цими напрямами: хто, що, коли, де, чому і як взаємодіє з клієнтами.

Основна відмінність SCRM від CRM полягає в можливості контролю та взаємодії з клієнтами. Контроль більш розосереджений і визначений споживачами, а в центрі уваги знаходиться взаємодія, а не угоди (рис. 9.6).

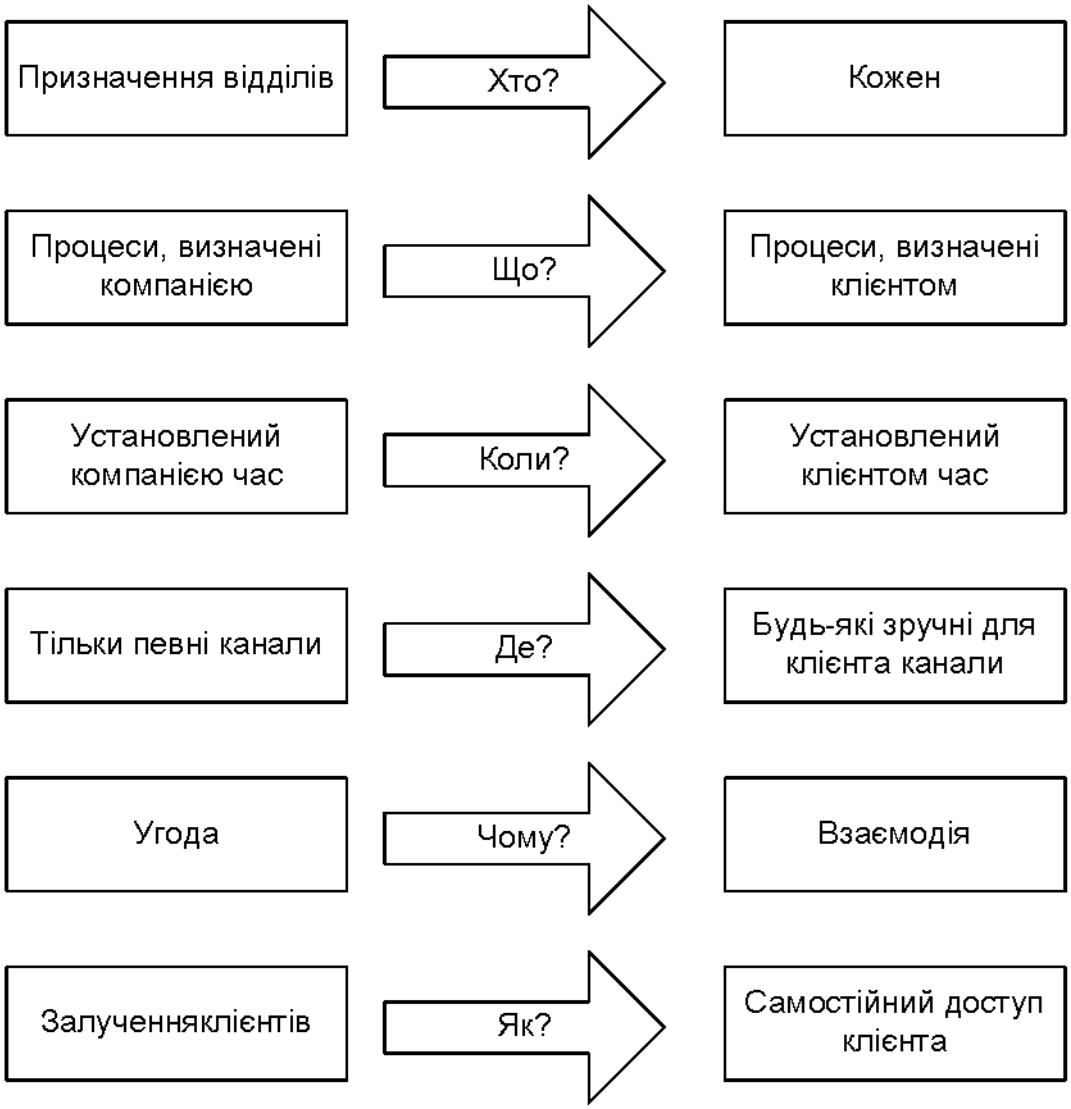


Рис. 9.6. **Еволюція CRM у SCRM**

CRM складається з продажів, маркетингу і функцій на базі обслуговування/підтримки, метою яких було просування клієнтів через канал і утримання клієнтів, які б поверталися за покупками.

Традиційний CRM був заснований на інформації, які бренди можуть збирати про своїх клієнтів, всі з яких увійдуть до CRM-системи. Потім це дозволить компанії краще зорієнтувати різних клієнтів.

PR-відділ у даний час відіграє дуже активну роль у SCRM. Зазвичай PR-віддід здійснює бюджетний контроль і володіє повноваженнями щодо кроків у соціальних медіа порівняно з іншими відділами.

У більшості організацій PR-відділи управляють присутністю бренда в соціальних медіа і залученням клієнтів.

Майбутні зміни щодо до формування лояльності клієнтів проявляться вже в тому, що робота з просування бренда і турбота про інформування клієнтів є найважливішими компонентами SCRM, що обертається навколо клієнта. Клієнт насправді не був частиною CRM – а якщо немає співпраці, то немає відносин.

У SCRM це цілком інакше. Клієнт фактично став координаційним центром, навколо якого працює фірма. Замість нав’язливого маркетингу бренди зараз говорять і співпрацюють з клієнтами для вирішення бізнес-проблем, дають можливості клієнтам розділити з іншими свій власний досвід.

Згідно з аналізом, проведеним агентством Cone Communication, споживачі виділяють три найбільш важливих фактори при виборі компанії [439]:

особистий досвід (98 %);

репутація компанії чи бренда (92 %);

рекомендації друзів і родини (88 %).

41 % клієнтів вважають, що компанії повинні використовувати інструменти соціальних медіа для отримання відгуків про товари та послуги. 43 % споживачів кажуть, що компанії повинні використовувати соціальні мережі для вирішення задач клієнтів.

Тільки 7 % організацій розуміють значення CRM у соціальних медіа.

Перш ніж прийняти рішення про покупку рекомендованих продуктів або послуг, більше чотирьох з п’яти споживачів (81 %) буде виходити в мережу Інтернет, щоб перевірити ці рекомендації, зокрема шляхом дослідження продукту/послуги інформації (61 %), читання для користувача відгуків (55 %) або пошуку рейтингів сайтів (43 %).

Таким чином, соціальні платформи надають нові можливості для бізнесу більш осмислено спілкуватися зі споживачами, потенційними клієнтами, партнерами та співробітниками.

Але серйозним викликом для компаній зараз є адаптація та розвиток відповідно до потреб і запитів цих нових "соціальних" клієнтів. Незважаючи на суб'єктивні фактори ринок соціального CRM розвивається швидкими темпами і, щоб організаціям утримувати своїх клієнтів та залучати нових, треба взаємодіяти з ними через соціальні мереж та розповсюджувати інформацію про товари та послуги, що надаються організаціями, через соціальні мережі.

9.2. Аналіз методів імітаційного моделювання соціальних мереж

Проведено аналіз, який свідчить про те, що серед різноманіття імітаційних підходів моделювання соціальних мереж найбільш перспективними є системна динаміка, дискретно-подієве та агентне моделювання. Основа системної динаміки – побудова графічнних діаграм причинних зв'язків і глобальних впливів одних параметрів на інші в часі. Дискретно-подієве моделювання – це підхід, що пропонує абстрагуватися від безперервної природи подій і розглядати тільки основні події модельованої системи, такі, як: "очікування", "обробка замовлення", "рух з вантажем" та інші.

Найбільш перспективним для моделювання процесів, що відбуваються в соціальних мережах, є агентне моделювання. Це напрям в імітаційному моделюванні, який використовується для дослідження децентралізованих систем, динаміка функціонування яких визначається не глобальними правилами і законами, а навпаки, тоді коли ці глобальні правила і закони є результатом індивідуальної активності членів групи.

Моделювання є одним з основних методів пізнання, формою відображення дійсності і полягає у з'ясуванні або відтворенні тих чи інших властивостей реальних об'єктів, предметів і явищ за допомогою інших об'єктів, процесів, явищ, або за допомогою абстрактного опису у вигляді зображення, плану, карти, сукупності рівнянь, алгоритмів і програм тощо.

Отже, в процесі моделювання завжди існує оригінал (об'єкт) і модель, яка відтворює (моделює, описує, імітує) деякі риси об'єкта, при

цьому під моделлю розуміють абстрактний опис системи (об'єкта, процесу, проблеми, поняття) деякою формою відмінний від форми її реального існування.

Моделювання засноване на наявності у природних і штучних систем, що відрізняються як цільовим призначенням, так і фізичним втіленням, схожості або подібності деяких властивостей: форми, структури, функціональності, поведінки тощо. Ця схожість може бути повною (ізоморфізм) і частковою (гомоморфізм).

Для дослідження сучасних складних систем використовуються різні класи моделей. Розвиток інформаційних технологій можна в відомому сенсі інтерпретувати як можливість реалізації моделей різного виду в рамках інформаційних систем різного призначення: інформаційні системи, системи розпізнавання образів, системи штучного інтелекту, системи підтримки прийняття рішень. В основі цих систем лежать моделі різних типів: семантичні, логічні, математичні тощо.

Слід навести загальну класифікацію основних видів моделювання [130; 131; 133; 168; 222; 384]:

концептуальне моделювання – подання системи з допомогою спеціальних знаків, символів, операцій над ними або за допомогою природних або штучних мов;

фізичне моделювання – модельований об'єкт або процес відтворюється, виходячи зі співвідношення подоби, що випливає зі схожості фізичних явищ;

структурно-функціональне – моделями є схеми (блок-схеми), графіки, діаграми, таблиці, рисунки із спеціальними правилами їх об'єднання і перетворення;

математичне (логіко-математичне) моделювання – побудова моделі здійснюється засобами математики і логіки;

імітаційне (програмне) моделювання – при якому логіко-математична модель досліджуваної системи є алгоритмом функціонування системи, що може бути програмно реалізована на комп'ютері.

Зазначені види моделювання можуть застосовуватися самостійно або одночасно, в деякій комбінації (наприклад, в імітаційному моделюванні використовуються практично всі з перерахованих видів моделювання або окремі прийоми).

Домінуючою тенденцією сьогодні є взаємопроникнення всіх видів моделювання, симбіоз різних інформаційних технологій в галузі моделю-

вання, особливо для складних додатків і комплексних проектів з моделювання. Так, наприклад, імітаційне моделювання включає в себе концептуальне моделювання (на ранніх етапах формування імітаційної моделі) і логіко-математичне (включаючи методи штучного інтелекту) – для цілей опису окремих підсистем моделі, а також у процедурах обробки та аналізу результатів обчислювального експерименту і прийняття рішень. Технологія проведення і планування обчислювального експерименту з відповідними математичними методами запозичена в імітаційне моделювання з фізичного моделювання. Структурно-функціональне моделювання використовується як при створенні стратифікованого опису багатомодельних комплексів, так і для формування різних діаграмних уявлень при створенні імітаційних моделей.

Поняття комп'ютерного моделювання сьогодні трактується [133] ширше традиційного поняття моделювання на комп'ютері, тому потребує уточнення.

Комп'ютерне моделювання – метод рішення задач аналізу або синтезу складної системи на основі використання її комп'ютерної моделі.

До комп'ютерному моделюванню відносять:

структурно-функціональне;

імітаційне.

Під терміном "комп'ютерна модель" частіше за все розуміють:

умовний образ об'єкта або деякої системи об'єктів (або процесів), описаний за допомогою взаємопов'язаних комп'ютерних таблиць, блок-схем, діаграм, графіків, малюнків, анімаційних фрагментів, гіпертекстів тощо, які відображають структуру і взаємозв'язки між елементами об'єкта. Комп'ютерні моделі такого виду називають структурно-функціональними;

окрему програму (сукупність програм, програмний комплекс), що дозволяє за допомогою послідовності обчислень і графічного відображення їх результатів, відтворювати (імітувати) процеси функціонування об'єкта, системи об'єктів за умови впливу на об'єкт різних, як правило, випадкових факторів. Такі моделі називають імітаційними.

Суть комп'ютерного моделювання полягає в одержанні кількісних і якісних результатів на наявній моделі. Якісні результати аналізу виявляють невідомі раніше властивості складної системи: її структуру, динаміку розвитку, стійкість, цілісність та ін. Кількісні висновки в основному носять характер аналізу існуючої складної системи або прогнозу майбут-

ніх значень деяких змінних. До речі, можливість отримання не тільки якісних, а й кількісних результатів є істотною відмінністю імітаційного моделювання від структурно-функціонального. Становлення комп'ютерного моделювання пов'язане з імітаційним моделюванням. Імітаційне моделювання передувало структурно-функціональному і без комп'ютера ніколи не існувало. Імітаційне моделювання має цілий ряд специфічних рис.

Порівняно, наприклад, з математичним моделюванням, де методологічною основою найчастіше є: дослідження операцій, теорія математичних моделей, теорія прийняття рішень, теорія ігор і багато інших, методологією комп'ютерного моделювання є системний аналіз (кібернетика, загальна теорія систем). Тому в освоєнні цього методу домінуюча роль відводиться системним аналітикам.

Центральною процедурою системного аналізу є побудова узагальненої моделі, що відбиває всі фактори і взаємозв'язки реальної системи. Предметом комп'ютерного моделювання може бути будь-яка складна система, будь-який об'єкт або процес. Категорії цілей при цьому можуть бути найрізноманітними. Комп'ютерна модель повинна відображати всі властивості, основні чинники та взаємозв'язки реальної складної системи, критерії, обмеження.

Комп'ютерне моделювання сьогодні пропонує сукупність методологічних підходів і розвинених технологічних засобів, використовуваних для підготовки та прийняття рішень економічного, організаційного та соціального чи технічного характеру.

Метод імітаційного моделювання в узагальненому вигляді визначається як експериментальний метод дослідження реальної системи за її імітаційної моделі, який поєднує особливості експериментального підходу і специфічні умови використання обчислювальної техніки [130].

У цьому визначенні підкреслюється, що імітаційне моделювання є машинним методом моделювання, власне без комп'ютера ніколи не існувало, і лише розвиток інформаційних технологій привів до становлення цього виду комп'ютерного моделювання. В цьому визначенні також акцентується увага на експериментальній природі імітації, застосовується імітаційний метод дослідження (здійснюється експериментування з моделлю). Дійсно, в імітаційному моделюванні важливу роль відіграє не тільки проведення, але і планування експерименту на моделі. Однак це визначення не прояснює, що є самою імітаційною моделлю.

У процесі імітаційного моделювання (рис. 9.7) мають справу з чотирма основними елементами:

реальна система;

логіко-математина модель модельованого об’єкта;

імітаційна (машинна) модель;

комп’ютер, на якому здійснюється імітація.

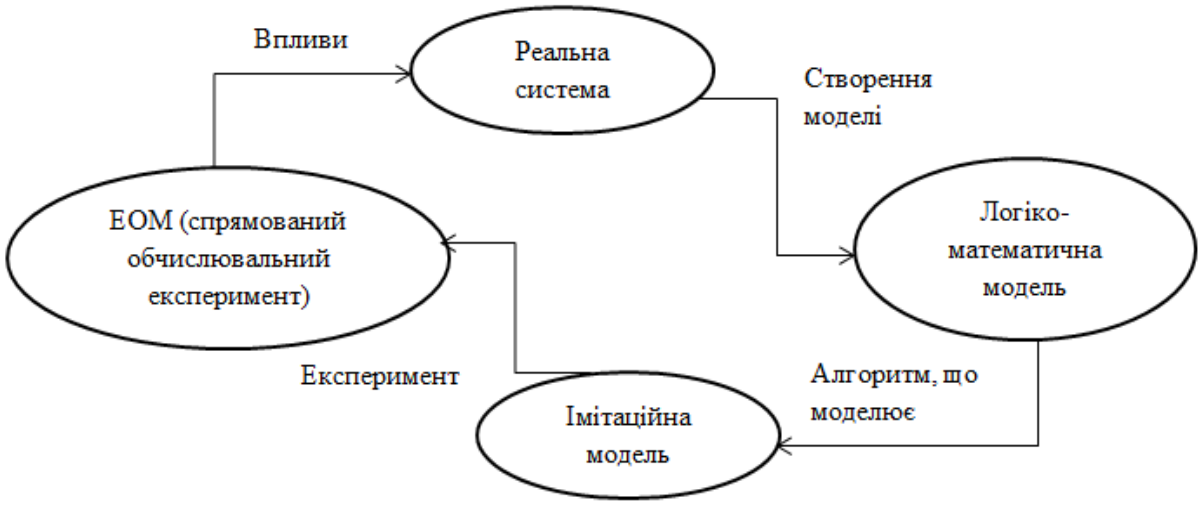


Рис. 9.7. **Процес імітаційного дослідження**

Реальну складну систему можна визначити як сукупність взаємодіючих елементів, що функціонують у часі. Дослідник вивчає реальну систему, розробляє логіко-математичну модель реальної системи. Імітаційний характер дослідження припускає наявність логіко-математичних моделей, що описують досліджуваний процес.

Визначення складної системи диктує подання її моделі у такому вигляді:

$$<E, S, T>, \qquad (9.1)$$

де E – безліч елементів (до їх числа входить і зовнішнє середовище);

S – безліч допустимих зв’язків між елементами (структура моделі);

T – безліч розглянутих моментів часу.

Особливістю імітаційного моделювання є те, що імітаційна модель дозволяє відтворювати модельовані об’єкти зі збереженням їх логічної структури; поведінкових властивостей (послідовності чергування у часі подій, що відбуваються в системі), тобто динаміки взаємодій.

При імітаційному моделюванні структура системи, що моделюється, адекватно відображається в моделі, а процеси її функціонування програються (імітуються) на побудованій моделі. Тому побудова імітаційної моделі полягає в описі структури та процесів функціонування модельованого об'єкта або системи. В описі імітаційної моделі виділяють дві складові: статичний опис системи, який за своєю суттю є описом її структури (при розробці імітаційної моделі необхідно виконувати структурний аналіз модельованих процесів); динамічний опис системи, або опис динаміки взаємодій її елементів. При його виконанні фактично потрібна побудова функціональної моделі модельованих динамічних процесів.

Ідея методу імітаційного моделювання, з точки зору його програмної реалізації, полягає в наступному. Елементам системи поставити у відповідність деякі програмні компоненти, а стани цих елементів описувати за допомогою змінних стану. Елементи, за визначенням, взаємодіють (або обмінюються інформацією), – значить може бути реалізований алгоритм функціонування окремих елементів – моделюючий алгоритм. Крім того, елементи існують у часі, тому треба задати алгоритм зміни змінних станів. Динаміка в імітаційних моделях реалізується за допомогою механізму просування модельного часу.

Відмінною особливістю методу імітаційного моделювання є можливість опису і відтворення взаємодії між різними елементами системи. Таким чином, щоб скласти імітаційну модель, треба:

подати реальну систему (процес), як сукупність взаємодіючих елементів;

алгоритмічно описати функціонування окремих елементів;

описати процес взаємодії різних елементів між собою і з зовнішнім середовищем.

Ключовим моментом в імітаційному моделюванні є виділення і опис станів системи. Система характеризується набором змінних станів, кожна комбінація яких описує конкретний стан. Отже, шляхом зміни значень цих змінних можна імітувати перехід системи з одного стану в інший. Таким чином, імітаційне моделювання – це подання динамічної поведінки системи за допомогою просування її від одного стану до іншого відповідно певних операційних правил. Ці зміни станів можуть відбуватися або безперервно, або в дискретні моменти часу. Імітаційне моделювання – це динамічне відображення змін стану системи з часом [130]. Отже, при імітаційному моделюванні логічна структура реальної системи

відображається в моделі, а також імітується динаміка взаємодій підсистем в системі, що моделюється.

Для опису динаміки модельованих процесів в імітаційному моделюванні реалізований механізм завдання модельного часу. Ці механізми вбудовані в керуючі програми будь-якої системи моделювання.

Якби на комп'ютері імітувалася поведінка однієї компоненти системи, то виконання дій в імітаційній моделі можна було б здійснити послідовно, з перерахунком на часовій координати. Щоб забезпечити імітацію паралельних подій реальної системи вводять деяку глобальну змінну (забезпечує синхронізацію всіх подій в системі) t_0, яку називають модельним (або системним) часом.

Існують два основні способи зміни t_0:

покроковий (застосовуються фіксовані інтервали зміни модельного часу);

подієвий (застосовуються змінні інтервали зміни модельного часу, при цьому величина кроку вимірюється інтервалом до наступної події).

У разі покрокового методу просування часу відбувається з мінімально можливою постійною довжиною кроку (принцип t). Ці алгоритми не дуже ефективні з точки зору використання машинного часу на їх реалізацію.

Подієвий метод (принцип "особливих станів"). У ньому координати часу міняються тільки коли змінюється стан системи. В подієвих методах довжина кроку часового зсуву максимально можлива. Модельний час з поточного моменту змінюється до найближчого моменту настання наступної події. Застосовується подієвий метод переважно у випадку, якщо частота настання подій невелика, тоді велика довжина кроку дозволить прискорити хід модельного часу. На практиці подієвий метод набув найбільшого поширення.

Спосіб фіксованого кроку застосовується:

якщо закон зміни від часу описується інтегро-диференційними рівняннями. Характерний приклад: рішення інтегро-дифференційних рівнянь чисельним методом. У подібних методах крок моделювання дорівнює кроку інтегрування. При їх використанні динаміка моделі є дискретним наближенням реальних безперервних процесів;

коли події розподілені рівномірно і можна підібрати крок зміни часової координати;

коли складно передбачити появу певних подій;

коли подій дуже багато і вони з'являються групами.

В інших випадках застосовується подієвий метод. Він кращий, коли події розподілені нерівномірно на часовій осі і з’являються через значні часові інтервали.

Таким чином, внаслідок послідовного характеру обробки інформації в компютері, паралельні процеси, що відбуваються в моделі, перетворюються з допомогою розглянутого механізму в послідовні. Такий спосіб подання носить назву квазіпаралельного процесу.

Найпростіша класифікація на основні види імітаційних моделей пов’язана із застосуванням двох цих способів просування модельного часу. Розрізняють імітаційні моделі [222]:

безперервні;

дискретні;

безперервно-дискретні.

У безперервних імітаційних моделях змінні змінюються безперервно, стан модельованої системи міняється як безперервна функція часу, і, як правило, це зміна описується системами диференціальних рівнянь. Відповідно просування модельного часу залежить від чисельних методів розв’язання диференціальних рівнянь.

У дискретних імітаційних моделях змінні змінюються дискретно в певні моменти імітаційного часу (настання подій). Динаміка дискретних моделей є процесом переходу від моменту настання поточної події до моменту настання наступної події.

Оскільки в реальних системах безперервні і дискретні процеси часто неможливо розділити, були розроблені безперервно-дискретні моделі, в яких поєднуються механізми просування часу, характерні для цих двох процесів.

Слова "simulation", "експеримент", "імітація" одного плану. Тому імітаційне моделювання було визначено як експериментальний метод дослідження реальної системи за допомогою її імітаційної моделі. Але поняття методу завжди ширше за поняття "імітаційна модель". Методологією імітаційного моделювання, як було зазначено раніше, є системний аналіз. Саме це дає право імітаційне моделювання називати "системним моделюванням".

Експериментальна природа імітації також визначила походження назви методу. Мета будь-якого дослідження полягає в тому, щоб дізнатися якомога більше про досліджувану систему, зібрати і проаналізувати інформацію, необхідну для прийняття рішення. Суть дослідження реаль-

ної системи за її імітаційної моделі полягає в отриманні (зборі) даних про функціонування системи в результаті проведення експерименту на імітаційній моделі.

Імітаційні моделі – це моделі прогонового типу, у яких є вхід і вихід. Тобто якщо подати на вхід імітаційної моделі певні значення параметрів (змінних, структурних взаємозв'язків), можна отримати результат, який дійсний тільки при цих значеннях. На практиці дослідник стикається з такою специфічною рисою імітаційного моделювання. Імітаційна модель дає результати, які дійсні тільки для певних значень параметрів, змінних і структурних взаємозв'язків, закладених в імітаційну програму. Зміна параметра або взаємозв'язку означає, що імітаційна програма повинна бути запущена знову. Тому, для отримання необхідної інформації або результатів треба здійснювати прогон імітаційних моделей, а не вирішувати їх. Імітаційна модель не здатна формувати своє власне рішення в тому вигляді, як це має місце в аналітичних моделях, а може слугувати в якості засобу для аналізу поведінки системи в умовах, що визначаються експериментатором.

Для пояснення слід розглянути такі випадки:

детермінований випадок;

стохастичний випадок.

Стохастичний випадок. Імітаційна модель – зручний апарат для дослідження стохастичних систем. Стохастичні системи – це такі системи, динаміка яких залежить від випадкових факторів, вхідні, вихідні змінні стохастичної моделі, як правило, описуються як випадкові величини, функції, процеси, послідовності. Слід розглянути основні особливості моделювання процесів з урахуванням дії випадкових факторів. Результати моделювання, отримані при відтворенні єдиної реалізації процесів, в силу дії випадкових факторів будуть реалізаціями випадкових процесів, і не зможуть об'єктивно характеризувати досліджуваний об'єкт. Тому шукані величини при дослідженні процесів методом імітаційного моделювання зазвичай визначають як середні значення за даними великого числа реалізацій процесу (задача оцінювання). Тому експеримент на моделі містить кілька реалізацій, прогонів і передбачає оцінювання з даними сукупності (вибірки). Ясно, що за законом великих чисел, чим більше число реалізацій, тим одержувані оцінки все більше набувають статистичну стійкість.

Отже, у випадку зі стохастичною системою необхідно здійснювати збір та оцінювання статистичних даних на виході імітаційної моделі, для цього проводити серію прогонів і статистичну обробку результатів моделювання.

Детермінований випадок. У цьому випадку достатньо провести один прогін, з певних операційним правилам при конкретному наборі параметрів.

Якщо цілями моделювання є дослідження системи при різних умовах, оцінка альтернатив, знаходження залежності виходу моделі від ряду параметрів і, нарешті, пошук деякого оптимального варіанта. В цих випадках дослідник може проникнути в особливості функціонування модельованої системи, змінюючи значення параметрів на вході моделі, при цьому виконуючи численні машинні прогони імітаційної моделі.

Таким чином, проведення експериментів з моделлю на комп'ютері полягає в проведенні багаторазових машинних прогонів з метою збору, накопичення і подальшої обробки даних про функціонування системи. Імітаційне моделювання дозволяє досліджувати модель реальної системи, щоб вивчати її поведінку шляхом багаторазових прогонів на комп'ютері при різних умовах функціонування реальної системи.

При імітаційному моделюванні виникають такі проблеми: як зібрати дані, провести серію прогонів, як організувати цілеспрямоване експериментальне дослідження. Вихідних даних, отриманих у результаті такого експериментування, може виявитися дуже багато. Їх обробка і вивчення може перетворитися в самостійну проблему, набагато складнішу, ніж завдання статистичного оцінювання.

У імітаційному моделюванні важливим питанням є не тільки проведення, а й планування імітаційного експерименту відповідно до поставленої мети дослідження.

Таким чином, перед дослідником, що використовують методи імітаційного моделювання, завжди постає проблема організації експерименту, тобто вибору методу збору інформації, який дає необхідний (для досягнення поставленої мети дослідження) її обсяг при найменших витратах (зайве число прогонів – це зайві витрати машинного часу). Основна мета – зменшити часові витрати на експлуатацію моделі, скоротити машинний час на імітацію, відображає витрати ресурсу часу комп'ютера на проведення великого кількості імітаційних прогонів.

Ця проблема отримала назву стратегічного планування імітаційного дослідження. Для її вирішення використовуються методи регресійного аналізу, планування експерименту та ін.

Стратегічне планування – це розробка ефективного плану експерименту, в результаті якого або з'ясовується взаємозв'язок між керованими змінними, або перебуває комбінація значень керованих змінних, що мінімізує або максимізує відгук (вихід) імітаційної моделі.

Поряд з поняттям стратегічного існує поняття тактичного планування, яке пов'язане з визначенням способів проведення імітаційних прогонів, намічених планом експерименту: як провести кожен прогін у рамках складеного плану експерименту. Тут вирішуються завдання: визначення тривалості прогону, оцінка точності результатів моделювання та ін. Такі імітаційні експерименти з імітаційної моделлю називаються спрямованими обчислювальними експериментами.

Імітаційний експеримент, зміст якого визначається попередньо проведеним аналітичним дослідженням (тобто є складовою частиною обчислювального експерименту) і результати якого достовірні і математично обґрунтовані, називаються спрямованим обчислювальним експериментом.

На першому етапі формулюється проблема, що стоїть перед дослідником і приймається рішення про доцільність застосування методу імітаційного моделювання. Потім визначаються цілі, які повинні бути досягнуті в результаті імітації. Від формулювання цілей значною мірою залежить вибір типу імітаційної моделі і характер подальшого імітаційного дослідження на імітаційній моделі.

На цьому етапі визначається і детально вивчається об'єкт моделювання, ті сторони його функціонування, які становлять інтерес для дослідження. Результатом робіт на даному етапі є змістовний опис об'єкта моделювання з зазначенням цілей імітації і тих аспектів функціонування об'єкта моделювання, які необхідно вивчити на імітаційній моделі. Змістовний опис складається у термінології реальної системи, мовою предметної області, зрозумілою клієнту.

У ході складання змістовного опису об'єкта моделювання встановлюються межі вивчення модельованого об'єкта, дається опис зовнішнього середовища, з яким він взаємодіє. Формулюються також основні критерії ефективності, за якими передбачається проводити порівняння на моделі різних варіантів рішень, проводиться генерація і опис розглянутих альтернатив. Загального рецепту складання змістовного опису не існує. Успіх залежить від інтуїції розробника і знання реальної системи.

Загальна технологія чи послідовність дій на цьому етапі така [130]:

збір даних про об'єкт моделювання і складання змістовного опису об'єкта моделювання;

вивчення проблемної ситуації – визначення діагнозу і постановка завдання;

уточнення цілей моделювання;

обґрунтування необхідності моделювання;

вибір методу моделювання. На цьому етапі чітко, конкретно формулюються цілі моделювання. Цілі моделювання визначають загальний задум моделі і пронизують всі наступні етапи імітаційного моделювання;

формування концептуальної моделі досліджуваного об'єкта.

Робота, що виконується системним аналітиком на ранніх етапах виключно важлива для всіх наступних етапів імітаційного моделювання. Саме тут фахівець з імітаційного моделювання демонструє себе як системний аналітик, який володіє мистецтвом моделювання. Процес, за допомогою якого інженер, який займається системами, чи вчений, що досліджує питання управління, створює модель досліджуваної системи, може бути краще за все визначений як інтуїтивне процес. При побудові моделей треба покладатися на знання, досвід та інтуїцію. Сучасний теоретичний апарат опису систем не може гарантувати того, що буде виконане оптимальне для поставлених цілей моделювання. Вивчення конкретних зразків моделей не сприяє розвитку творчого підходу до створення моделей.

Структурування вихідної проблеми. Формулювання проблеми. Перш за все, системний аналітик повинен вміти аналізувати проблему. Він виконує вивчення і структурування вихідної проблеми, чітке формулювання проблеми.

Аналіз проблеми необхідно починати з детального вивчення всіх аспектів функціонування (тут важливе розуміння деталей – тому треба бути фахівцем у певній предметній області або тісно спілкуватися з експертами). Розглянута система пов'язана з іншими системами, тому з позицій системного підходу треба розглянути комплекс проблем. Важливо правильно поставити завдання. Загальна задача моделювання при цьому розбивається на детальні.

Системний підхід до вирішення проблем передбачає [249]:

а) системний розгляд сутності проблеми:

- обґрунтування сутності та місця досліджуваної проблеми;
- формування загальної структури досліджуваної системи;
- виявлення повної множини значущих чинників;
- визначення функціональних залежностей між факторами;

б) побудову єдиної концепції вирішення проблеми:

- дослідження об’єктивних умов вирішення проблеми;
- обґрунтування цілей, завдань, необхідних для вирішення проблеми – структуризація задач, формалізація цілей;
- розробку засобів і методів вирішення проблеми: опис альтернатив, сценаріїв, вирішальних правил і керуючих впливів для відпрацювання в подальшому на моделі процедур прийняття рішень;

в) системне використання методів моделювання:

- системна класифікація (структуризація) завдань моделювання;
- системний аналіз можливостей методів моделювання;
- вибір ефективних методів моделювання.

Виявлення цілей. Перший і найважливіший крок при створенні будь-якої моделі полягає у визначенні її цільового призначення. Цілі – антиподи проблеми. Може бути застосований метод декомпозиції цілей, що припускає поділ цілого на частини: цілей – на підцілі, завдань – на підзадачі тощо – на практиці цей підхід призводить до ієрархічних деревовидних структур (побудови дерева цілей). Вся ця процедура є завданням експертів з проблеми, фахівців. Тому тут присутній суб’єктивний фактор, кожен експерт зробить по-своєму. Практичне завдання полягає в тому, наскільки повно все структуроване. Побудоване в результаті цієї процедури дерево цілей може надалі виявитися корисним при формуванні множини критеріїв.

При виконанні цих кроків можуть виникнути такі проблеми. Те, що для одного рівня мета – для іншого засіб. Часто їх плутають, відбувається змішання цілей. Мета – це опис бажаного майбутнього, тому тут легко помилитися. Для складної системи з великою кількістю підсистем цілі можуть бути суперечливими. Мета рідко буває єдиною: існує небезпека неправильного ранжування при безлічі цілей.

Сформульовані і структуровані на першому етапі цілі моделювання пронизують весь хід подальшого імітаційного дослідження.

Найбільш вживані категорії цілей в імітаційному дослідженні – це оцінка, прогнозування, оптимізація, порівняння альтернатив та ін.

Експерименти з моделюванню проводяться з досить різноманітними цілями, в числі яких можуть бути:

- оцінка – визначення, наскільки добре система пропонованої структури буде відповідати деяким конкретним критеріям;

- порівняння альтернатив – зіставлення конкуруючих систем, розрахованих на виконання певної функції, або ж на зіставлення декількох пропонованих робочих принципів або методик;
- прогноз – оцінка поведінки системи при деякому передбачуваному поєднанні робочих умов;
- аналіз чутливості – виявлення з великого числа діючих факторів тих, які найбільшою мірою впливають на загальну поведінку системи;
- виявлення функціональних співвідношень – визначення природи залежності між двома або кількома діючими факторами, з одного боку, і відгуком системи з іншого;
- оптимізація – точне визначення такого поєднання діючих факторів і їх величин, при якому забезпечується найкращий відгук всієї системи в цілому.

Формування критеріїв. Виключно важливо чітке і однозначне визначення критеріїв. Це впливає на процес створення і експериментування моделі, крім того неправильне визначення критерію веде до неправильних висновків. Розрізняють критерії, за допомогою яких оцінюється ступінь досягнення мети системою, і критерії щодо яких оцінюється спосіб руху до мети (або ефективність засоби досягнення цілей). Для багатокритеріальних модельованих систем формується набір критеріїв, їх необхідно структурувати за підсистемами або ранжувати за важливістю.

На третьому етапі імітаційного дослідження здійснюється формалізація об’єкта моделювання. Процес формалізації складної системи включає:

- вибір способу формалізації;
- складання формального опису системи.

У процесі побудови моделі можна виділити такі рівні її уявлення:

- неформалізований – концептуальна модель;
- формалізований – формальна модель;
- програмний – імітаційна модель.

Кожен рівень відрізняється від попереднього ступенем деталізації модельованої системи і способами опису її структури та процесу функціонування. При цьому рівень абстрагування зростає.

Концептуальна модель – це систематизований змістовний опис модельованої системи (або проблемної ситуації) неформальною мовою. Неформалізований опис імітаційної моделі, що розробляється, включає визначення основних елементів модельованої системи, їх характерис-

тики і взаємодії між елементами власною мовою, можуть використовуватися таблиці, графіки, діаграми і т. д. Неформалізований опис моделі необхідний як самим розробникам (при перевірці адекватності моделі, її модифікації і т. д.), так і для взаєморозуміння з фахівцями інших профілів.

Концептуальна модель містить вихідну інформацію для системного аналітика, виконує формалізацію системи та використовує для цього певну методологію і технологію, тобто на підставі неформалізованого опису здійснюється розробка більш суворого і докладного формалізованого опису. Далі формалізований опис перетворюється в програму-імітатор також відповідно до деякої методики (технології програмування).

Аналогічна схема має місце і при виконанні імітаційних експериментів: змістовна постановка відображається на формальну модель, після чого вносяться необхідні зміни та доповнення в методику спрямованого обчислювального експерименту.

Основне завдання етапу формалізації – дати формальний опис складної системи, вільне від другорядної інформації, наявної в змістовному описі, алгоритмічне подання об’єкта моделювання. Мета формалізації – отримати формальне подання логіко-математичної моделі, тобто алгоритмів поведінки компонент складної системи і відобразити на рівні моделювання алгоритму питання взаємодії між собою цих компонент.

Може виявитися, що інформації, наявної в змістовному описі, недостатньо для формалізації об’єкта моделювання. В цьому випадку необхідно повернутися до етапу складання змістовного опису та доповнити його даними, необхідність у яких виявляється при формалізації об’єкта моделювання. На практиці таких повернень може бути декілька. Формалізація корисна в певних межах і для простих моделей невиправдана.

Спостерігається істотна різноманітність схем (концепцій) формалізації та структуризації, що знайшли застосування в імітаційному моделюванні. Схеми формалізації орієнтуються на різні математичні теорії і виходять з різних уявлень про досліджувані процеси – звідси їх різноманіття та проблема вибору підходящої (для опису даного об’єкта моделювання) схеми формалізації.

Для дискретних моделей, наприклад, можуть застосовуватися процесно-орієнтовані системи (process description), системи, засновані на мережних парадигмах (network paradigms), для безперервних – потокові діаграми моделей системної динаміки.

Найбільш відомі і широко використовуються на практиці концепції нормалізації: агрегатні системи і автомати; мережі Петрі і їх розширення; моделі системної динаміки.

У рамках однієї концепції формалізації можуть бути реалізовані різноманітні алгоритмічні моделі. Як правило, та чи інша концепція структуризації (схема подання алгоритмічних моделей) або формалізації на технологічному рівні закріплена в системі моделювання, мові моделювання. Концепція структуризації більш-менш явно лежить в основі всіх імітаційних систем та підтримується спеціально розробленими прийомами технології програмування. Це спрощує побудову та програмування моделі. Наприклад, мова моделювання GPSS, має блокову концепцію структуризації, структура модельованого процесу зображується у вигляді потоку транзактів, що проходить через обслуговуючі пристрої, черги та інші елементи систем масового обслуговування.

У ряді сучасних систем моделювання, поряд з апаратом, що підтримує ту чи іншу концепцію структуризації, є спеціальні засоби, що забезпечують застосування в системі певної концепції формалізації.

В основі побудови імітаційних моделей лежать сучасні методи структуризації складних систем і опису їх динаміки. Широко використовуються в практиці аналізу складних систем такі моделі і методи:

- мережі кусково-лінійних агрегатів, що моделюють дискретні і безперервно-дискретні системи;
- мережі Петрі (мережі подій, Е-мережі, КОМБІ-мережі та ін. розширення), застосовувані при структуризації причинних зв’язків і моделюванні систем з паралельними процесами, що слугують для стратифікації і алгоритмізації динаміки дискретних і дискретно-безперервних систем;
- потокові діаграми і рівняння системної динаміки, які є моделями безперервних систем;
- та інші.

В умовах зростання взаємозалежностей між процесами та різними сферами діяльності людей, які раніше не впливали один на одного, є ще одне важливе завдання сучасного комп’ютерного імітаційного моделювання – створення засобів і механізмів для підтримки діяльності людей в скоординованому стані, нетривіальність якої визначають такі два важливих чинники [384]:

- велика кількість і швидке збільшення кількості взаємодіючих учасників,
- збільшення інтенсивності змін у можливостях/намірах учасників і в загальних умовах для діяльності, які необхідно погоджувати в реальному часі.

При імітаційному моделюванні алгоритм, що реалізує модель, відтворює процес функціонування системи в часі, причому імітуються елементарні явища, що становлять процес із збереженням їх логічної структури і послідовності протікання в часі, що дозволяє за вихідними даними отримати відомості про стан процесу в певні моменти часу, що дають можливість оцінити характеристики системи.

Основною перевагою імітаційного моделювання порівняно з аналітичним, є можливість вирішення більш складних завдань. Імітаційні моделі дозволяють досить просто враховувати такі фактори, як наявність дискретних і безперервних елементів, нелінійні характеристики системи і її елементів, численні випадкові впливу.

Коли результати, які виходять при відтворенні на імітаційній моделі процесу функціонування системи, є реалізаціями випадкових величин і функцій, тоді для знаходження характеристик процесу, потрібно його багаторазове відтворення з подальшою статичною обробкою.

Імітаційне моделювання може застосовуватися в найрізноманітніших сферах діяльності. Особливо ефективно моделювання при вирішенні таких завдань [248]:

- проектування та аналіз виробничих систем;
- оцінка різних систем озброєнь;
- визначення вимог до обладнання та протоколів мереж зв’язку;
- модернізація різних процесів у діловій сфері, визначення політики в системах управліннями запасами;
- аналіз фінансових і економічних систем.

Застосування імітаційних моделей дає безліч переваг порівняно з виконанням експериментів над реальною системою і використанням інших методів.

Вартість. Наприклад, якщо компанія звільнила частину співробітників, що в подальшому призвело до зниження якості обслуговування і втрати частини клієнтів. Прийняти обґрунтоване рішення допомогла б імітаційна модель, витрати на застосування якої складаються лише з вартості програмного забезпечення і вартості консалтингових послуг.

Час. У реальності оцінити ефективність, наприклад, нової мережі розповсюдження продукції або зміненої структури складу можна лише через місяці або навіть роки. Імітаційна модель дозволяє визначити оптимальність таких змін за лічені хвилини, необхідні для проведення експерименту.

Повторюваність. Сучасне життя вимагає від організацій швидкої реакції на зміну ситуації на ринку. Наприклад, прогноз обсягів попиту продукції повинен бути складений у термін, і його зміни критичні. За допомогою імітаційної моделі можна провести необмежену кількість експериментів з різними параметрами, щоб визначити найкращий варіант.

Точність. Традиційні розрахункові математичні методи вимагають застосування високого ступеня абстракції і не враховують важливі деталі. Імітаційне моделювання дозволяє описати структуру системи та її процеси в природному вигляді, не вдаючись до використання формул і строгих математичних залежностей.

Наочність. Імітаційна модель має можливості візуалізації процесу роботи системи в часі, схематичного завдання її структури і видачі результатів у графічному вигляді. Це дозволяє наочно подати отримане рішення і донести закладені в нього ідеї до клієнта і колег.

Універсальність. Імітаційне моделювання дозволяє вирішувати завдання з будь-яких областей: виробництва, логістики, фінансів, охорони здоров'я і багатьох інших. В кожному випадку модель імітує, відтворює, реальне життя і дозволяє проводити широкий набір експериментів без впливу на реальні об'єкти.

Однак імітаційне моделювання поряд з перевагами має і недоліки:

- розробка імітаційної моделі часто обходиться дорожче, ніж створення аналітичної моделі і вимагає великих часових витрат;
- може виявитися, що імітаційна модель неточна (що буває часто), і немає можливості виміряти ступінь цієї неточності;
- часто дослідники звертаються до імітаційного моделювання, не уявляючи тих труднощів, з якими вони зустрінуться і здійснюють при цьому ряд помилок методологічного характеру.

І, тим не менш, імітаційне моделювання є одним з найбільш широко використовуваних методів при вирішенні завдань синтезу та аналізу складних процесів і систем.

Серед різноманіття імітаційних підходів моделювання соціальних мереж найбільш перспективними є системна динаміки, дискретно-подієве та агентне моделювання, які будуть більш докладно розглянуті далі [26; 52; 133; 134; 384].

Системна динаміка.

Системна динаміка – парадигма моделювання, де для досліджуваної системи будуються графічні діаграми причинних зв'язків і глобаль-

них впливів одних параметрів на інші в часі, а потім створена на основі цих діаграм модель імітується на комп'ютері. По суті, такий вид моделювання більше всіх інших парадигм допомагає зрозуміти суть того, що відбувається виявлення причинно-наслідкових зв'язків між об'єктами і явищами. За допомогою системної динаміки будують моделі бізнес-процесів, розвитку міста, моделі виробництва, динаміки популяції, екології та розвитку епідемії.

Системна динаміка – це потужна методологія і техніка комп'ютерної імітаційного моделювання для позначення, розуміння і обговорення складних питань і проблем. Системна динаміка була створена в кінці 1950-х рр. Дж. Форрестером у Масачусетському технологічному інституті.

Методологія системної динаміки базується на припущенні, що поведінка (або історія розвитку у часі) організації головним чином визначається її інформаційно-логічної структурою. Вона відображає не тільки фізичні і технологічні аспекти виробничих процесів, але, що набагато важливіше, політику і традиції, які явно чи неявно визначають процес прийняття рішень в організації. Така структурна схема містить джерела посилення часових затримок і інформаційних зворотних зв'язків, подібних тим, які зустрічаються в складних інженерних системах [26].

Інший аспект системної динаміки полягає у припущенні, що організація більш ефективно представляється в термінах, що лежать в основі її потоків, ніж в термінах окремих функцій. Потоки людей, грошей, матеріалів, заявок і обладнання, а також інтегровані потоки інформації можуть бути виявлені в усіх організаціях. Спрямованість на потокову структуру змушує аналітика природним чином долати внутрішньо організаційні кордони.

В основі системної динаміки лежать чотири принципи, сформульовані вперше Дж. Форрестером.

Перший принцип свідчить, що дослідження динаміки поведінки будь-якого складного бізнес-процесу можна звести до дослідження змін рівнів деяких операційних "фондів", регульованих темпами поповнення або вичерпання цих фондів вхідними або вихідними "потоками" модельних одиниць. Рівень фонду подібний рівню води в басейні, а регулювання – зусиллям, прикладеним до "вентиля", встановленим на "трубі", через яку здійснюється протікання.

В основі другого принципу лежить припущення, що нетривіальна поведінка будь-якого інтегрованого бізнес-процесу пов'язана з регулю-

ванням контурів позитивних і негативних зворотних зв’язків. Регульований контур (цикл) зворотного зв’язку дозволяє в динаміці враховувати поточний і попередній досвід розвитку поведінки. У зв’язку з цим з’являється приваблива можливість формувати дисципліну нового управління на базі накопиченого досвіду.

Третім принципом системної динаміки допускається збереження невизначеностей і непередбачуваності поведінки концептуальних моделей через можливість виникнення (в нетривіальних конструкціях з циклами зворотних зв’язків) композицій нелінійних пар, які недоступні строгому опису в рамках імітаційного підходу. Це означає, що поведінка фрагментів бізнес-процесу через зворотні зв’язки впливає на інші фрагменти в непропорційному режимі. І тоді побудова концептуальної моделі правдоподібного поведінки може виявитися досить складною.

Четвертий принцип стверджує, що системна динаміка – суто прагматичний апарат, який здатний найбільш адекватно відобразити нетривіальну поведінку мережі взаємодіючих фрагментів, зворотних зв’язків та нелінійних пар. Його доцільно застосовувати при аналізі складних ситуацій для бізнес-процесів, поведінка яких не піддається точному математичному опису.

Концепція взаємодіючих фондових потоків (ВФП), дотримуючись базовим принципам системної динаміки, дозволяє висунути припущення, що поведінка практично будь-якого бізнес-процесу може бути описана в термінах переміщуваних ресурсів, тобто аналіз її поведінки може бути зведений до аналізу взаємодіючих "фондових потоків".

ВФП як концепція йде ще далі і прагне практично всю діяльність з концептуального проектування бізнес-процесів вивести на образотворчий і понятійний рівень потокових моделей, які:

здатні відображати причинно-наслідкові зв’язки;

графічно досить прості і прозорі;

придатні для інтерпретації не тільки безперервних, але і дискретних взаємодій.

Нотація ВФП досить проста і будується на основі таких чотирьох базових графічних елементів:

час;

прямокутник – фонд;

стилізована стрілка з кружечком – потік (з конвертором);

ізольований кружечок – конвертор;

проста стрілка – коннектор.

Час є первинною змінної для імітаційної моделі динамічної системи: її значення генерується системним таймером і змінюється дискретно, тобто, починаючи з деякого початкового значення, час за кожен такт збільшується на заздалегідь задану величину, яка слугує одиницею модельного часу. Число тактів і одиниця часу є параметрами "прогону" моделі і визначаються заздалегідь.

Фонд – змінна, що дорівнює обсягу (кількості) деякого "продукту", накопиченого в деякому сховищі за час "життя" моделі з початкового по поточний момент. Так, фонд може накопичувати модельні одиниці грошової готівки, матеріальних запасів, інвентарю, службовців і т. д. Фонди можна використовувати для накопичення і нематеріальних модельних одиниць, таких, як рівень кваліфікації, продуктивність, мотивація, інфляційні очікування, якість і т. д. І хоча ці нематеріальні накопичення можна оцінювати, як правило, лише в якісних категоріях ("висока" продуктивність, "слабка" мотивація, "низька" якість і т. д.), вони часто виявляються істотними факторами, що впливають. Продукт може надходити до фонду та/або вилучатись з нього. Тому значення фонду в поточний момент часу можна обчислити як суму його значення в попередній момент і величини, рівної різниці величин вхідного і вихідного потоків продукту за одиницю модельного часу.

Потік – змінна, що дорівнює обсягу (кількості) продукту, який надходить або витягується з відповідного фонду в одиницю модельного часу. Значення цієї змінної може змінюватися залежно від зовнішніх впливів на неї. Зокрема, потік можна представити як функцію від значень інших потоків і фондів. Приклади потоків: наймання співробітників, надходження замовлень, виплати зарплати і т. д. Дії змінюють поточні рівні фондів, поповнюють їх або вичерпують. Важче від способу дії, накопичують або вичерпні нематеріальні фонди, такі, як вивчення, формування або падіння. Потік зручно асоціювати з трубопроводом, який наповнює модельними одиницями деякий резервуар-фонд, або його спорожняє. Потік забезпечується регулятором, керуючим за допомогою значення обчислюваного алгебраїчного виразу інтенсивністю наповнення або спорожнення фонду. Фонди характеризують статичний стан системи, а потоки – її динаміку. Якщо, наприклад, уявити собі, що в якийсь момент часу всі процеси в системі зупиняться, то фонди будуть мати ті значення, які були на момент зупинки, а потоки будуть рівні нулю. З іншого боку, про величину потоку можна судити тільки за певний проміжок часу.

Конвертор – перетворювач найпростіше асоціювати зі змінною, яка формує поточне значення при обчисленні алгебраїчного виразу (подібно висловом, формованому при регулюванні інтенсивності потоку). Конвертори, зокрема, використовуються для завдання і зберігання постійних значень. Так, конвертор міг би використовуватися для зберігання значення необхідної кількості службовців компанії та виступати в якості регулятора інтенсивності потоку найму [138].

Коннектор (з'єднувач) можна асоціювати з проводом, що передає інформацію з метою регулювання інтенсивності потоків. Коннектори можуть впливати на потоки або конвертори, але ніколи на фонди. Проте рівень фондів часто побічно все ж регулюється інформацією, що передається коннекторами і керуючої інтенсивністю вхідних або вихідних потоків. Наприклад, коннектор може використовувати інформацію щодо поточного числа службовців у компанії і, передаючи її потоку найму, контролювати норму прийому.

Дискретно-подієве моделювання.

Дискретно-подієве моделювання – підхід до моделювання, що пропонує абстрагуватися від безперервної природи подій і розглядати тільки основні події модельованої системи, такі, як: "очікування", "обробка замовлення", "рух з вантажем", "розвантаження" та інші. Дискретно-подієве моделювання найбільш розвинене і має величезну сферу додатків – від логістики та систем масового обслуговування до транспортних та виробничих систем. Цей вид моделювання найбільш підходить для моделювання виробничих процесів. Заснований Джефрі Гордоном в 1960-х роках [26].

Термін "дискретно-подієво моделювання" історично закріпився за моделюванням систем обслуговування потоків об'єктів деякої природи: клієнтів банку, автомобілів на заправній станції, телефонних дзвінків, пацієнтів у поліклініках тощо. Саме такі системи називаються системами масового обслуговування.

Зазначені прості системи не вичерпують всього різноманіття систем масового обслуговування. Наприклад, конвеєрні системи для поточного виробництва і збірки виробів також можуть розглядатися як системи масового обслуговування, але вони вимагають при аналізі облік характеристик самих конвеєрів (наприклад, їх форми, швидкості) і алгоритмів складання. Крім того, великий клас систем включає такі процеси обслуговування, які вимагають для окремих операцій виконання специфічних умов, наприклад, наявність ресурсів конкретного типу.

Дискретно-подієве моделювання використовується для побудови моделі, що відбиває розвиток системи в часі, коли стану змінних змінюються миттєво в конкретні моменти часу.

Структура дискретно-подієвого моделювання включає в себе такі компоненти: сутності (entity), дії та події (activities and events), ресурси (resources), глобальні змінні (global variables), генератор випадкових чисел (random number generator), збирачі статистики (statistics collectors).

Сутності – це динамічні об'єкти, які створюються, переміщуються з будь-якої частини модельованої системи, а потім зазвичай виключаються. Прогін моделі завершується, коли в системі не залишається жодної активної сутності. Кожна сутність має унікальний набір властивостей. Значення властивостей можуть змінюватися по ходу просування сутності і впливати на шлях сутності в моделі.

Дії – це процеси, що відбуваються по ходу моделювання і логіка моделі. Події – обставини, які в певний момент часу змінюються стан системи. Подія виникає, коли над сутністю проводиться будь-яку дію. Є три основних типи дій: затримка – дія, що затримує сутність на певний час. Черга – місце, де сутність очікує протягом невизначеного проміжку часу. Черги розміщуються перед ресурсами (див. нижче) або перед логічними діями для очікування потрібного стану. Логічні дії – дії, що дозволяють організувати нелінійність моделі.

Ресурси є тим, що має обмежену ємність. Найбільш типовими прикладами ресурсів є робітники, верстати, вузли мереж зв'язку, транспортні розв'язки і т. д. Глобальні змінні – змінні доступні в будь-якому місці моделі в будь-який час. У кожному пакеті моделювання є генератор випадкових чисел. Генератор випадкових чисел - алгоритм, що генерує послідовність чисел, елементи якої майже незалежні один від одного і підкоряються заданому розподілу. Збирачі статистики – частина моделі, що збирає статистику про певні стани системи, значних глобальних змінних або властивостей сутностей.

Дискретно-подієве моделювання має величезну сферу додатків – від логістики та систем масового обслуговування до транспортних та виробничих систем. Деякі вчені вважають, що дана парадигма моделювання насправді є єдиним представником імітаційного моделювання.

Агентне моделювання. Останнім досягненням у галузі імітаційного моделювання стало агентне моделювання. З'явилася можливість описувати соціально-економічні взаємодії та породжувані ними процеси прак-

тично без спрощень, в їх реалістичному вигляді. В останні роки також відбулися істотні зрушення в області створення доступних масовому користувачеві засобів для комп'ютерного імітаційного моделювання, включаючи і його агентний напрям. Є підстави вважати, що ці досягнення в істотному ступені збільшили доступність комп'ютерного імітаційного моделювання та кордон, що відокремлює його від масового використання, скоро буде перейдено [26; 52; 361; 133; 134; 137; 138; 384; 432].

Агентне моделювання – відносно нове. Напрям в імітаційному моделюванні, який використовується для дослідження децентралізованих систем, динаміка функціонування яких визначається не глобальними правилами і законами (як в інших парадигмах моделювання), а навпаки, коли ці глобальні правила і закони є результатом індивідуальної активності членів групи.

Мета агентних моделей – отримати уявлення про ці глобальні правила в загальній поведінці системи, виходячи з припущень про індивідуальну, приватну поведінку її окремих активних об'єктів і взаємодії цих об'єктів в системі. Агент – якась сутність, що володіє активністю, автономною поведінкою, може приймати рішення відповідно з деяким набором правил, взаємодіяти з оточенням, а також самостійно змінюватися.

Агентний підхід займає в сучасному імітаційному моделюванні соціально-економічних систем центральне місце. Його появу можна розглядати як результат еволюції методології моделювання: перехід від моно-моделей (одна модель – один алгоритм) до мультимоделей (одна модель – безліч незалежних алгоритмів). Агентне моделювання органічно включає в себе інші наявні підходи імітаційного моделювання, оскільки вони можуть застосовуватися "всередині" агентної моделі при формалізації її окремих активних об'єктів або агентів.

Агент є індивідуалізованим активним об'єктом, який може позначати людину, транспортний пристрій, компанію, населений пункт тощо. Залежно від того, який об'єкт є агентом, модель може відповідати високому рівню абстракції (агент – компанія, країна), середньому (агент – транспортна одиниця), низькому (агент – окрема людина) або поєднувати кілька рівнів. Таким чином, дана парадигма є найбільш універсальною. Основною відмінністю агентного підходу від перших двох є побудова моделі за принципом знизу-догори. Залежності між агрегованими величинами не задаються, виходячи зі знань про реальний світ, а виходять у процесі моделювання індивідуальної поведінки десятків, сотень або тисяч аген-

тів, їх взаємодії один з одним і з об’єктами, моделюючими навколишнє середовище. Наприклад, дослідження соціальної мережі буде відбуватися не в поняттях загальної думки її членів спільноти, а в моделі будуть закладені можливі реакції окремої людини на зміну повідомлення, ступінь довіри до людини, що його надіслала та інформативності самого повідомлення.

У агентів з’являється можливість "спілкуватися" між собою, обмінюватися інформацією, уподобаннями, впливаючи, тим самим, на поведінку один одного. Модель може враховувати просторові характеристики, взаєморозташування агентів один до одного і об’єктів навколишнього середовища.

Формалізоване визначення багатоагентної системи, де не деталізується зміст її складових, наведено у формулі [235]:

$$MAS = (A,E,R,ORG, ACT,COM,EV), \quad (9.2)$$

де *A* – множина агентів;

E – безліч середовищ, що знаходяться в певних відносинах *R* і взаємодіють один з одним, формують деяку організацію *ORG*, що володіють набором індивідуальних і сумісних дій *ACT* (стратегія поведінки і вчинків), включаючи можливі комунікативні дії *COM* і можливість еволюції *EV*.

До переваг агентного підходу слід віднести: відсутність визначеності в поведінці системи на глобальному рівні, що може привести до появи нових гіпотез про її функціонування в ході симуляції моделі; реалізм і гнучкість в описі системи, можливість моделювати найскладніші нелінійні зворотні зв’язки, використовувати будь-який необхідний рівень деталізації та абстракції. В агентному моделюванні відсутні обмеження на гетерогенність елементів моделі; з’являється можливість моделювання спілкування та обміну інформацією. До потенційних бар’єрів для побудови агентної моделі слід віднести, по-перше, наявність адекватних даних. Як правило, зібрати статистику за характеристиками індивідуальних об’єктів складніше, ніж за агрегованими показниками. По-друге, доведеться визначити логіку поведінки окремого агента в термінах, доступних для обробки комп’ютером. Якщо це складний об’єкт, наприклад людина, то доводиться моделювати такі ірраціональні речі, як психологію поведінки, вибору, звички. В процесі імітаційних експериментів можуть виникнути обчислювальні складності, оскільки агентні моделі

в середньому вимагають великих апаратних і програмних потужностей для проведення симуляції, ніж системна динаміка або дискретно-подієве моделювання.

Агентний підхід є найбільш молодим і тому найменш знайомим світовим ученим. Бізнес-проблематику, де успішно застосовується агентний підхід, можна розділити на такі напрями:

моделювання з потоками;

моделювання ринків;

моделювання інновацій в бізнесі;

оптимізаційне моделювання.

До першого належать задачі з різного роду потоками. Вони можуть складатися з людей (проблеми пропускної здатності приміщень, евакуації), одиниць транспорту (моделювання міського трафіку, планування аеропортів, вокзалів).

Часто для цього застосовується дискретно-подієвий підхід. Якщо ж об'єкти моделювання занадто різнорідні або необхідно врахувати їх просторове взаєморозташування, то переважно використання агентного підходу.

Прикладом завдання першого напряму служить моделювання евакуації при тисняві в місцях масового скупчення громадян.

Поведінка людей в таких ситуаціях часто стає ірраціональною і не піддається моделюванню традиційними методами.

Агентний підхід зарекомендував себе для відшукання оптимальних методів евакуації та мінімізації можливих ризиків.

Агентне моделювання часто застосовується західними компаніями при проектуванні парків розваг, супермаркетів.

У таких задачах оптимізується геометричне розташування елементів системи щодо один одного (наприклад, атракціонів та кафе, або кас і полиць з продуктами).

Метою може служити збільшення пропускної здатності, скорочення часу стояння в чергах, оптимальне розташування рекламних матеріалів.

Наприклад, зібравши статистику про переваги відвідувачів та характерних для них шляхах прямування, розробники використовували агентних підхід у поєднанні з генетичними алгоритмами для поліпшення розташування елементів супермаркетів.

Слід зазначити, що вирішувати подібні завдання аналітичними або статистичними методами вкрай важко, і агентне моделювання є одним з небагатьох можливих засобів підтримки прийняття рішень.

Другий напрям належить до моделювання ринків, споживчих або фінансових. Агентний підхід дозволяє зробити акцент на індивідуальні переваги, стереотипи поведінки споживачів при виборі ними продуктів і послуг. Агентний підхід добре застосовувати для моделювання функціонування бірж. Результати торгів залежать від поведінки безлічі незалежних людей з різними цільовими функціями, і їх поведінка логічно моделювати в рамках агентного підходу. Підтвердженням цьому служить, наприклад, модель Bios Group фондової біржі NASDAQ. Модель вимірювання та мінімізації операційних ризиків управління активами банку Societe Generale є прикладом застосування АМ у фінансових інститутах і банках.

Третій напрям об'єднує завдання моделювання інновацій в бізнесі, їх первісного поширення на ринку. До четвертого напрямку відносять завдання, пов'язані з оптимізацією організаційної структури, бізнес-процесів і зниженням операційних ризиків.

Таким чином, для систем подібного типу агентно моделювання є підходом більш універсальним і потужним, оскільки воно дозволяє врахувати будь-які складні структури і поведінки. Інша важлива перевага агентного моделювання в тому, що розробка моделі можлива у відсутності знання про глобальні залежності: потрібні мінімальні знання про те, які фактори впливають один на одного на глобальному рівні, або яка глобальна послідовність операцій, тощо, але, розуміючи індивідуальну логіку поведінки учасників процесу, можна побудувати агентну модель і вивести з неї глобальні поведінку. Тому, іноді, навіть якщо є можливість побудувати модель системної динаміки або дискретно-подієву модель, побудувати агентну модель може бути простіше. Важливою перевагою агентного моделювання є можливість врахування властивостей індивідуальних об'єктів з локальними правилами поведінки, тому що оточуюче середовище також може мати динаміку. Агенти взаємодіють прямо і побічно через середовище. Крім того агентну модель простіше підтримувати: уточнення зазвичай робляться на локальному рівні і не вимагають глобальних змін.

9.3. Агентне моделювання впливу соціальних мереж на лояльність клієнтів засобами пакета ANYLOGIC

Проведено порівняльний аналіз ринку пакетів імітаційного моделювання за різними характеристиками, на підставі якого для моделювання впливу соціальних мереж на лояльність клієнтів був обраний

пакет AnyLogic 6.7.1. Подано предметну технологію моделювання, яка включає: моделювання впливу реклами на формування лояльності клієнтів з врахуванням впливу спілкування агентів, моделювання повторних покупок та перевірку адекватності моделі. Побудовано модель та здійснено моделювання впливу соціальних мереж на лояльність клієнтів у середовищі пакета AnyLogic.

У світі інформаційних технологій імітаційне моделювання переживає друге народження. Інтерес до цього виду комп'ютерного моделювання пожвавився в зв'язку з істотним технологічним розвитком систем моделювання, які на сьогоднішній день є потужним аналітичним засобом, що увібрали в себе весь арсенал новітніх інформаційних технологій, включаючи розвинені графічні оболонки для цілей конструювання моделей та інтерпретації вихідних результатів моделювання, мультимедійні засоби і відео, що підтримують анімацію в реальному масштабі часу, об'єктно-орієнтоване програмування, Internet-рішення та ін.

У силу своєї привабливості і доступності ці технології імітаційного моделювання з легкістю покинули академічні стіни і сьогодні освоюються IT-фахівцями в бізнесі.

У даний час в Україні, слідом за США, Європою та Росією, що правда, в силу відомих економічних причин, з деяким відставанням, позначився інтерес у застосуванні цього класу програмних продуктів у різних аналітичних програмах і в інформаційних бізнес-системах різного призначення.

За даними останніх оглядів [396; 403; 432], що публікуються в Інтернет, куди інформація надається компаніями-виробниками програмного забезпечення для імітаційного моделювання, сьогодні на ринку інформаційних технологій фігурує близько 150 програмних продуктів аналітичного типу, орієнтованих на імітаційне моделювання.

Діапазон і різноманітність такого програмного забезпечення продовжує зростати, відбиваючи тенденцію стійкого попиту на нього.

Протягом декількох років вивчалися технологічні та функціональні можливості цих систем моделювання, що дозволило скласти загальне уявлення про ситуацію на ринку інформаційних технологій, виявити основні тенденції в області сучасних систем моделювання.

У якості домінуючих базових концепцій формалізації і структуризації в сучасних системах моделювання використовуються такі пакети:

AnyLogic, Arena, AutoMod, eM-Plant, Extend Industry, ProModel, QUEST, Witness.

Технологічні можливості сучасних систем моделювання характеризуються універсальністю і гнучкістю базової та альтернативної до базової концепцій структуризації і формалізації модельованих динамічних процесів, закладених у систему моделювання.

Сьогодні популярними серед систем моделювання дискретного типу є процесно-орієнтовані концепції структуризації, засновані на мережних парадигмах, автоматному підході і деякі інші; серед систем моделювання безперервного типу – моделі та методи системної динаміки;

наявністю засобів проблемної орієнтації, коли система моделювання містить набори понять, абстрактних елементів, мовні конструкції з предметної області відповідного дослідження;

застосуванням об’єктно-орієнтованих спеціалізованих мов програмування, що підтримують авторське моделювання та процедури управління процесом моделювання;

наявністю зручного і легко інтерпретованого графічного інтерфейсу; коли блок-схеми дискретних моделей і системні потокові діаграми реалізуються на графічному рівні, параметри моделей визначаються через підменю;

використанням розвиненою двох- і трьохмірної анімації в реальному часі;

можливістю для реалізації декількох рівнів подання моделі, засобами для створення стратифікованих описів. Сучасні системи моделювання застосовують структурно-функціональний підхід, багаторівневі ієрархічні, вкладені структури та інші способи подання моделей на різних рівнях опису;

наявністю лінійок та інструментів для проведення і аналізу результатів сценарних, варіантних розрахунків на імітаційної моделі;

математичної та інформаційною підтримкою процедур аналізу вхідних даних, аналізу чутливості та широкого класу обчислювальних процедур, пов’язаних з плануванням, організацією і проведенням спрямованого обчислювального експерименту на імітаційній моделі.

експериментальні дослідження на імітаційній моделі є інформативними, тому необхідна реалізація підходу Simulation Data Base, заснованого на доступі до баз даних моделювання.

Технологічно це вирішується за допомогою власних спеціалізованих аналітичних блоків системи моделювання або за рахунок інтеграції з іншими програмними середовищами;

виконавчий модуль може функціонувати поза середовищем для розробки моделі;

застосуванням багатокористувальницкого режиму роботи, інтерактивного розподіленого моделювання, розробками в області взаємодії імітаційного моделювання з всесвітньою павутиною та ін.

Порівняльна характеристика для перерахованих раніше найбільш популярних систем імітаційного моделювання наведена в табл. 9.4 – 9.8.

Таблиця 9.4

Характеристики систем моделювання за параметрами: виробник, типові модулі пакета, області застосування пакета, потреба в ОЗУ, ОС

Пакет	Виробник	Типові модулі пакета	Області застосування пакета	Потреба в ОЗУ	ОС
1	2	3	4	5	6
Any Logic 6.7.1	XJ Technologies	Аналіз системної динаміки, аналіз ризиків, оптимізація, планування, підтримка ухвалення рішення, агентний підхід	Стратегічний менеджмент, виробництво, обслуговування, логістика, ланцюжки поставок, медицина, транспорт, IT управління, телекомунікації, наука	128MB мін., 512MB рекомен.	Windows NT, 2000, XP, 7
Arena	Rockwell Software	Виробництво, ланцюжки поставок, бізнес-процеси, медицина, ВПК, складування і логістика	Виробництво, ланцюжки поставок/ логістика, управління бізнес-процесами, медицина	64MB мін., 128MB рекомен.	Windows 95, 98, ME, NT, 2000 and XP
Auto Mod	Brooks Automation	Транспортні системи, складування, лінії фасування, виробництво	Автомобільна, аерокосмічна галузі, аеропорти, виробництво, складування і збут	512MB або вище рекомен.	Windows OS

Закінчення табл. 9.4

1	2	3	4	5	6
eM-Plant	Tecno-matix Techno-logies Inc	Виробництво, транспор-тування, розвантажу-вально-навантажувальні операції, симуляція біз-нес-процесів, логістика, продажі, календарне планування, вироблення ритму виробництва, верифікація процесів	Дискретне вироб-ництво (автомо-більна галузь, електроніка, судно-будування, верста-тобудування, скла-дальні лінії і т. д.), логістика, збут, консалтіг, охорона здоров'я, банків-ський бізнес	64MB мін., 512MB рекомен.	Windows NT, 2000 and XP
Extend Industry	Imagine That, Inc	Моделювання крупно-маштабних систем з ве-ликими навантаження-ми. Включає внутрішню реляційну базу даних і модуль для моделю-вання	Системи масового обслуговування, включаючи збутову логістику, call-цент-ри, пакувальні лінії і т. д.	64MB мін., 128MB+ рекомен.	Windows XP, 2000, NT, ME, 98; Power Macin-tosh OS
Pro-Model	ProModel Solutions	Аналіз відхилень, шість сигм; проектування і планування портфеля; оцінка потужностей, аналіз витрат; моделю-вання циклічних удос-коналень у часі; ланцю-га поставок	Виробництво і ло-гістика, фармацев-тика	64MB мін., 128MB рекомен.	Windows 98 or later
QUEST	Delmia		Виробництво (автомобілебуду-вання, авіобуду-вання, космонав-тика, електроніка, суднобудування)		–
Witness	Lanner Group ltd	Виробництво, оптиміза-ція, планування, кален-дарне планування, мо-делювання бізнес-процесів	Шість сигм, call-центри, ВНЗ, моде-лювання бізнес про-цесів, виробництво	–	–

Таблиця 9.5

Характеристики систем моделювання за параметрами: графічна побудова моделі, побудова моделі з використанням програмування, покрокове налагодження

Пакет	Графіка	Використання програмування	Покрокове налагодження
AnyLogic 6.7.1	Так	Так	Так
Arena	Так	Так	Так
AutoMod	Так	Так	Так
eM-Plant	Так	Так	Так
Extend Industry	Так	Так	Так
ProModel	Так	Так	Так
QUEST	Так	Так	Так
Witness	Так	Ні	Так

Таблиця 9.6

Характеристики систем моделювання за параметрами: установка вхідного розподілу, підтримка аналізу вихідної інформації, пакетне введення і розробка експерименту

Пакет	Установка вхідного розподілу	Підтримка аналізу вихідної інформації	Пакетне введення і розробка експерименту
1	2	3	4
AnyLogic 6.7.1	Stat::Fit підтримує більше 40 математичних розподілів	Збір даних і статистична обробка (відхилення від середньої, імовірнісні розподілу і т. д.), представлення (графіки Ганта, гістограми і т. д.)	Підтримувані типи експерименту: симуляція, оптимізація, Монте Карло, аналіз чутливості, користувальницький алгоритми
Arena	Ні	Output Analazer (відхилення від середньої, Anova, гістограми, графіки)	Ні
AutoMod	З використанням ExpertFit	Модуль AutoStat забезпечує збільшений статистичний аналіз протягом всієї фази експериментування над модельованим об’єктом	Пакетне введення при використанні AutoStat; AutoMod дозволяє планувати експеримент

Закінчення табл. 9.6

1	2	3	4
eM-Plant	Включено Стандартний інструмент аналізу даних (DataFit)	Стандартний включений інструмент аналізу даних DataFit (Довірчий інтервал, середні і т. д.)	Система управління експериментом, підтримка пакетного режиму роботи, розрахунок довірчих інтервалів, нейронні мережі
Extend Industry	Ні	Довірчі інтервали і т. д.	Автоматичне виконання різних сценаріїв
ProModel	Визначені користувачем розподіли, 15 зумовлених розподілів, плюс розподіли, що поставляються з Stat::Fit (включене програмне забезпечення)	Повний аналіз вихідних даних, використання діаграм; також експорт в Excel і Access для подальшого аналізу	Необмежена кількість сценаріїв може бути задана в експерименті за параметрами
QUEST	Ні	Здійснює комбінований аналіз, стохастичний аналіз спільних ймовірностей всіх подій	Ні
Witness	Містить близько 10 математичних розподілів. Крім цього можливе програмування власного розподілу	Ні	Ні

Таблиця 9.7

Характеристики систем моделювання за параметрами: оптимізація, використання коду, передача моделі

Пакет	Оптимізація	Повторне використання коду	Передача моделі	Інструменти підтримки передачі
1	2	3	4	5
AnyLogic 6.7.1	Вбудований механізм OptQuest може працювати як з класичними, так і дуже об’ємними завданнями, включаючи структурну оптимізацію	Так	Так	Додаткові кошти непотрібні
Arena	Ні	Так	Так	Ні
AutoMod	Оптимізація заснована на алгоритмі еволюційної стратегії	Так	Так	Робочий модуль (платний) або програвач (безкоштовний)

Закінчення табл. 9.7

1	2	3	4	5
eM-Plant	Генетичні алгоритми, нейромережі	Так	Так	Різні види пакетів: бібліотеки (просте моделювання), моделі (зміна параметрів), перегляд (тільки імітація)
Extend Industry	Еволюційний оптимізатор з відкритим кодом включений в усі версії Extend	Так	Так	Завантажувані безкоштовно програвач та демо-версія дозволяють відкривати, переглядати і виконувати моделі
ProModel	Доступна оптимізація з використанням OptQuest та/або SimRunner	Так	Так	ПЗ упаковує моделі, моделі і дані можуть проглядатися безкоштовним програвачем
QUEST	Ні	Так	Ні	Так
Witness	Спеціальний модуль WITNESS Optimizer	Так	Так	Так

Таблиця 9.8

Характеристики систем моделювання за параметрами: анімація, можливість перегляду в режимі реального часу, експорт анімації

Пакет	Анімація	Перегляд в режимі реального часу	Експорт анімації	Сумісне анімаційне ПЗ
AnyLogic 6.7.1	Так	Так	Так	Ні
Arena	Так	Так	Ні	Так
AutoMod	Так	Так	Так	Так
eM-Plant	Так	Так	Так	Так
Extend Industry	Так	Так	Ні	Так
ProModel	Так	Так	Ні	Ні
QUEST	Так	Так	Так	Так
Witness	Так	Так	Так	Ні

Перевагами пакета AnyLogic є те, що його типові модулі відповідають предметній області, що моделюється; потреба в ОЗУ невелика; в перерахованих ОС є Windows 7; можна побудувати графічну модель; є можливість використовувати засоби програмування та покрокове налагодження; можна симулювати експеримент.

Модель може бути запущена навіть якщо у користувача не встановлений пакет AnyLogic; є можливість перегляду анімації в режимі реального часу та її експорту.

Не зважаючи на те, що для AnyLogic немає сумісного анімаційного ПЗ, всіх зазначених переваг достатньо для того, щоб обрати пакетом моделювання саме AnyLogic 6.7.1, який є найбільш підходящим інструментом для моделювання інформаційного впливу на лояльність клієнта.

Розглянуті технологічні можливості сучасних систем моделювання багато в чому визначають сьогодні пожвавлення інтересу до імітаційного моделювання не тільки в галузі державного, глобального моделювання, але і в комерційній сфері.

Споживачами такого роду аналітичної продукції виступають аналітичні відділи банків, промислові компанії, фінансово-промислові групи, страхові та інвестиційні компанії, консультаційні, проектні організації, регіональні органи влади, галузі та ін.

За допомогою імітаційного моделювання ефективно вирішуються завдання найширшої проблематики – в області стратегічного планування, бізнес-моделювання та реінжинірингу, менеджменту та управління виробництвом, ланцюжками поставок.

Для візуалізації впливу соціальних мереж на формування лояльності клієнтів був використаний пакет моделювання бізнес-процесів BPWin.

На рис. 9.8, 9.9 подані контекстна діаграма та її декомпозиція відповідно.

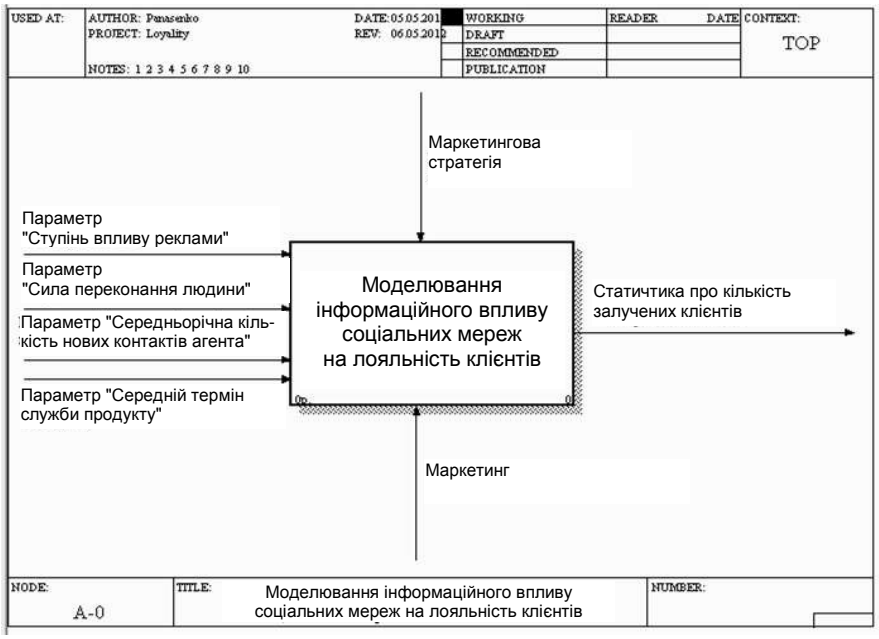


Рис. 9.8. **Контекстна діаграма "Моделювання інформаційного впливу соціальних мереж на лояльність клієнтів"**

Контекстна діаграма "Моделювання інформаційного впливу соціальних мереж на лояльність клієнтів" поділяється на чотири роботи: "Моделювання впливу реклами на формування лояльності клієнтів", "Моделювання врахування впливу спілкування агентів", "Моделювання повторних покупок", "Перевірка адекватності моделі".

Робота "Моделювання впливу реклами" отримує на вході параметр "Ступінь впливу реклами", а на виході видає модель впливу реклами на формування лояльності клієнта та кількість залучених потенційних клієнтів. Дана модель є елементарною, тому що кількість залучених клієнтів залежить лише від ступеня впливу реклами.

У роботі "Моделювання впливу спілкування агентів" на вхід подаються параметри "Середньорічна кількість нових контактів агента", "Сила переконання людини" та елементарна модель. На виході – модель врахування впливу спілкування агентів та кількість залучених потенційних клієнтів.

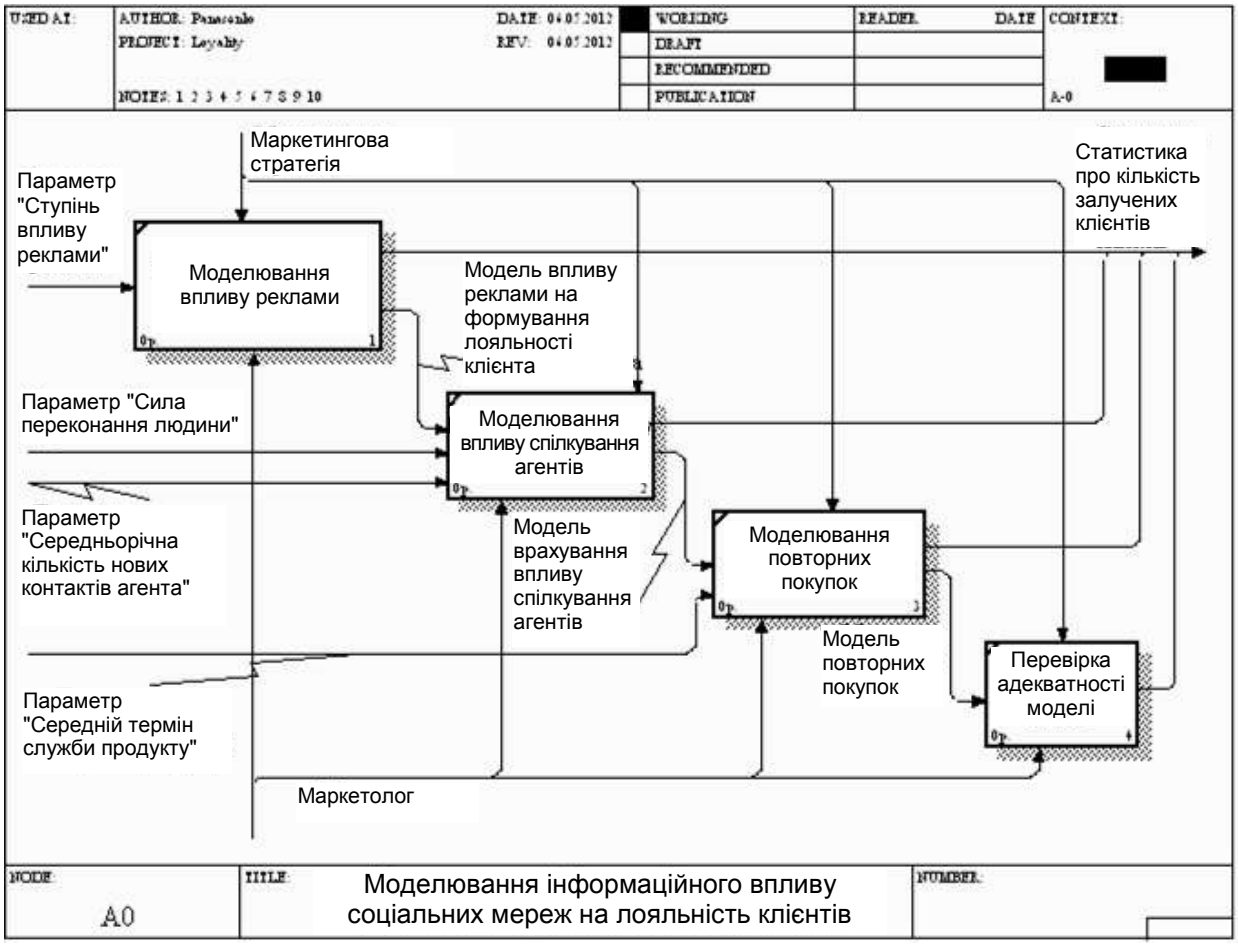


Рис. 9.9. **Декомпозиція контекстної діаграми "Моделювання інформаційного впливу соціальних мереж на лояльність клієнтів"**

Робота "Моделювання повторних покупок" отримує на вході модель врахування впливу спілкування агентів та параметр "Середній термін служби продукту". На виході дана робота перетворюється у модель повторних покупок та видає кількість залучених потенційних клієнтів.

У роботі "Перевірка адекватності моделі" на вхід подається модель повторних покупок, а на виході видається статистика про кількість залучених клієнтів.

Виконує всі роботи маркетолог.

Далі будуть побудовані всі зазначені моделі та перевірена адекватність моделі з можливістю здійснення повторних покупок.

Елементарна модель впливу соціальних мереж на лояльність клієнта – це модель, в основу якої покладено факт, що на лояльність клієнта впливає всього один параметр "ступінь впливу реклами".

Дифузна модель Френка Басса є основою побудови елементарної моделі. Ймовірність того, що в момент T буде здійснена покупка нового продукту є лінійна функція від кількості попередніх клієнтів:

$$P(T) = p + \frac{q}{m} \cdot Y(T), \tag{9.3}$$

де p – ймовірність покупки в момент T=0 (const);

$Y(T)$ – кількість попередніх клієнтів;

q та m – деякі константи.

Одним із способів побудови складних моделей у комп'ютерному моделюванні є поетапна побудова, коли за початкову основу береться базова модель, а далі в результаті поетапного ускладнення на кожному кроці виходить нова модель, що входить у безліч ієрархічних моделей зі збільшуваною складністю. Базова модель – це імітаційна модель, основні властивості якої можна сформулювати точно у вигляді теорем, що були отримані строгими аналітичними методами.

За допомогою пакета AnyLogic було створено агентну модель на 1 000 агентів. Мережа на 1 000 агентів є малою мережею. В даній роботі було обрано саме її, тому що чим мережа є меншою, тим більше довіра до агентів та тим більш наглядним є вплив будь-яких показників.

Поведінка агента зазвичай описується в класі цього агента (в моделі – це клас Person) за допомогою діаграми станів (стейтчарт). Стейтчарт складається із двох станів: потенційний клієнт (людина, яка ще не купила

продукт компанії) та існуючий клієнт. Між цими станами існує перехід. Цей перехід буде моделювати покупку продукту. Для побудови елементарної моделі слід припустити, що людина, одного разу придбавши продукт, назавжди залишається його споживачем, і, відповідно, переходу зі стану "клієнт" (Client) в стан "потенційний клієнт" (PotentialClient) поки що бути не повинно. Параметром, за яким визначається чи стане потенційний клієнт реальним, є ступінь впливу реклами соціальних мереж на агентів, які там зареєстровані. Час, через який людина купить продукт, експоненціально залежить від ступеня впливу реклами продукту.

$$t_{пок}=exp(a), \tag{9.4}$$

де $t_{пок}$ – час, через який людина купить продукт;

a – ступінь впливу реклами – інформаційний вплив соціальної мережі, тобто те, наскільки інформаційне повідомлення є ефективним та впливає на потенційного клієнта.

Елементарна модель передбачає, що людина назавжди залишається споживачем продукту, якщо хоча б раз придбала його. Тобто переходу із стану Client до стану PotentialClient не має (рис. 9.10).

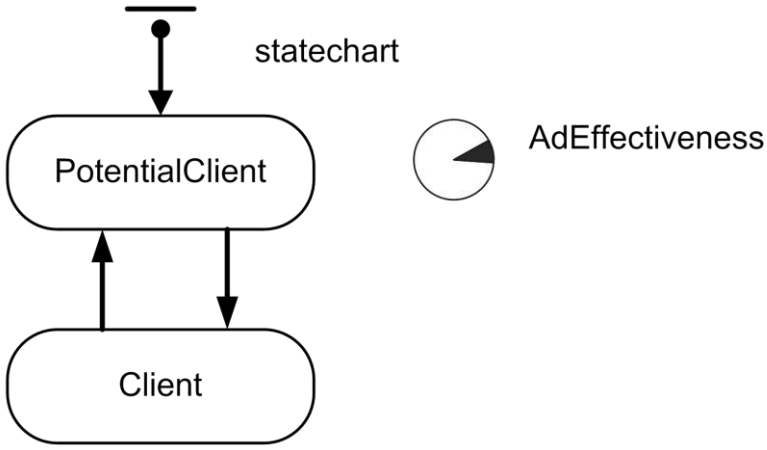


Рис. 9.10. **Стейтчарт елементарної моделі впливу на лояльність клієнта**

Побудовану модель за 7 одиниць модельного часу, що у житті може бути інтерпретовано як тиждень, наведено на рис. 9.11. На ній видно, як число потенційних клієнтів (сірих) переходить у розряд реальних (чорних).

Головним завданням моделі розповсюдження продукту є вивчення того, як швидко люди купують новий продукт. Для цього необхідно підрахувати кількість клієнтів та потенційних клієнтів. У AnyLogic це можна зробити за допомогою функцій збору статистики.

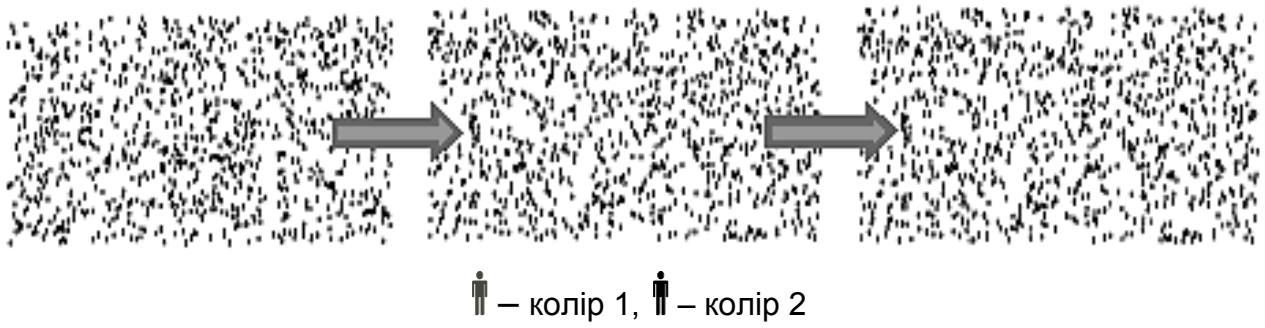


Рис. 9.11. **Моделювання переходу клієнтів із стану потенційних до стану реальних**

Для підрахунку потенційних клієнтів була створена функція збору статистики potentialClients з умовою:

item.statechart.isStateActive(item.PotentialClient).

Ця функція буде вести підрахунок кількості агентів, для яких виконується задана умова, тобто тих агентів, які знаходяться в поточний момент часу в стані PotentialClients. Тут item – це агент (елемент реплікованого об’єкта people).

Також було створено ще одну функцію збору статистики clients з умовою:

item.statechart.isStateActive(item.Client).

Ця функція буде вести підрахунок кількості агентів, які знаходяться в стані Client (тобто вже придбали продукт).

Також для візуалізації результатів був доданий часовий графік, що відображає динаміку зміни чисельності споживачів і потенційних споживачів продукту.

На рис. 9.12 показаний результат динаміки процесу, що моделюється.

Висновок за моделлю: таку модель можна будувати на будь-яку кількість агентів і результат буде ідентичним – кількість потенційних клієнтів зменшується, в той час як кількість реальних – збільшується, а в результаті всі агенти моделі стануть реальними клієнтами. Це є недоліком даної

моделі, тому вона не може бути застосована у такому вигляді в реальному житті постійно, оскільки враховує тільки один фактор "ступінь впливу реклами", час дії якого є обмеженим. Також ця модель не враховує того факту, що реальний клієнт знову може стати потенційним. Тому далі дана модель буде модифікована з додаванням параметрів, які враховують ступінь довіри агентам та середньорічну кількість нових контактів.

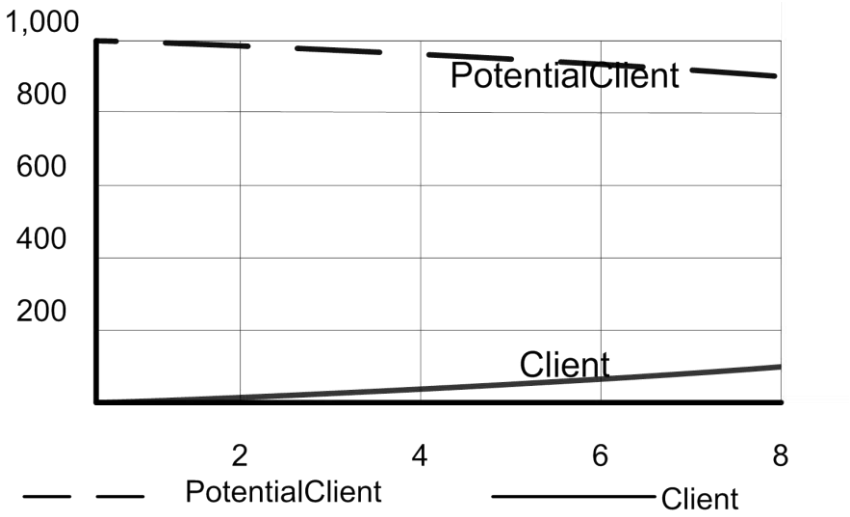


Рис. 9.12. **Результат динаміки процесу впливу соціальних мереж на лояльність клієнтів у мережі на 1000 агентів**

Спілкування – це життя, а отже, люди не можуть не спілкуватися. Рекламний ефект відіграє значну роль лише в момент випуску продукту на ринок. Надалі все більшу роль буде відігравати спілкування людей зі своїми знайомими, які цей продукт вже придбали. В основному люди здобувають нові продукти саме під впливом переконання своїх знайомих; даний процес чимось схожий з поширенням епідемії. Для розширення моделі такими параметрами, що будуть використовуватися при побудові моделі, є:

1) параметр ContactRate – середньорічна кількість нових контактів агента. Варто припустити, що агент у середньому має контакт зі 100 агентами на рік;

2) параметр ClientFraction – сила переконання людини, що впливає на те, скільки людей він зможе переконати в необхідності придбати продукт. Значення за замовчуванням – 0.015. Тип – double.

Також необхідно внести зміни до стейтчарту. В стан Client додано внутрішній перехід. Інтенсивність, за якою відбувається перехід, – це

ContactRate. Даний перехід буде моделювати покупку продукту знайомим цієї людини. Швидкість, з якою клієнт зуміє переконати свого знайомого в необхідності покупки, буде залежати від сили переконання цієї людини і від того, скільки знайомих він зустрічає за рік. Дією переходу є:

send ("Buy!", RANDOM).

Такий перехід посилає повідомлення випадково обраній людині. Метод "send ()" відсилає повідомлення іншому агенту. Перший аргумент задає повідомлення, яке буде надіслано, а другий задає агента, якому повідомлення буде адресовано. У даному випадку посилається повідомлення якомусь випадково обраному агенту, тому що значення аргумента використовує спеціальну константу RANDOM.

Даний перехід генерує сигнал для стейтчарта якогось знайомого. Потім спрацьовує перехід стейтчарта, що моделює покупку продукту цим знайомим.

Також ще один перехід зі стану PotentialClient в стан Client було додано (рис. 9.13). Він буде спрацьовувати за сигналом, який буде генеруватися внутрішнім переходом стану Client.

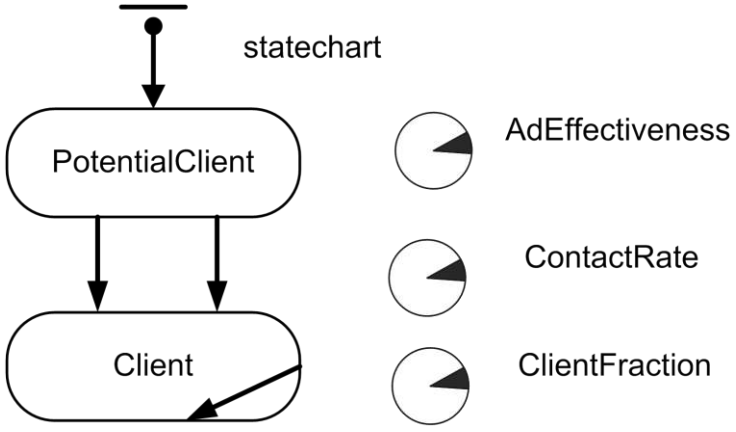


Рис. 9.13. **Стейтчарт моделі, що враховує вплив спілкування агентів**

Далі було змінено властивості цього переходу. Імовірність прийняття рішення про покупку продукту буде залежати від сили переконання людини. У даній моделі ця характеристика задається параметром ClientFraction.

У поле "Доп. умова" було введено:

randomTrue (ClientFraction).

У результаті введення додаткового умови продукт купується з ймовірністю, що задається параметром ClientFraction.

Перехід буде спрацьовувати, коли діаграма станів цього агента одержить повідомлення "Buy!" ("Купи!") Від іншого агента – свого знайомого.

Далі було змінено властивості агента. В поле "Дія при отриманні повідомлення" було введено:

statechart.receiveMessage(msg).

Створену модель показано на рис. 9.14.

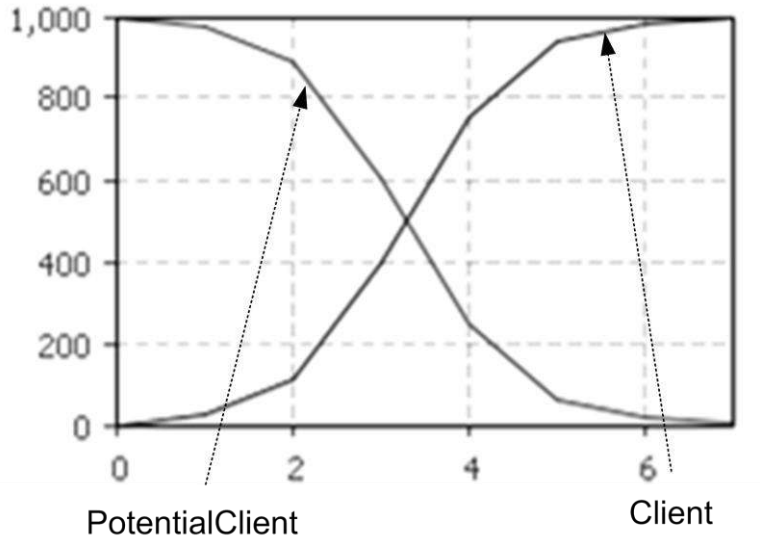


Рис. 9.14. **Модель, що враховує вплив спілкування людей**

Висновки: після вивчення динаміки зміни числа клієнтів та потенційних клієнтів можна зробити висновок, що кількість реальних та потенційних клієнтів плавно змінюється.

Графіки змінних представляють S-подібні криві.

Кількість потенційних клієнтів змінюється від максимуму до мінімуму, в той час, як кількість реальних – навпаки – від мінімуму до максимуму.

Але дана модель не враховує той факт, що клієнти можуть переходи також зі стану реальних клієнтів до стану потенційних.

У наступній моделі буде промодельовано можливість здійснення повторних покупок та, відповідно, відображено можливість зміни стану клієнта від реального до потенційного.

Це може статися, коли продукт, який було придбано, стає непридатним.

До структурної діаграми класу Main було додано параметр DiscardTime – середній термін служби продукту.

Нехай середній термін служби продукту дорівнює одному року (рис. 9.15).

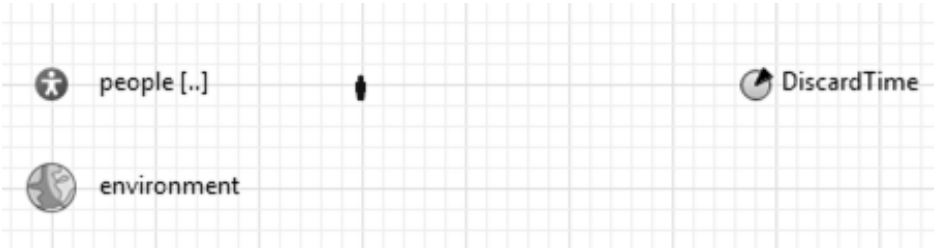


Рис. 9.15. **Параметр DiscardTime на структурній діаграмі класу Main**

Також було змінено стейтчарт агента – додано перехід зі стану Client в стан PotentialClient (рис. 9.16).

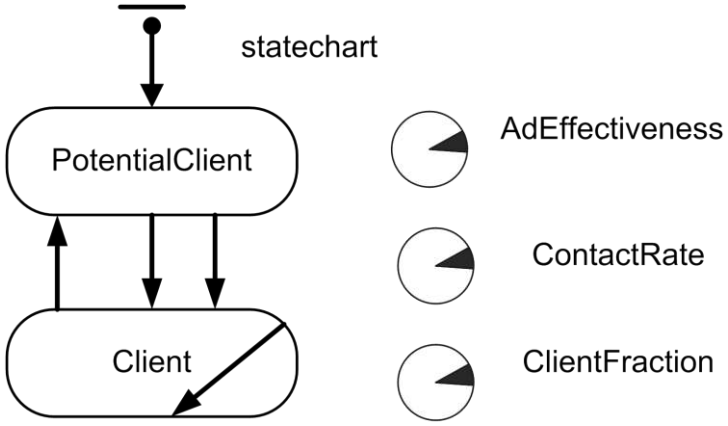


Рис. 9.16. **Стейтчарт агента з переходом з Client в PotentialClient**

Модель без умови зупинки за часом показана на рис. 9.17 та 9.18.

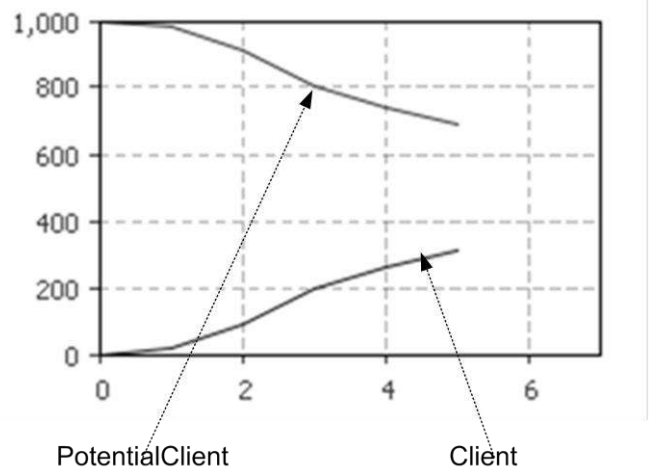


Рис. 9.17. **Модель з урахуванням можливості здійснення повторних покупок з початкового до 5-го моменту часу**

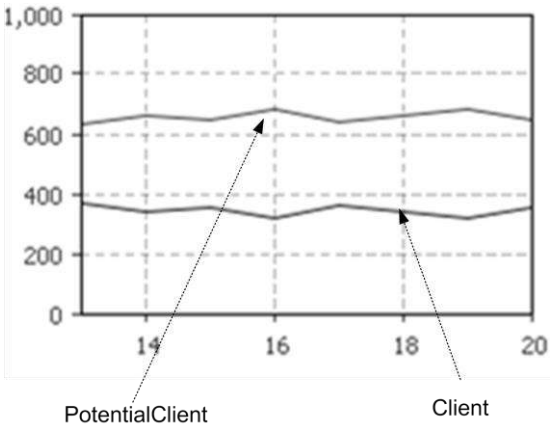


Рис. 9.18. **Модель з урахуванням можливості здійснення повторних покупок з 12-го по 20-й момент часу**

Висновки за моделлю: за допомогою діаграми була простежена динаміка зміни числа споживачів продукту.

На діаграмі видно, що насичення ринку в моделі з повторними покупками не досягається, на відміну від попередніх моделей.

Це найбільш відповідає дійсності, тому що майже не можливо, щоб усі агенти соціальної мережі 100-відсотково купували один і той самий продукт.

AnyLogic дозволяє створювати інтерактивну анімацію з можливістю зміни параметрів системи по ходу моделювання процесу.

Для створення анімації було додано в модель необхідні змінні.

На структурній діаграмі класу Person було створено допоміжну змінну isClient (тип змінної – boolean, початкове значення – false).

За допомогою даної змінної буде визначатися чи є дана людина клієнтом компанії (рис. 9.19).

На структурній діаграмі класу Main було створено дві змінні: clients з початковим значенням 0 і potclients з початковим значенням 0. Ці змінні будуть використовуватися для підрахунку чисельності клієнтів і потенційних клієнтів (рис. 9.20).

На діаграмі стейтчарта також внесено зміни. У вікні властивостей стану PotentialClient було задано дію при вході:

```
Main.potadopters++;
isAdopter=false;
```

І дією при виході з цього стану є:

```
Main.potadopters--;
```

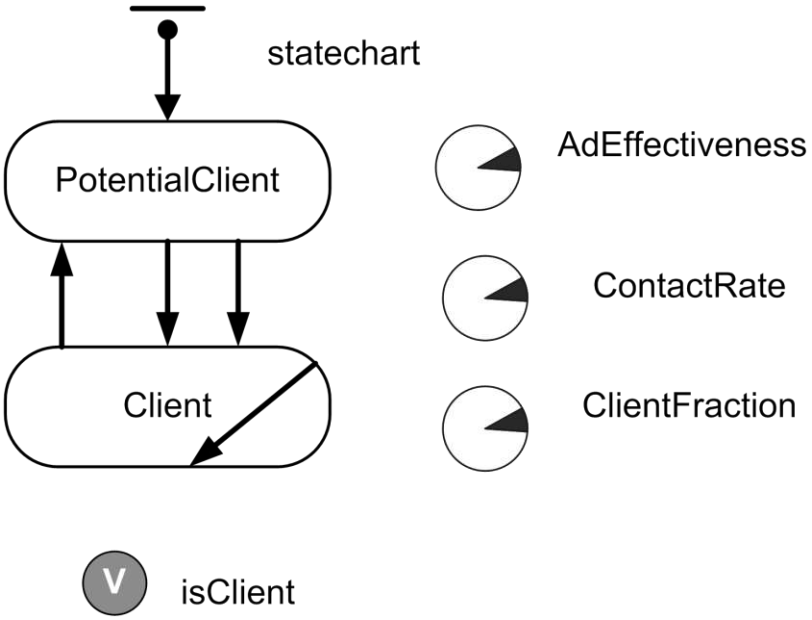


Рис. 9.19. **Стейтчарт з доданою змінною isClient**

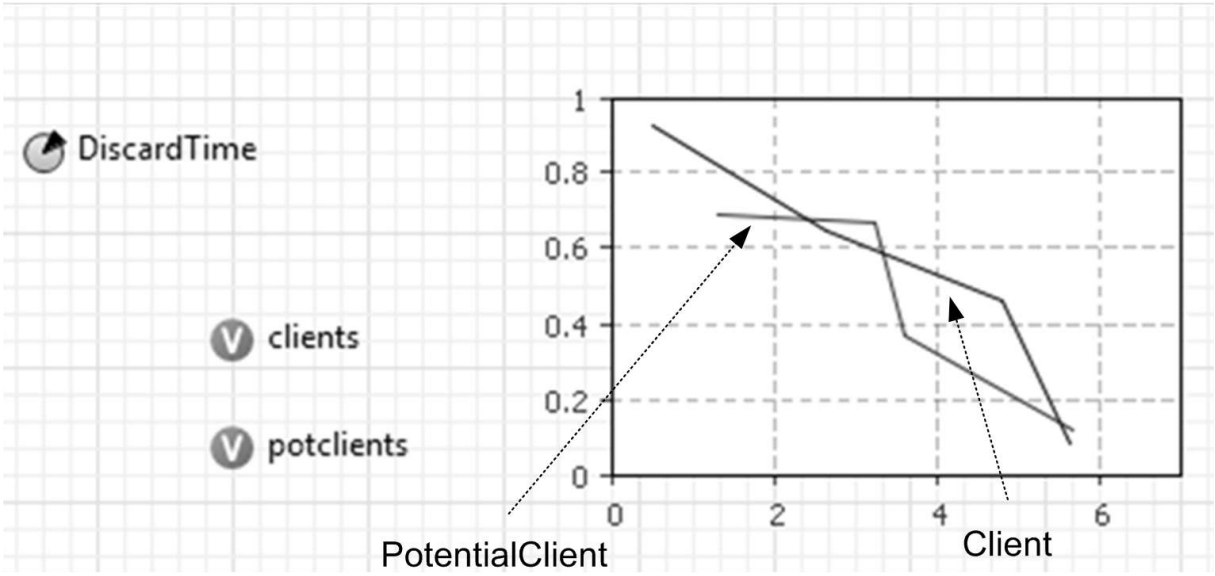


Рис. 9.20. **Структурна діаграма класу Main з доданими змінними clients та potclients**

При вході в стан значення змінної збільшується на одиницю, підраховується кількість потенційних споживачів продукту. При виході зі стану зменшується значення цієї змінної. Крім того, змінюється значення змінної isClient, щоб показати, чи купила ця людина продукцію організації (якщо так, то значення змінної – true, якщо ні, то false).

Для того, щоб створити анімаційну модель, додається стовпчиковий індикатор числа потенційних споживачів продукту (змінна, яку буде

відображати цей індикатор – potclients; максимальне відображуване значення – 1 000).

Аналогічним чином додається стовпчиковий індикатор числа клієнтів (змінна для відображення – clients).

Потім було додано елемент управління бігунок, за допомогою якого змінюється термін служби продукту (змінна, значення якої буде змінюватися за допомогою цього елемента управління, – DiscardTime). Після цього запустили модель та отримали результати, наведені на рис. 9.21 – 9.23.

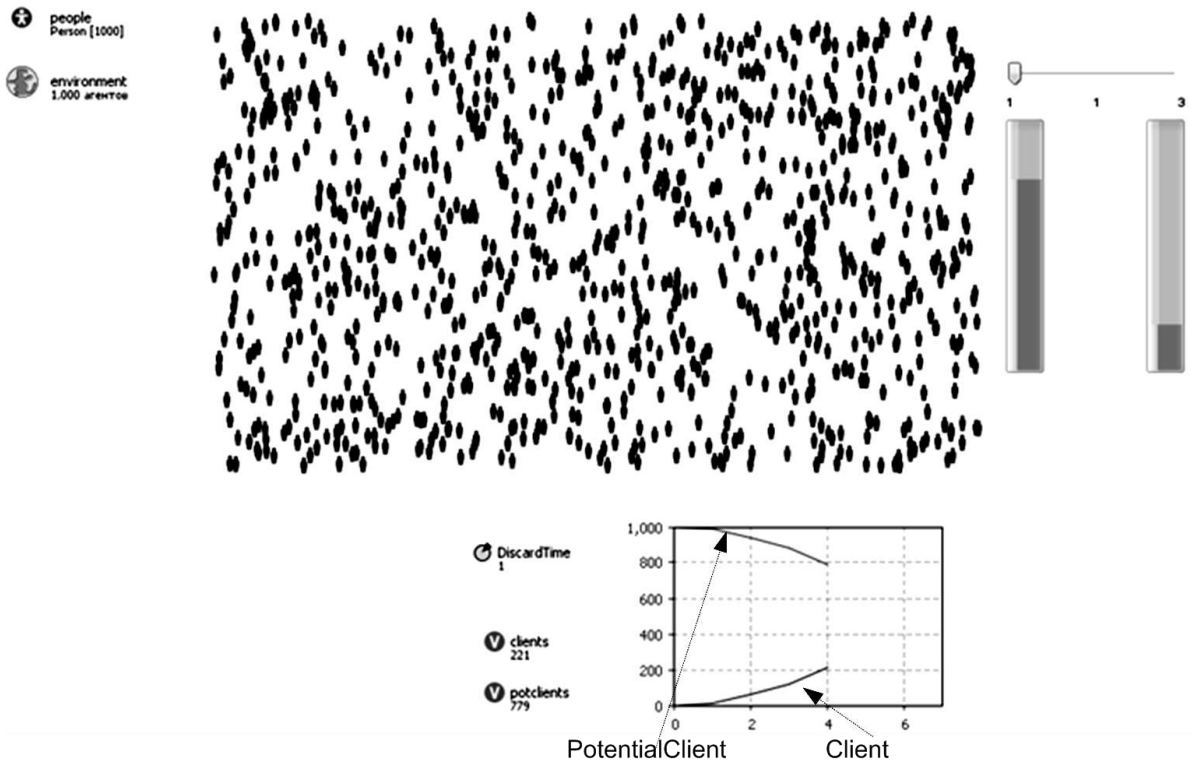


Рис. 9.21. **Анімаційна модель із середнім терміном служби рік**

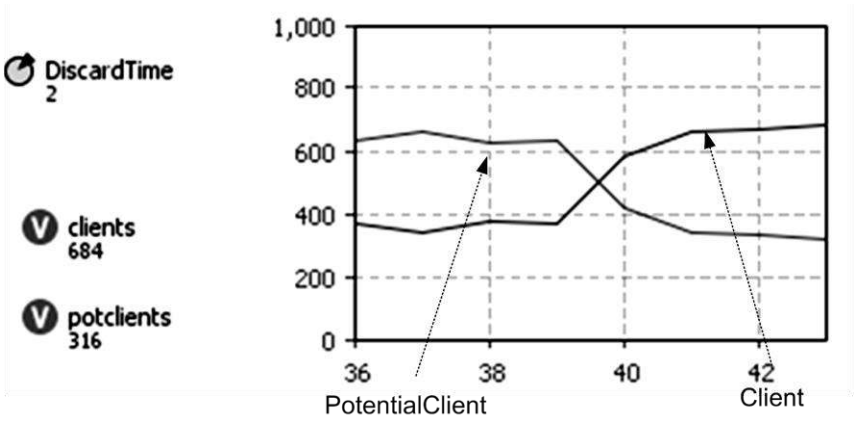


Рис. 9.22. **Анімаційна модель із середнім терміном служби два роки**

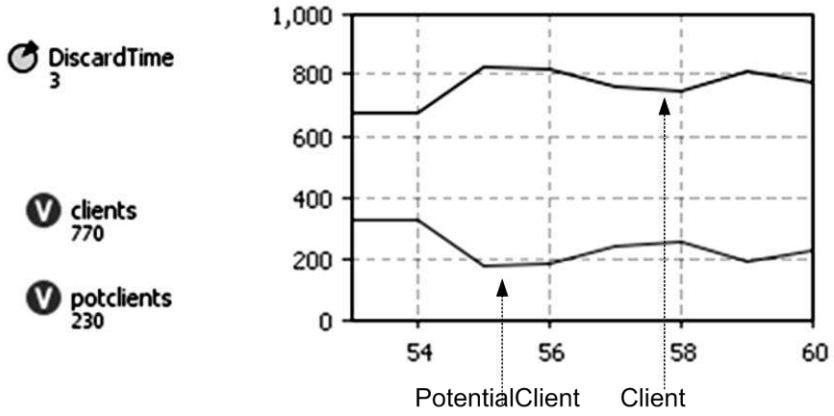


Рис. 9.23. **Анімаційна модель із середнім терміном служби три роки**

AnyLogic підтримує кілька типів мереж агентів: випадкова, решітково-упорядковане кільце, малий світ. У табл. 9.9 занесені результати експериментів зі згаданими трьома типами мереж при зміні значення параметра "Середній термін служби продукту" від 1 до 3. Всього були занесено результати трьох експериментів, потім була знайдена середня.

Існують такі способи перевірки адекватності моделі: метод експертних оцінок та емпіричний. За допомогою методу експертних оцінок оцінюється експертами, використовуючи існуючи параметри моделі, можливий вихідний результат, з яким потім буде порівняно отриманий результат моделі.

При емпіричному способі модель застосовується на практиці і після цього стає відомим вихідний результат, з яким потім порівнюється отриманий результат моделі.

Використано емпіричний спосіб перевірки моделі на адекватність, тобто заздалегідь відомий вихідний результат реально існуючої моделі.

Таблиця 9.9

Результати проведення експериментів

Тип мережі	Одиниця часу	Значення параметру "Середній термін служби продукту"	Кількість потенційних клієнтів				Кількість реальних клієнтів			
			1 експеримент	2 експеримент	3 експеримент	Середнє значення серед 3-х експериментів	1 експеримент	2 експеримент	3 експеримент	Середнє значення серед 3-х експериментів
1	2	3	4	5	6	7	8	8	10	11
Випадкова	4	1	774	707	715	732	226	293	285	268
Випадкова	4	2	388	509	307	401	612	491	693	599
Випадкова	4	3	430	298	356	361	570	702	644	639

Закінчення табл. 9.9

1	2	3	4	5	6	7	8	8	10	11
Решітково-упорядковане кільце	4	1	707	702	682	697	293	298	318	303
Решітково-упорядковане кільце	4	2	326	406	401	378	674	594	599	622
Решітково-упорядковане кільце	4	3	176	418	345	313	824	582	655	687
Малий світ	4	1	664	687	738	696	336	313	262	304
Малий світ	4	2	275	392	388	370	725	608	612	648
Малий світ	4	3	171	209	294	259	829	791	706	775
Випадкова	14	1	665	664	675	672	335	336	325	332
Випадкова	14	2	337	332	318	324	663	668	682	671
Випадкова	14	3	223	218	255	244	777	782	745	768
Решітково-упорядковане кільце	14	1	652	652	691	678	348	348	309	335
Решітково-упорядковане кільце	14	2	332	331	342	339	668	669	658	665
Решітково-упорядковане кільце	14	3	237	234	228	231	763	766	772	767
Малий світ	14	1	652	641	625	632	348	359	375	361
Малий світ	14	2	335	324	299	309	665	676	701	681
Малий світ	14	3	258	230	245	245	742	770	755	756

Вченими було запропоновано перенести увагу з питання про те, чи була установлена придатність моделі, на питання про ступінь її експериментального підтвердження. Припускається, якщо у послідовності емпіричних іспитів моделі не отримано негативних результатів, то довіра до моделі крок за кроком зростає. Опираючись в роботі на другий метод було проведено емпіричне тестування моделі: сплановано експерименти над моделлю та виконано порівняльний аналіз отриманих результатів.

Для перевірки адекватності моделі була використана сторінка соціальної мережі VKontakte [52]. Ця сторінка має близько 1 000 агентів, розповсюджуваним продуктом є лак для зовнішніх робіт, необхідність повторного використання якого виникає кожні 1 – 3 роки в домогосподарстві. Після проведення рекламної кампанії за половину тижня було залучено близько 250 нових клієнтів (середній термін служби продукту

близько одиниці), що є близьким значенням порівняно з розробленою моделлю повторних покупок, яка включає елементарну модель та врахування впливу спілкування людей. Тобто похибка складає 5 %, що є допустимою нормою.

Після проведеного аналізу можна зробити висновки, що є певна залежність між середнім терміном служби та кількістю потенційних та реальних клієнтів. Чим більше термін служби, тим більше реальних клієнтів приходить до організації та купує цей продукт. Це можна пояснити тим, що клієнти хочуть як можна довше користуватися певними товарами (за виключенням якихось специфічних товарів, де термін служби або строк придатності товару чим менше, тим краще). Тому треба приділяти особливу увагу такому параметру, як середній термін служби.

Таким чином, були вирішені такі завдання: розкрита сутність маркетингової стратегії до лояльності клієнтів, досліджена концепція CRM, розглянуті соціальні мережі як засіб впливу на лояльність клієнта, проаналізовані та класифіковані методи імітаційного моделювання, обґрунтовано вибір агентного методу для моделювання впливу соціальних мереж на лояльність клієнтів, був проведений аналіз ринку пакетів імітаційного моделювання та аналіз предметної технології моделювання, побудована та проаналізована модель інформаційного впливу соціальних мереж на лояльність клієнта, яка еволюціонувала від елементарної моделі до моделі, що відображає повторні покупки клієнтом.

У результаті аналізу літературних джерел було визначено, що наявність лояльності, тобто сприятливого відношення клієнта до даної компанії, продукту і є основою для стабільного обсягу продажів. Це у свою чергу є стратегічним показником успішності компанії і робить завдання підвищення лояльності необхідним, але разом з тим дуже складним, адже вимагає трудомісткого аналізу факторів та параметрів, що впливають на формування лояльності клієнта.

Проведений аналіз методів імітаційного моделювання соціальних мереж дозволяє зробити такі висновки: для імітаційного моделювання соціально-економічних процесів найбільш поширеними є три методи.

По-перше – метод системної динаміки, де для досліджуваної системи будуються графічні діаграми причинних зв’язків і глобальних впливів одних параметрів на інші в часі, а потім створена на основі цих діаграм модель імітується на комп’ютері.

По-друге – дискретно-подієвий метод, що пропонує абстрагуватися від безперервної природи подій і розглядати тільки основні події моделюваної системи.

По-третє – агентний метод, який дає можливість описувати соціально-економічні взаємодії та породжувані ними процеси практично без спрощень, в їх реалістичному вигляді. Таким чином, найбільш прийнятним методом для моделювання впливу соціальних мереж на лояльність клієнта є агентний.

Проведений порівняльний аналіз сучасних засобів імітаційного моделювання, який показав переваги пакета імітаційного моделювання AnyLogic. За допомогою агентного методу імітаційного моделювання була побудована модель, що ускладнювалася шляхом введення нових параметрів впливу на лояльність клієнта. Таким чином, спочатку була побудова елементарна модель з одним параметром – ступінь впливу реклами. Далі модель була розширена і були додані ще три параметри – середньорічна кількість нових контактів агента, сила переконання агента та середній термін служби продукту. Потім була промодельована здатність клієнта здійснювати повторні покупки. Це здійснювалось за допомогою додавання переходу із стану реального клієнта в стан потенційного в стейтчарті. Модель була перевірена на адекватність: відхилення від реального значення в межах норми.

Розділ 10. Моделювання інформаційного пошуку в мережі Інтернет з використанням метаданих

10.1. Огляд методів та засобів інформаційного пошуку в мережі Інтернет

Розглянуто традиційні методи інформаційного пошуку, концептуальні засади семантичної "павутини", проаналізовані засоби інформаційного пошуку в семантичній "павутині".

Класичне поняття інформаційного пошуку базується на необхідності задоволення інформаційної потреби користувачів. Процес інформаційного пошуку в загальному вигляді містить послідовність операцій, які направлені на збір, обробку і надання необхідної інформації зацікав-

леним особам. Процес інформаційного пошуку складається з таких етапів [279]:

визначення (уточнення) інформаційної потреби і формулювання інформаційного запиту;

визначення сукупності можливих інформаційних джерел;

отримання інформації з виявлених інформаційних джерел;

ознайомлення з отриманою інформацією і оцінювання результатів пошуку.

На даний час існує чимало методів інформаційного пошуку [117], наприклад:

з використанням просторово-векторного подання;

з використанням імовірності появи пошукового терміну в документі;

з використанням булевої моделі;

з використанням нейронних мереж;

з використанням нечітких множин, коли документу ставиться у відповідність нечітка множина.

Деякі з методів слід розглянути більш докладно.

При інформаційному пошуку з використанням просторово-векторного подання, пошуковий запит та документи подаються у вигляді просторових векторів. Пошукова система відбирає документи, просторові вектори яких подібні до просторового вектора пошукового запиту. В основі просторово-векторного подання документа лежить припущення, що зміст документа передається словами, що в ньому знаходяться. Просторово-векторне подання будується для пошукового запиту і для кожного документа. Просторово-векторне подання документа – це вектор у n-мірному просторі, кожний вимір якого відповідає пошуковому терміну. Координати кінця вектора чисельно визначаються тим, скільки разів пошуковий термін зустрічається в документі. Тобто кожний компонент вектора відповідає числу появи відповідного терміна в документі. Пошукова система обчислює коефіцієнт відповідності просторово-векторного подання документа до просторово-векторного подання пошукового запиту. Фактично пошукова система обчислює кут між цими векторами. Найбільш відповідними вважаються документи, просторові вектори яких спрямовані туди ж куди і просторові вектори пошукового запиту.

При імовірнісному пошуку присутність чи відсутність пошукового терміна в документі використовується для визначення імовірності того, що документ відповідає інформаційному запитові. Визначення імовірності

базується на попередніх статистичних даних про те, наскільки імовірно, що документ, який містить пошуковий термін А, відповідатиме пошуковому запитові, що містить термін А. Припускаючи, що пошукові терміни в пошуковому запиті є незалежними, можна обчислити таку імовірність для кожного пошукового терміна з пошукового запиту. Загальна імовірність відповідності документа обчислюється як добуток ймовірностей відповідності для кожного терміна. Незалежність пошукових термінів у пошуковому запиті рідко спостерігається в дійсності, тому обчислення сумарної імовірності відповідності значно ускладнюється, що збільшує час інформаційного пошуку. Крім того, необхідно мати попередні дані про входження термінів у документи.

Метод, базований на булевій моделі, ґрунтується на теорії множин та математичній логіці. Популярність цієї моделі пов’язана передусім з простотою її реалізації, що дозволяє індексувати і виконувати пошук у великих документальних масивах. У рамках булевої моделі документи і запити подаються у вигляді безлічі термів – ключових слів і стійких словосполучень. Кожен терм поданий як булева змінна: 0 (терм із запиту не присутній в документі) або 1 (терм із запиту присутній у документі). Запит користувача є логічним виразом, в якому терми зв’язуються логічними операторами кон’юнкції, диз’юнкції і заперечення.

Ідея розширеного булевого пошуку полягає у створенні можливостей для визначення ступеня відповідності документів пошуковому запитові. Це досягається присвоєнням ваги пошуковим термінам. Вага термінів враховується при побудові списку відповідності документів до інформаційного запиту.

При інформаційному пошуку з використанням нейронних мереж, вузли нейронної мережі "активуються" пошуковим запитом. Кожний зв’язок нейронної мережі передається документу і використовується для обчислення коефіцієнта відповідності документа до пошукового запиту. Для цього зв’язкам присвоюється вага згідно з наперед визначеною відповідністю чи невідповідністю документів.

При пошуку з використанням нечітких множин документ перетворюється в нечітку множину. Далі для кожного документа додається інформація, отримана з операцій об’єднання, перетину, комплементарності нечітких множин, яка говорить про ступінь відповідності кожного документа до пошукового запиту.

Розглянуті методи мають ряд недоліків. Так метод, заснований на булевій моделі, має невисоку ефективність пошуку, жорсткий набір опе-

раторів, неможливість ранжування. Метод, базований на просторово-векторній моделі, малопридатний для обробки великих масивів даних. Метод, що базується на імовірнісній моделі, характеризується низькою обчислювальною масштабованістю, необхідністю постійного навчання системи.

Загальним недоліком традиційних методів інформаційного пошуку є те, що в результаті пошуку формується величезний список Web-сторінок, які можуть зовсім не відповідати пошуковому запиту.

Існує чимало сучасних засобів інформаційного пошуку [387]. Це спеціальні програми, які займаються пошуком сторінок у мережі, витягають гіпертекстові посилання на цих сторінках і автоматично індексують інформацію, яку вони знаходять для побудови бази даних.

Кожен пошуковий механізм має власний набір правил для збору документів. Деякі йдуть за кожним посиланням на кожній знайденій сторінці і потім, у свою чергу, досліджують кожне з посилань на кожній з нових сторінок, і так далі. Деякі ігнорують посилання, які ведуть до графічних і звукових файлів.

Загальний пошук інформації в мережі Інтернет здійснюють програми, відомі як "павуки". "Павуки" повідомляють про зміст знайденого документа, індексують його і добувають підсумкову інформацію. Також вони переглядають заголовки Web-сторінок, деякі посилання і посилають проіндексовану інформацію базі даних пошукового механізму.

Краулери переглядають заголовки Web-сторінок і повертають тільки перше посилання.

Роботи можуть бути запрограмовані так, щоб переходити з різних посилань різної глибини вкладеності, виконувати індексацію і навіть перевіряти посилання в документі. Через їх природу вони можуть зациклюватися, тому, проходячи по посиланнях, їм потрібні значні часові ресурси. Проте, є методи, призначені для того, щоб заборонити роботам пошук сайтами, власники яких не бажають, щоб вони були проіндексовані.

Агенти – найбільш "інтелектуальні" з пошукових засобів. Вони можуть робити більше, ніж просто шукати: вони можуть виконувати навіть транзакції від імені користувача. Вже зараз вони можуть шукати сайти специфічної тематики та повертати списки сайтів, відсортованих за їх відвідуваністю. Агенти можуть обробляти зміст документів, знаходити й індексувати не лише Web-сторінки, а також інші види ресурсів. Вони можуть також бути запрограмовані для вилучення інформації з уже

існуючих баз даних. Незалежно від інформації, яку агенти індексують, вони передають її назад до бази даних пошукового механізму.

Агенти витягують і індексують різні види інформації. Деякі, наприклад, індексують кожне окреме слово у знайденому документі, в той час як інші індексують лише 100 найбільш важливих слів у кожному, розмір документа, кількість слів у ньому. Вид побудованого індексу визначає, який пошук може бути зроблений пошуковим механізмом і як отримана інформація буде інтерпретована. Агенти можуть також переміщатися по Інтернету та знаходити інформацію, після чого поміщати її в базу даних пошукового механізму.

Проблема інформаційного пошуку в мережі Інтернет сьогодні отримала нове звучання: "пошук інформації в необмеженому неоднорідному динамічному інформаційному середовищі". Таким чином, пошук інформації в мережі Інтернет стає усе більш складним і трудомістким. Це пов’язано з ускладненням структури інформаційних ресурсів Інтернет та постійним збільшенням обсягу наявної інформації.

Традиційні пошукові системи пропонують лише часткове вирішення цієї проблеми. Періоди індексації у них становлять від тижнів до декількох місяців. Традиційними підходам до організації інформаційного пошуку притаманні такі недоліки, як низька оперативність, залежність від набору джерел і обмеженість спектру цих джерел, середні пошукові можливості, відсутність засобів повідомлення про появу нових даних.

Саме недостатня ефективність сучасних методів та відповідних засобів інформаційного пошуку є на сьогоднішній день головною проблемою на шляху перетворення Інтернет в інтелектуальну мережу. В рамках вирішення даної проблеми пропонуються різні методи і підходи, розробляються прототипи "інтелектуальних" пошукових систем.

Одним із головних напрямів удосконалення ефективності інформаційного пошуку вважається впровадження семантичної "павутини" [418]. Результати досліджень за цією темою щорічно оприлюднюються на спеціалізованих конференціях, які стосуються проблем інформаційного пошуку в мережі Інтернет [393; 435; 437].

Поняття семантична "павутина" виникло з моделі семантичної мережі, де інформаційна модель предметної області має вигляд орієнтованого графа, вершини якого відповідають об’єктам предметної області, а дуги задають відношення між ними. Об’єктами можуть бути поняття, події, властивості, процеси. Таким чином, семантична мережа є одним

із способів подання знань та відображає семантику предметної області у вигляді понять і відносин.

Проект створення семантичної мережі на основі всесвітньої "павутини" – WWW отримав назву семантичної "павутини".

Семантична "павутина" – це надбудова над WWW, яка покликана зробити інформацію, що розміщена в мережі, більш "зрозумілою" для комп'ютерів [418].

З точки зору машинної обробки даних – семантична "павутина" – це ідея зберігання даних в Інтернет таким чином, щоб вони були визначені й пов'язані для подальшої автоматизованої обробки.

З точки зору обслуговування людських потреб – ідея семантичної "павутини" полягає в звільненні людини від обтяжливих рутинних завдань з видобутку, пошуку, обліку та індексації інформації, що міститься в WWW. Семантична "павутина" – це наступне покоління Інтернет, яке дозволить Web-додаткам автоматично збирати Web-документи з різних джерел, враховувати і обробляти інформацію, а також взаємодіяти з іншими додатками для виконання складних завдань.

При автоматичній обробці інформації в рамках семантичної "павутини" сервіси, що взаємодіють один з одним, на основі аналізу смислових зв'язків між об'єктами і поняттями, що зберігаються в Інтернет, повинні відбирати лише ту інформацію, яка буде реально корисна користувачам.

Чітко сформульований семантичний базис предметної області дозволяє організувати більш "осмислений" аналіз інформації в електронних документах. Це виражається в тому, що, по-перше, будь-які природно-мовні конструкції, за допомогою яких може виражатися та чи інша інформація, містить в явному або неявному вигляді предмет обговорення, семантичну ідентифікацію, яку можна реалізувати завдяки наявності онтології предметної області, крім того, можуть бути визначені потенційні взаємозв'язки між об'єктами та ідентифіковані в тексті. По-друге, інформація в електронних документах, особливо та, яка публікуються в Інтернет, часто або структурована, або містить структуровані острівці інформації, у вигляді списків, таблиць. Ідентифікація опису інформації, у вигляді назв атрибутів, складових заголовки структурованої інформації, також може бути здійснена за допомогою онтології. Не маючи онтології, області структурованої інформації, можуть бути неправильно розділені програмним обробником на значення і опису цих

значень, тобто будуть неправильно побудовані ланцюжки "атрибут-значення", що описують список або таблицю. Тому доцільним є використання онтології предметної області для організації ідентифікації семантичних об’єктів і їх взаємозв’язків у поданні інформації в електронних документах.

Використання семантичних зв’язків – це ефективний спосіб подання даних в Інтернет. Таку структуру також можна символічно ототожнити з базою даних, яка пов’язана в глобальному масштабі зі змістом документів в Інтернет. Причому цей зв’язок здійснюється способом, зрозумілим комп’ютеру.

Завдання семантичної "павутини" полягають у такому:

індексація і пошук інформації;

розроблення та підтримка метаданих;

розроблення та підтримка методів анотування;

подання WWW у вигляді великої бази даних;

організація машинного збору даних;

виявлення та надання Web-орієнтованих сервісів;

дослідження в галузі інтелектуальних програмних агентів.

Технологія семантичної "павутини" на даний час успішно вирішує таки завдання:

забезпечення незалежності даних від програм;

семантична інтеграція даних;

створення основи для широкого використання комп’ютерних пошукових агентів.

Основні ідеї семантичної "павутини":

зробити Web-ресурси більш доступними для автоматичних процесів;

розширити існуючу розмітку, призначену для візуалізації, семантичною розміткою – анотаціями за допомогою метаданих, що описують зміст доступних ресурсів;

використання онтологій, що надають "словник" для анотацій.

Семантична "павутина" передбачає використання унікальної глобальної ідентифікації ресурсу, метаданих для декларування фактів про ресурси, а також спільної мови для вираження метаданих і знань, які реалізований за допомогою онтологій для загальнодоступного розуміння, загального словника метаданих і правил для додавання нових метаданих та знань. На рис. 10.1 наведено основні елементи семантичної "павутини" [6].

Рис. 10.1. **Модель семантичної "павутини"**

Слід розглянути цю модель більш детально.

Базисом семантичної "павутини" є URI (Uniform Resource Identifier) – універсальний ідентифікатор ресурсів, що використовується у WWW для ідентифікації елементів. URI можна присвоїти будь-чому. Це може бути людина, книга, абстрактна концепція, тобто все, що має назву.

У семантичній "павутині" широко використовується мова XML для подання синтаксису для інших мов розмітки та семантичної розмітки Web-сторінок. Вона дозволяє кожному створювати свій власний формат документів і потім розробляти документи в цьому форматі. Ці формати документів можуть включати розмітку, яка уточнює зміст контенту документа. Документ з розміткою може "читатися" комп’ютером.

Основний акцент концепції семантичної "павутини" робиться на використання метаданих.

Метадані – це структуровані дані, що є характеристиками описуваних сутностей з метою їх ідентифікації, пошуку, оцінки, та керуванням ними.

Базовими стандартами для опису метаданих у семантичній "павутині" в даний момент визнаються Dublin Core, FOAF, SIOC і DOAP [420; 421; 431; 436].

FOAF (Friend-Of-A-Friend) – це формат машинно-оброблюваних сторінок, що описують персональну інформацію про людей і їх діяльності (фотографії, календарі, блоги та інше) у форматі XML.

SIOC (Semantically-Interlinked Online Communities) – документи, що описують онлайн-спільноти. SIOC забезпечує взаємозв’язок таких засобів обговорення інформації, як блоги, форуми і поштові розсилки між собою.

Description of a Project Description of a Project (DOAP) – документи, що описують в Інтернет проекти з відкритим вихідним кодом.

Dublin Core – це набір елементів (властивостей) для опису документів, який сприяє впровадженню опису і автоматичної індексації документоподібних мережевих об’єктів за принципом, подібним карткам бібліотечного каталогу.

Набір метаданих Dublin Core призначається для використання засобами дослідження ресурсів Інтернет, такими, як Web-краулери пошукових систем. Також передбачається, що Dublin Core буде досить простим набором для розуміння і використання широким колом авторів Web-контенту. Елементи стандарту Dublin Core широко використовуються в документуванні Інтернет-ресурсів.

Метадані можуть бути вбудованими в сам Web-ресурс, наприклад, в HTML-сторінки або документи. Також вони можуть зберігатися і оновлюватися незалежно від ресурсів. Багато виробників програмного забезпечення вже випускають ряд продуктів, які автоматично формують деякий невеликий блок описів всередині документа.

У випадку розміщення метаданих окремо від ресурсу, самі метадані переважно зберігаються і передаються у форматі XML.

Для опису предметної області ресурсів використовується стандарт RDF (Resource Description Framework) [428], прийнятий у 1999 році консорціумом W3C і підтриманий багатьма провідними виробниками програмного забезпечення та постачальниками контенту. RDF є моделлю опису та одночасно – мовою опису метаданих. Ця мова використовує XML-синтаксис.

Стандарт RDF містіть дві основні частини: спосіб опису ресурсів, а також спосіб завдання схем, якій має відповідати опис.

Перша частина стандарту RDF визначає просту модель для опису об’єкта, що розглядається в якості ресурсу. Друга частина – RDF-схема, призначена для завдання структури понять предметної області.

Базовий будівельний блок у RDF – це твердження про ресурси у вигляді, придатному для машинної обробки. Ресурсом в RDF може бути будь-яка сутність – як інформаційна (наприклад, Web-сайт або зображення), так і неінформаційна (наприклад, людина, місто або якесь абстрактне поняття).

Твердження є трійкою "об’єкт – атрибут – значення", який часто записують у вигляді A(O, V) тобто об’єкт O має атрибут A зі значенням V.

Таким чином, RDF надає можливість формулювати твердження у вигляді, придатному для обробки комп'ютером, що є основою семантичної "павутини".

RDF-схема – це робочий проект RDF Vocabulary Description Language 1.0, що був запропонований 23 січня 2003 року. Дана специфікація описує те, як використовувати RDF для опису RDF-словників. Вона визначає базовий словник, призначений для цих цілей і прийняті угоди, які можуть бути використані при створенні додатків семантичної "павутини" для підтримки більш складних словників RDF-описів. Мова опису словника RDF визначає класи і властивості, які можуть бути використані для опису інших класів і властивостей, а також робити деякі більш складні речі, такі, як створення діапазонів і областей для властивостей.

RDF і RDF-схема використовують три найбільш важливих поняття: "Ресурс" (rdfs: Resource), "Клас" (rdfs: Class) і "Властивість" (rdfs: Property). Ці поняття є "класами" в тому розумінні, що до них можуть належати терміни. Всі словники RDF використовують деяку базову структуру: вони описують класи ресурсів і типи зв'язків між ресурсами. Ця спільність дозволяє використовувати різнорідні словники, створені для машинної обробки, і відповідає вимогам щодо створення метаданих, в яких твердження можуть бути отримані з безлічі різнорідних децентралізованих словників, створених різними спільнотами за різними принципами і різними методами.

Опис за допомогою RDF не обмежується тільки описом документів Інтернет. Цей стандарт досить універсальний і гнучкий для того, щоб описувати більшість типів структурованих даних. Наприклад, у RDF природно виражаються діаграми сутність-зв'язок, які широко застосовувана для проектування баз даних. Опис семантики ресурсу на RDF може бути як "зовнішнім", коли описується ресурс в цілому, так і "внутрішнім", коли описується внутрішня структура ресурсу – або це база даних, XML-документ, або цілий Web-сайт.

Важливою особливістю стандарту RDF є розширюваність. На RDF можна задати структуру опису джерела, використовуючи і розширюючи вбудовані поняття RDF-схем, такі, як класи, властивості, типи, колекції.

Крім опису структури, RDF дозволяє оперувати твердженнями. Вираз "ресурс R1 як властивість P має ресурс R2" можна проінтерпретувати і як предикат P (R1, R2), а потім використовувати це твердження як об'єкт інших тверджень. Така інтерпретація дозволяє описувати за

допомогою RDF концептуальну інформацію. Таким чином, RDF цілком підходить на роль універсальної мови опису семантики ресурсів і взаємозв'язків між ними.

Онтології визначаються як спільно використовувані формальні концепції конкретних предметних областей, вони дають загальне уявлення про поняття, якими можуть обмінюватися люди та програми [304].

Онтології – це подання знань про певну предметну область деякою мовою. Онтологію неодмінно супроводжує деяка концепція цієї області інтересів. Найчастіше ця концепція виражається за допомогою визначення базових об'єктів і відношень між ними. Визначення цих об'єктів і відношень між ними зазвичай називають концептуалізацією. Онтологія загальноприйнята і загальнодоступна концептуалізація певної області знань, яка містить базис для моделювання цієї області знань і визначає протоколи для взаємодії між агентами, які використовують знання з цієї області, і включає домовленості про представлення теоретичних основ даної області знань

Розмітка документів семантичній "павутині" за допомогою онтологічних термінів дозволить виконувати автоматичну обробку їх контенту. Таким чином, онтології є ключовою технологією для розвитку семантичної "павутини".

Інформаційний пошук у семантичній "павутині" дає можливість робити висновки на основі семантично розмічених даних. Це дозволяє без особливих проблем зібрати воєдино інформацію про людину, організації, фірму з усіх доступних джерел, використовуючи унікальні ідентифікатори, такі, як ім'я, адреса електронної пошти. Така агрегація сама може повідомити цікаві факти, не подані безпосередньо ні в одній з баз даних. Можливість логічних висновків на основі розміченій інформації, пропонована інструментарієм семантичної "павутини", допомога автоматизувати цей процес, забезпечуючи швидкий і ефективний збір інформації про конкретний суб'єкт.

Слід розглянути існуючі пошукові машини семантичної "павутини".

Пошукова система Swoogle [434] призначена для індексування та подальшого пошуку в мережі Інтернет різних документів, створених із застосуванням семантичних форматів (рис. 10.2). Підтримуються документи як цілком створені за допомогою RDF / XML, N-Triples, N3 (RDF), так і ті, які містять окремі фрагменти RDF / XML-коду. Дані збираються за допомогою індексування відкритих джерел мережі. В даний час індекс

цього пошукового програмного агенту об'єднує близько трьох мільйонів документів у семантичних форматах, а також трохи більше мільйона документів, що містять окремі елементи семантичного коду. Загалом, Swoogle охоплює більше мільярда ресурсів з урахуванням документів, які семантично не розмічені.

Доступні кілька режимів пошуку, які виділені окремими посиланнями, розташованими поруч з полем введення запиту. Перший режим – пошук по онтологіям. У цьому випадку повертаються тільки документи, що розмічені за всіма правилами семантичних технологій та містять визначення класів і властивостей об'єктів.

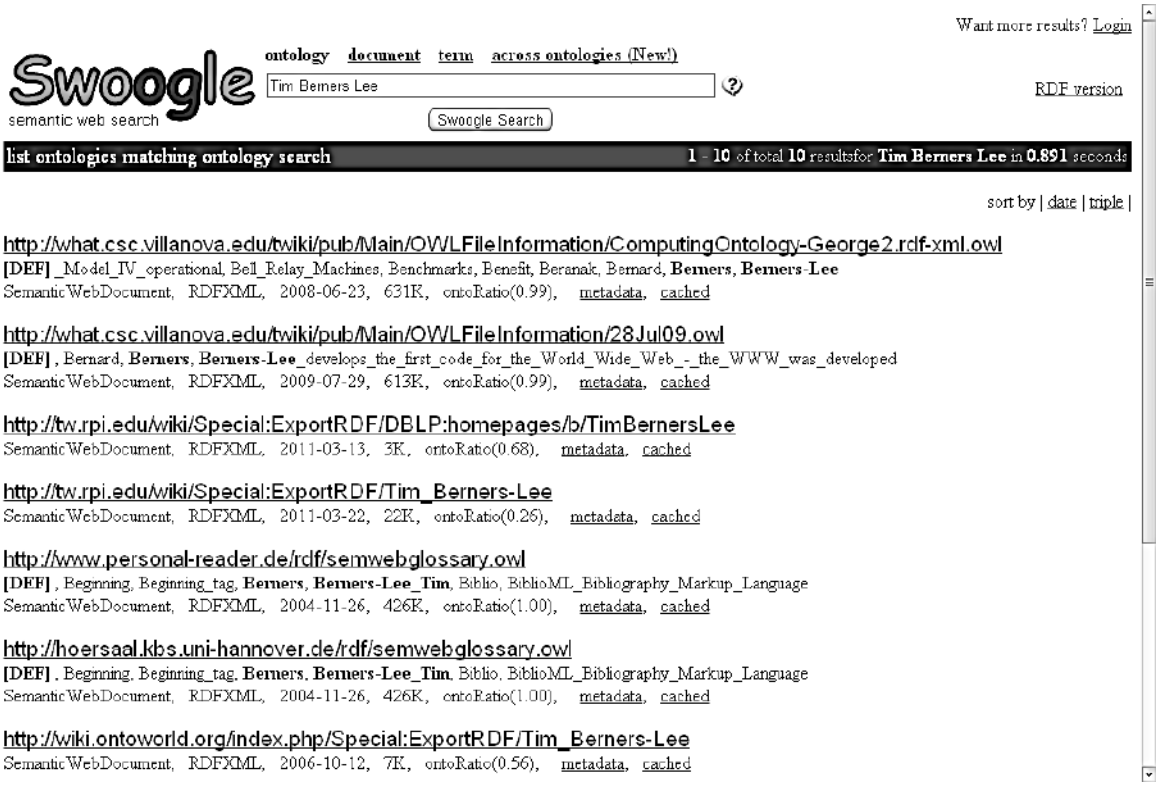


Рис. 10.2. **Графічний інтерфейс пошукової системи Swoogle**

Крім того, можна шукати будь-які документи з семантичною розміткою або вести пошук окремих термінів, що зустрічаються в проіндексованих Swoogle документах. У системі реалізована власна, досить детальна мова запитів.

Інтерфейс сторінки Swoogle простий: лише посилання і мінімум довідкової інформації. Swoogle здатний видавати результати пошуку в форматі RDF, що дозволяє звертатися до нього за допомогою власних програм.

Пошукова система Twine [422] дозволяє зберігати посилання на цікаві проекти і ділитися ними з іншими користувачами (рис. 10.3).

Співпраця користувачів тут будується навколо тематичних "твайнів", які містять усі повідомлення і посилання по темі і в наповненні яких можуть брати участь кілька користувачів. Крім закладок і текстових фрагментів Web-сторінок в обліковому записі Twine допустимо зберігати зображення та відеоролики, а крім того, складати невеликі власні нотатки. Підтримується завантаження аналогічних файлів з локального комп'ютера.

Всередині Twine широко використовуються технології RDF та OWL. Накопичений масив даних у семантичних форматах дозволив реалізувати ряд цікавих інструментів.

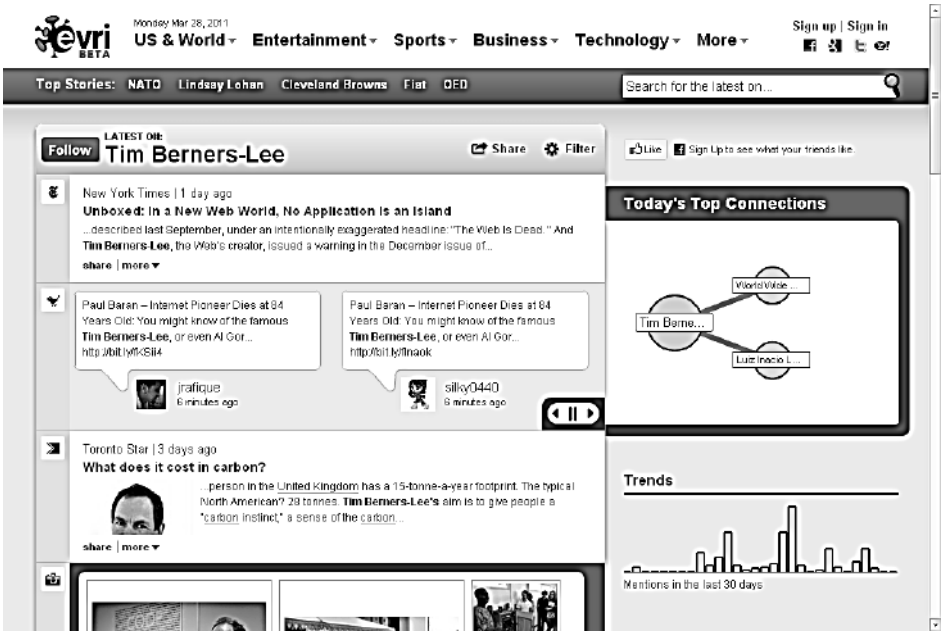


Рис. 10.3. **Графічний інтерфейс пошукової системи Twine**

Перший з них – автоматичний пошук та збереження в тексті Web-сторінки ключових слів. Працює він поки що лише для англійської мови. З досвіду застосування Twine можна додати, що цей механізм, поступово вдосконалюється, зараз функціонує досить гідно, незважаючи на деякий відсоток помилок.

Найбільш помітною реалізацією семантичних технологій в Twine є система пошуку. Якщо подивитися на бічну панель інтерфейсу програми, то можна побачити не тільки звичні списки тегів, але й тематичні фільтри.

Семантичні інструменти використовуються і в роботі системи рекомендацій, звичної для багатьох інших соціальних сервісів. Вона повідомляє користувачеві про потенційно цікавих "твайнах", повідомленнях, а також про інших користувачів зі схожими інтересами.

У теперішній час найбільш цікавими й зручними в роботі є гібридні програми, що поєднують можливості звичних сервісів і технології семантичної "павутини". Одним з гарних прикладів такого злиття є проект Sig.ma [430]. Даний ресурс призначений для пошуку документів у семантичних форматах та має зручний інтерактивний інтерфейс користувача (рис. 10.4).

Пошук починається звичним способом – зазначенням ключових слів у полі пошуку. Далі система проводить його за власною індексною базою документів з семантичної розміткою.

Рис. 10.4. **Графічний інтерфейс пошукової системи Sig.ma**

Після відпрацювання запиту робочий простір ділиться на дві панелі: у лівій панелі з’являється зведена інформація про предмет пошуку, в правій – загальний список тих джерел, звідки вона наповнюється.

Для сортування списку пропонуються фільтри, за допомогою яких можна виключати з нього не відповідні запиту документи. При цьому зведення на сусідній панелі автоматично перебудовується.

Панель відомостей ділиться на тематичні розділи, в яких виводяться відповідні текстові фрагменти або зображення. Склад розділів залежить від об’єкта пошуку. Наприклад, при пошуку інформації про людину система спробує знайти його фото, біографічні відомості та список публікацій, якщо у даної персони такі є. Більш того, подано відомості про пов’язаних з нею людей, наприклад про колег або членів

родини. Окремо пропонуються посилання на сайти пов'язаних з об'єктом пошуку установ, інформація про участь у деяких соціальних мережах, а також список людей з тим же прізвищем. Слід зауважити, що в даний час настільки докладну інформацію можна отримати лише про досить відомих людей. Аналогічним чином обробляється і демонструється інформація про організації та об'єкти тематичного пошуку за ключовими словами.

Крім проведення безпосереднього пошуку на сайті проекту, Sig.ma може бути використаний для створення віджетів, які можна запровадити на своєму сайті або у своєму блозі. Відповідно до вимог Web 3.0 пропонується і програмний інтерфейс, що дозволяє звертатися до системи зовнішнім програмам-агентам. Інформація видається у форматах RDF і JSON.

Пошукова система Sig.ma використовує бази даних семантичної пошукової системи Sindice (рис. 10.5).

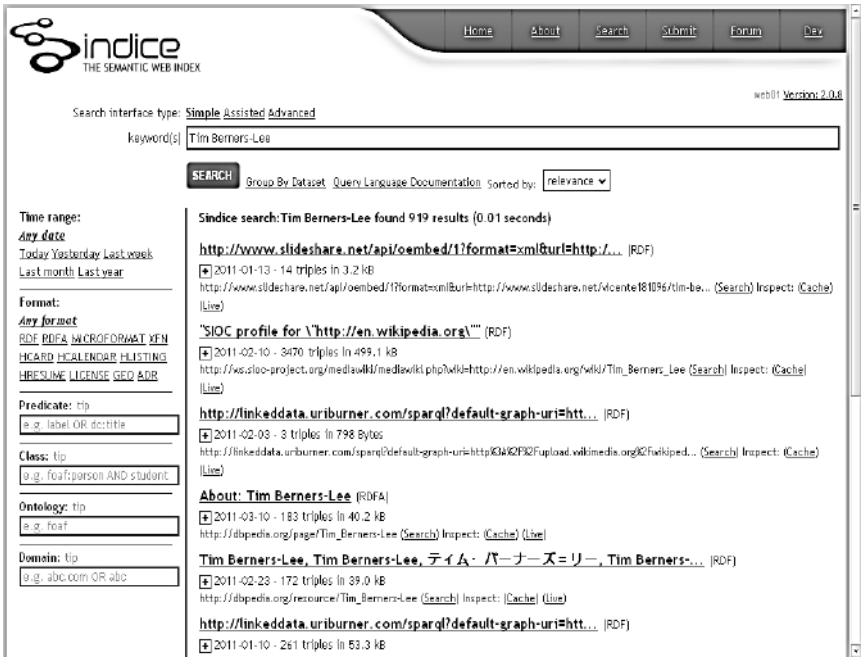


Рис. 10.5. **Web-інтерфейс пошукової системи Sindice**

Sindice – пошукова система та система індексації для документів семантичної "павутини" [438]. У першу чергу Sindice є не додатком для кінцевих користувачів, а сервісом, що призначений для використання будь-яким клієнтським додатком семантичної "павутини" для пошуку релевантних джерел даних.

Sindice надає три послуги клієнтським додаткам:

синтаксичний аналіз файлів та кінцевих точок SPARQL;

пошук ресурсів та повернення URL-адрес RDF-документів, де ці ресурси розташовані;

повнотекстовий пошук опису та видачу URL-адрес джерел, в яких ці ресурси знайдені.

Для відповідності даним вимогам, абстрактний Sindice API, надає таку функціональність:

синтаксичний аналіз та індексація по URL – аналізує та індексує документи або кінцеві точки SPARQL за даним URL;

пошук ресурсу, що проводиться по заданому URI;

пошук ресурсу, який унікально ідентифікується парою "властивість-значення";

пошуку по тексту – перегляд бази даних по текстовому запиту.

Крім того, Sindice забезпечує виконання не функціональних вимог:

зведено до мінімуму розмір індексу, з тим щоб дозволити індексування семантичного веб-сайту в цілому;

зведено до мінімуму час пошуку, з тим щоб дозволити програмам використовувати Sindice за замовчуванням для пошуку додаткової інформації про ресурси.

Архітектура Sindice складається з кількох незалежних компонентів, які працюють у кількох потоках для сканування, індексації і обробки запитів:

зовнішній інтерфейс є головною точкою входу та поділяється на користувальницький інтерфейс, призначений для роботи кінцевих користувачів, та HTTP API для програмних агентів;

модулі сканування та індексації RDF-документів;

"сторож" оцінює кожен елемент в черзі, і вирішує з яким пріоритетом індексувати його залежно від останньої дати модифікації, його змісту та ін.;

Sindice має низку інструментів для Web-розробника:

інструменти для аналізу семантичної розмітки сторінки;

інструменти для побудови онтологій;

інструменти для побудови графової моделі сайта тощо.

Ще однією семантичною пошуковою машиною є система AskNet [395]. Web-інтерфейс пошукової системи AskNet наведений на рис. 10.6. Під час отримання запиту AskNet визначає найбільш ймовірний об’єкт пошуку, враховуючи синоніми, обробляючи абревіатури і словесні записи

цифр (наприклад дати). Вільно сформульоване питальне речення буде коректно розібрано системою тільки в тому випадку, якщо в ньому міститься не більше двох присудків або трьох інших однорідних членів. Питання також повинно бути граматично правильним і синтаксично узгодженим. AskNet може обробити і речення з помилками, але чекати в такому разі гідного результату не варто. Можна зауважити, що ця система не перевіряє орфографію в запиті і не має спроможність формулювати відповіді на основі логічної комбінації даних. Відповідь буде видано тільки, якщо відповідна інформація в якійсь формі прописана в базі проіндексованих текстів.

Семантичні технології в AskNet також працюють на етапі формування відповіді: зв'язки між словами в пошуковій фразі враховуються при сортуванні результатів. Відповіді представлені традиційним списком посилань, супроводжуваних короткими витягами з тексту знайденої Web-сторінки, на якій червоним кольором виділяються ключові поняття запиту, а зеленим – слова, сформульовані системою на основі семантичної обробки. Оригінальний документ можна переглянути, не покидаючи сервісу, – досить клацнути на посилання "Перегляд", розташовано біля кожної позиції. Воно відкриває на сторінці результатів фрейм, в який і завантажується джерело.

Рис. 10.6. **Web-інтерфейс пошукової системи AskNet**

10.2. Методика дослідження ефективності інформаційного пошуку в мережі Інтернет

Розглянуто критерії релевантності, вибрані показники ефективності інформаційного пошуку, наведено методику дослідження ефективності інформаційного пошуку в мережі Інтернет.

Для задоволення інформаційної потреби користувачів важливим є застосування методів інформаційного пошуку та відповідних інформаційно-пошукових систем, які забезпечують високий ступінь відповідності результатів інформаційного пошуку запиту користувача.

При цьому виникає завдання оцінювання ступеню відповідності результатів пошуку очікуванням користувача, який звернувся з пошуковим запитом, тобто релевантності.

Для оцінки релевантності існує два типа критеріїв: внутрішні та зовнішні [392].

Найбільш значимим внутрішнім критерієм релевантності є ключові слова, а саме частота їх появи в тексті. Пошукові системи здатні враховувати цей параметр і при частому повторенні будь-якого словосполучення вважати його за ключову фразу. Велике значення має місце розташування ключових слів. Перш за все це їх наявність у різних заголовках. Якщо запит користувача збігається з назвою документа, ймовірність того, що пошукова система оцінить цю сторінку, стане вище. В якості додаткових факторів, що впливають на вагу ключових слів, також виступають:

близькість до початку сторінки. Чим ближче до початку сторінки знаходиться ключове слово, тим воно більш значуще;

наявність ключових слів у деяких місцях сторінки;

близькість ключових слів один до одного. Має значення, коли в ролі пошукового запиту виступає будь-яка фраза, особливо стійке словосполучення;

наявність синонімів ключових слів. Пошукові системи часто "звертають увагу" на присутність у текстах інших форм ключових слів, які свідчать про те, що в документах дійсно є інформація з даної тематики.

В основі зовнішніх критеріїв релевантності знаходиться принцип посилальної популярності. Даний фактор є тим, що релевантність сайта може визначатися його популярністю в мережі Інтернет, тобто кількістю

інших ресурсів, що посилаються на розглянуту сторінку. Чим вище їх число, тим більше популярний сайт, а, викладена на ньому інформація є більш якісною.

Для оцінки релевантності існує чимало методів, які можна розділити на інтрасистемні і позасистемні. Основна відмінність між ними полягає в тому, що інтрасистемні методи передбачають оцінку функціонування пошукової системи в природному середовищі. При цьому оцінка проводиться на основі відомих даних. Позасистемні методи засновані на використанні доступних відомостей і передбачають створення експериментальної обстановки для оцінки ефективності функціонування пошукової системи. Одним з таких методів є метод експертних оцінок.

Методи експертних оцінок можна розділити на дві групи: методи колективної роботи експертної групи і методи отримання індивідуальної думки членів експертної групи.

Методи колективної роботи експертної групи передбачають отримання загальної думки в ході спільного обговорення розв’язуваної проблеми. Іноді ці методи називають методами прямого отримання колективної думки. Основна перевага цих методів полягає в можливості різнобічного аналізу проблем. Недоліками методів є складність формування групової думки з використанням індивідуальних суджень експертів, можливість тиску авторитетів у групі.

Методи колективної роботи включають методи "мозкової атаки", "сценаріїв", "ділових ігор", "нарад" і "суду".

Метод "мозкової атаки". Методи цього типу відомі також під назвою колективної генерації ідей, мозкового штурму, дискусійних методів. Усі ці методи засновані на вільному висуненні ідей, спрямованих на вирішення проблеми. Потім з цих ідей відбираються найбільш цінні.

Перевагою методу "мозкової атаки" є висока оперативність отримання необхідного рішення. Його основним недоліком є складність організації експертизи, так як іноді неможливо зібрати разом необхідних фахівців, створити невимушену атмосферу і виключити вплив посадових взаємовідносин.

Метод "сценаріїв" є сукупністю правил по викладу в письмовому вигляді пропозицій фахівців з розв’язуваної проблеми. Сценарій − це документ, що містить аналіз проблеми та пропозиції щодо її реалізації. Пропозиції спочатку пишуть експерти індивідуально, а потім вони узгоджуються і викладаються у формі єдиного документа. Основною

перевагою сценарію є комплексне охоплення розв'язуваної проблеми в доступній для сприйняття формі. До недоліків можна віднести можливу неоднозначність, нечіткість викладення питань і недостатню обґрунтованість окремих рішення.

"Ділові ігри" засновані на моделюванні функціонування соціальної системи управління при виконанні операцій, спрямованих на досягнення поставленої мети. На відміну від попередніх методів, де експертні оцінки формуються в ході колективного обговорення, ділові ігри припускають активну діяльність експертної групи, за кожним членом якої закріплений певний обов'язок відповідно до заздалегідь складених правил і програми. Основною перевагою ділових ігор є можливість вироблення рішення в динаміці з урахуванням всіх етапів досліджуваного процесу при взаємодії всіх елементів суспільної системи управління. Недолік полягає в складності організації ділової гри в умовах, наближених до реальної проблемної ситуації.

Метод "нарад" ("комісій", "круглого столу") – найпростіший і традиційний. Він передбачає проведення наради або дискусії з метою вироблення єдиної колективної думки з розв'язуваної проблеми. На відміну від методу "мозкової атаки" кожен експерт може не тільки висловлювати свою думку, а й критикувати пропозиції інших. В результаті такого ретельного обговорення зменшується можливість помилок при виробленні рішення.

Перевагою методу є простота його реалізації. Однак на нараді може бути прийнято помилкова думка одного з учасників в силу його авторитету, службового становища, наполегливості або ораторських здібностей.

Метод "суду" є різновидом методу "нарад" і реалізується за аналогією з веденням судового процесу. У ролі "підсудних" виступають обрані варіанти рішення; в ролі "суддів" – особи, які приймають рішення; в ролі "прокурорів" і "захисників" – члени експертної групи. Роль "свідків" виконують різні умови вибору і доводи експертів. При веденні такого "судового процесу" відхиляються або приймаються ті чи інші рішення. Метод "суду" доцільно використовувати при наявності декількох груп експертів, які дотримуються різних варіантів рішення.

Методи отримання індивідуальної думки членів експертної групи засновані на попередньому отриманні інформації від експертів, опитуваних незалежно один від одного, з подальшою обробкою отриманих

даних. До цих методів можна віднести методи анкетного опитування, інтерв'ю та методи "Дельфі". Основні переваги методів індивідуального експертного оцінювання полягають у їх оперативності, можливості повною мірою використовувати індивідуальні здібності експерта, відсутність тиску з боку авторитетів і в низьких витратах на експертизу. Головним їх недоліком є висока ступінь суб'єктивності одержуваних оцінок через обмеженість знань одного експерта.

Метод "Дельфі", або метод "дельфійського оракула", є ітеративною процедурою анкетного опитування. При цьому дотримується вимога відсутності особистих контактів між експертами та забезпечення їх повною інформацією за всіма результатами оцінок після кожного туру опитування з збереженням анонімності оцінок, аргументації і критики. Процедура методу містить декілька послідовних етапів опитування. На першому етапі проводиться індивідуальне опитування експертів, зазвичай у формі анкет. Експерти дають відповіді, не аргументуючи їх. Потім результати опитування обробляються і формується колективна думка групи експертів, виявляються і узагальнюються аргументації на користь різних суджень. На другому – вся інформація повідомляється експертам і їх просять переглянути оцінки і пояснити причини своєї незгоди з колективним судженням. Нові оцінки знову обробляються і здійснюється перехід до наступного етапу. Практика показує, що після трьох-чотирьох етапів відповіді експертів стабілізуються, і необхідно припинити процедуру.

Перевагою методу "Дельфі" є використання зворотного зв'язку в ході опитування, що значно підвищує об'єктивність експертних оцінок. Однак даний метод вимагає значного часу на реалізацію всієї багатоетапної процедури.

Слід розглянути докладно, як розраховується експертна оцінка методом "Дельфі".

У першу чергу нас будуть цікавити способи вимірювання, що дозволяють розташувати об'єкти порядковою або інтервальною шкалою, оскільки саме такий тип оцінок найчастіше використовується при проведенні експертизи. Це пояснюється тим, що оцінка за номінальною шкалою передбачає лише два варіанти відповідей – ТАК, НІ. За шкалою відносності вимірюються фактори, що мають кількісний характер. Значення цих факторів часто можна отримати розрахунковим шляхом без використання експертних оцінок.

Слід виділити способи вимірювання об’єктів, що найчастіше застосовуються при оцінці за порядковою або інтервальною шкалою: ранжування, парне порівняння, безпосередня оцінка.

Ранжування – це розташування об’єктів у порядку зростання або зменшення будь-якої притаманної їм властивості. Ранжування дозволяє вибрати з досліджуваної сукупності факторів найбільш істотний. Результатом проведення ранжування є ранжировка. Якщо є n об’єктів, то в результаті їх ранжування j-им експертом кожен об’єкт отримує оцінку X_{ij} – ранг, приписуваний і-му об’єкту j-им експертом. Значення X_{ij} знаходяться в інтервалі від 1 до n.

Ранг найважливішого фактора дорівнює одиниці, найменш значимого – числу n. Ранжуванням j-го експерта називається послідовністю рангів $X_{1j}, X_{2j}, \ldots, X_{nj}$.

Перевагою методу є його простота, а недоліком – обмежені можливості використання. При оцінці великої кількості об’єктів експертам дуже важко будувати ранжований ряд, оскільки доводиться враховувати безліч складних зв’язків.

Парне порівняння – це встановлення переваги об’єктів при порівнянні всіх можливих пар.

Тут не потрібно, як при ранжуванні, упорядковувати всі об’єкти, необхідно в кожній з пар виявити більш значимий об’єкт або встановити їх рівність.

Парне порівняння можна проводити при великому числі об’єктів, а також у тих випадках, коли відмінність між об’єктами настільки незначна, що практично нездійсненно ранжування експертних оцінок.

При використанні методу найчастіше складається матриця розміром n x n, де n – кількість порівнюваних об’єктів (табл. 10.1).

Таблиця 10.1

Загальний вид матриці парних порівнянь

Об’єкти	1	2	…	j	…	N	∑
1							
2							
…							
I							
…							
N							

При порівнянні об’єктів матриця заповнюється елементами a_{ij} таким чином (формула 10.1):

$$a_{ij} = \begin{cases} 2, \text{якщо } i > j \\ 1, \text{якщо } i = j \\ 0, \text{якщо } i < j \end{cases}. \quad (10.1)$$

Сума (по рядку) в даному випадку дозволяє оцінити відносну значимість об’єктів. Той об’єкт, для якого ця сума виявиться найбільшою, може бути визнаний найбільш важливим (значущим).

Підсумовування можна виконувати і за стовпцями, тоді найістотнішим буде фактор, який набрав найменшу кількість балів.

Часто буває бажаним не тільки впорядкувати (ранжувати об’єкти аналізу), а й визначити, на скільки один фактор більш значущий, ніж інші.

У цьому випадку діапазон зміни характеристик об’єкта розбивається на окремі інтервали, кожному з яких приписується певна оцінка (бал), наприклад, від 0 до 10.

Саме тому метод безпосередньої оцінки іноді називають також бальним методом.

Сенс методу полягає в тому, що експерт поміщає кожен з аналізованих об’єктів у певний інтервал (приписує бал).

Вимірником при цьому є ступінь володіння об’єкта тією чи іншою властивістю.

Кількість інтервалів, на які розбивається діапазон зміни властивості, може бути різним для різних експертів.

Крім того, метод дозволяє давати одну і ту ж оцінку (тобто поміщати в один і той же інтервал).

Для оцінювання ефективності інформаційного пошуку використовується ряд показників: повнота, точність, втрата інформації, інформаційний шум, F-міра тощо [393].

Найбільш важливими є такі показники ефективності інформаційного пошуку, як повнота, точність та F-міра.

Вони базуються на оцінюванні семантичної відповідності пошукового запиту та пошукового образу документа, тобто релевантності.

Для розрахунку цих показників потрібно скористатися матрицею класифікації (табл. 10.2).

Таблиця 10.2

Основні категорії відповідей інформаційно-пошукової системи

	Релевантні документи	Не релевантні документи
Знайдено системою	A	B
Не знайдено системою	C	D

Повнота – це відношення кількості знайдених релевантних документів, до загальної кількості релевантних документів у базі інформаційно-пошукової системи:

$$recall = \frac{A}{A + C}. \tag{10.2}$$

Повнота характеризує здатність системи знаходити документи, потрібні користувачеві, але не враховує кількість не релевантних документів, які йому видаються.

Точність визначається як відношення кількості знайдених релевантних документів до загальної кількості знайдених документів:

$$precision = \frac{A}{A + B}. \tag{10.3}$$

Вона характеризує здатність інформаційно-пошукової системи щодо пошуку релевантних документів.

Доброю мірою для спільної оцінки точності і повноти є F-міра, яка визначається як їх середнє гармонійне:

$$F = \frac{2}{\frac{1}{precision} + \frac{1}{recall}}. \tag{10.4}$$

Суть дослідження ефективності інформаційного пошуку полягає в порівнянні ефективності інформаційного пошуку в глобальній мережі Інтернет з використанням традиційного підходу та підходу, який ґрунтується на семантичному описі інформаційних ресурсів з використанням метаданих.

Як інструмент інформаційного пошуку в мережі Інтернет, що базується на традиційному підході, вибрана найбільш популярна пошукова система Google (частка ринку – біля 50 %, щомісячна кількість відвідувачів – близько 900 мільйонів). Вона також має потужні засоби для індексації та підтримки Web-сайтів.

В якості семантичної пошукової системи використано Sindice, тому що на даний момент це найбільш повна система, яка реалізує концепцію семантичної "павутини".

Для дослідження ефективності інформаційного пошуку в семантичній "павутині" пропонується методика, яка складається з декількох етапів:

створення пошукового "простору", що складається з декількох інформаційних ресурсів, кожний з яких має наперед визначену тематику;

додавання до інформаційних ресурсів звичайних мета-тегів та семантичного опису (метаданих);

розміщення розроблених інформаційних ресурсів у мережі Інтернет;

індексація інформаційних ресурсів з використанням традиційного підходу та підходу, який ґрунтується на семантичному описі цих ресурсів;

оцінювання ефективності інформаційного пошуку для підходів, що порівнюються;

аналіз результатів дослідження ефективності.

10.3. Дослідження ефективності інформаційного пошуку

Розглянуто практичне використання методики дослідження ефективності інформаційного пошуку в мережі Інтернет, розроблено програмний засіб для дослідження ефективності інформаційного пошуку, наведено результати порівняльного аналізу ефективності інформаційного пошуку з використанням традиційного підходу до інформаційного пошуку та підходу, який ґрунтується на семантичному описі інформаційних ресурсів з використанням метаданих.

Слід розглянути етапи дослідження, які були проведені відповідно до запропонованої методики.

Першим етапом є створення пошукового "простору". Він складається з таких інформаційних ресурсів:

Web-сайт з інформацією про семантичну "павутину" (рис. 10.7);

Web-сайт, присвячений стандарту RDF (рис. 10.8);

Web-сайт щодо інформаційного пошуку (рис. 10.9).

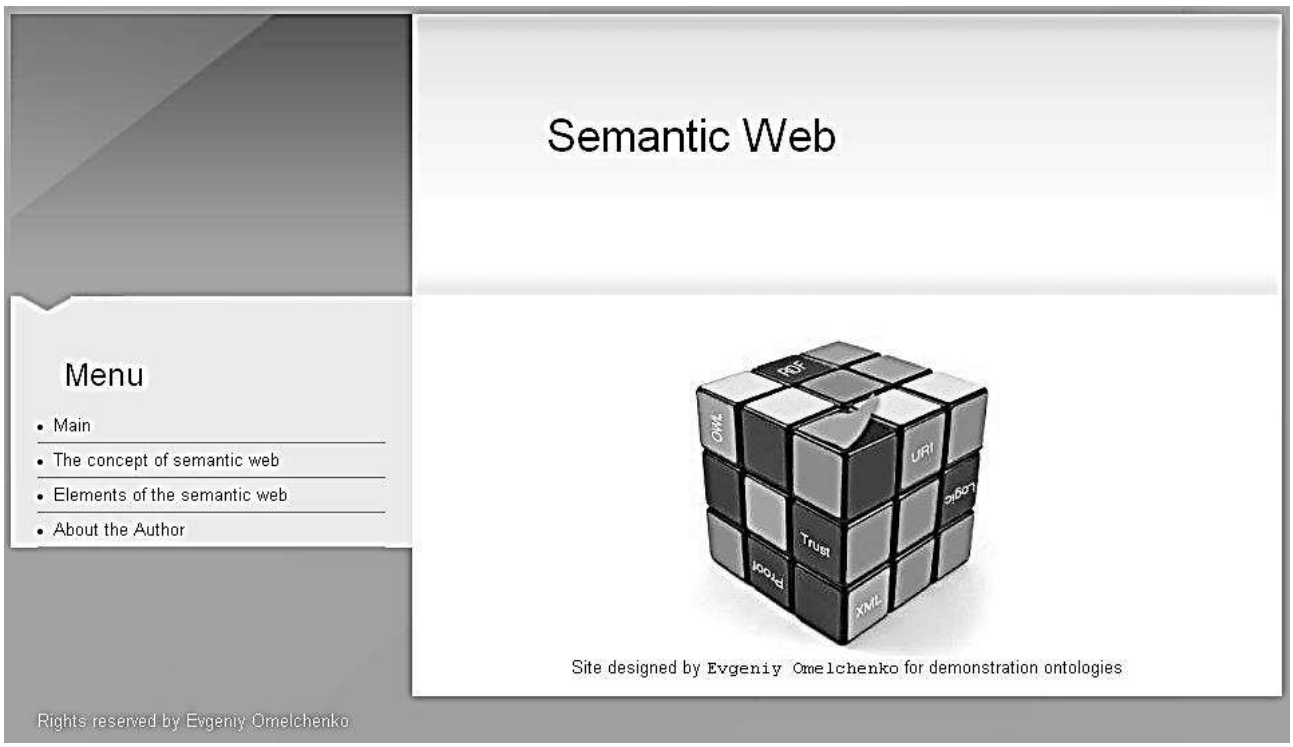


Рис. 10.7. **Головна сторінка Web-сайта про семантичну "павутину"**

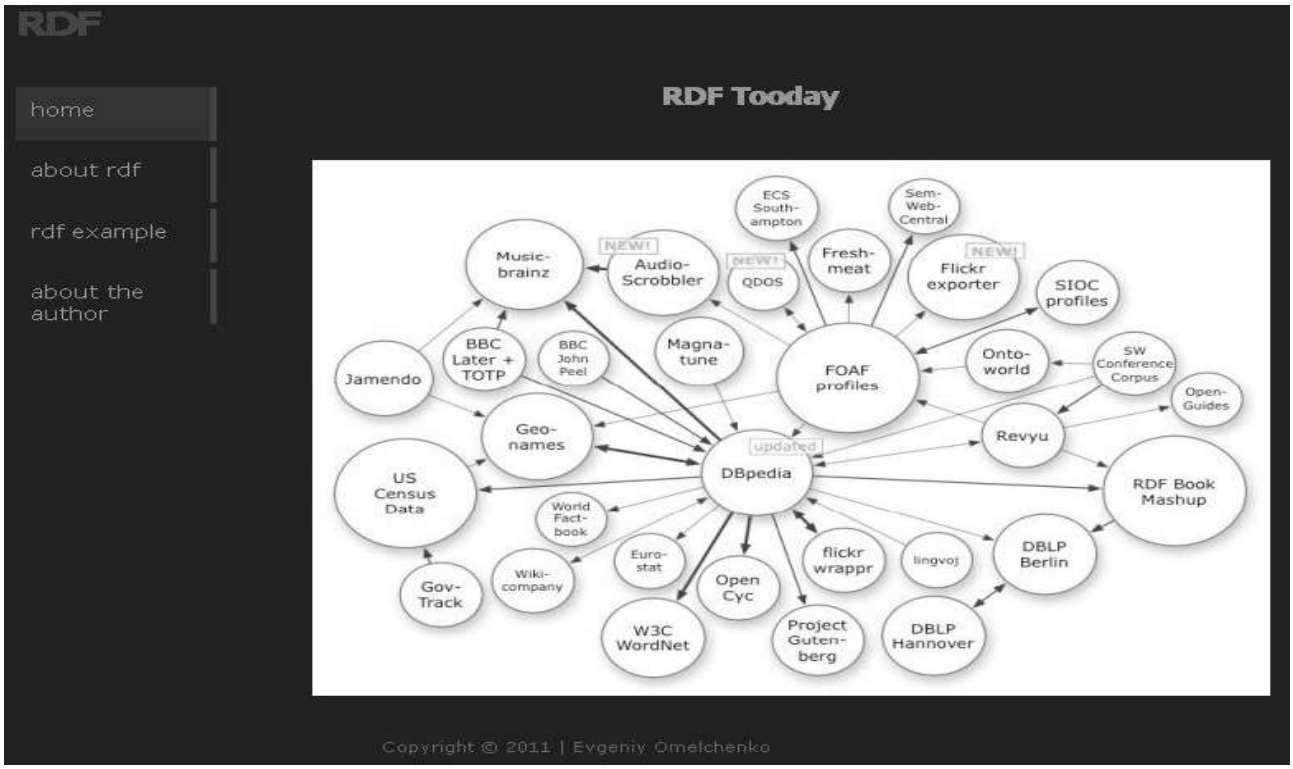


Рис. 10.8. **Головна сторінка Web-сайта про стандарт RDF**

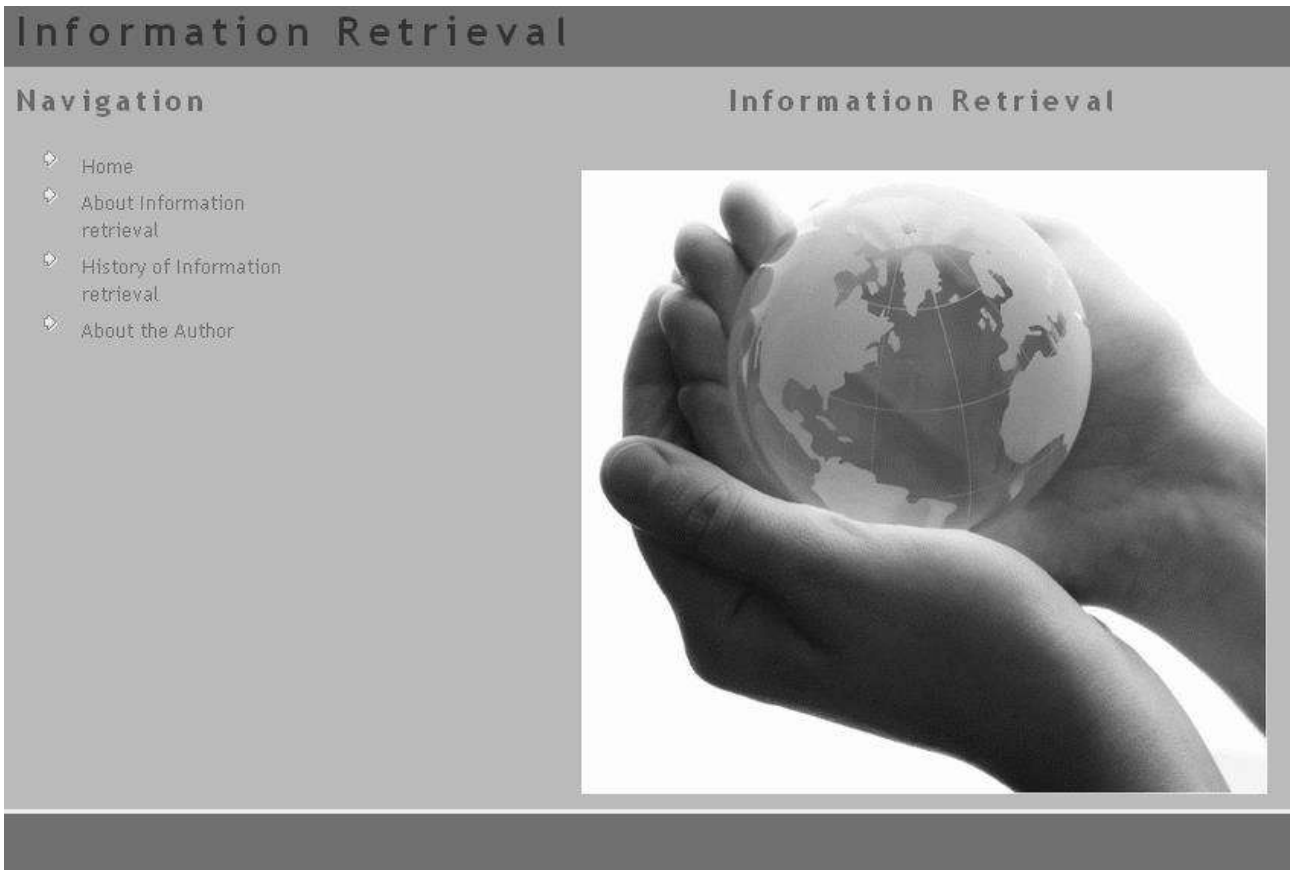


Рис. 10.9. **Головна сторінка Web-сайта про інформаційний пошук**

На наступному етапі для забезпечення можливості подальшої індексації Web-сайтів за допомогою пошукової системи Google необхідно додати до Web-сторінок їх короткий опис та ключові поняття ресурсу. Це виконується за допомогою тегу <meta>.

Одним з найбільш важливих елементів цього тегу є description (опис документа). Інформація, що міститься в ньому, впливає на результати пошуку пошуковими системами, оскільки вона є першим ключем пошуку, і саме вона відображається при виводі результатів пошуку.

Набір слів і фраз, що найбільш повно характеризують даний документ, вказується за допомогою елементу "keywords" (ключові слова). Вони є основним критерієм пошуку Web-сторінки традиційними пошуковими системами.

Для індексації Web-сайтів за допомогою пошукової системи Sindice необхідно додати до Web-сторінок семантичний опис. Він може бути виконаний відповідно до стандарту RDF.

Використовуючи декілька простих XHTML-атрибутів, можна виконати розмітку даних за допомогою індикаторів, які будуть інтерпретуватися браузерами та іншими програмами.

Результат опису Web-сторінки можна переглянути за допомогою інструменту SindiceInspectorTool.

Далі розроблені Web-сайти розміщуються в мережі Інтернет, наприклад на вузлах, що надають послуги безкоштовного хостингу.

Наступним етапом дослідження є індексація цих Web-сайтів.

Надання необхідних даних для індексації за допомогою пошукової системи Google виконується за допомогою програмного засобу "Google Инструменти для Web-мастеров" (рис. 10.10).

Перш за все необхідно додати сайт, індексацію якого необхідно виконати. Наступним кроком додається карта сайта. Для отримання карти сайта можна скористуватися безкоштовним сервісом SiteMap-Genarator (http://sitemapgenerator.ru/unregister/).

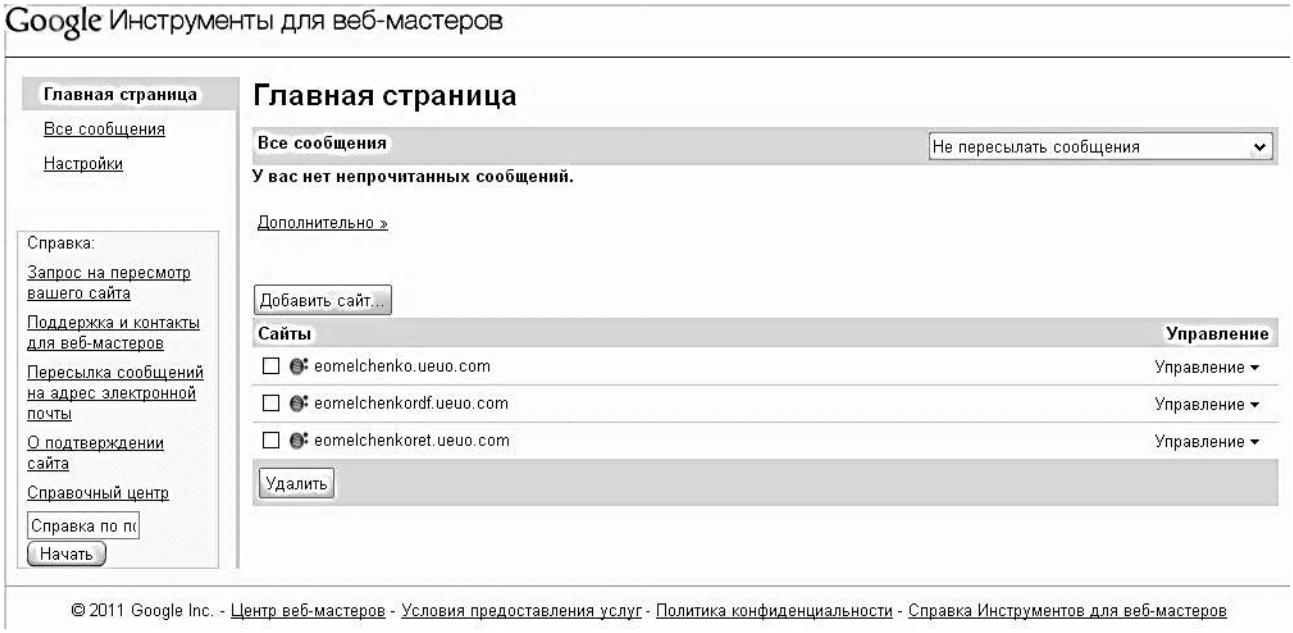


Рис. 10.10. **Інтерфейс користувача програмного засобу "Google Инструмент для Web-мастеров"**

Отриману карту сайта необхідно завантажити на сервер та додати до цільового Web-сайта за допомогою "Google Инструмент для Web-мастеров".

Залежно від черги індексації "Google-індексатору", через деякий час сайт буде проіндексований. В середньому процес індексації займає 24 години. Слід зазначити, що індексація всіх сторінок Web-сайтів виконується автоматично при індексації головної сторінки, адже вони пов’язані гіперпосиланнями. Процедура індексації інших сайтів є аналогічною.

Надання необхідних даних для індексації з використанням пошукової системи Sindice виконується за допомогою програмного засобу SindiceSubmit (рис. 10.11). У режимі індексації по сторінках необхідно вказати всі сторінки сайта, що необхідно індексувати. Кожна URL-адреса сторінки вказується з нового рядка у відповідному текстовому полі.

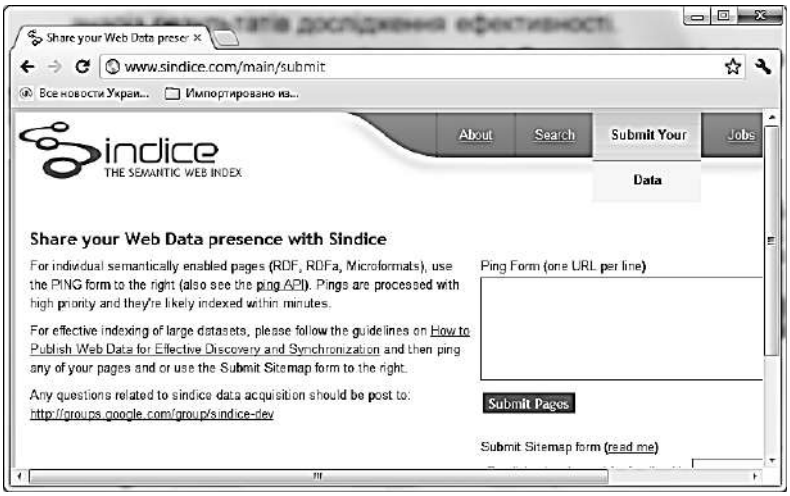


Рис. 10.11. **Інтерфейс користувача програмного засобу SindiceSubmit**

Після виконання індексації Web-сайтів, є можливість приступити до дослідження ефективності інформаційного пошуку з використанням традиційного підходу та підходу, який ґрунтується на семантичному описі цих ресурсів.

Для автоматизації процесу дослідження була розроблена програмна система, яка надає можливість виконання пошуку за допомогою традиційної пошукової машини та семантичної пошукової машини. Вона також дозволяє оцінити ефективність інформаційного пошуку на основі визначених раніше показників ефективності.

Розроблена програмна система дозволяє зручно виконувати запити до обох пошукових машин. Після введення необхідних вихідних даних підраховуються значення показників ефективності: точності, повноти та F-міри. На основі отриманих значень показників ефективності будуються діаграми, що дозволяє порівняти ефективність інформаційного пошуку за допомогою традиційної пошукової машини та семантичної пошукової машини.

Розроблена програмна система складається з двох підсистем (рис. 10.12): пошукової підсистеми, що призначена для виконання інформаційного пошуку; аналітичної підсистеми, яка необхідна для обробки результатів пошуку та розрахунку показників ефективності.

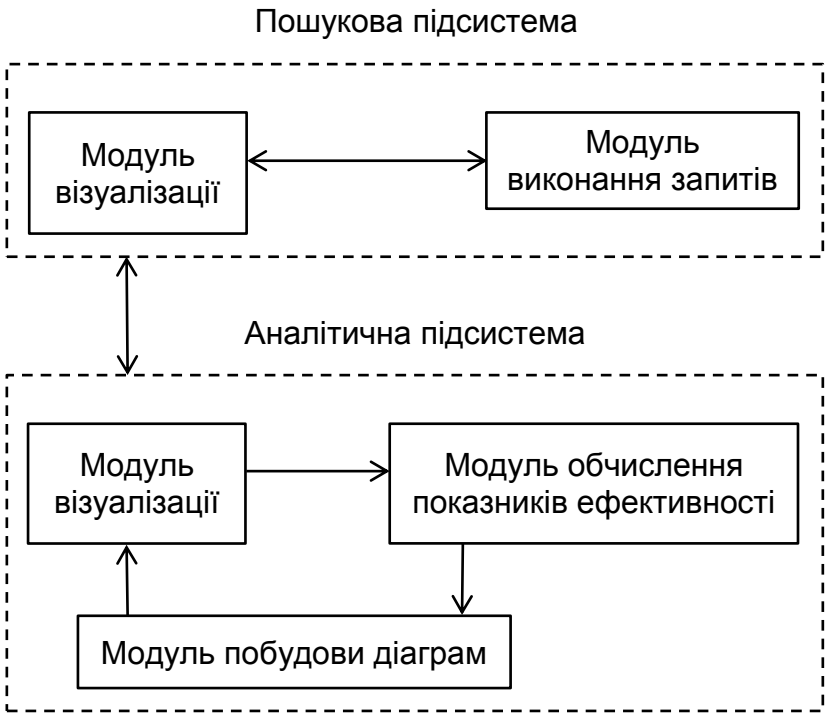


Рис. 10.12. **Структурна схема програмної системи**

Пошукова підсистема складається з модуля візуалізації та модуля виконання запитів. Ці два модулі взаємопов'язані між собою.

Модуль візуалізації надає Web-інтерфейс користувача, що дозволяє ввести дані запиту та відобразити його результат (рис. 10.13).

Рис. 10.13. **Інтерфейс користувача модуля візуалізації пошукової підсистеми**

Модуль виконання запитів відповідає за передачу запитів, які надходить до нього з модуля візуалізації, до пошукових машин Google та Sindice. Результат обробки запиту повертається до модуля візуалізації у вигляді списку знайдених документів.

Аналітична підсистема використовує дані, які надходять з пошукової підсистеми. Вона складається з трьох модулів:

модуля обчислення показників ефективності;

модуля побудови діаграм;

модуля візуалізації.

Модуль обчислення показників ефективності відповідає за оброку вихідних даних, які надходять до нього з модуля візуалізації. Ці дані є кількістю знайдених та кількістю релевантних документів. Кількість релевантних документів може бути визначена на основі використання методу експертних оцінок.

Результат у вигляді значень показників ефективності передається модулю побудови діаграм.

Модуль побудови діаграм, використовуючи дані з модуля обчислення показників ефективності, будує діаграми та передає ці дані до модуля візуалізації, який в свою чергу відображує результат користувачеві (рис. 10.14).

Рис. 10.14. **Приклад діаграми показників ефективності**

Розроблена програмна система базується на використанні технології ASP .NET. Для відображення діаграм показників ефективності інформаційного пошуку використовується компонент Google Chart [437].

Для того, щоб провести аналіз ефективності інформаційного пошуку, необхідно мати кількісні дані про результати пошуку. Тому для отримання цих даних було проведено ряд експериментів, усереднені результати яких наведені в табл. 10.2.

Таблиця 10.2

Вихідні дані для розрахунку показників ефективності

	Кількість знайдених релевантних документів	Кількість релевантних документів у базі пошукової системи	Загальна кількість знайдених документів
Пошукова система Google	7	9	26
Пошукова система Sindice	8	9	15

Обчислення значень показників ефективності інформаційного пошуку виконувалося за допомогою аналітичної підсистеми. Спочатку отримали результати обчислення повноти (рис. 10.15, 10.16), на яких: 0 – процент релевантних документів, знайдених пошуковою системою; 1 – процент релевантних документів, не знайдених пошуковою системою.

Рис. 10.15. **Результат обчислення повноти пошуку для Google**

Рис. 10.16. **Результат обчислення повноти пошуку для Sindice**

На основі аналізу одержаних результатів можна зробити висновок, що пошукова система Sindice забезпечує повноту пошуку кращу приблизно на 11 % ніж Google. Тобто Sindice має ліпші можливості щодо пошуку релевантних документів, але без урахування кількості не релевантних документів, що видаються користувачу.

Результати обчислення точності пошуку наведені на рис. 10.17, 10.18, де: 0 – процент знайдених релевантних документів; 1 – процент знайдених не релевантних документів.

На основі аналізу одержаних результатів можна зробити висновок, що пошукова система Sindice забезпечує точність пошуку кращу приблизно на 27 % порівняно з пошуковою системою Google.

Це свідчить про те, що пошукова система Sindice має ліпші можливості щодо пошуку релевантних документів серед усіх документів, що знаходяться в базі пошукової системи.

Для обчислення значень F-міри використовувалися значення точності та повноти що були отримані раніше.

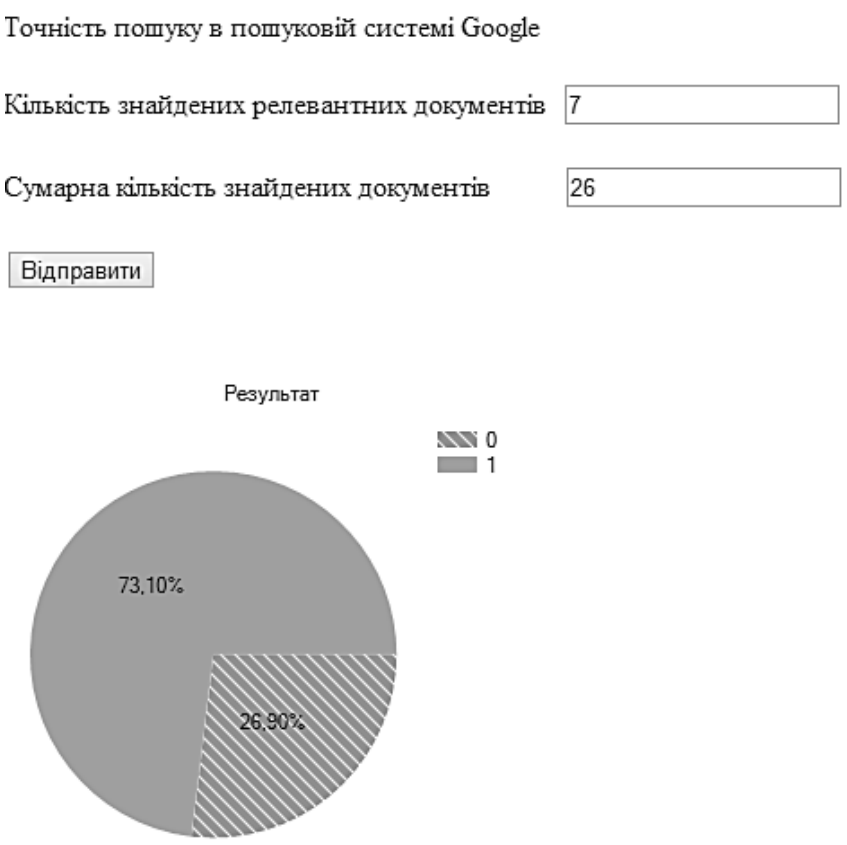


Рис. 10.17. **Результат обчислення точності пошуку для Google**

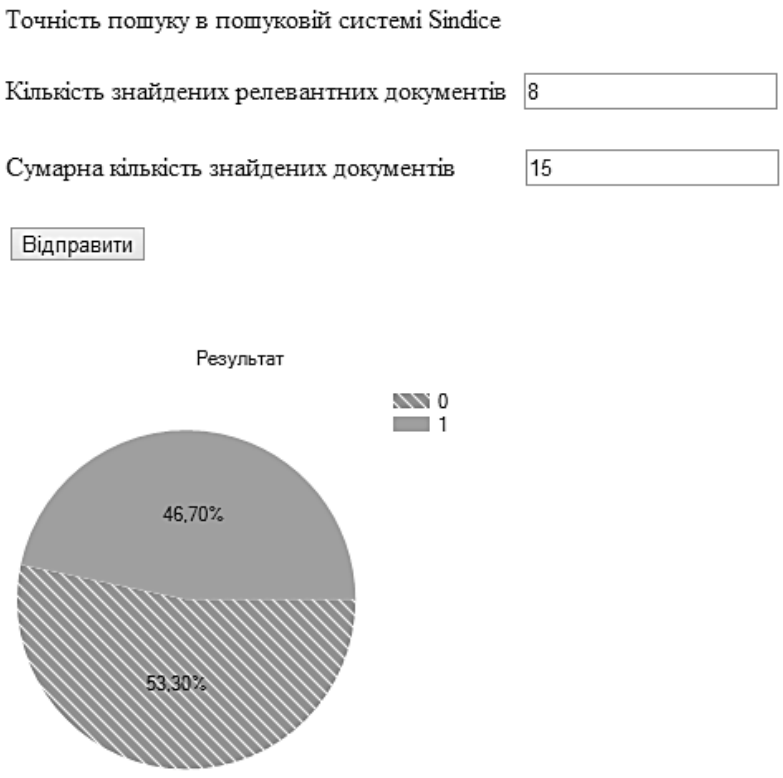


Рис. 10.18. **Результат обчислення точності пошуку для Sindice**

Результати обчислення F-міри наведені на рис. 10.19, де:

1 – пошукова система Sindice;

2 – пошукова система Google.

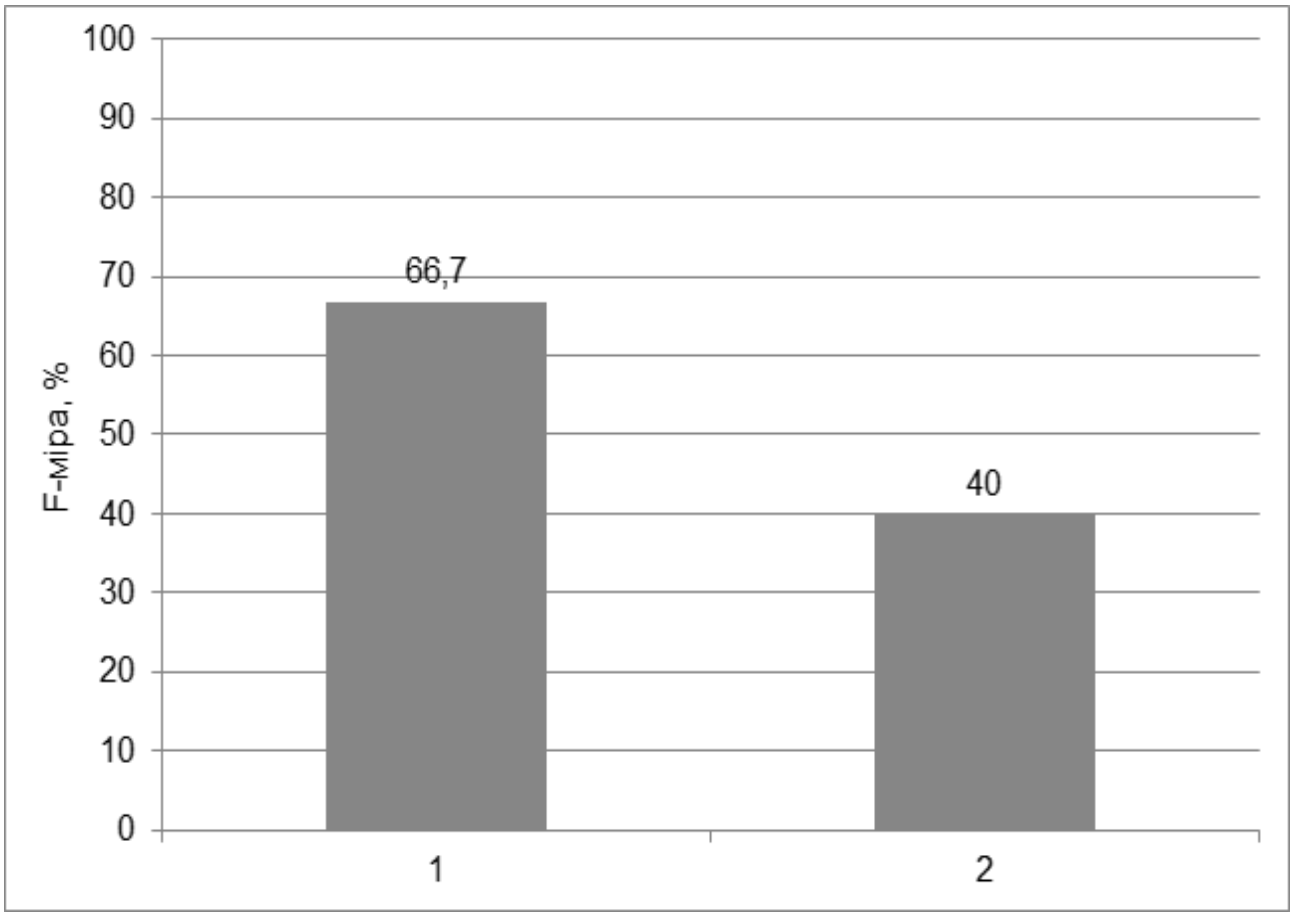


Рис. 10.19. **Результати обчислення F-міри**

Отримані результаті показують, що значення F-міри для пошукової системи Sindice на 26,7 % більше, ніж для пошукової системи Google.

Оскільки F-міра є узагальненим показником ефективності, який враховує повноту та точність інформаційного пошуку, то можна зробити висновок що пошукова система Sindice забезпечує ефективність інформаційного пошуку в середньому більшу на 26,7 % порівняно з пошуковою системою Google.

Таким чином, ефективність інформаційного пошуку в глобальній мережі Інтернет з використанням підходу, який ґрунтується на семантичному описі інформаційних ресурсів з використанням метаданих, є значно кращою, ніж при традиційному підході.

Розділ 11. Моделювання елементів навчального процесу вищого навчального закладу

11.1. Аналіз сучасного стану моделювання елементів навчального процесу

Проведено аналіз організації навчального процесу вищого навчального закладу. Зроблено висновок про доцільність використання моделювання для дослідження питань підвищення якості навчального процесу ВНЗ.

Розглянуто можливі підходи та сучасний стан моделювання елементів навчального процесу ВНЗ. Стверджується, що питання розробки адекватних моделей елементів навчального процесу вирішено не в повному обсязі і вимагає проведення додаткових наукових досліджень.

Сучасний етап розвитку суспільства висуває нові вимоги до системи вищої освіти з боку вдосконалення навчального процесу. У зв'язку з високим рівнем і швидким темпом науково-технічного прогресу різко зросли і вимоги до підготовки майбутніх фахівців.

Рівень загальної та професійної освіти випускника вищого навчального закладу визначається не тільки його творчим потенціалом, але і реалізацією навчального процесу.

Сучасний спеціаліст, випускник того чи іншого навчального закладу, повинен мати більш високий рівень підготовки, ніж випускники попередніх років, при цьому якість підготовки фахівця багато в чому визначається програмою його навчання.

Організація ефективного управління та оптимізація навчального процесу є найважливішими завданнями, що стоять перед адміністрацією різних рівнів ВНЗ. Основною метою навчального процесу є оволодіння студентами необхідними знаннями та навичками, відповідними майбутній професії. Обмеженнями є навчальний план спеціальності, навчальні робочі програми дисциплін. Складність управління навчальним процесом полягає в тому, що оцінка якості управління та коригування навчальних планів, розподілу навантаження, розкладу занять можливі тільки після завершення певного циклу навчання (семестру, навчального року тощо). Безпосереднє проведення експериментів на такій реальній системі

практично можливе, але небажане. Альтернативою реального експерименту при вирішенні завдань управління та оптимізації є моделювання.

Моделюванням називається заміщення одного об'єкта, званого системою, іншим об'єктом, званим моделлю, і проведення експериментів з моделлю (або на моделі), дослідження властивостей моделі, спираючись на результати експериментів з метою отримання інформації про систему [128].

В умовах різкого збільшення обсягів навчальної, методичної та адміністративно-управлінської інформації рішення задач управління, інтенсифікації та оптимізації освітньої системи вищого навчального закладу, пов'язане з використанням комп'ютерних систем підтримки прийняття рішень у сфері ідентифікації та прогнозуванні стану освітньої системи на основі математичних методів та імітаційного моделювання при різних стратегіях процесу навчання, є актуальним науковим завданням.

Великий внесок у загальну теорію освітнього процесу і його інформатизацію на основі інженерно-психологічних і математичних методів аналізу процесів навчання і діяльності освітнього закладу внесли роботи Венди В. Ф., Галактіонова А. І., Темникова Ф. Е., Кушелева Ю. Н. [118], Свиридова А. П., Протопопова І. І., Чачко А. Г., Васильєва В. Н. [33], М. Весни [38], Ю. Вєтрова, Балабана В. А., Архангельського С. І., Беспалько В. П. [20] та ін.

У багатьох працях вчених [29; 71; 123; 124; 136; 296; 309; 329] розглядається методологія управління вузом і якістю підготовки фахівців протягом усього часу навчання від абітурієнтів до випускників на основі статистичної інформації та експертних оцінок. Описуються математичні моделі управління процесами самоосвіти і самовиховання студентів і викладачів університету [136], а також математичні моделі оцінки залишкових знань [33; 123]. Велика увага приділяється технологіям електронного і дистанційного навчання, підготовки електронних підручників та тестового контролю, мультимедійним засобам та педагогічним технологіям.

При цьому явно недостатньо використовуються принципи системного аналізу та математичного моделювання освітнього процесу як великої соціальної інформаційної системи з безліччю взаємопов'язаних елементів, що об'єднуються спільною метою; багатофакторними процесами подання, передачі і сприйняття навчальної інформації; психофізіологічними факторами ефективності взаємодії викладача з групою студентів у середовищі навчання та накопичення знань.

Навчальний процес є досить складною системою, в якій подані детермінований розклад і випадкові події. Дуже часто збіг таких випадковостей істотно ускладнює ведення навчального процесу. Не завжди при плануванні лабораторних робіт, іспитів та заліків враховуються реальні відхилення часу зайнятості від запланованих ідеальних. Стан системи освіти в більшості випадків непередбачуваний і не може бути прогнозованим від початку аналітично або шляхом логічного аналізу, оскільки він є результатом багатокрокової взаємодії безлічі активних елементів системи і середовища навчання.

Застосовувані аналітичні методи аналізу та оцінки ефективності навчального процесу в своїй основі використовують рейтингову або статистичну оцінку стану системи без урахування динаміки стану, поведінки і взаємодії активних елементів (викладачів і студентів) при заданих і умовах, що змінюються та стратегіях управління.

Вивчення динаміки накопичення знань і навичок у процесі інформаційної взаємодії викладача і студентів з урахуванням впливу різних факторів середовища навчання в заданій предметній області; форм, стратегій і технологій навчального процесу, а також особистісних характеристик студентів і викладачів на загальну успішність і якість підготовки фахівця можливо за допомогою імітаційного моделювання.

Імітаційна модель навчального процесу описує його функціонування у вигляді послідовності операцій або груп операцій, виконуваних комп'ютерами. Складовими частинами імітаційної моделі є описи елементів, що складають систему, і опис структури системи. Опис подається у вигляді програм.

Тому процес імітаційного моделювання зводиться до проведення експериментів, що складаються з серії реалізації програм на комп'ютері при різних вихідних даних.

Імітаційні моделі елементів навчального процесу залежно від використовуваних вхідних даних можна розділити на трасоорієнтовані та статистичні. У трасоорієнтованих імітаційних моделях вхідні дані задаються трасою, тобто потоком подій, що мають місце при роботі системи, які реєструються в хронологічному порядку. У статистичних імітаційних моделях вхідні дані задаються за допомогою датчиків випадкових чисел, характеристики яких відомі.

Перевагою імітаційних моделей є можливість підміни процесу зміни подій у досліджуваній системі в реальному масштабі часу на прискорений процес зміни подій в темпі роботи програми.

У результаті за кілька хвилин можна відтворити навчальний процес протягом декількох днів, а то й місяців, що дає можливість оцінити навчальний процес у широкому діапазоні параметрів.

Результатом роботи імітаційної моделі є зібрані в ході спостереження за подіями, які моделюються, статистичні дані про найбільш важливі характеристики навчального процесу.

Існують спеціальні мови імітаційного моделювання, які полегшують процес створення програмної моделі порівняно з використанням універсальних мов програмування.

Прикладами мов імітаційного моделювання можуть служити такі мови, як SIMULA, GPSS, SIMDIS.

Існують також системи імітаційного моделювання, які орієнтуються на вузький клас систем, що вивчаються і дозволяють будувати моделі без програмування.

Основними недоліками імітаційного моделювання, незважаючи на ті, що з'явилися останнім часом різні системи моделювання, залишаються складність, висока трудомісткість і вартість розробки моделей, а іноді й велика ресурсомісткість моделей при реалізації на комп'ютері.

Хоча проблемі організації навчального процесу приділяється багато уваги, проте цього не достатньо й існуюча система організації навчального процесу, моделі та методи оцінки ефективності застосування і управління не повною мірою відповідають сучасним вимогам [275].

Використання імітаційного моделювання в організації навчального процесу вищого навчального закладу та його управлінні надасть можливість ілюструвати динаміку показників системи освіти, інтерпретувати статистичні дані, прогнозувати розвиток, з'ясовувати вплив прийнятих рішень на майбутній розвиток.

11.2. Обґрунтування вибору математичного апарату та розробка системи імітаційного моделювання

Обґрунтовано необхідність використання імітаційного моделювання для вирішення поставленного завдання. Проаналізовано сучасні системи імітаційного моделювання. Запропоновано використання математичного апарату Е-мереж для імітаційного моделювання елементів навчального процесу. Наведено основні положення теорії Е-мереж, принципи побудови моделей та їх функціонування.

Подано опис програмної реалізації системи імітаційного моделювання, виконаної на кафедрі інформаційних систем ХНЕУ. Запропонована система є спеціалізованим інструментальним програмним засобом для створення, редагування та дослідження моделей на основі Е-мереж. Показано приклади використання цієї системи для створення імітаційних моделей.

За останні 15 – 20 років імітаційне моделювання стало одним з найпоширеніших і найбільш потужних інструментів дослідження складних динамічних систем і процесів. Як і будь-яке комп'ютерне моделювання, воно дає можливість проводити обчислювальні експерименти з ще тільки проектованими системами і вивчати системи, реальні експерименти з якими, через міркування безпеки або дорожнечі, не доцільні. У той же час, завдяки своїй близькості за формою до фізичного моделювання, цей метод дослідження доступний більш широкому колу користувачів.

У наш час на ринку програмного забезпечення для імітації пропонується понад 50 потужних програмних засобів імітаційного моделвання. Усього ж на ринку інформаційних технологій фігурує близько 150 програмних продуктів, що дозволяють проводити імітаційні експерименти. Діапазон і різноманітність такого програмного забезпечення продовжують зростати, відбиваючи тенденцію стійкого попиту на нього.

Сучасні засоби імітаційного моделювання подані інтегрованими системами імітаційного моделювання. Вони дозволяють автоматизувати процес створення моделі за рахунок використання різних компонент, з яких будується модель, а також графічного інтерфейсу. У них розвинені середовище для редагування моделей, планування експериментів, управління моделюванням та аналізу результатів.

Програмні засоби імітаційного моделювання можна розділити на такі групи [146]:

Програмування комп'ютерної моделі із застосуванням спеціалізованих мов моделювання (наприклад, GPSS, AnyLogic), написаних універсальними мовами. Динаміка системи відображається взаємодією елементів моделі у часі і просторі. Спеціалізовані мови імітаційного моделювання компактні і мають широке коло застосувань, проте вимагають спеціальної підготовки користувача, який повинен написати програму в термінах мови для конкретного об'єкта моделювання.

Побудова комп'ютерних моделей і проведення імітаційних експериментів за допомогою спеціалізованих комп'ютерних середовищ (наприк-

лад, Arena, AnyLogic, GPSS World, VisSim). Імітаційні середовища не вимагають програмування у вигляді послідовності команд. Замість написання програми користувачі складають модель з бібліотечних графічних модулів, та/або заповнюють спеціальні форми. Як правило, імітаційне середовище забезпечує можливість візуалізації процесу імітації, дозволяє проводити сценарний аналіз і пошук оптимальних рішень.

Включення засобів імітаційного моделювання в стандартні математичні комп'ютерні системи (наприклад, пакет Simulink системи Matlab, Mathcad, Mathematica). Це програмні середовища, призначені для виконання різноманітних математичних та технічних розрахунків, які надають користувачеві інструменти для роботи з формулами, числами, графіками, текстом, містять засоби для керування змінними, введенням і виведенням даних, а також забезпечені графічним інтерфейсом.

Слід зауважити, що програмних засобів моделювання, які охоплюють і динамічні системи, і агентне моделювання, і дискретно-подієве моделювання, і системну динаміку на ринку ще дуже мало, а найбільш представницькою є група систем імітаційного моделювання, орієнтованих на дискретні системи.

Більшість систем моделювання мають зручний, що легко інтерпретується графічний інтерфейс, системні потокові діаграми або блок-схеми реалізуються на ідеографічному рівні. Зберігаються елементи програмування (на мовах загального призначення або об'єктно-орієнтованих) для окремих елементів моделі або створення спеціалізованих блоків підготовленим користувачем, так зване авторське моделювання [132].

Нова методологія наукового дослідження в комп'ютерному моделюванні, яка передбачає організацію і проведення обчислювального експерименту на імітаційній моделі, вимагає серйозної математичної та інформаційної підтримки процесу системного моделювання, особливо в частині обчислювальних процедур, пов'язаних з плануванням експерименту, оптимізацією, організації роботи з великим обсягом даних у процедурах прийняття рішень. Багато систем моделювання забезпечені засобами для інтеграції з іншими програмними середовищами, здійснюють доступ до процедурних мов, пов'язаних з кодом імітаційної моделі, для реалізації спеціальних обчислень, доступу до баз даних (підхід Simulation Data Base). У більш потужних пакетах здійснюється інтеграція через додаткове програмне забезпечення зі спеціалізованими блоками різного призначення. Це можуть бути блоки аналізу вхідних даних, гнучкі

засоби аналізу чутливості, що дозволяють здійснювати багаторазові прогони з різними вхідними даними (у системах GPSS/H-PROOF, Pro-Model та ін.) Перспективне створення систем моделювання з функціонально широкими, орієнтованими на специфіку імітаційного моделювання, блоками оптимізації (в цьому сенсі показовими системи WITNESS, TAYLOR). Інтеграція програмних систем, може здійснюватися і на інших рівнях. Реалізований у ряді систем багатокористувацький режим, застосування інтерактивного розподіленого моделювання, розробки в області взаємодії імітаційного моделювання з Інтернетом, розширюють можливості імітаційного моделювання, дозволяючи відпрацьовувати спільні або конкуруючі стратегії різним компаніям.

Серед засобів моделювання дискретних процесів інтенсивно розвивається апарат Е-мереж, перевагами якого є його наочність, можливість адекватного опису процесів з паралельно функціонуючими елементами і пристосованість моделей для аналізу за допомогою комп'ютера.

В основі Е-мережевого моделювання лежить подієво-кероване моделювання, що, в сукупності з методами генерації випадкових чисел для встановлення часу спрацьовування переходів, дає один з найбільш поширених способів моделювання. Той факт, що модель управляється подіями, свідчить про те, що стан системи змінюється тільки при спрацьовуванні переходів і залишається незмінним між спрацьовуваннями. Оскільки, час спрацьовування переходів є випадковою величиною, то для отримання статистично достовірних результатів потрібна відповідна кількість запусків моделі.

Передумовою появи Е-мереж став математичний апарат мереж Петрі. Мережі Петрі були описані ще в 1962 році Карлом Петрі [143]. Це був перший математичний апарат, який дозволив проводити моделювання динамічних дискретних систем.

Формально мережа Петрі становить набір:

$$C = (P, T, E), \tag{11.1}$$

де P – непорожня кінцева множина позицій мережі;

T – непорожня кінцева множина переходів;

$E = (P \times T) \cup (T \times P)$ – відношення інцидентності позицій і переходів (множина дуг мережі) – логічно обумовлені причинно-наслідкові зв'язки між подіями та умовами.

Також можуть бути задані:

W: F→N – функція кратності дуг (кожній дузі ставиться у відповідність *n> 0* – кратність дуг);

M: P→N – функція початкової розмітки.

У результаті розвитку апарату мереж Петрі був розроблений ряд розширень. Найбільш потужними є, так звані Е-мережі, запропоновані Г. Натом. Літера Е в назві – початкова в англійському слові evalution – "обчислення" або "оцінка", тому Е-мережі називають оціночними мережами. В даний час вони знайшли застосування в імітаційному моделюванні дискретних систем, перш за все, завдяки своїм розвиненим моделюючим можливостям. Е-мережі мають здатність обробляти дані і тим самим проводити кількісний аналіз модельованих процесів [366]. Можливості Е-мереж щодо моделювання та їх ефективність в програмах пояснюються тим, що Е-мережі – це інтеграція графа і дискретної динамічної системи. Тобто вони можуть служити і статичною, і динамічною моделлю представленого з її допомогою об’єкта.

Е-мережа – граф особливого виду, що складається з двох типів вершин – позицій і переходів [73; 142], з’єднаних один з одним орієнтованими ребрами, або дугами, причому кожна дуга може пов’язувати лише перехід з позицією або позицію з переходом. Отже, структура Е-мережі еквівалентна орієнтованому дводольному графу, у якого одна множина вершин містить тільки позиції, а інша множина вершин – тільки переходи.

Позиція – пасивний елемент Е-мережі, призначений для зберігання фішок. Позиція позначається на зображенні Е-мережі окружністю (або овалом). Позиція, пов’язана дугою з входом переходу, називається вхідною позицією даного переходу. Позиція, пов’язана дугою з виходом переходу, називається вихідною позицією даного переходу.

Кожна позиція в Е-мережі є вхідною для одного переходу і вихідною для іншого.

Перехід – активний елемент Е-мережі, призначений для переміщення фішок з одних позицій в інші. Перехід позначається на графічному зображенні Е-мережі вертикальною лінією.

Фішка – рухомий елемент Е-мережі, призначений для обміну інформацією в Е-мережі. Фішка позначається на графічному зображенні Е-мережі точкою (або маленьким кружечком) у простих позиціях. Якщо ж фішка (фішки) знаходяться в позиції-черзі, то їх кількість відображається числом у середині зображення позиції-черги.

Однак Е-мережі у своїй топології і логіці роботи мають суттєві відмінності від мереж Петрі [73]. На відміну від мереж Петрі, в Е-мережах:

є кілька типів вершин-позицій: прості позиції, позиції-черги, дозволяючі позиції;

фішки (мітки) можуть забезпечуватися набором ознак (атрибутів);

з кожним переходом може бути пов'язана ненульова затримка і функція перетворення атрибутів фішок;

введені додаткові види вершин-переходів;

в будь-яку позицію може входити не більше однієї дуги і виходити також не більше однієї.

У зв'язку з цим будь-який перехід може бути описаний трійкою параметрів:

$$d_j = (S, t(d_j), p(d_j)). \qquad (11.2)$$

Тут S – тип переходу, $t(d_j)$ – функція затримки, що відображає тривалість спрацьовування переходу, $p(d_j)$ – функція перетворення атрибутів міток. Ще одна важлива відмінність Е-мереж від мереж Петрі полягає в тому, що мітки інтерпретуються як транзакти, які переміщаються мережею, а вершини-переходи трактуються як пристрої, що виконують ту або іншу обробку транзактів. Наслідком такого підходу є вимога: жодна вершина-позиція Е-мережі не може містити більше однієї мітки (тобто, будь-яка Е-мережа є безпечною).

Слід розглянути більш детально кожний з елементів Е-мережі.

Фішка. Фішку умовно можна представити як певний "шматок" інформації, що переміщується по Е-мережі. Фішка складається з декількох атрибутів (числових характеристик). У кожний атрибут фішки можна записувати інформацію чи зчитувати з нього. Оскільки фішки переміщуються по Е-мережі, то передачу інформації по мережі можна здійснювати через атрибути фішок:

в одному місці інформація записується відправником в атрибут;

потім фішка переміщається по Е-мережі до одержувача;

потім інформація зчитується одержувачем.

Фішки зберігаються в Е-мережі в позиціях.

Позиція. Позиції призначені для зберігання фішок. Залежно від того, скільки фішок може зберігатися в одній позиції, розрізняють три типи позицій:

прості позиції (можуть містити не більше однієї фішки);

позиції-черги (можуть містити довільне число фішок);

дозволяюча позиція.

Прості позиції позначаються окружністю (рис. 11.1), позиції-черги – овалом (рис. 11.2), дозволяюча позиція, зазвичай, зображується у вигляді шестигранника або квадрата (рис. 11.3). Якщо в позиції є хоча б одна фішка – така позиція називається маркерованою.

Оскільки в позиції-черзі може перебувати декілька фішок, то для кожної позиції-черги визначається дисципліна обслуговування, відповідно до якої фішки потрапляють у позицію-чергу.

Залишають чергу фішки в порядку розташування в черзі починаючи з її початку.

Рис. 11.1. **Проста позиція**

Рис. 11.2. **Позиція-черга**

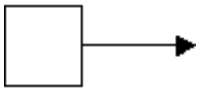


Рис. 11.3. **Дозволяюча позиція**

Кожна позиція має одну вхідну і одну вихідну дуги (окрім дозволяючої позиції). Не може бути такої позиції, у якої немає хоча б однієї дуги (вхідної або вихідної) – таке завдання позиції є помилковим.

Таким чином, позиції можуть зберігати фішки, але не можуть переміщати їх по Е-мережі. Цю функцію виконують переходи.

Перехід. Перехід є найбільш складним елементом Е-мережі. Якщо існує всього три різновиди позицій, то різних типів переходів можна визначити скільки завгодно. Ця можливість визначається тим, що по-перше, немає обмежень на кількість входів і виходів для переходу (під входами і виходами розуміються вхідні і вихідні дуги відповідно), по-друге, немає обмежень на логіку роботи переходу.

Базові переходи Е-мережі:

T-перехід ("виконання", "простий перехід"). Його графічне подання аналогічне поданням вершини-переходу мережі Петрі (рис. 11.4). Перехід спрацьовує при наявності мітки у вхідній позиції і відсутності її у вихідній позиції.

T-перехід дозволяє відобразити в моделі зайнятість деякого пристрою (підсистеми) протягом деякого часу, визначеного параметром $t(d_j)$.

Рис. 11.4. **Графічне подання *T*-переходу**

F-перехід ("розгалуження"). Графічне подання наведено на рис. 11.5. Спрацьовує при тих же умовах, що й *T*-перехід.

Зі змістовної точки зору *F*-перехід відображає розгалуження потоку інформації (транзактів) у системі.

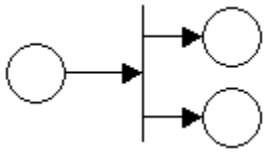


Рис. 11.5. **Графічне подання *F*-переходу**

J-перехід ("об'єднання"). Графічне позначення показано на рис. 11.6. Перехід спрацьовує при наявності міток в обох вхідних позиціях і відсутності мітки у вихідній позиції.

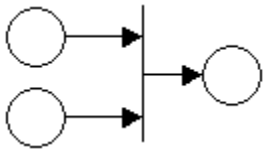


Рис. 11.6. **Графічне подання *J*-переходу**

Він моделює об'єднання потоків або наявність декількох умов, що визначають деяку подію.

X-перехід ("перемикач"). Порівняно з трьома попередніми типами переходів, він містить додаткову керуючу ("роздільну") позицію, яка

графічно позначається зазвичай або квадратиком, або шестикутником (рис. 11.7).

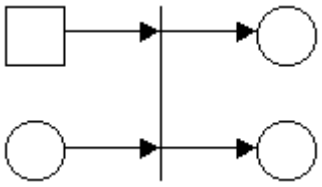


Рис. 11.7. **Графічне подання *X*-переходу**

X-перехід змінює напрям потоку інформації (транзактів). У загальному випадку роздільна процедура може бути як завгодно складною, але сутність її роботи полягає в перевірці виконання умов розгалуження потоку (з точки зору програміста, роздільна позиція аналогічна умовної інструкції типу if).

Y-перехід ("вибір", "пріоритетний вибір"). Цей перехід також містить роздільну позицію (рис. 11.8).

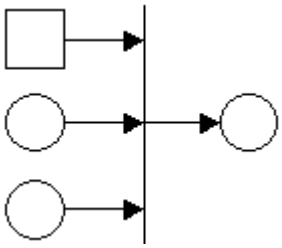


Рис. 11.8. **Графічне подання *Y*-переходу**

Y-перехід відображає пріоритетність одних потоків інформації (транзактів) порівняно з іншими. При цьому дозволяюча процедура може бути визначена різним чином: як операція порівняння фіксованих пріоритетів міток; як функція від атрибутів міток (наприклад, чим менше час обслуговування, тим вищий пріоритет). У певному сенсі він працює аналогічно інструкції вибору типу case.

Для завдання будь-якого переходу необхідно визначити такі характеристики:

функція збудження;

процедура спрацьовування;

функція управління;

процедура обчислення тимчасової затримки;

процедура перетворення атрибутів.

Функція збудження. Функція збудження визначає умови, при яких перехід збуджується. Вона повинна повертати значення "істина" (true), якщо умови збудження виконуються і "хибність" (false) – в протилежному випадку. Як правило (це відноситься до всіх стандартних переходів) в якості умови збудження для переходу вибирається маркування його вхідних і вихідних позицій. У загальному випадку немає обмежень на умови збудження переходів, що визначаються користувачем.

Процедура спрацьовування. Процедура спрацьовування визначає правила переміщення фішок переходом у кінці фази активності. Всі стандартні переходи переміщують фішки з вхідних позицій у вихідні. Для користувацьких типів переходів немає обмежень на їх дії, внаслідок чого перехід може маніпулювати фішками, що знаходяться в довільних позиціях Е-мережі.

Функція управління. Всі переходи діляться на два класи: керовані і некеровані. Керовані переходи позначаються на графічному поданні Е-мережі так само, як і некеровані з додаванням горизонтальної риси зверху. Функція управління визначена тільки для керованих переходів. Вона визначає номер вихідної позиції, в яку буде переміщена фішка процедурою спрацьовування. Крім цього функція управління може впливати на результат, що повертається функцією збудження. Якщо функція управління повертає значення нуль, то функція збудження поверне значення false.

Функція управління використовується функцією збудження для додаткової перевірки готовності керованого переходу до спрацьовування.

Процедура обчислення тимчасової затримки. Процедура обчислення тимчасової затримки визначає затримку переходу у фазі активності чи інакше тривалість фази активності. Визначено кілька стандартних процедур обчислення часової затримки:

фіксована;

рівномірна;

нормальна;

експонентна.

Процедура перетворення атрибутів. Процедура перетворення атрибутів може виконувати будь-які дії визначені користувачем, зокрема маніпулювати з атрибутами фішок.

Слід розглянути динаміку роботи Е-мережі.

Модельний час. Е-мережа функціонує в модельному часу. У початковому стані модельне час дорівнює нулю.

Фази переходу. З плином модельного часу кожний перехід може перебувати в одній з двох фаз:

фаза активності;

фаза пасивності.

У початковому стані всі переходи знаходяться у фазі пасивності. Потім відбуваються перемикання переходів між цими двома фазами.

Алгоритм роботи переходу. Варто розглянути алгоритм роботи окремо взятого переходу з плином модельного часу.

1. У початковому стані перехід знаходиться у фазі пасивності.

2. Перевіряється функція збудження переходу. Якщо вона не виконується, то слід перейти до пункту 2.

3. Перехід перемикається у фазу активності.

4. Виконується процедура обчислення тимчасової затримки. У результаті обчислення виходить величина інтервалу часу, протягом якого перехід буде перебувати у фазі активності.

5. У кінці фази активності виконується процедура спрацьовування.

6. Виконується процедура перетворення атрибутів (не обов'язково).

7. Перехід перемикається в фазу пасивності.

8. Перехід до пункту 2.

За поданим алгоритмом працюють всі переходи, наявні в Е-мережі.

Динаміка Е-мережі визначається переміщенням фішок з одних позицій в інші в результаті спрацьовування переходів.

Одночасно (мається на увазі модельне час) варто припустити переміщення фішок кількома переходами. Тим самим забезпечується можливість подання паралельних процесів у системі, що моделюється.

У сучасному світі при швидких темпах розвитку технологій апарат Е-мереж не міг не модифікуватися. Він був розширений, структура будь-якої кінцевої Е-мережі вже подається у вигляді:

$$E = (P, T, I, O, M), \qquad (11.3)$$

де P – кінцева непорожня множина позицій, що складається з непересічних підмножин простих позицій, позицій-черг і дозволяючих позицій;

T – кінцева непорожня множина переходів;

$I: T \rightarrow P$ – вхідна функція, яка для кожного переходу задає множину його вхідних позицій, тобто таких позицій, з яких дуги спрямовані до переходу;

$O: T \rightarrow P$ – вихідна функція, яка для кожного переходу задає множину його вихідних позицій, тобто таких позицій, на яких закінчуються дуги, що починаються на переході;

$M: P \rightarrow \{0, 1, 2, \ldots\}$ – функція розмітки, яка визначає маркування, або стан, позицій у формі невід'ємних цілих чисел.

Подальші модифікації змінили вид структури Е-мережі до такого:

$$E = (P, H, L, D, A, M_0), \tag{11.4}$$

де P – кінцева множина позицій, у тому числі підмножини B та R (B – кінцева множина периферійних позицій, R – кінцева множина вирішальних позицій);

H – кінцева множина переходів, що включає множини T, F, J, X, Y (різні типи переходів);

L – пряма функція інцидентності;

D – зворотна функція інцидентності;

A – кінцева множина характеристик переходів, що включає $\alpha=(\tau(\alpha_i),q)$, ($\tau(\alpha_i)$ – час спрацьовування переходу; q – процедура переходу);

M_0 – початкова розмітка мережі.

Множини P, H задовольняють такі умови:

$$P \neq \varnothing,\ H \neq \varnothing,\ P \cap H = \varnothing. \tag{11.5}$$

Граф Е-мережі повинен містити хоча б один перехід і одну позицію, причому вершина графа не може бути одночасно елементом множин P та H.

Функції прямої і зворотної інцидентності L, D, задаючи такі правила: $L: B \times H \rightarrow \{0,1\}$, $D: H \times B \rightarrow \{0,1\}$, визначають те, що елементи однієї множини дугами з'єднані бути не можуть, а також описують набори вхідних і вихідних елементів.

У даний час структуру E-мережі вже можна подати у вигляді:

$$E=((P, B, R), A, (I(A), O(A)), Z, V, Q, \psi, M_0). \tag{11.6}$$

Перший елемент набору Р – кінцева непорожня множина позицій мережі $P=\{p_i\}$; $B=\{b_k\} \subset P$ – множина периферійних (не внутрішніх) позицій; $R=\{r_m\} \subset P$ – множина вирішальних позицій.

У кожному стані мережі позиції можуть мати або не мати мітку. Число міток у кожній позиції $d1(M: P \rightarrow \{0,1\})$. Відмічаються мітки жирною крапкою.

Другий елемент набору – кінцева непорожня множина переходів $A=\{a_n\}$, які задаються бар'єрами.

Третій елемент набору $I(A), O(A)$ – множина позицій, суміжних з переходами по входу (I) і виходу (O). Пари $(p_i, a_n) \in I(A) \times A$ та $(p_i, a_n) \in A \times O(A)$, складені із суміжних позицій і переходів, відповідають дугам мережі.

Четвертий елемент набору функція $Z: A \rightarrow R^+$, за допомогою якої в Е-мережах задаються значення часу виконання переходів, таким чином імітуються тимчасові затримки, пов'язані з реалізацією модельованих подій.

П'ятий елемент набору $V=\{v_s\}$ задає непорожню кінцеву множину змінних – кількісних оцінок стану моделі.

Шостий елемент набору $Q=\{q_m\}$ описує множину вирішальних процедур, які застосовуються для вирішення конфліктів на переходах і синхронізації подій.

Сьомий елемент набору – множина $\Psi=\{\Psi_n\}$ процедур переходу.

Восьмий елемент набору $M_0=(M_0(p_1),\ldots M_0(p_{|p|}))$ позначає початкове маркування позицій.

При побудові Е-мереж використовується обмежений набір типів переходів: *T, I, F, X, Y, MX, MY*. Два останні є макророзширеннями *X* та *Y* переходів.

Кожен перехід Е-мережі має три характеристики і записується як $a_n=(\pi_n, z_n, \Psi_n)$, де $\pi_n \in \Pi$ – тип переходу, $z_n \in Z$ – час переходу; Ψ_n – процедура переходу [380]. Перехід виконується у 3 етапи:

перевіряються умови активності переходу, а для X і Y переходів ще й знаходяться значення вирішальної позиції і визначається конкретна схема спрацьовування;

реалізується затримка виконання переходу на час Z і перераховуються значення атрибутів мітки за правилами, зазначеним у процедурі Ψ_n;

відповідно до схеми переходу змінюються маркування його вхідних і вихідних позицій.

Слід ще раз підкреслити, що в Е-мережі всі переходи мають властивість безпеки.

Це означає, що у вихідних позиціях (які, у свою чергу, можуть бути вхідними для наступного переходу) ніколи не може бути більше однієї мітки.

Разом з тим, в Е-мережах існують поняття макропереходу і макропозиції, які дозволяють відображати в моделі процеси накопичення транзактів, які обслуговуються в тих чи інших вузлах системи, а також розширити логічні можливості Е-мереж.

Макропереходи визначаються дещо складніше, ніж відповідні схеми *X* та *Y* переходів.

Однак, головним у них як і раніше залишається порівняння значень вирішальної позиції і міток інцидентних переходу дуг.

Макропозиція черга є лінійною композицією Т-переходів (рис. 11.9); сумарна кількість вихідних вершин-позицій визначає "ємність" черги.

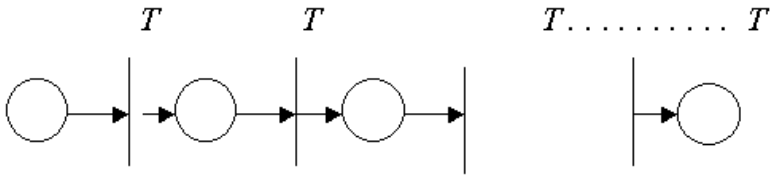


Рис. 11.9. **Графічне подання макропозиції "Черга"**

З метою підвищення компактності і наочності Е-мережі для позначення макропозиції черги використовується спеціальний символ (рис. 11.10).

Рис. 11.10. **Компактне зображення макропозиції "Черга"**

Макропозиція генератор (рис. 11.11, 11.12) дозволяє представляти в мережі джерело міток (транзактів).

Якщо необхідно задати закон формування міток, то "генератор" може бути доповнений роздільною позицією.

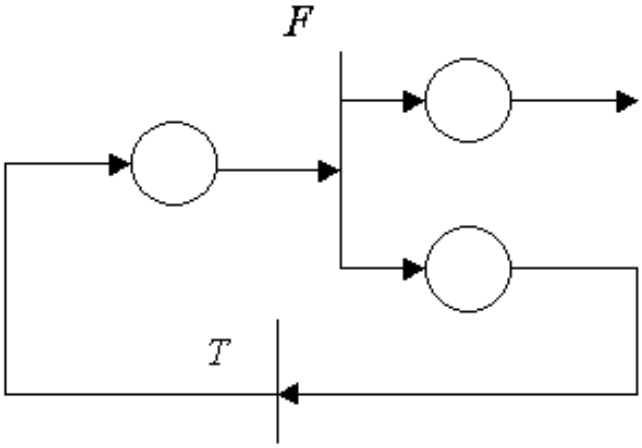


Рис. 11.11. **Графічне подання макропозиції "Генератор"**

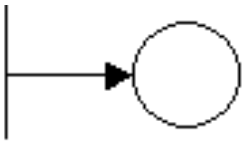


Рис. 11.12. **Компактне позначення макропозиції "Генератор"**

Якщо необхідно задати закон формування міток, то генератор може бути доповнений дозволяючою позицією (рис. 11.13).

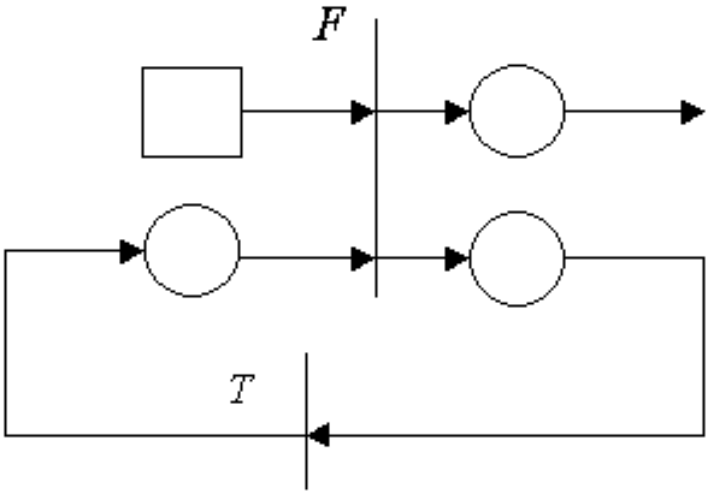


Рис. 11.13. **Макропозиція "Генератор" з можливістю задати закон формування міток**

Оскільки в Е-мережі не можна "накопичувати" мітки, то вводиться макропозиція поглинання або акумулятор (рис. 11.14, 11.15).

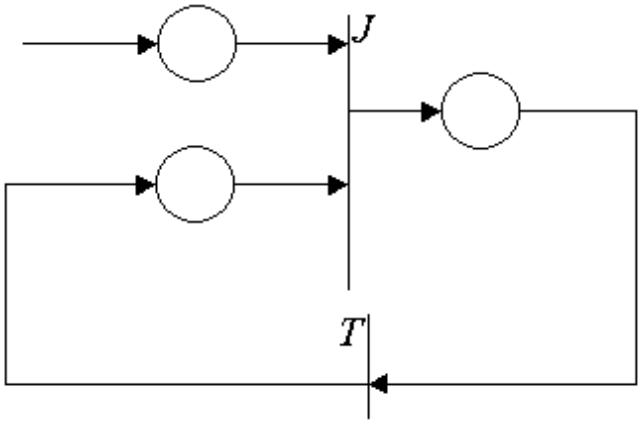


Рис. 11.14. **Графічне подання макропозиції "Акумулятор"**

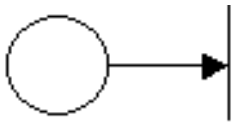


Рис. 11.15. **Компактне позначення макропозиції "Акумулятор"**

З метою підвищення компактності і наочності Е-мережі для позначення макропозиції використовують спеціальні символи:

Q-черга (рис. 11.10);

G-генератор (рис. 11.13);

A-акумулятор (рис. 11.15).

Аналогічним чином шляхом композиції *N* однотипних переходів можуть бути отримані макропереходи всіх типів: *XN, YN, JN*.

Розглянуті особливості Е-мереж істотно розширюють їх можливості для моделювання дискретних систем взагалі і паралельних процесів зокрема.

До основних переваг апарату Е-мереж можна віднести можливість опису паралельних взаємодіючих асинхронних процесів; можливість різного трактування своїх елементів за рівнем абстракції (деталізації), що дозволяє будувати ієрархічні моделі, в яких перехід може транслюватися в підмережі більш низького рівня деталізації. Застосування даного апарату також дозволить оцінити часові характеристики аналізованої системи (час реакції, пропускна спроможність). Однією з особливостей даного апарату є здатність аналізу систем не тільки за допомогою імітаційного моделювання (кількісний аналіз), а й аналітичними засобами (якісний аналіз). Використання засобів якісного аналізу

дозволяє виявити послідовності розміток, що призводять до тупикових і конфліктних, що є ще однією перевагою.

Крім очевидних переваг Е-мереж, проявлена до них увага пояснюється ще й тим, що вони постійно розвиваються. Технологія моделювання систем у вигляді Е-мереж дуже ефективно реалізується за допомогою інструменту SIMULINK, що входить до складу пакета MATLAB.

Треба зазначити, що програми для імітаційного моделювання на основі математичного апарату Е-мереж, яка б задовольняла всі вимоги, на сьогоднішній день не існує. Тому на кафедрі інформаційних систем ХНЕУ силами викладачів та студентів було розроблено власну систему імітаційного моделювання на основі Е-мереж, яка отримала назву SVC Enet.

Розроблена програмна система є Windows-додатком, який містить набір бібліотек. Серед цих бібліотек слід виділити основні, такі, як IWidget, що містить основні інтерфейси та базові типи, які можна використовувати для створення власних віджетів; Core, що відповідає за взаємодію віджетів з системою та логування. Також до стандартної поставки входить набір базових віджетів, зібраних у бібліотеці BasicWidgets.

На логічному рівні система представлена двома основними підсистемами: підсистемою візуалізації та підсистемою моделювання. Підсистема візуалізації слугує для побудови моделі, яка потім буде досліджуватись. Підсистема моделювання надає можливість дослідження моделі в динаміці.

Для додавання нових типів переходів, які б реалізували свою логіку роботи з фішками (транзактами), потрібно клас переходу унаслідувати від класу Transition, і перевизначити методи Init в якому вказати базові характеристики переходу, як то імя за замовчуванням, можлива кількість входів та віходів тощо; метод GetImage, в якому вказати, з яким зображенням буде зображуватись цей перехід на панелі компонент; метод GetTypeDisplayName, в якому вказати назву цього переходу, яка буде зображуватись на панелі компонент; Ready, в якому визначити умови, за яких перехід повинен спрацьовувати. У деяких випадках може з’явитись необхідність перевантажити методи From і To, в яких вказати, за якими критеріями обирати позицію, з якої потрібно перемістити фішку і за якими критеріями обирати позицію, в яку потрібно перемістити фішку відповідно. У деяких окремих випадках та у випадку, коли потрібно перемістити одразу кілька фішок, може виникнути необхідність перевантаживши метод MoveChip.

Для того, щоб новий перехід з’явився на панелі інструмент програмної системи і з ним можна було працювати, бібліотеку з ним слід помістити до каталогу з редактором та перезапустити редактор.

Основні структурні елементи програми наведені на рис. 11.16.

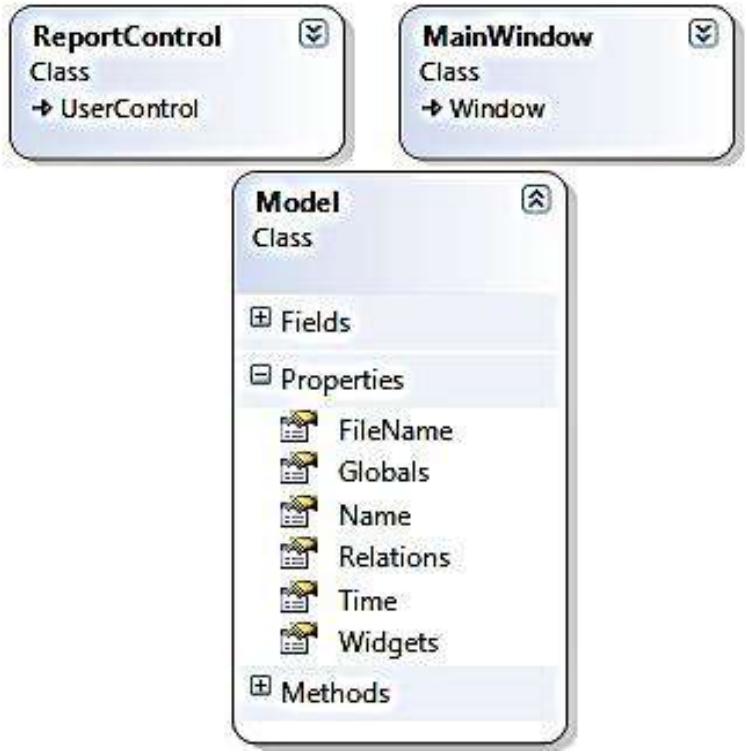


Рис. 11.16. **Основні структурні елементи програми**

Клас ReportControl надає можливість спостерігати за змінами глобальних параметрів моделі.

Клас Model є моделлю, яка складається з Позицій, Переходів, Дуг, та додаткових параметрів, як то поточний час, назва моделі чи глобальні атрибути моделі.

Клас MainWindow – головний інтерфейсний компонент системи, становить головне вікно програми та містить екземпляри класів ReportControl, яке демонструється користувачу за необхідності, та Model, власне модель, яку, завдяки наявному у цьому вікні інструментарію, можна створювати, редагувати, завантажувати, зберігати, налаштовувати, запускати моделювання, спостерігати за змінами у станах моделі та інше. Зміни в моделі здійснюються за допомогою додаткових класів, також існує список виконаних користувачем дій і, за необхідності, ці дії можна відмінити. Ці елементи наведено на рис. 11.17.

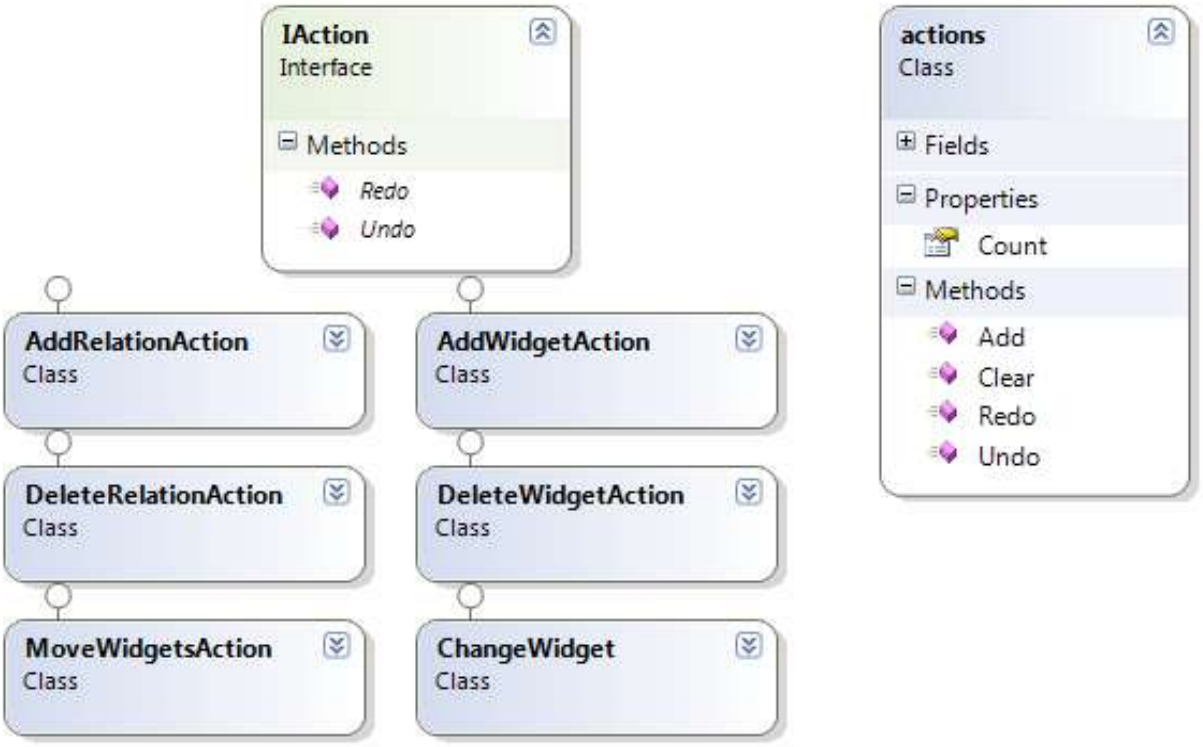


Рис. 11.17. **Дії над моделлю**

На рис. 11.18 наведені загальнодоступні перерахування, які спрощують роботу з елементами програми.

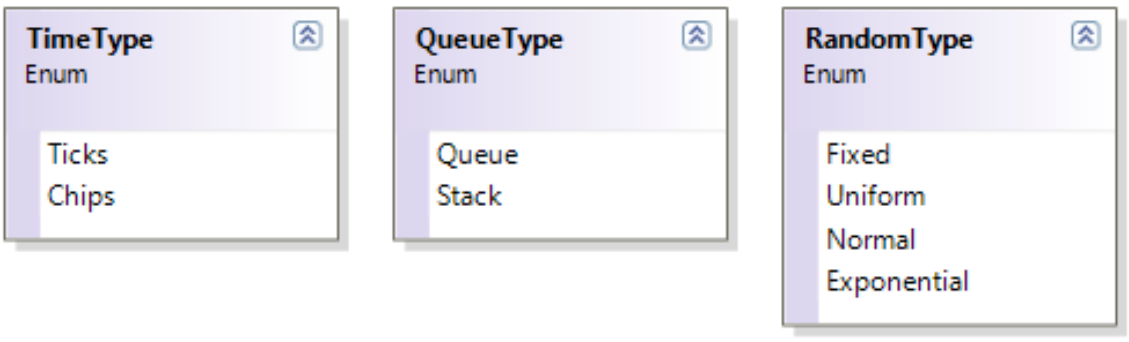


Рис. 11.18. **Основні перерахування використані в програмі**

На рис. 11.19, 11.20 наведено ієрархію класів, з яких будується модель. На рис. 11.21 наведені класи вікон властивостей віджетів. Редагування властивостей Позицій та Переходів відбувається шляхом виклику такого вікна подвійним кліком миші по потрібному елементу.

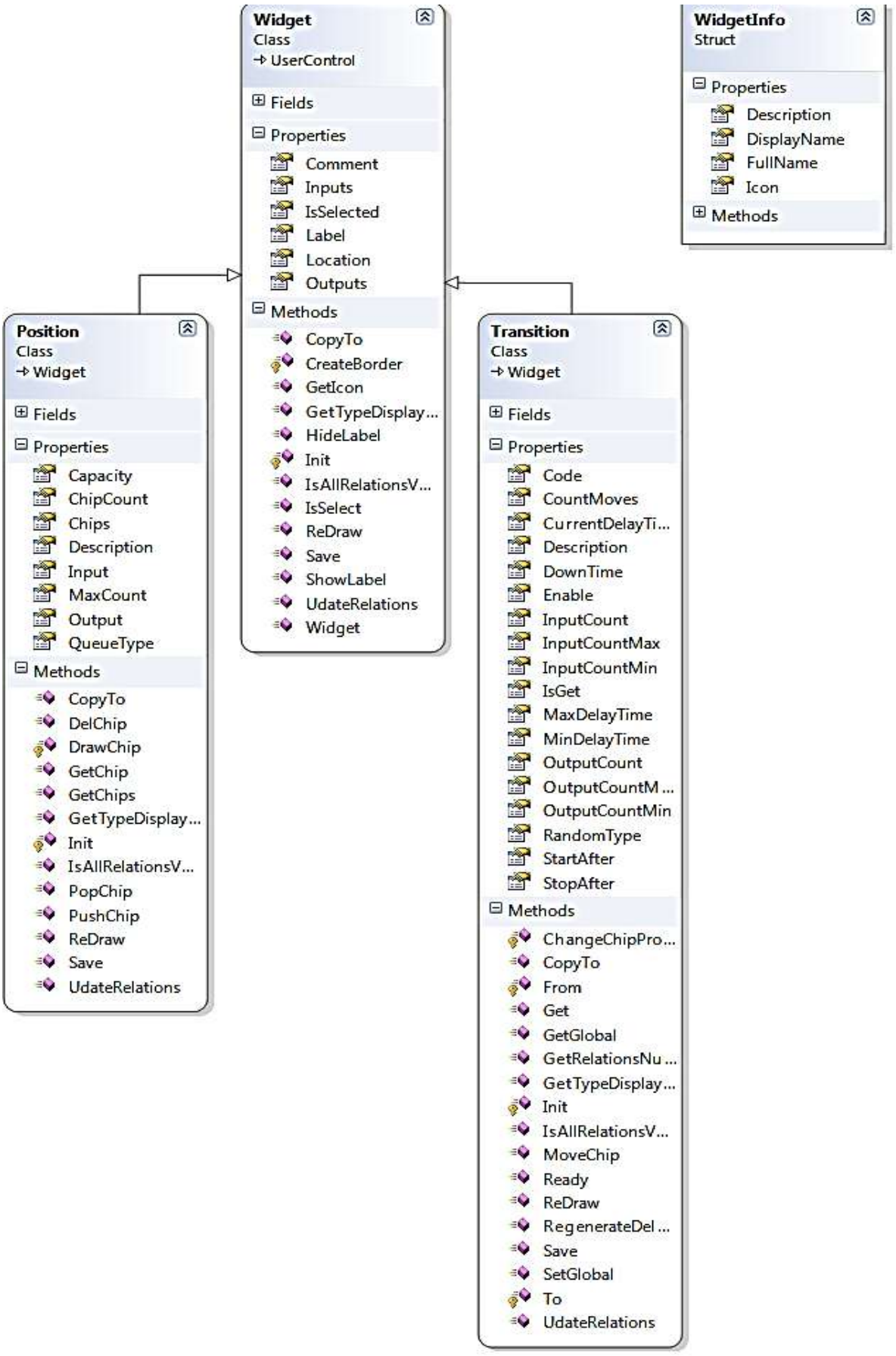


Рис. 11.19. **Базові класи для віджетів, з яких будуються Е-мережі**

Рис. 11.20. **Дуги та Фішки**

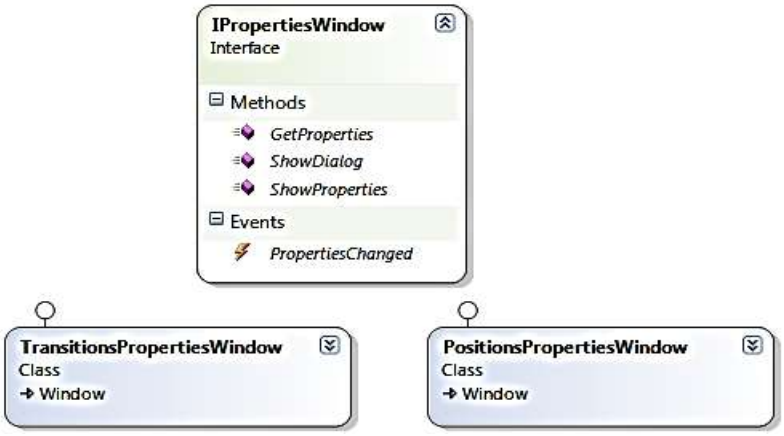


Рис. 11.21. **Вікна властивостей віджетів**

На рис. 11.22 наведено класи стандартних типів позицій та переходів, які поставляються разом із системою.

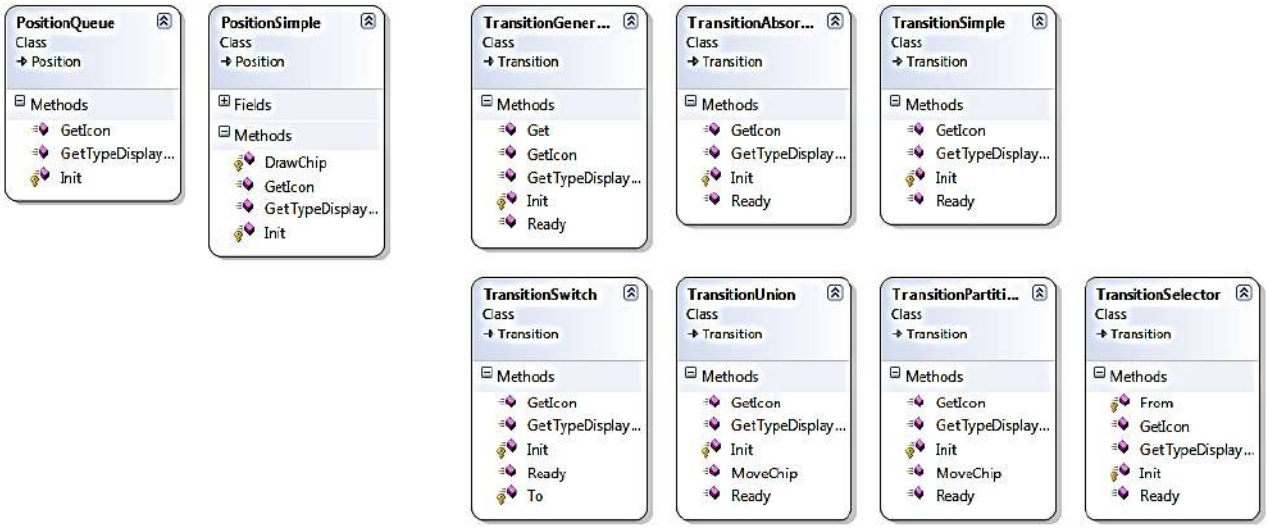


Рис. 11.22. **Базові типи позицій та переходів**

На рис. 11.23 наведено граф, який показує взаємозв’язки між основними архітектурними елементами системи.

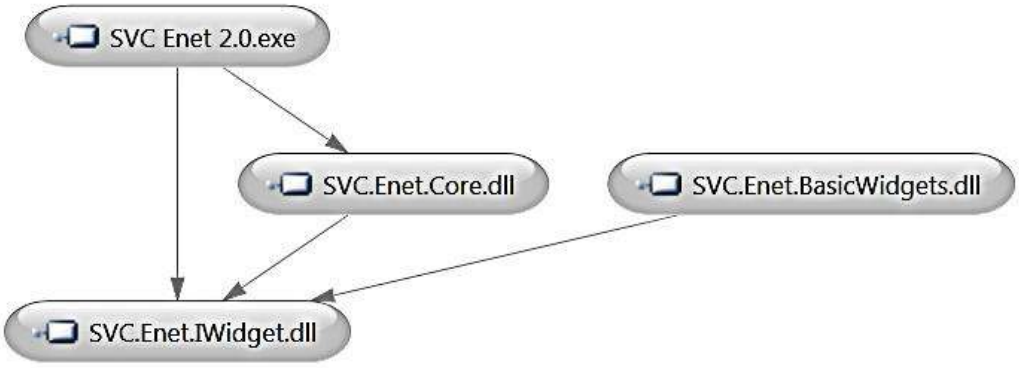


Рис. 11.23. **Взаємозв’язки між основними складовими програмної системи**

Програмна система, якщо розглядати укрупнену схему, може бути у двох станах: режимі створення моделі та режимі імітації. Кожен з цих станів можна деком позувати ще на декілька станів. Для відстежування цих станів реалізовано кінцевий автомат. Укрупнену діаграму станів системи наведено на рис. 11.24.

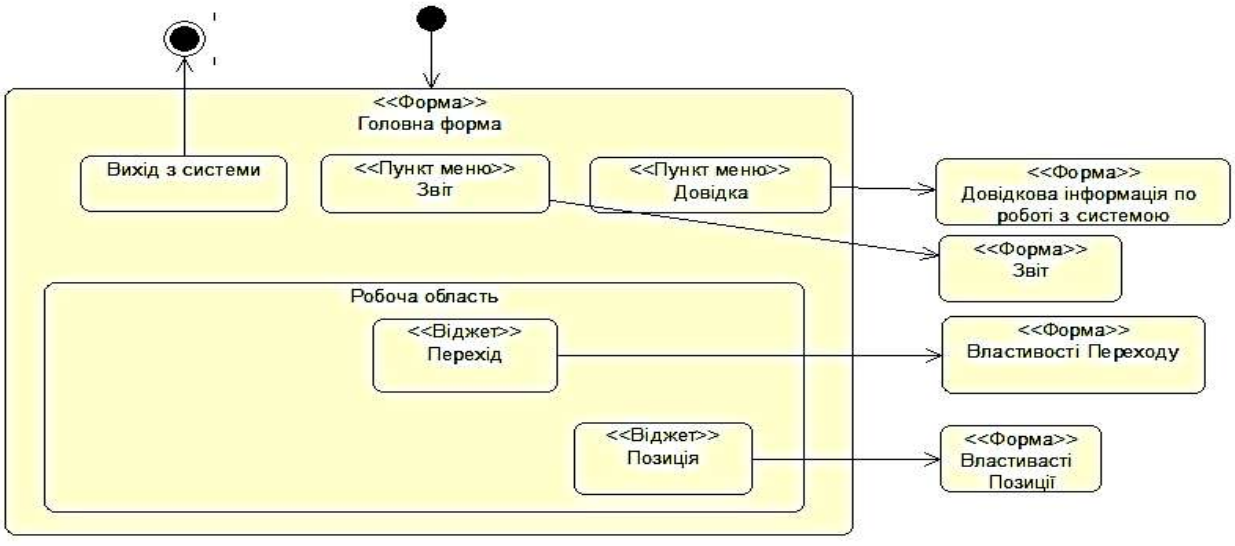


Рис. 11.24. **Діаграма станів елементів графічного інтерфейсу користувача**

У процесі запуску програми буде створено пусту модель і програма одразу після запуску дозволить її редагувати додаючи позиції та переходи

або завантажити збережену у файлі на диску і працювати з нею. Після запуску програми з'являється головне вікно програми як на рис. 11.25.

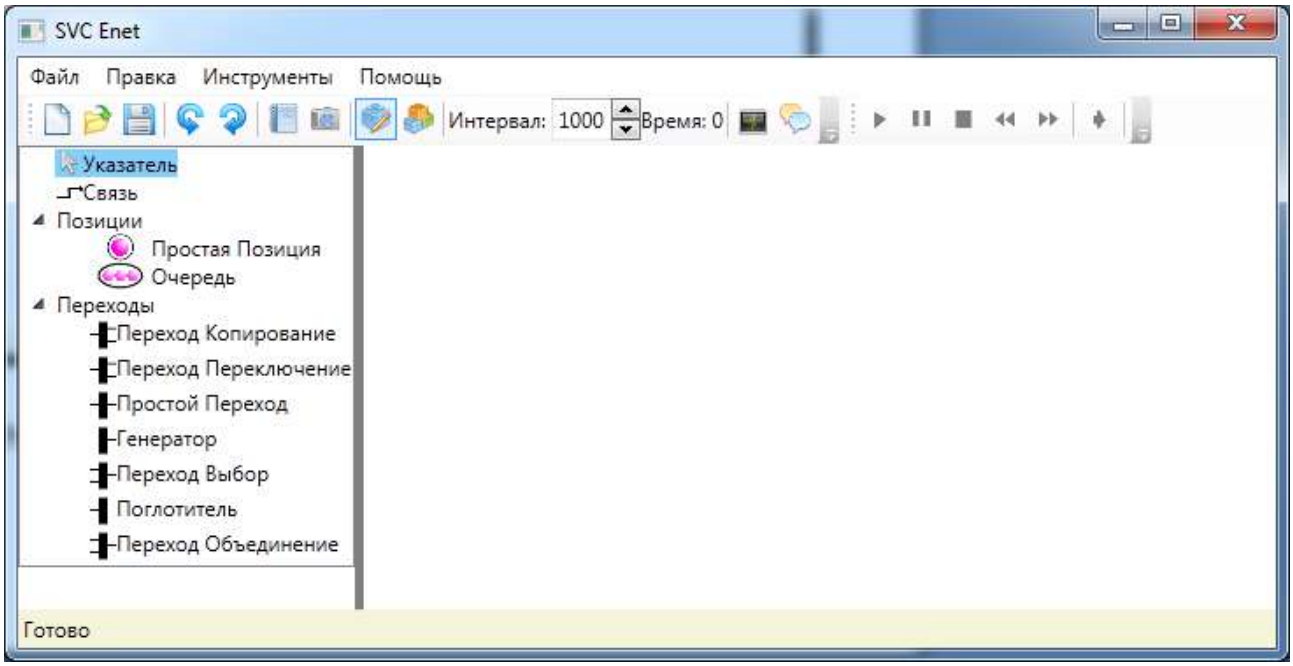


Рис. 11.25. **Головне вікно програми**

У центральній частині вікна знаходиться робоча область, яка позначена на рис. 11.26. На ній здійснюється побудова моделі.

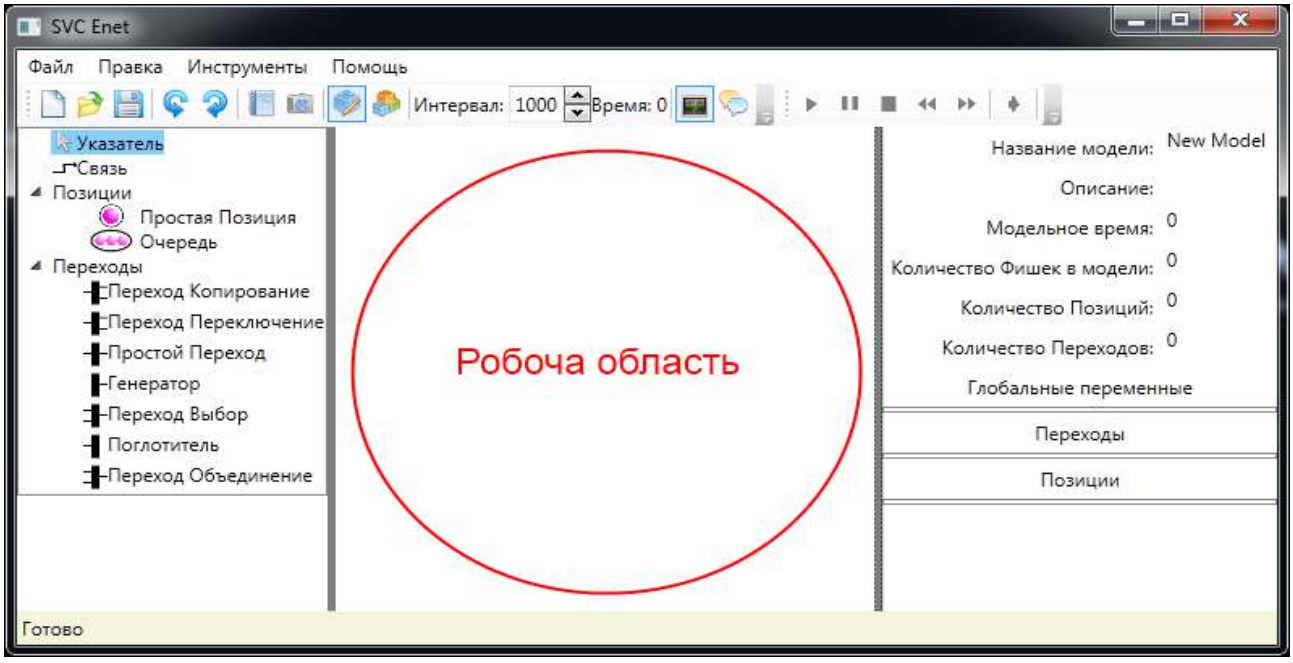


Рис. 11.26. **Робоча область програми**

У верхній частині вікна знаходиться головне меню та панель управління процесом імітації моделей, як на рис. 11.27.

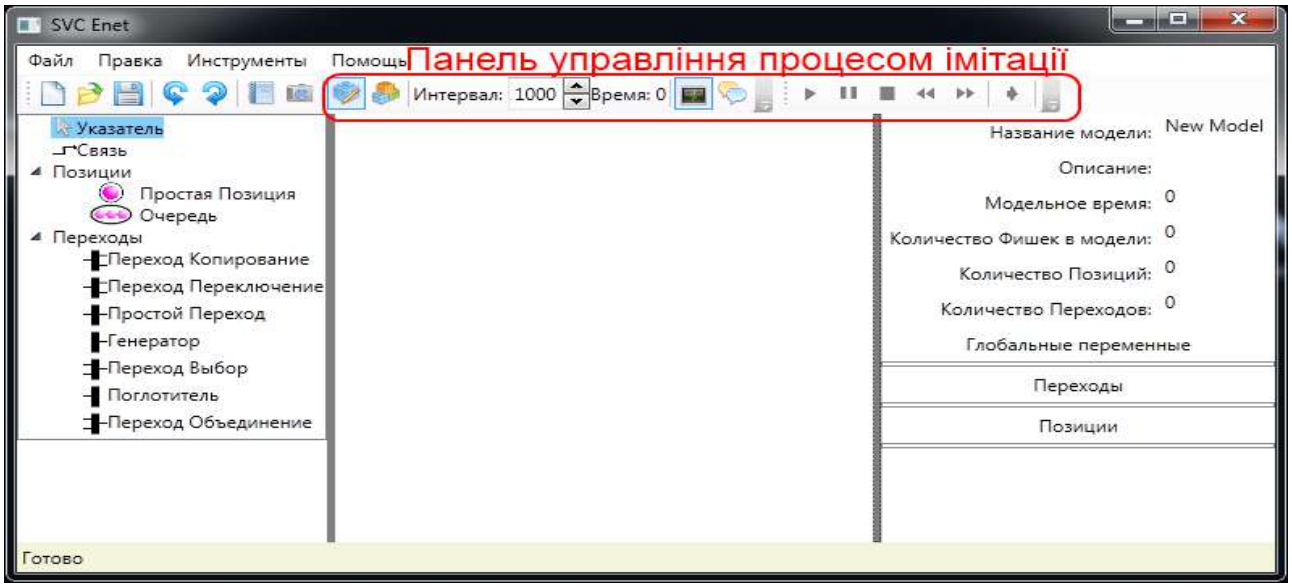


Рис. 11.27. **Панель управління режимом імітації**

У правій частині вікна знаходиться панель перегляду параметрів стану моделі, як на рис. 11.28. Ця панель дозволяє спостерігати за процесом імітації більш докладно.

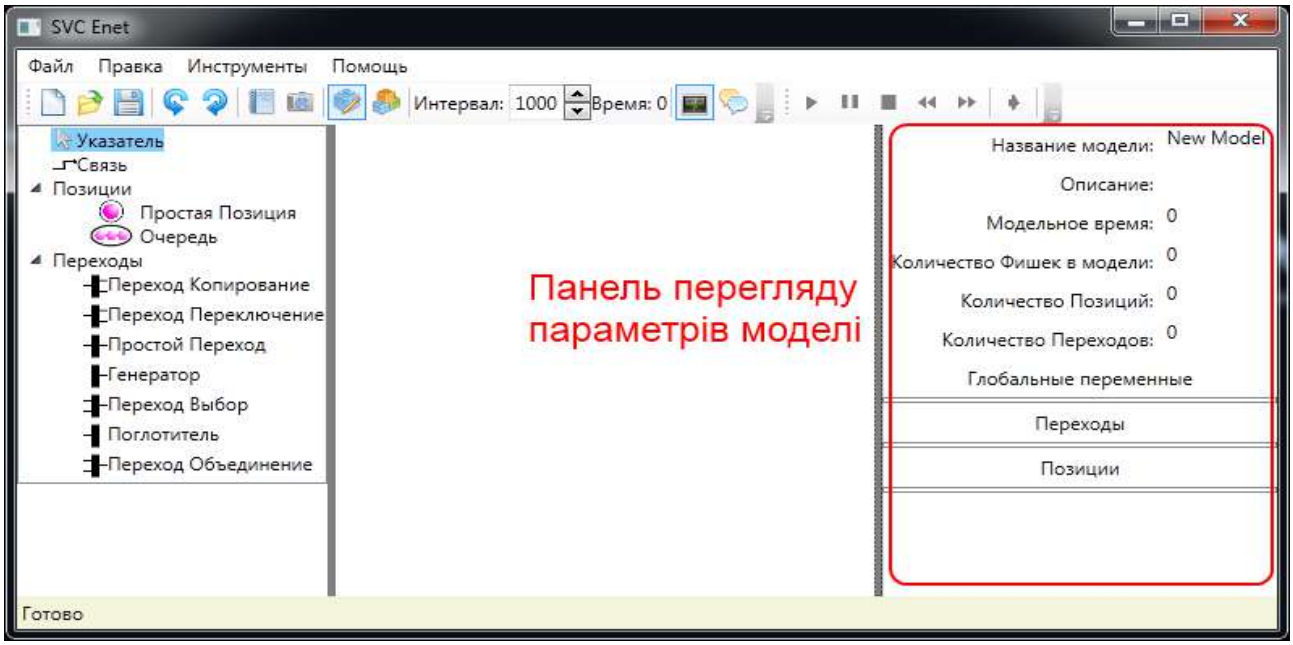


Рис. 11.28. **Панель перегляду параметрів моделі**

У лівій частині вікна знаходиться панель компонент, з яких можна будувати моделі. Панель компонент позначена на рис. 11.29.

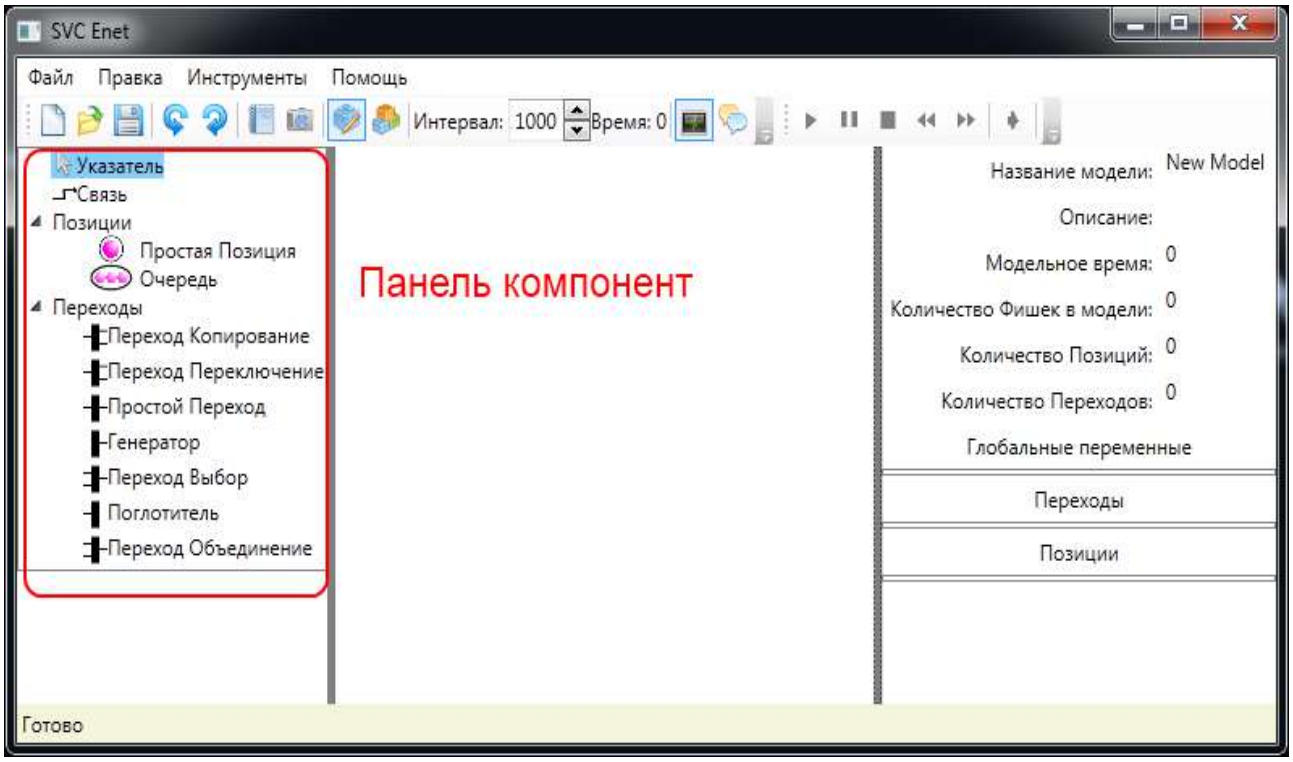


Рис. 11.29. **Панель компонент**

Для побудови моделі досліджуваної системи, насамперед, потрібно провести аналіз предметної області і побудувати укрупнену структуру моделі без використання спеціалізованих програмних засобів. Потім для побудові Е-мережі в редакторі потрібно на робочу частину помістити потрібні позиції та переходи. Для цього клацнути мишкою на назві потрібного елемента на панелі компонент та клацнути по робочій області редактора. Або натиснути ліву кнопку миші на назві потрібного елемента на панелі компонент і не відпускаючи її перемістити курсор на робочу область редактора і відпустити кнопку миші. В результаті виконаних дій вибраний віджет з’явиться на робочій області, рис. 11.30.

Процес побудови моделі складається з розміщення в робочій області програми необхідної кількості позицій та переходів, а також з’єднання всіх розміщених елементів в єдину Е-мережу. Для цього на панелі компонент потрібно вибрати пункт "Связь".

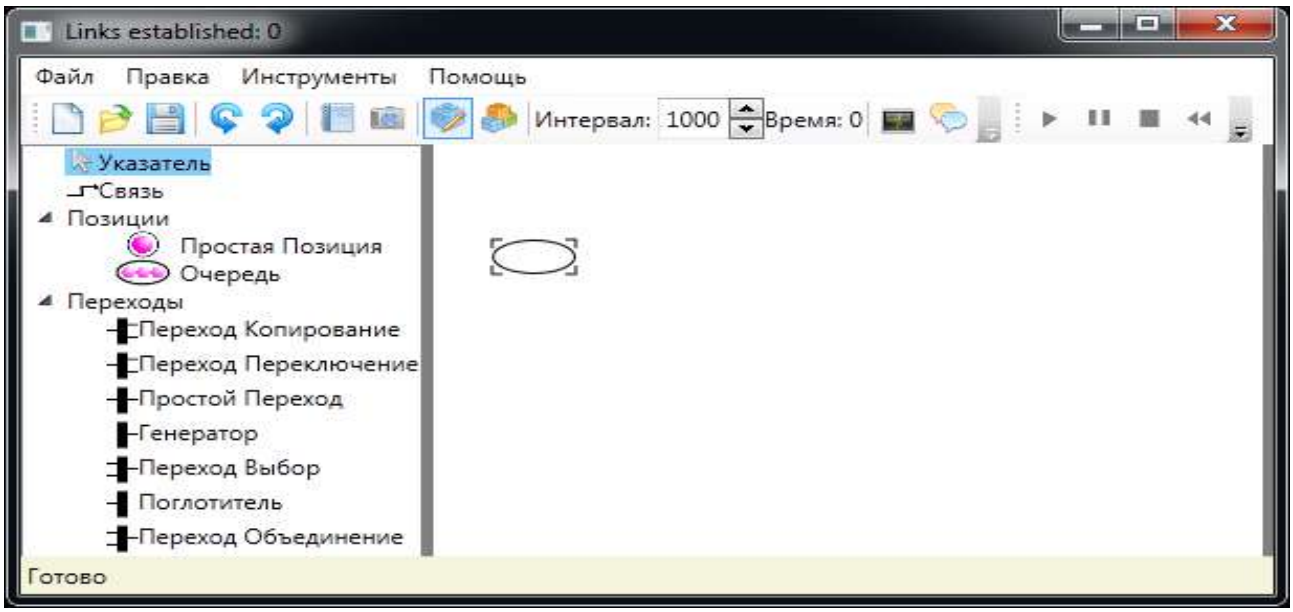


Рис. 11.30. **Додавання елементів Е-мережі**

Програма також дозволяє встановлювати та змінювати основні властивості позицій та переходів моделі. Для цього потрібно два рази клацнути по потрібному переходу чи позиції. Після подвійного кліку по елементу з'явиться вікно з його властивостями, деякі з яких можна редагувати, рис. 11.31 – 11.33.

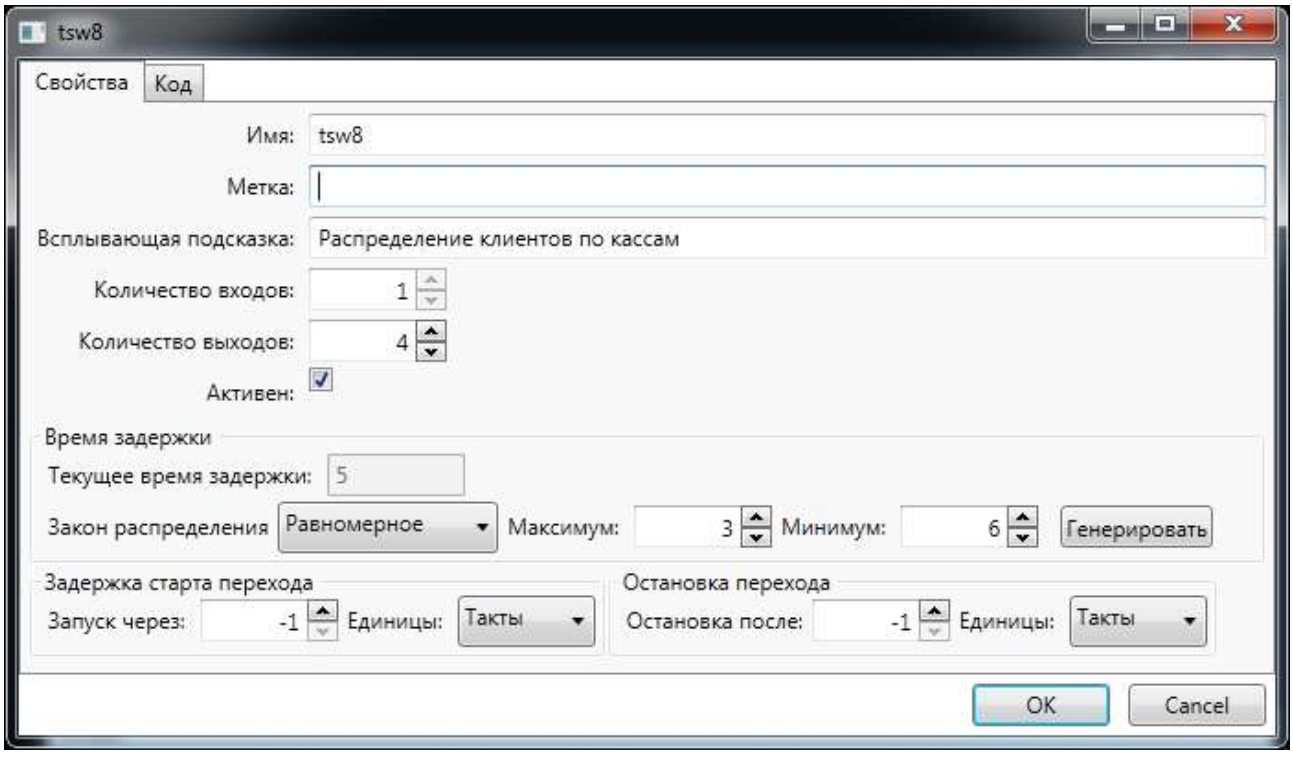


Рис. 11.31. **Вікно редагування властивостей переходу**

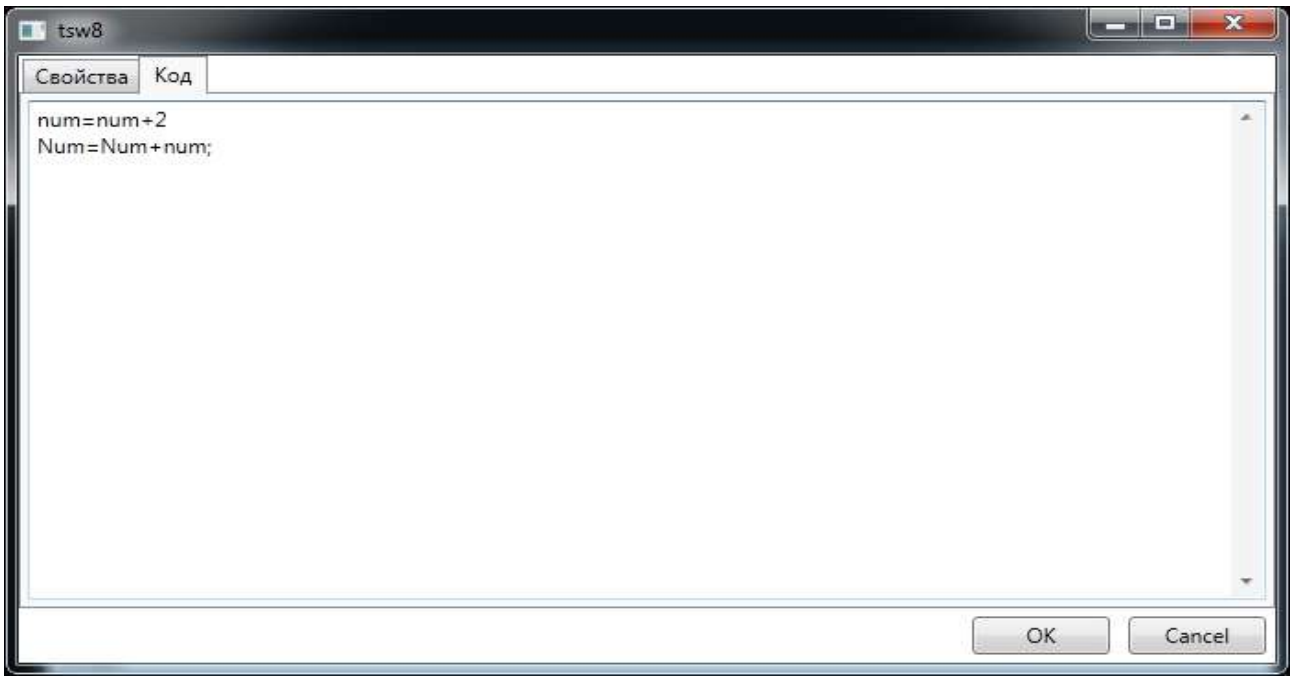


Рис. 11.32. **Вікно редагування функції переходу**

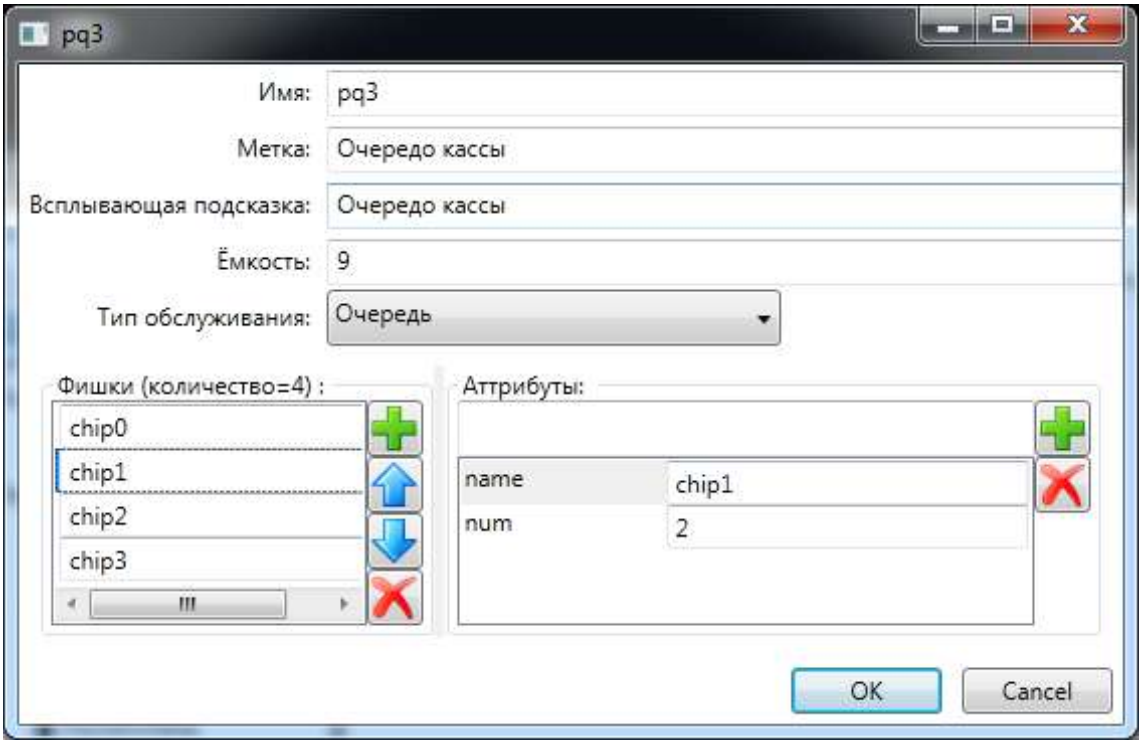


Рис. 11.33. **Вікно редагування властивостей позиції**

Також можна вручну додавати та вилучати Фішки з моделі та додавати, змінювати, видаляти їх атрибути на формах редагування властивостей Позиції.

Елементи для додавання, видалення, перегляду у виді списку, перемішування Фішок у відповідній Позиції показані на рис. 11.34.

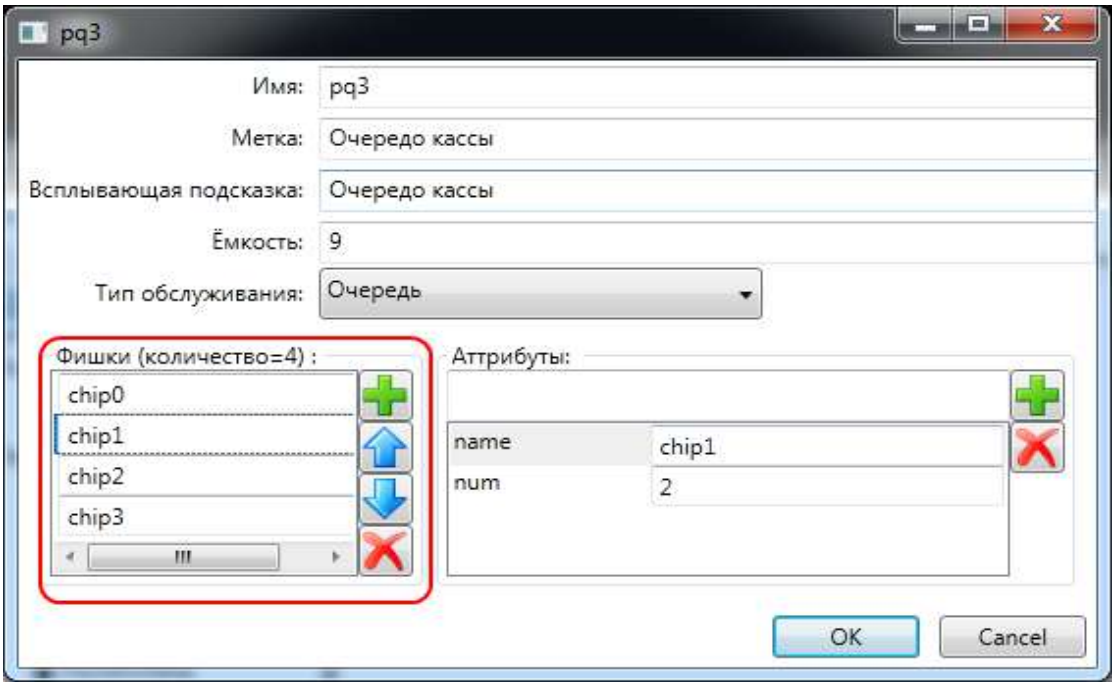


Рис. 11.34. **Елементи для виконання операцій з фішками**

Для додавання, редагування, видалення атрибутів вибраної фішки виконується за допомогою елементів, показаних на рис. 11.35.

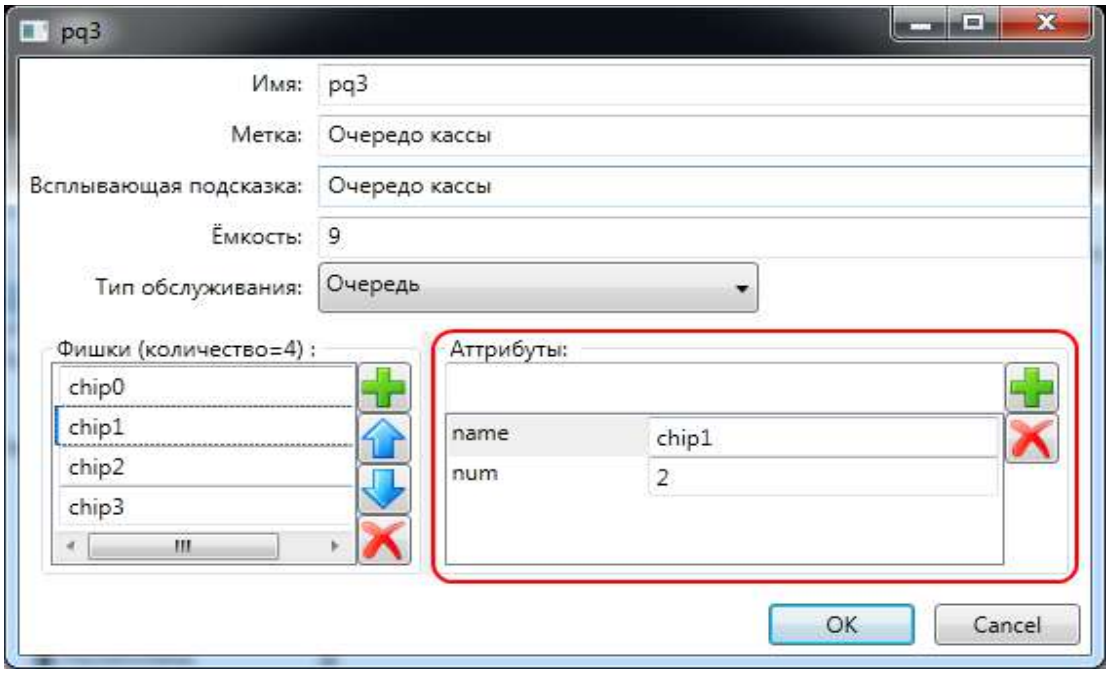


Рис. 11.35. **Елементи для виконання операцій з атрибутами фішок**

Також є можливість програмно змінювати атрибути фішок при переході їх через Переходи.

Для цього на формі властивостей потрібного Переходу на вкладці "Програма" потрібно у вигляді формул вказати, які атрибути і як потрібно змінювати.

Такі вирази повинні бути у форматі:

Імя_атрибуту = Параметр1 Операція Параметр2.

Такі вирази відділяються між собою крапкою з комою.

Регістр важливий, тобто атрибути з іменами "ПАРАМЕТР" і "параметр" – різні атрибути.

Якщо назва атрибуту починається з прописної літери, то це глобальний атрибут на рівні моделі і його остаточне значення буде роздруковане у звіт.

Якщо назва атрибуту починається з великої літери, то це атрибут поточної фішки.

У випадку, коли в розрахунках фігурує атрибут, який до цього не було ініціалізовано, то він автоматично створюється і ініціалізується нулем.

Параметрами можуть бути цілі числа, числа з плаваючою крапкою або атрибути.

Операція – це один з символів: ’+’, ’-’, ’*’, ’/’ і означає дію, яку потрібно виконати.

Встановити зв’язки між компонентами мережі можна вибравши відповідну опцію на панелі компонент, потім нажати ліву кнопку миші на потрібній позиції і не відпускаючи її перевести курсор миші на відповідний вхід потрібного переходу та відпустити кнопку миші.

У результаті цих дій до моделі додасться дуга від позиції до переходу.

Дуга від переходу до позиції додається аналогічно.

Приклад віджетів з’єднаних дугами наведено на рис. 11.36.

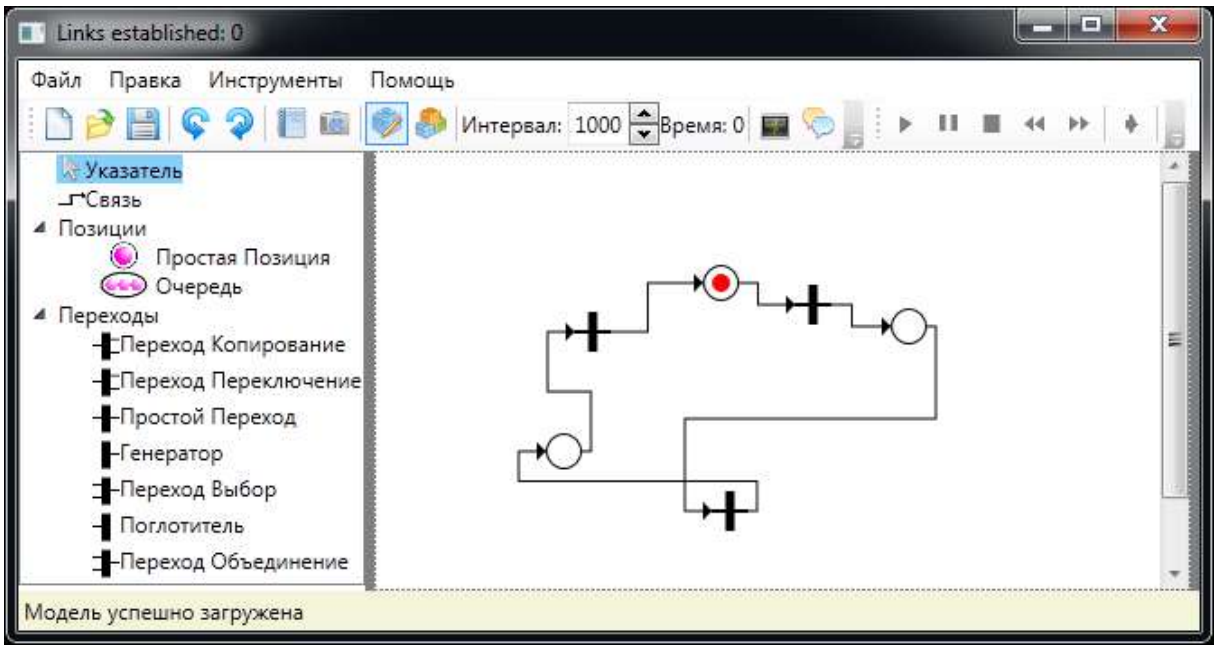


Рис. 11.36. **Приклад віджетів з’єднаних дугами**

Виділити віджети та/або дуги можна за допомогою миші, як показано на рис. 11.37.

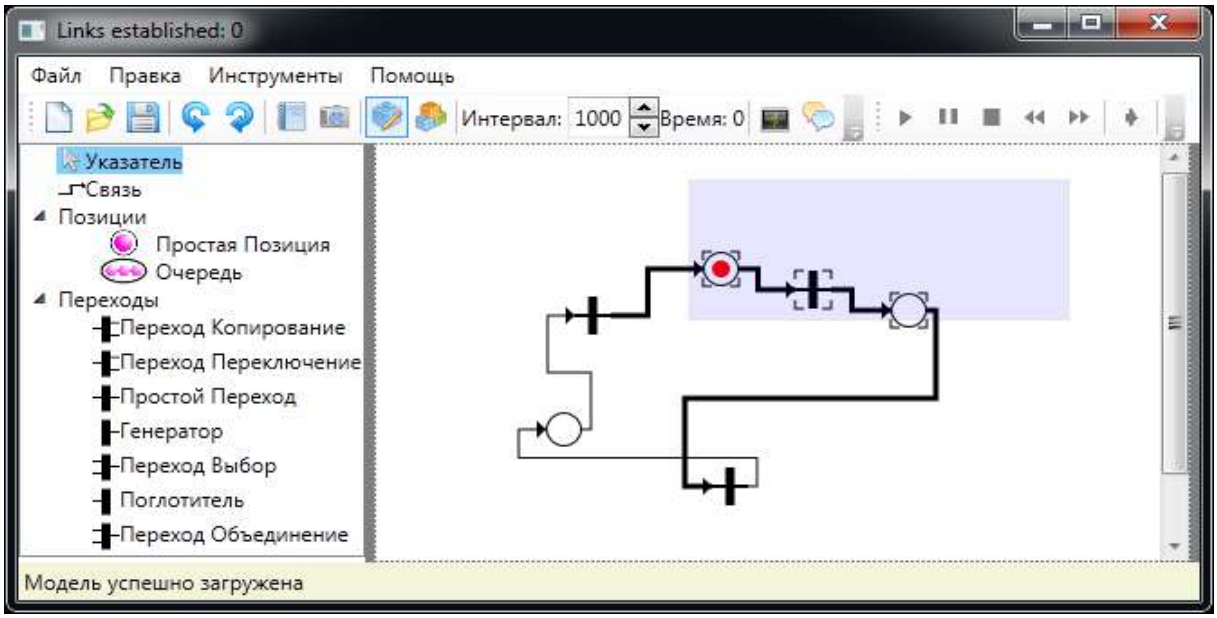


Рис. 11.37. **Виділення віджетів та дуг за допомогою миші**

Переміщення виділених віджетів по моделі відбувається за допомогою миші, як це показано на рис. 11.38.

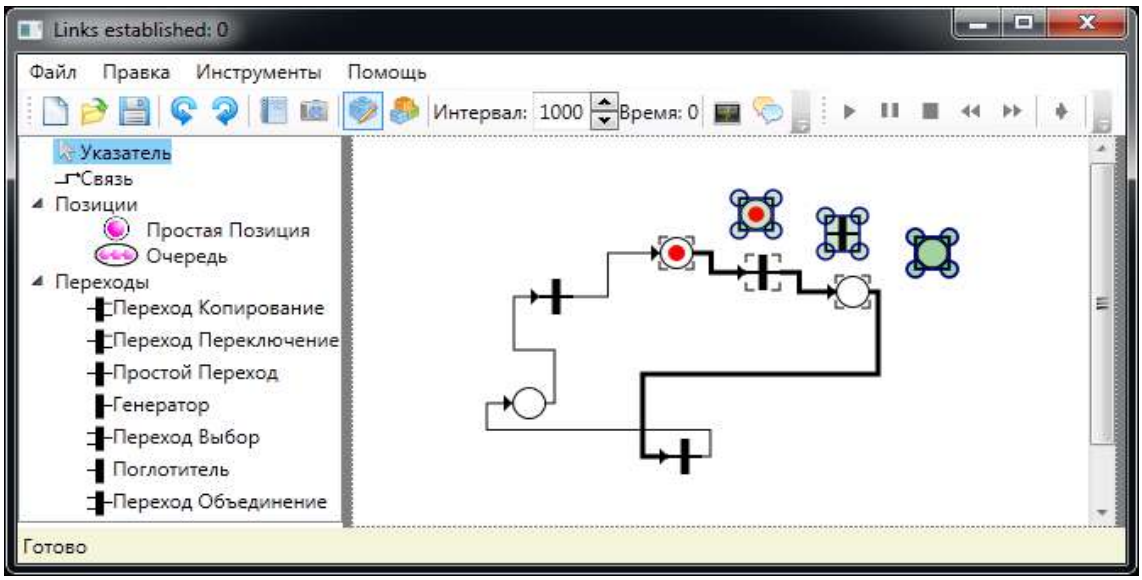


Рис. 11.38. **Переміщення віджетів**

Для того, щоб видалити віджет чи дугу, потрібно виділити їх та натиснути клавішу Delete.

Для збереження побудованої моделі потрібно в меню "Файл" вибрати підпункт "Зберегти як", або скористатися комбінацією клавіш Ctrl+C і вказати місце, куди потрібно зберегти модель, як на рис. 11.39.

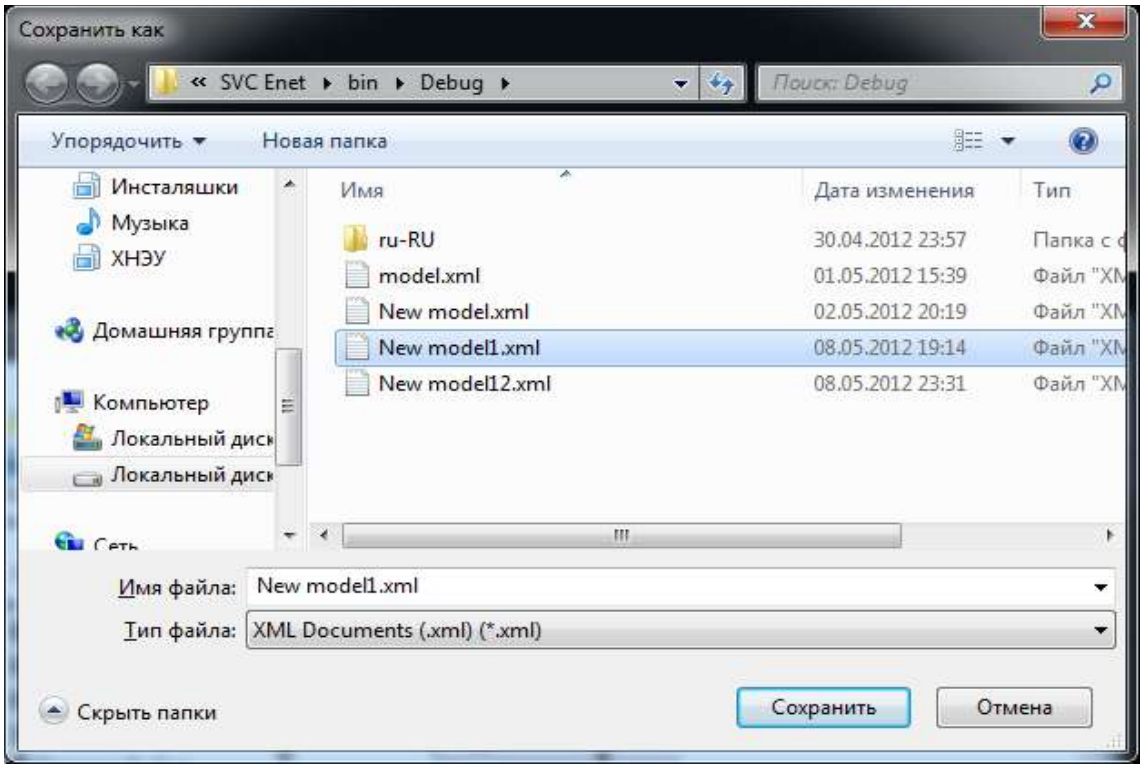


Рис. 11.39. **Вибір місця збереження моделі**

Для завантаження в програму збереженої моделі з файла вибрати пункт меню "Файл" підпункт "Відкрити" або скористатися комбінацією клавіш Ctrl+O і вказати файл, з якого потрібно завантажити модель, як на рис. 11.40.

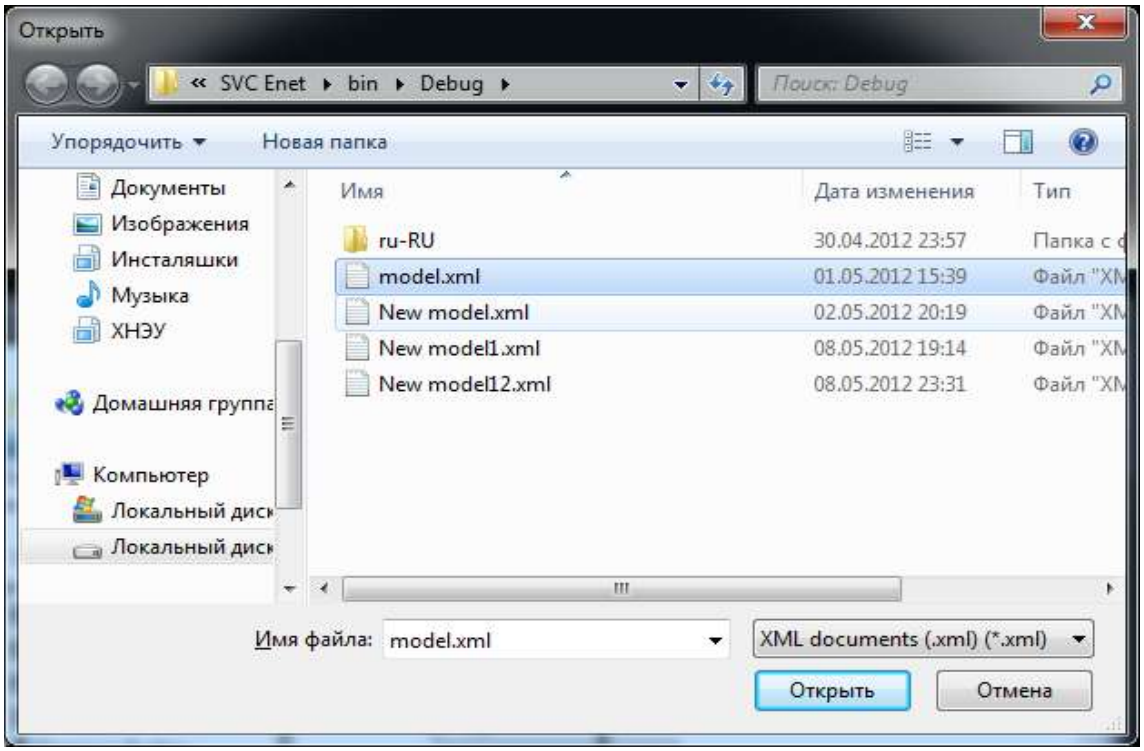


Рис. 11.40. **Вибір файла моделі**

Режим імітації дозволяє досліджувати побудовану та налаштовану модель в динаміці та робити відповідні висновки.

Перед запуском моделі можна налаштувати, скільки часу потрібно на один такт моделювання у полі "Інтервал" на панелі управління режимом імітації. Час вводиться в мілісекундах (тобто для того, щоб такти моделі відбувались через кожну секунду, інтервал в моделі повинен бути встановлено у 1000 одиниць).

Для того, щоб перейти в режим імітації, потрібно перевірити модель на відповідність стандартам побудови Е-мереж. Для цього потрібно вибрати в пункту меню "Інструменти" підпункт "Компілювати модель". Якщо модель побудована коректно, стане активним панель управлянням процесом імітації з можливостями запуску імітації, зупинки, покрокової імітації та кнопкою, за допомогою якої можна визвати панель перегляду глобальних параметрів у режимі реального часу.

Для запуску процесу імітації потрібно натиснути на кнопку "Старт" на панелі управління режимом імітації.

Для зупинки процесу імітації потрібно натиснути на кнопку "Стоп" на панелі управління режимом імітації.

Для паузи в процесі імітації потрібно натиснути на кнопку "Пауза" на панелі управління режимом імітації.

Для покрокового перегляду процесу імітації потрібно натискати на кнопку "Наступний крок" на панелі управління режимом імітації.

У процесі імітації в моделі будуть генеруватись фішки, переміщуватись по мережі, виводитись з мережі завдяки чому модель буде змінювати свої стани і буде мінятись маркування позицій, як наведено на рис. 11.41.

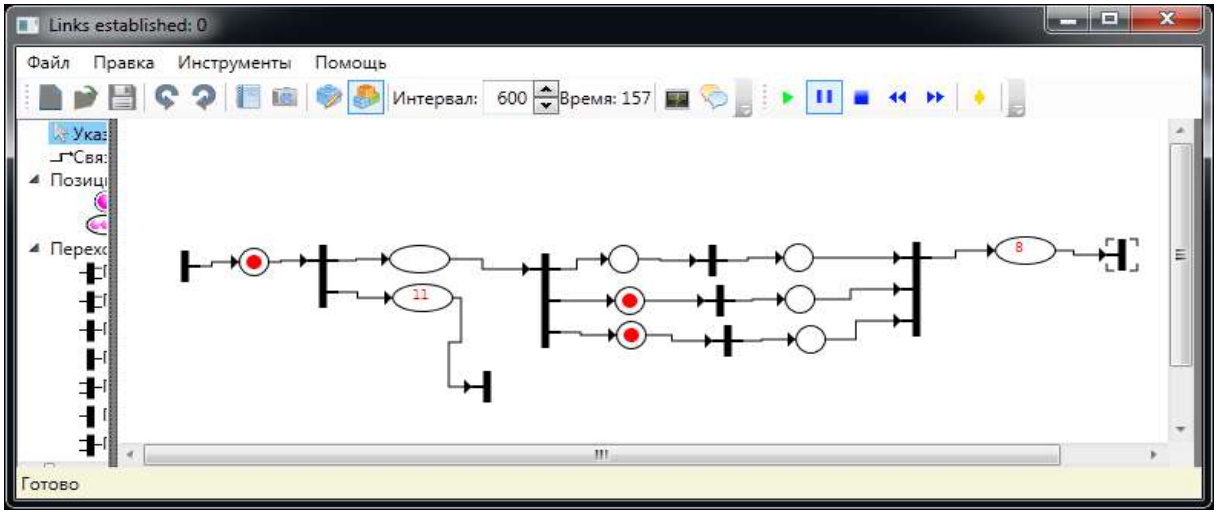


Рис. 11.41. **Процес імітації**

У полі "Час" на панелі управління режимом імітації відбивається час роботи моделі в тактах.

Після натискання на "Пауза", імітація призупиняється і після наступного запуску режиму імітації вона продовжується з того ж місця.

Якщо зупинити імітаційний режим кнопкою "Стоп", то режим імітації зупиниться і при подальшому запуску усі накопичені параметри обнуляться, тобто, процес імітації почнеться з самого початку.

Кнопка "Наступна ітерація" ініціює чергову ітерацію режиму імітації.

Розроблюваний редактор можна застосовувати для будування та дослідження процесів без прив’язки до конкретної предметної області.

За результатами моделювання можна будувати звіт. Для цього потрібно вибрати в пункту меню "Інструменти" підпункт "Генерувати звіт". Приклад такого звіту наведено на рис. 11.42.

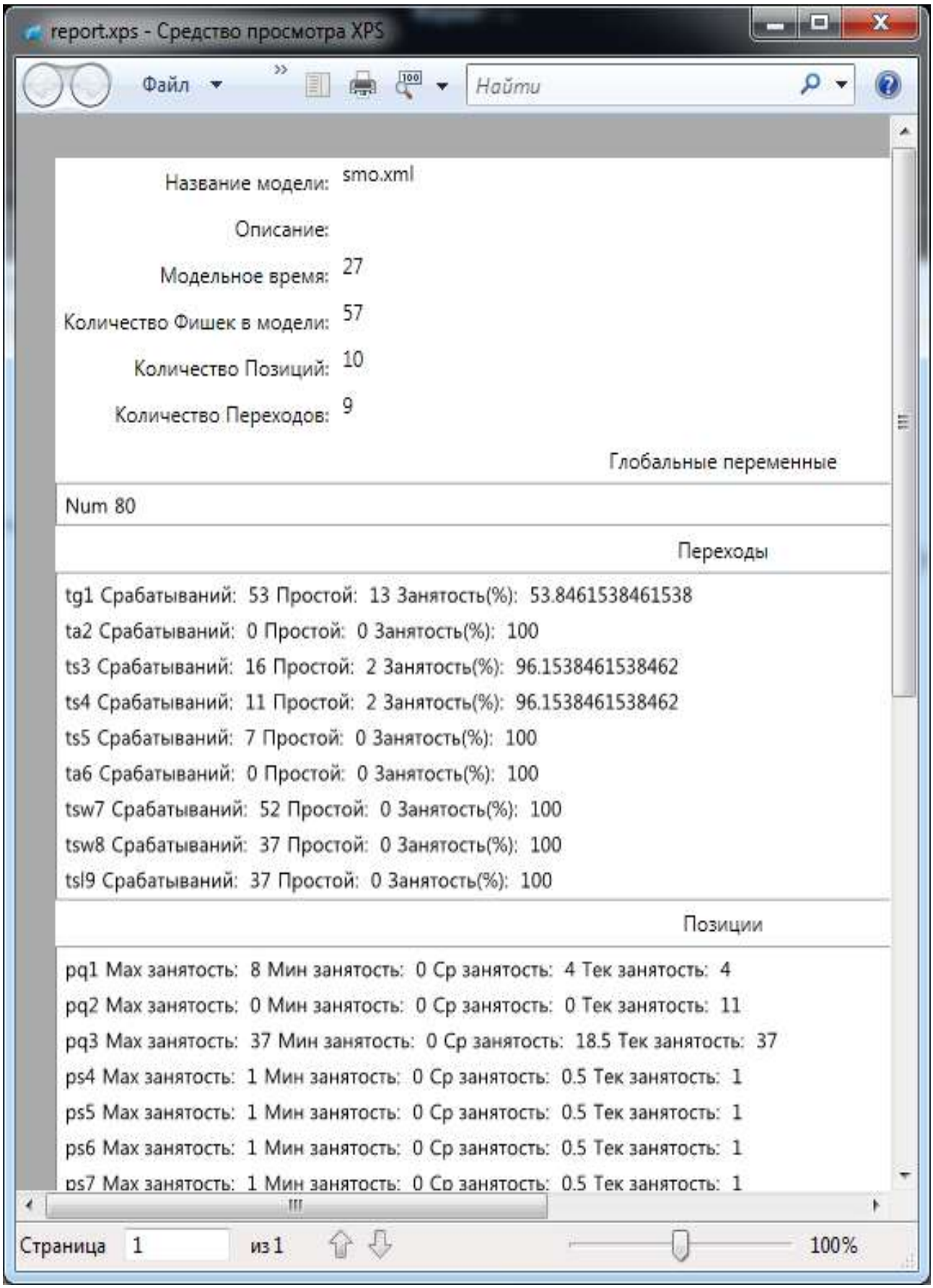


Рис. 11.42. **Звіт за результатами моделювання**

11.3. Розробка імітаційних моделей елементів навчального процесу вищого навчального закладу

Запропоновано декілька моделей різних елементів навчального процесу. Проведено дослідження моделей окремих видів занять, таких, як лабораторне заняття або самостійна робота студентів. Доведено можливість використання запропонованого підходу для побудови моделей процесу вивчення окремої навчальної дисципліни та навчального плану підготовки бакалаврів у цілому. Наведено окремі результати моделювання процесу адаптації студентів до системи навчання за курсом.

Навчальний процес – це поняття, яке охоплює всю навчальну діяльність вищого навчального закладу [27].

Він складається з безлічі компонентів: процесу навчання студента з конкретної спеціальності протягом п’яти років, семестрового навчального процесу на потоці, процесу вивчення дисципліни, процесу контролю знань студента.

Вищий навчальний заклад має жорсткий надлишковий набір ресурсів, який дозволяє реалізувати навчальний процес у будь-якій його інтерпретації.

Однак такий фіксований набір призводить до витрат планування проведення процесу навчання.

Тому модель навчального процесу має набір більш гнучких властивостей, таких, як неприв’язаність до місця і до часу.

Вищий навчальний заклад здійснює педагогічну діяльність відповідно до встановлених стандартів.

Нормативні документи регламентують такі види аудиторних занять у ВНЗ: лекції, семінари, практичні заняття, лабораторні роботи, контрольні роботи [187], а також позааудиторні – самостійна робота студентів.

Умовно можна розділити всі види занять на два типи: теоретичні та практичні.

Лекція – одна з форм організації навчання. Її основою є системне усне викладання викладачем навчального матеріалу, головний зміст якого становлять аналіз та узагальнення фактів, а провідними прийомами є пояснення і міркування.

Залежно від теми лекції в ній можуть переважати характеристика, опис, розповідь про певні факти, процеси, явища [170].

Лабораторне (практичне) заняття – одна з основних форм організації навчального процесу, яка полягає у виконанні студентами під керівництвом викладача комплексу навчальних завдань з метою засвоєння науково-теоретичних основ навчального предмета, набуття навичок і досвіду творчої діяльності, оволодіння сучасними методами практичної роботи із застосуванням технічних засобів [402].

Провідною дидактичною метою практичних занять є формування практичних умінь – професійних (умінь виконувати певні дії, операції, необхідні в подальшому у професійній діяльності) або навчальних, необхідних у подальшій навчальній діяльності по загальнопрофесійних і спеціальних дисциплін.

Під самостійною роботою розуміється навчальна діяльність студента, яка планується, виконується за завданням під методичним керівництвом і контролем викладача, але без його прямої участі [111; 180].

Слід розглянути Е-мережу, яка моделює виконання та перевірку самостійних робіт студентів (рис. 11.43), як одну із складових навчального процесу.

Досить актуальними на сьогодні є питання дослідження ефективності самостійної роботи студентів, а особливо недостатня наукова обґрунтованість нормативів часу на самостійну роботу студентів, слабкий облік реальних умов протікання навчального процесу, необхідність визначення динаміки фактичних витрат часу на самостійну роботу студентів [180; 241; 275].

Імітаційна модель організації та проведення самостійної роботи студентів дозволяє оцінити фактичні затрати часу на даний вид роботи студента і викладача [275].

При цьому алгоритм перевірки результатів роботи полягає у виконанні таких паралельних дій: перевірки власного рішення, перевірки самостійності рішення, перевірки оформлення звіту.

Приступати до наступного етапу перевірки рішення має сенс тільки тоді, якщо попередній етап був виконаний тією чи іншою мірою правильно.

При цьому існують випадки, коли етап перевірки вважається пройденим успішно і здійснюється перехід до наступного етапу, етап перевірки провалений, і весь звіт відхиляється.

Завдання в цілому приймається, якщо рішення виявилося правильним, самостійним і правильно оформленим.

Переходи моделі (рис. 11.43):

T1 – завдання розробляються викладачем;

T2 – завдання видаються студенту;

T3 – студент не отримав завдання;

T4 – виконання завдання студентом;

T5 – студент не виконав завдання;

T6 – завдання здано викладачу на перевірку;

T7 – перевірка рішення;

T8 – перевірка самостійності виконання завдання;

T9 – перевірка оформлення звіту;

T10 – викладач приймає правильно виконане завдання;

T11 – викладач не приймає виконане завдання;

T12 – студент переробляє завдання;

T13 – перевірка переробленого завдання викладачем;

T14 – виставлення незадовільної оцінки за виконане завдання;

T15 – виставлення задовільної оцінки за виконане завдання;

T16 – завдання приймається викладачем.

Позиції моделі (рис. 11.43):

Q1 – сукупність завдань розглянутого навчального періоду;

Q2 – студенту видано завдання;

Q3 – колектор невиданих за навчальний період завдань;

S4 – студент виконав завдання;

Q5 – завдання, які не зміг виконати студент;

Q6 – викладач починає перевірку рішення;

Q7 – викладач починає перевірку самостійності виконання завдання;

Q8 – викладач починає перевірку оформлення звіту;

S9 – рішення завдання правильне;

S10 – рішення завдання не правильне;

S11 – завдання виконано самостійно;

S12 – завдання виконано не самостійно;

S13 – звіт оформлений правильно;

S14 – звіт оформлений не правильно;

S15 – завдання прийнято;

S16 – завдання не прийнято і повернене на доопрацювання;

Q17 – студент переробив завдання;

Q18 – студент не переробив завдання

S19 – завдання перевірене;

S20 – оцінка виставлена.

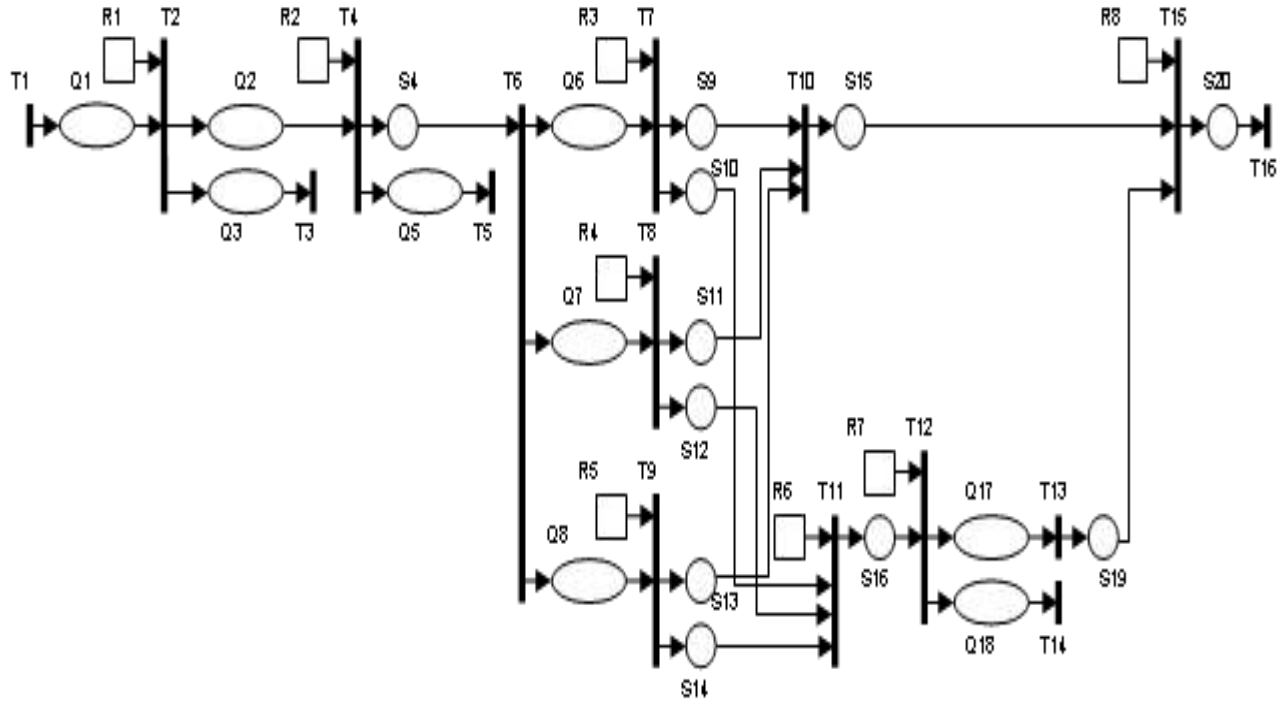


Рис. 11.43. **Е-мережа, яка моделює виконання та перевірку самостійних робіт студентів**

Розглянута модель дозволяє розрахувати фактичні витрати часу на самостійну роботу з вирішення завдань по дисциплінах і за різними темами всередині дисциплін [275]. Ці розрахунки можуть бути використані для виявлення найбільш трудомістких розділів курсу, виявлення характеру перевантаження і перерозподілу часу з урахуванням взаємного впливу предметів.

Слід розглянути Е-мережу, яка моделює виконання та перевірку лабораторних робіт студентів (рис. 11.44).

Імітаційна модель виконання та перевірки лабораторних робіт студентів дозволяє оцінити фактичні затрати часу на даний вид роботи студента і викладача [275].

При цьому алгоритм перевірки результатів роботи полягає у виконанні таких паралельних дій: перевірки правильності виконання лабораторної роботи та захисту студентом виконаної лабораторної роботи.

Приступати до наступного етапу роботи моделі має сенс тільки тоді, якщо попередній етап був виконаний тією чи іншою мірою правильно.

При цьому існують випадки, коли етап перевірки правильності виконання лабораторної роботи вважається пройденим успішно і здійснюється перехід до наступного етапу, коли етап перевірки провалений, і весь звіт відхиляється.

Так само і стосовно захисту студентом виконаної лабораторної роботи: коли етап вважається пройденим успішно – здійснюється перехід до наступного етапу, коли етап перевірки провалений – весь звіт відхиляється. Лабораторна робота в цілому приймається, якщо рішення виявилося правильним та робота захищена студентом.

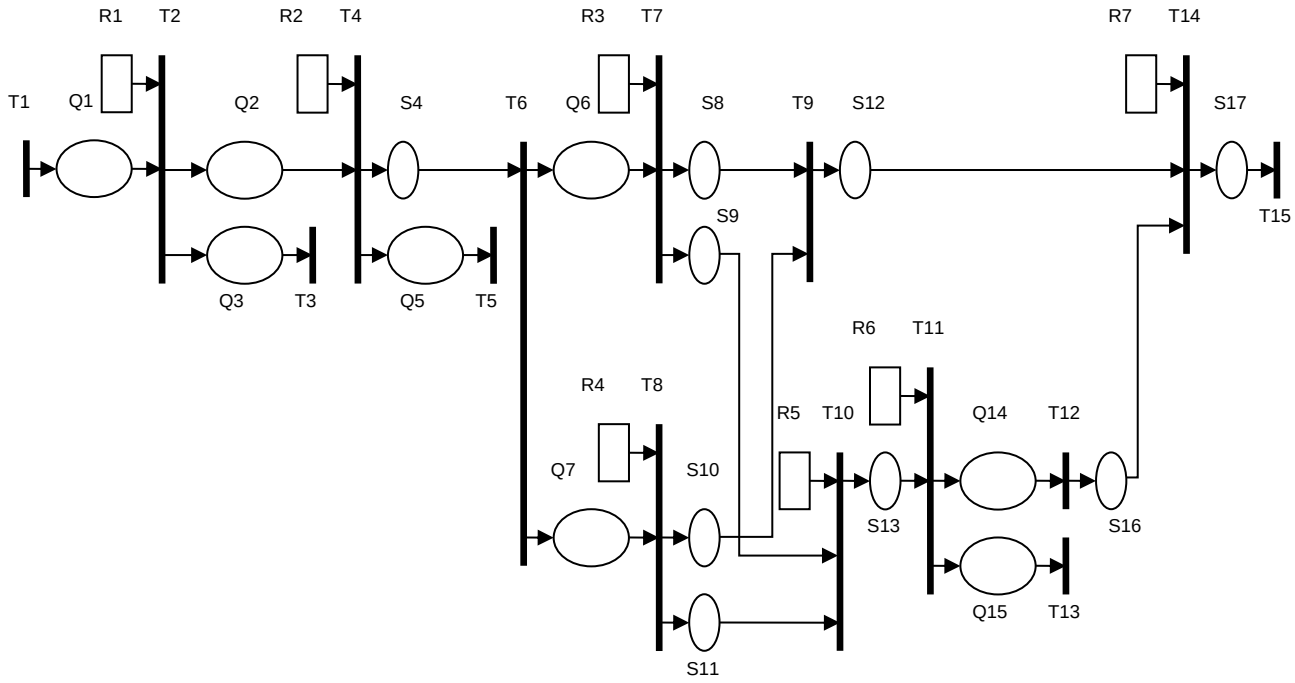


Рис. 11.44. **Е-мережа, яка моделює виконання та перевірку лабораторних робіт студентів**

Переходи моделі (рис. 11.44):

T1 – завдання з лабораторних робіт розробляються викладачем;

T2 – лабораторна робота видається студенту;

T3 – студент не отримав завдання з лабораторної роботи;

T4 – виконання лабораторної роботи студентом;

T5 – студент не виконав лабораторну роботу;

T6 – виконані лабораторні роботи віддані викладачу на перевірку;

T7 – перевірка правильності виконання лабораторної роботи;

T8 – захищення студентом виконаної лабораторної роботи;

T9 – викладач приймає правильно виконану та захищену лабораторну роботу;

T10 – викладач не приймає виконану лабораторну роботу;

T11 – студент переробляє лабораторну роботу;

T12 – перевірка перероблених лабораторних робіт викладачем;

T13 – виставлення незадовільної оцінки за виконану лабораторну роботу;

T14 – виставлення задовільної оцінки за виконану лабораторну роботу;

T15 – робота приймається викладачем.

Позиції моделі (рис. 11.44):

Q1 – сукупність завдання з лабораторних робіт розглянутого навчального періоду;

Q2 – студенту видана лабораторна робота;

Q3 – колектор невиданих за навчальний період лабораторних робіт;

S4 – студент виконав лабораторну роботу;

Q5 – лабораторні роботи, які не зміг виконати студент;

Q6 – викладач починає перевірку правильності виконання лабораторної роботи;

Q7 – студент допускається до захисту лабораторної роботи;

S8 – лабораторна робота виконана правильно;

S9 – лабораторна робота виконана не правильно;

S10 – лабораторна робота захищена студентом;

S11 – лабораторна робота не захищена студентом;

S12 – лабораторна робота виконана правильно та захищена студентом;

S13 – студент відправляється на доопрацювання лабораторної роботи;

Q14 – студент переробив лабораторну роботу;

Q15 – студент не переробив лабораторну роботу;

S16 – перевірені викладачем перероблені лабораторні роботи;

S17 – оцінка виставлена.

Слід розглянути Е-мережу, яка моделює викладання студентам навчальної дисципліни (рис. 11.45).

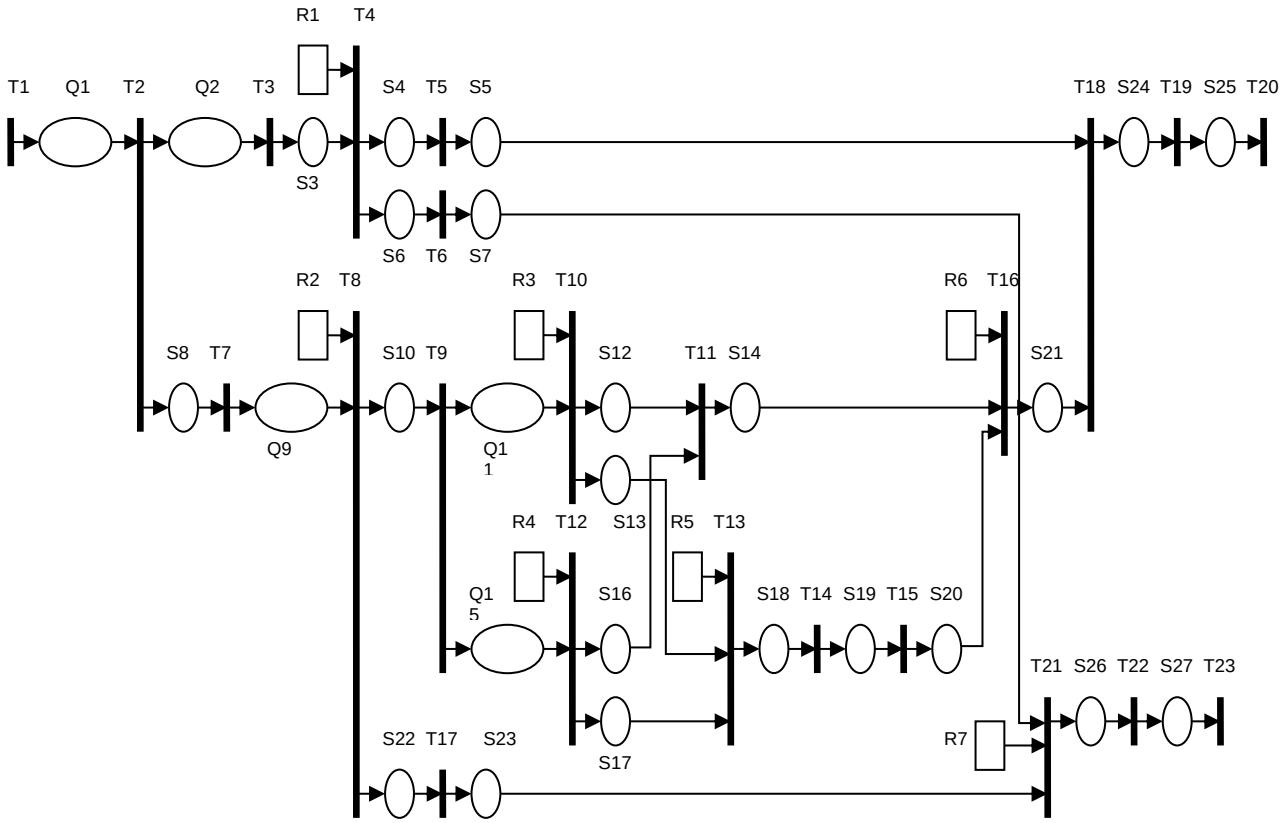


Рис. 11.45. **Е-мережа, яка моделює викладання студентам навчальної дисципліни**

Переходи моделі (рис. 11.45):

T1 – початок викладання навчальної дисципліни;

T2 – початок лекційних та лабораторних занять;

T3 – проведення лекційних занять;

T4 – модульний контроль студентів з теоретичної частини;

T5 – отримання задовільної оцінки за теоретичну частину;

T6 – отримання незадовільної оцінки за теоретичну частину;

T7 – студенту видаються завдання з лабораторних робіт;

T8 – виконання студентом лабораторних робіт;

T9 – початок перевірки викладачем виконаних лабораторних робіт;

T10 – перевірка викладачем правильності виконання лабораторних робіт;

T11 – отримання задовільної оцінки за лабораторні роботи;

T12 – студент захищає виконані лабораторні роботи;

T13 – студент відправлений на доопрацювання лабораторних робіт;

T14 – перевірка лабораторних робіт, які студент доопрацював;

T15 – отримання задовільної оцінки за лабораторні роботи;

T16 – отримання задовільної оцінки за практичну частину;

T17 – отримання незадовільної оцінки за практичну частину;

T18 – отримання задовільної оцінки за дисципліну;

T19 – закінчення вивчення навчальної дисципліни;
T20 – студент "закрив" дисципліну;
T21 – отримання незадовільної оцінки за навчальну дисципліну;
T22 – відправлення студента на перездачу;
T23 – студент не "закрив" дисципліну.

Позиції моделі (рис. 11.45):

Q1 – сукупність студентів розглянутого навчального періоду;
Q2 – відвідання лекційних занять студентами;
S3 – курс лекційних занять закінчено;
S4 – студент склав модульний контроль з теоретичної частини;
S5 – студент отримав оцінку за теоретичну частину;
S6 – студент не склав модульний контроль з теоретичної частини;
S7 – студент отримав незадовільну оцінку за теоретичну частину;
S8 – відвідання лабораторних занять студентами;
Q9 – студенту видано завдання;
S10 – студент виконав лабораторні роботи;
Q11 – студенти, які здали лабораторні роботи на перевірку;
S12 – лабораторні роботи виконані правильно;
S13 – лабораторні роботи виконані не правильно;
S14 – оцінки за лабораторні роботи отримані;
Q15 – студенти, які допущені до захисту лабораторних робіт;
S16 – студент захистив лабораторні роботи;
S17 – студент не захистив лабораторні роботи;
S18 – студент доопрацював лабораторні роботи;
S19 – лабораторні роботи перевірені;
S20 – оцінка виставлена;
S21 – студент отримав оцінку за практичну частину;
S22 – студент не виконав лабораторні роботи;
S23 – студент отримав незадовільну оцінку за практичну частину;
S24 – студент отримав задовільну оцінку за навчальну дисципліну;
S25 – студент "закрив" дисципліну;
S26 – студент отримав незадовільну оцінку за навчальну дисципліну;
S27 – студент відправлений на перездачу.

Варто розглянути Е-мережу, яка моделює навчання студента у вищому навчальному закладі протягом чотирьох років (рис. 11.46).

Переходи моделі (рис. 11.46):

T1 – прихід абітурієнтів, які поступили до університету;
T2 – початок навчання на першому курсі;
T3 – навчання студентів протягом розглянутого навчального періоду;
T4 – допущення студентів до складання сесій;
T5 – складання студентами сесій;
T6 – отримання оцінок за всі навчальні дисципліни;

T7 – закриття сесій на перездачі;

T8 – отримання оцінок за всі навчальні дисципліни;

T9 – написання дипломної роботи студентами;

T10 – захист дипломної роботи;

T11 – участь студента в олімпіадах;

T12 – отримання призового місця на олімпіадах;

T13, T14, T15, T18, T19, T20, T23, T24, T25, T27, T28 – допоміжні переходи;

T16 – навчання на курсах Microsoft IT Academy;

T17 – складання сертифікаційного екзамену Microsoft;

T21 – участь у конкурсі Imaging Cup;

T22 – отримання призового місця на конкурсі;

T26 – участь студентів у конференціях;

T29 – отримання диплому;

T30 – отримання кваліфікованих спеціалістів.

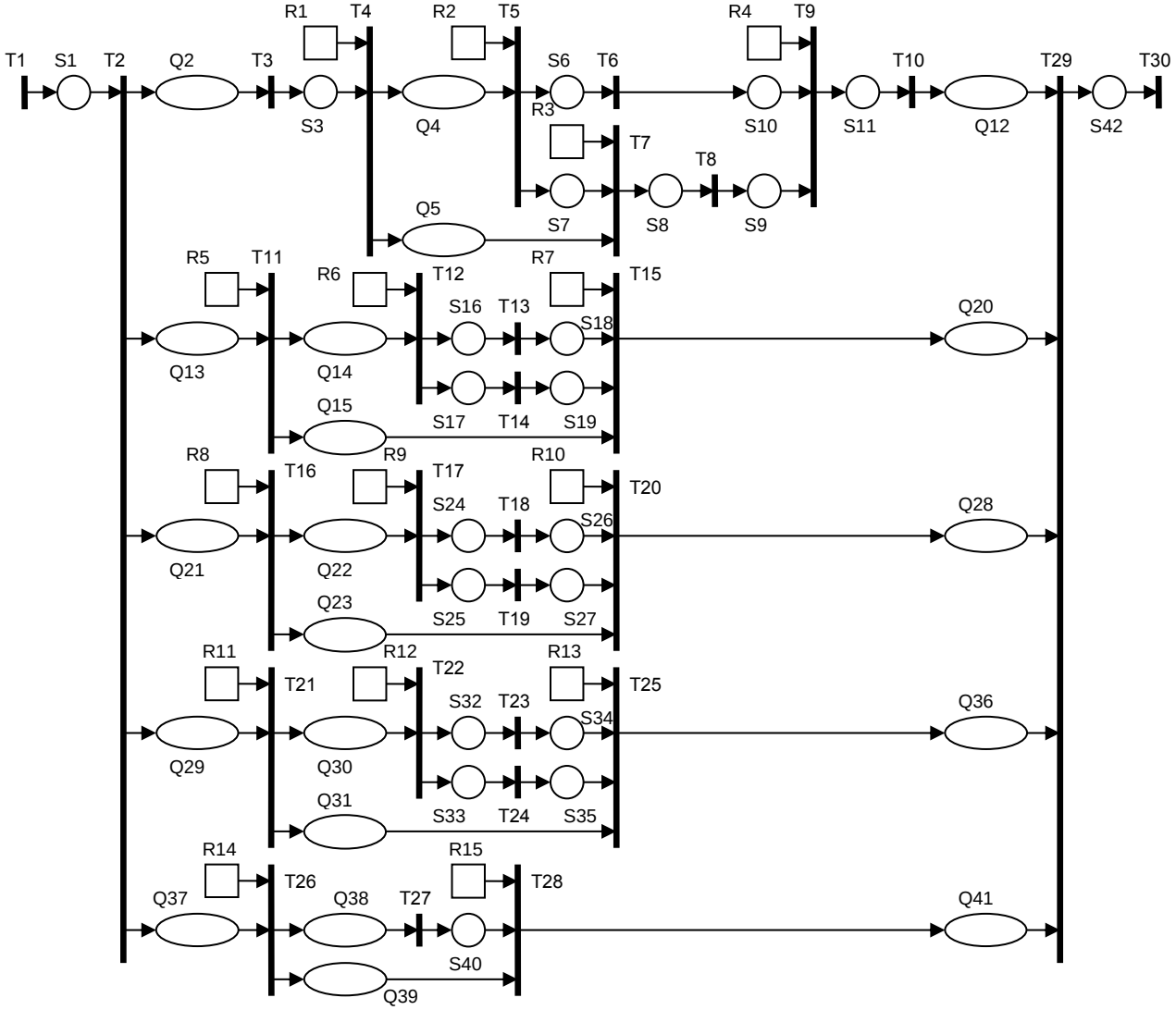


Рис. 11.46. **Е-мережа спрощеного виду, яка моделює навчання студента у вищому навчальному закладі протягом чотирьох років**

Позиції моделі (рис. 11.46):

S1 – сукупність студентів розглянутого навчального періоду;

Q2 – студенти, які почали навчання;

S3 – студенти, які пройшли навчання;

Q4 – студенти, які допущені до складання сесій;

Q5 – студенти, які не допущені до складання сесій;

S6 – студенти, які "закрили" сесії;

S7 – студенти, які не "закрили" сесії;

S8 – студенти, які "закрили" сесії на перездачі;

S9 – студенти, які отримали оцінки за всі навчальні дисципліни;

S10 – студенти, які отримали оцінки за всі навчальні дисципліни;

S11 – студенти, які написали дипломну роботу;

Q12 – студенти, які захистили дипломну роботу;

Q13 – студенти, які почали навчання;

Q14 – студенти, які брали участь в олімпіадах;

Q15 – студенти, які не брали участі в олімпіадах;

S16 – студенти, які отримали призове місце на олімпіадах;

S17 – студенти, які не отримали призового місця на олімпіадах;

S18, S19, Q20, S26, S27, Q28, S34, S35, Q36, S40, Q41 – допоміжні позиції;

Q21 – студенти, які почали навчання;

Q22 – студенти, які проходили навчання на курсах Microsoft IT Academy;

Q23 – студенти, які не проходили навчання на курсах Microsoft IT Academy;

S24 – студенти, які склали сертифікаційний екзамен Microsoft;

S25 – студенти, які не склали сертифікаційний екзамен Microsoft;

Q29 – студенти, які почали навчання;

Q30 – студенти, які брали участь в конкурсі;

Q31 – студенти, які не брали участі в конкурсі;

S32 – студенти, які отримали призове місце на конкурсі;

S33 – студенти, які не отримали призового місця на конкурсі;

Q37 – студенти, які почали навчання;

Q38 – студенти, які брали участь у конференціях;

Q39 – студенти, які брали участь у конференціях;

S42 – студенти, які отримали диплом.

Отримані в результаті моделі, можуть бути швидко модифіковані, що дозволяє використовувати їх для досліджування різних елементів навчального процесу і це є значною перевагою використання математичного апарату Е-мереж.

Аналіз результатів побудови моделей було проведено в програмі імітаційного моделювання на основі математичного апарату Е-мереж SVC Enet.

Слід розглянути реалізацію моделі організації та проведення самостійної роботи студентів (рис. 11.47).

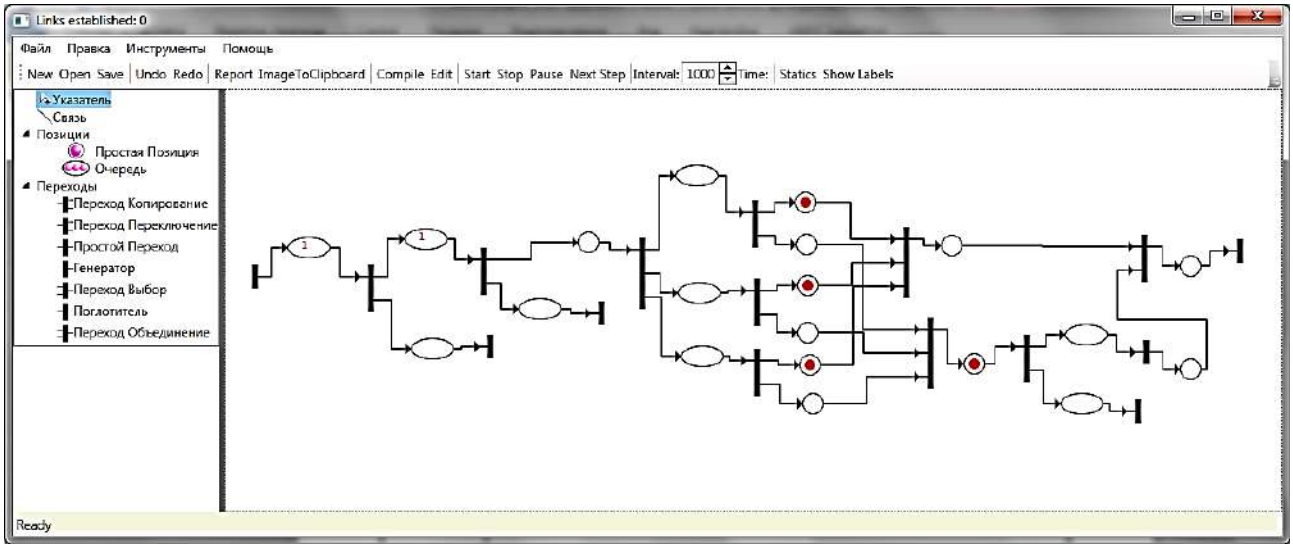


Рис. 11.47. **Е-мережа організації та проведення самостійної роботи студентів спрощеного виду, реалізована в програмі SVC Enet**

Фішки, які генеруються при запуску моделі, характеризуються поведінкою і параметрами. Представивши кожне самостійне завдання у вигляді активної фішки, визначимо її поведінку. В якості параметрів моделі використовуємо тривалість виконання завдання і тривалість його перевірки (задаються користувачем за допомогою розподілу). Оцінки ймовірностей переходів моделі визначаються на основі експериментальних даних, або задаються експертами. Взаємодія між фішками враховується шляхом підвищення ймовірності здати задачу при появі двох завдань з однаковими номерами з одночасним підвищенням ймовірності відхилення завдання з причини несамостійності виконання.

Таким чином, можна виділити такі етапи розрахунку навантаження на самостійну роботу учасників освітнього процесу: 1) вибір параметрів

моделі: кількість завдань в курсі, кількість студентів, 2) вибір коефіцієнтів тимчасових розподілів, що описують тривалість рішення і перевірки завдання; 3) робота моделі до тих пір, поки не будуть вичерпані всі завдання; 4) отримання тимчасових характеристик самостійного курсу. Можлива й інша форма експерименту – визначення кількості виконаних учням завдань за фіксований час (семестр, рік і т. д.).

Для дослідження процесу адаптації студентів до системи навчання за курсом застосований метод кореляційної адаптометрії. Метод розроблений Смірновою Е. В. і Горбанем А. Н. Суть методу полягає у вимірюванні динаміки адаптаційного навантаження за допомогою вагів кореляційного графа G [241]:

$$G = \sum_{|r_{ij}| \geq \alpha} |r_{ij}|, \qquad (11.7)$$

де r_{ij} – елементи кореляційної матриці характеристик, що розглядаються;

α – порогове значення коефіцієнта кореляції.

При цьому зростання показника G свідчить про вплив стресових факторів і підключенні механізмів адаптації для їх нейтралізації, а спад говорить про те, що процес адаптації пройшов успішно. Застосувавши метод до експериментальних даних, було з'ясовано, що адаптаційне навантаження студентів-першокурсників зростає протягом першого семестру і знижується у другому (рис. 11.48). Зниження адаптаційного навантаження показує успішну адаптацію до системи навчання з дисципліни.

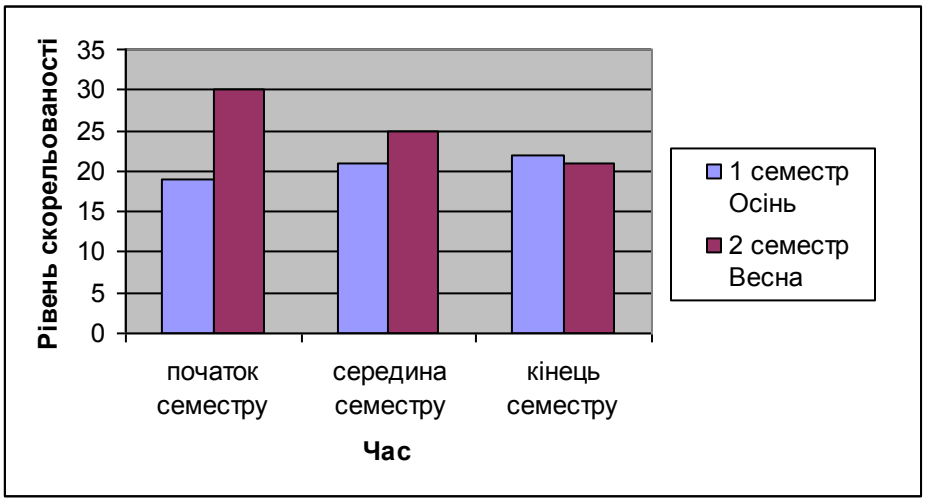


Рис. 11.48. **Динаміка вагів кореляційного графу студентів-першокурсників у 1 та 2 семестрах навчального року**

Досліджено динаміку адаптаційного навантаження в різних групах студентів: місцевих та приїжджих (рис. 11.49); чоловіків і жінок (рис. 11.50); які закінчили успішно курс і які не закінчили його (рис. 11.51). На осі абсцис відкладені відповідні частини семестру.

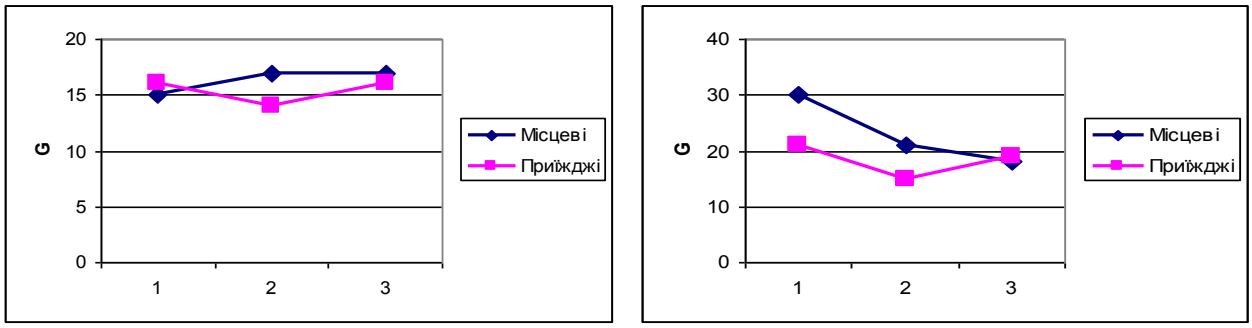


Рис. 11.49. **Динаміка вагів кореляційного графу залежно від проживання студента а) в осінньому семестрі; б) у весняному семестрі**

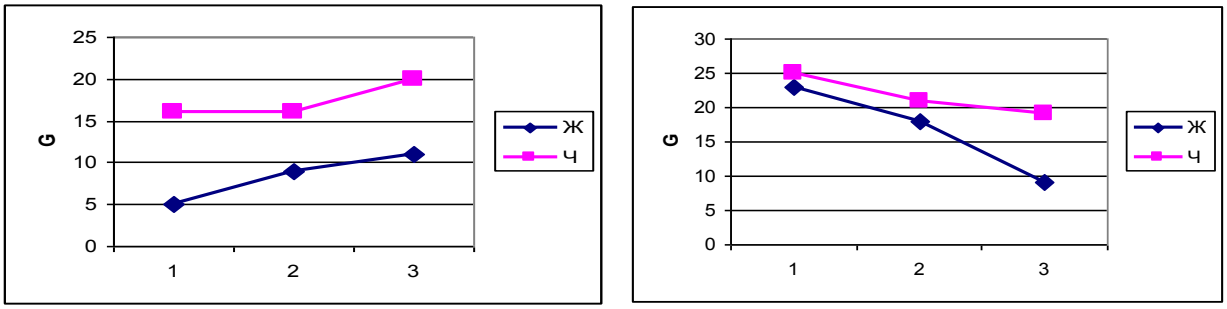


Рис. 11.50. **Динаміка вагів кореляційного графу залежно від статі студента а) в осінньому семестрі; б) у весняному семестрі**

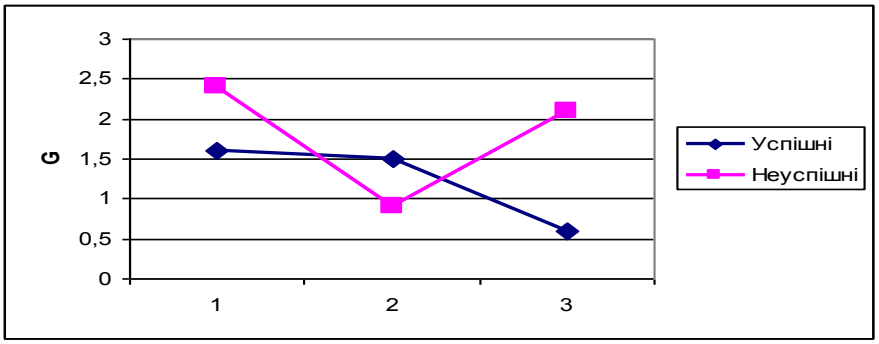


Рис. 11.51. **Динаміка вагів кореляційного графу залежно від підсумкової оцінки**

Можна зробити висновок про те, що адаптаційне навантаження вище у чоловіків, ніж у жінок, у місцевих ніж у приїжджих. У неуспішних студентів не спостерігається адаптації в процесі навчання. Розроблені моделі, дозволяють приймати обґрунтовані рішення в управлінні самостійною навчальною діяльністю студентів, що сприяє підвищенню ефективності управління і має важливе значення для освітньої галузі.

Розділ 12. Моделювання оцінки ефективності реклами культурно-масових заходів

12.1. Сучасні рекламні кампанії як невід'ємна складова бізнесу

Зазначено, що ринок товарів і послуг, що формується в Україні, усе наполегливіше вимагає залучення й використання реклами. Проведено аналіз видів рекламної кампанії та побудовано дерево функцій процесу "Прогнозування рекламної кампанії".

Запропоновано для прогнозування рекламної кампанії у сфері культури математичну модель, параметри якої можуть контролюватися.

Ринок товарів і послуг, що формується в Україні, усе наполегливіше вимагає залучення й використання реклами. Реклама, з одного боку, доводить до споживачів різні відомості, необхідні для покупки й використання виробів.

З другого боку, – сполучаючи свою інформативність із переконливістю й сугестивністю, реклама робить на людину емоційно-психічний вплив. Реклама, сама по собі, одночасно й бізнес і мистецтво [42; 160; 382].

Ефективність реклами виражається у знайомстві цільової аудиторії з інформацією про фірму та її товари або послуги, а також про те, що саме про них відомо, який образ фірми і товарів сформувався і яке ставлення до них у потенційних споживачів.

Створити уявлення про товари і фірму, а тим більше сформувати гарне відношення до них не завжди легко. Це потребує часу та визначеної стратегії.

Слід пам'ятати: відносини на ринку – це, в першу чергу, людські стосунки. Реклама дозволяє формувати необхідне уявлення про фірму у широкої аудиторії, на основі яких легше будувати відносини [383].

Рекламна програма підприємства – це система взаємопов'язаних рекламних заходів, що охоплюють рекламний період часу і передбачають комплекс застосування рекламних засобів для досягнення рекламодавцем конкретної маркетингової мети. Для успіху рекламної програми складається план рекламної компанії. Рекламні заходи в рекламній кампанії повинні мати одну форму, одну гаму кольорів і разом в кінцевому підсумку становити єдине ціле.

Сучасні рекламні кампанії спрямовані на просуванні брендів, що можна позначити як маркетингову та рекламну діяльність зі створення довгострокової переваги до конкретного товару (торгової марки), засновану на спільній посиленій дії на покупця упаковки, товарного знака, рекламних звернень та інших елементів реклами, об'єднаних певною ідеєю і однотипним оформленням, що виділяють товар серед конкурентів і створюють його образ [391].

Аналіз маркетингової ситуації включає: визначення загальних тенденцій ринкової кон'юнктури; становище підприємства на ринку відносно конкурентів; конкурентоспроможність товарів; особливості цільової аудиторії. Іншими словами на даному етапі проводиться дослідження всіх факторів, що впливають або можуть вплинути на хід рекламної кампанії, продаж, поведінка покупців, частку ринку та імідж торгової марки. Це має велике значення для кінцевого успіху задуманого заходу. На основі результатів вивчення інформації, що надійшла, робляться висновки, які стосуються проблем, з якими організатори рекламної кампанії ризикують зіткнутися в процесі роботи, і можливостей для проведення кампанії з максимальною ефективністю [407].

Рекламна мета – це специфічне комунікаційне завдання, що виконується в середовищі певної аудиторії і в заданий період часу. До необхідних умов для формування цілей рекламної кампанії визначення цільових сегментів, аналіз бажаного купівельної поведінки і аналіз комунікацій та процесу прийняття рішень.

При формуванні цілей і завдань рекламної кампанії необхідно враховувати, що цілі повинні бути точні, однозначні, мати кількісну оцінку. Чим конкретніше і точніше буде визначена мета рекламної акції, тим більше шансів на її досягнення. Важливо, щоб цілі кампанії були досяжними, реалістичними. Цілі і завдання рекламної кампанії визначаються такими факторами [358]:

- об'єкт рекламування;
- маркетингові цілі фірми;
- стадії життєвого циклу товару.

Далі визначається цільова аудиторія (споживчий сегмент), для якої в основному розробляється реклама. Споживчий сегмент може бути виділений за такими критеріями: географічний регіон; рівень доходу; вік; стиль життя; імідж. Помилка у виборі аудиторії належить до фатальних наслідків.

Визначення бюджету реклами може здійснюватися кількома способами [378]:

- метод минулого року – витрати встановлюються на рівні минулого року без урахування внутрішніх і зовнішніх змін в організації;
- метод фінансових можливостей – витрати на рекламу визначаються за залишковим принципом (в самому кінці);
- метод "відсоток від виручки" – розмір коштів, що виділяються на рекламу, визначається у відсотках від виручки (валового доходу);
- паритетний метод – витрати на рекламу встановлюються виходячи з витрат на рекламу фірм-конкурентів;
- метод цілей і завдань – спочатку визначаються цілі і завдання, яких організація хоче досягти при проведенні рекламної кампанії; потім вибираються найбільш ефективні засоби реклами і визначається бюджет реклами виходячи з тарифів.

Вибираючи засоби поширення реклами, необхідно обґрунтувати вибір того чи іншого засобу, визначити частоту та інтенсивність рекламної кампанії і розробити її графік. В самому кінці визначається ефективність рекламної кампанії. Для цього використовуються такі показники: приріст обсягу продажів; приріст прибутку; рентабельність реклами.

Певні особливості має процес планування рекламної кампанії в інтернеті, який вже міцно увійшов в наше життя. Її можна умовно розділити на такі основні етапи [370]:

1) визначення мети рекламної кампанії;
2) визначення цільової аудиторії;
3) попередній вибір рекламних майданчиків;
4) вибір форматів носіїв;
5) складання та оптимізація медіаплану.

Спочатку повинен бути визначений продукт, який буде рекламуватися з усіма його перевагами і недоліками. Часто з визначенням цілей рекламної кампанії зазвичай виникають певні труднощі. Або про це просто не думають, або визначають їх неправильно, або визначення дуже узагальнено. Насправді при складанні медіаплану потрібно зрозуміти, що

рекламується – конкретний товар чи бренд? Метою рекламної кампанії може служити або збільшення продажів конкретного товару в даний конкретний момент, який вплив на ставлення споживачів до марки.

Якщо мета кампанії – зміна ставлення споживача до бренда, то головним завданням кампанії буде максимальне охоплення представників цільової аудиторії в рамках бюджету із заданою частотою. У іміджевих кампаніях зазвичай потрібна висока частота показу – від семи показів на одну людину. Необхідно, щоб людина не тільки помітила рекламу, але також чітко зрозуміла рекламне посилання і, головне, – запам'ятала і пов'язала його з брендом. В іміджевій кампанії велике значення має креатив носія. Він повинен виробляти належне враження, а не просто доносити інформацію [276].

Якщо реклама націлена на збільшення кількості проданого конкретного товару в даний час, вибір майданчиків і форматів рекламних носіїв буде іншим, особливо це стосується інтернету.

Реклама в інтернеті поширюється двома носіями-банером і сайтом. Банер цілком може служити носієм іміджевої інформації, але продати товар він не в змозі. Продає сайт. Отже, завдання інтернет-реклами не в демонстрації банера, а в залученні людей на сайт рекламованого продукту.

При проведенні рекламної кампанії, націленої на продаж, максимальну увагу слід приділити тій сторінці, на яку людина потрапляє з банера. Саме вона, а не банер, є ключовим рекламним носієм. Від того, наскільки переконливо і просто ця сторінка розкаже споживачеві все, що йому потрібно знати для прийняття рішення про покупку, залежить результат кампанії [370].

Завдання банера в даному випадку не створення якогось емоційного посилу, а донесення інформації про пропозицію. Слід вибирати ті формати банера і місця розміщення, які дозволяли б забезпечити перехід на сайт за мінімальні гроші. Крім того, слід вибирати ті форми розміщення, які дозволяють чітко контролювати частоту показу рекламного повідомлення. Потрібно це для того, щоб звести її до мінімуму, тим самим, збільшивши обхват аудиторії.

Якщо ж брати банер досить великого розміру, розміщений в безпосередній близькості до контенту сторінки, – більше трьох показів на одного унікального користувача купувати просто безглуздо. У більшості випадків буде достатньо і одного – краще збільшити охоплення рекламної кампанії за рахунок зниження частоти показів.

Визначення цільової аудиторії (ЦА) – це та інформація, яка повинна допомагати при плануванні кампанії. Тому визначати ЦА потрібно тільки через ті параметри, на які можна впливати при плануванні.

Аудиторію мережі Інтернет можливо сегментувати лише за наступними параметрами [386]:

- географічна приналежність;
- стать;
- вік;
- інтереси;
- явна зацікавленість у продукті.

Географічна приналежність цільової аудиторії – найважливіший її параметр. Вона завжди точно визначена, але про це найчастіше забувають. І це призводить до того, що левова частка рекламних бюджетів витрачається даремно.

Стать цільової аудиторії також досить легко визначити. І знання цього параметра допоможе у виборі рекламних майданчиків [276].

Якщо реклама націлена на чоловіків – завдання зводиться до максимального відсікання жіночої аудиторії. Наприклад, можна розмістити банери на спортивних сайтах. Частка жінок у їх аудиторії мінімальна. І не важливо, що ваш товар до спорту відношення не має. В даному випадку, за допомогою вибору спортивних сайтів збільшується частка чоловіків у загальному охопленні рекламної кампанії.

Якщо цільовою аудиторією є жінки – необхідно додати в план жіночі ресурси, яких немало. Сайти про дітей, кулінарію, моду, стиль. Знову ж, товар може бути ніяк не пов’язаний з жодною з цих тем.

Вік – параметр, який також може бути корисним при виборі сайтів. Але спосіб його використання не настільки очевидний. В силу особливостей вікового поділу української аудиторії інтернету, простим вибором тематики сайта можна значно збільшити частку необхідної вікової групи в загальному охопленні.

Найбільшою віковою групою серед користувачів мережі є молодь у віці від 14 до 24 років – 36 %. У віці від 25 до 34 років 29 % аудиторії, від 35 до 44 років – 19 %, від 45 до 54 років – 12 %, старше 55-річного віку лише 4 % аудиторії. Чоловіків в Інтернеті дещо більше, ніж жінок – 51 %.

Чверть учасників дослідження повідомили про себе як про кваліфікованих робітників, 24 % – школярі та студенти, 10 % аудиторії – офісні співробітники, 9 % – топ-менеджмент, 5 % – робітники, по 4 % припадає на безробітних та домогосподарок, 2 % – на пенсіонерів [364; 406].

Явна зацікавленість у продукті – це коли людина активно шукає товар. У даному випадку вже не важливо, якої вона статі, віку і навіть де живе. Знайти таких зацікавлених людей можливо тільки на пошукових системах.

У ході рекламної кампанії для досягнення поставлених цілей часто використовуються методи та прийоми інших елементів маркетингових комунікацій: пропаганда, стимулювання збуту та інші [390]. До основних видів реклами можна віднести такі: інформативну, сповіщаючу, емоційну та нагадуючу [238].

Інформативна реклама

Інформативна реклама переважає в основному на етапі виведення товару на ринок, коли стоїть завдання створення первинного попиту. Так, виробникам харчової продукції потрібно спочатку проінформувати споживачів про поживні гідності і численні способи використання продукту, наприклад:

повідомлення ринку про новинку чи нове застосування існуючого товару;

інформування ринку про зміну ціни;

пояснення принципів дії товару;

опис послуг, що надаються;

виправлення неправильних уявлень чи розсіювання побоювань споживача;

формування образу фірми.

Сповіщаюча реклама

Сповіщаюча реклама набуває особливої значимості на етапі зростання, коли перед фірмою постає завдання формування виборчого попиту. Частина сповіщаючих оголошень зміщується в категорію порівняльної реклами, яка прагне затвердити перевагу однієї марки за рахунок конкретного порівняння її з однією або декількома марками в рамках даного товарного класу. Порівняльною рекламою користуються в таких товарних категоріях, як дезодоранти, зубна паста, шини й автомобілі. Про правильність створення порівняльної реклами судження досить неоднозначні.

Завдання:

- формування переваги до марки;
- заохочення до придбання конкретної марки;

• зміна сприйняття споживачем властивостей товару;

• переконання споживача зробити покупку не відкладаючи;

• переконання споживача в необхідності прийняти комівояжера.

Емоційна реклама

Реклама прагне запевнити нинішніх покупців у правильності зробленого ними вибору. У подібних рекламах часто фігурують задоволені покупці, дружня атмосфера.

Завдання:

• пробудження в споживачів симпатії до продукту;

• створення іміджу;

• підвищення довіри як до товару чи послуги, так і до самої фірми-виробника;

• залучення уваги споживачів до певного товару.

Нагадуюча реклама

Нагадуюча реклама надзвичайно важлива на етапі зрілості, для того, щоб змусити споживача згадати про товар. Мета дорогих оголошень добре відомої продукції фірм, що мають загальне і давно усталене визнання – нагадати людям про своє існування, а зовсім не в тому, щоб проінформувати або переконати їх.

Завдання:

• нагадування споживачам про те, що товар може знадобитися найближчим часом;

• нагадування споживачам про те, де можна купити товар;

• утримання товару в пам’яті споживачів у періоди міжсезоння;

• підтримка поінформованості про товар.

На практиці часто границі між наведеними видами розмиті, тому що одна реклама може носити (або поєднувати) як і інформаційний характер, так і, наприклад, увідомлюючий. Все залежить від конкретної рекламної ситуації, у якій знаходиться фірма. Наприклад, у магазин надійшла партія нової продукції. Фірма інформує про це споживача (інформаційна реклама) і нагадує адреси своїх магазинів (нагадуюча реклама).

Рекламна кампанія – це комплекс рекламних заходів, розроблений відповідно до програми маркетингу і спрямований на споживачів товару, що представляють відповідні сегменти ринку, з метою викликати їх реакцію, що сприяє вирішенню фірмою-виробником своїх стратегічних чи так-

тичних завдань. Під час проведення рекламних кампаній конкретизація окремих заходів залежить перш за все від маркетингової стратегії, яка може виражатися, наприклад, в захопленні ринку в цілому, його частки, сегмента; впровадженні в незайняту конкурентами нішу; утримання раніше захоплених ринкових позицій. Враховуються також: маркетингова інфраструктура, людські та технічні ресурси, рівень налагодженої комунікацій і постачання інформацією, характер екології рекламно-інформаційної і маркетингової діяльності. Ця сукупність є системою взаємопов'язаних функцій. Така система функцій розчленована на більш прості сукупності завдань і представлена деревом функцій (рис. 12.1).

Дерево функцій є систематизованим відображенням моделі підприємства в рамках процесного управління. Деревоподібна структура функцій є простою моделлю сукупності функцій бізнес процесу, хоча насправді модель функціонування підприємства має більш складну структуру і володіє більш складними і не завжди однозначними зв'язками. Дерево функцій перетинається із системою стратегічного управління підприємством, а саме, з деревом цілей. Дерево цілей розгортається від місії через стратегічні цілі до оперативних цілей підприємства, оперативні цілі в свою чергу реалізуються за допомогою бізнес-процесів.

Процес "Прогнозування рекламної кампанії" у виді дерева функцій є досить простою структурою з одним рівнем і включає 5 етапів:

- накопичення даних про інвестиції в види реклами. Завдання функції полягає в накопиченні та архівуванні даних про попередню діяльність підприємства для майбутнього аналізу і прийняття рішень на їх основі;
- оцінка параметрів моделі. В ході виконання даної функції за допомогою математично-статистичних методів розраховуються параметри моделювання;
- розподіл коштів у розрізі видів реклами. Результатом виконання даної функції є масив коефіцієнтів розподілу грошових засобів для інвестування види реклами;
- розподіл коштів у розрізі заходів. У ході виконання даної функції відбувається аналіз відвідуваності заходів та, на основі отриманих даних, розраховуються коефіцієнти розподілу грошових засобів за заходами;
- аналіз динамік пропорцій інвестування грошових заходів. Результати роботи даної функції є цінними даними для керівництва підприємства, що допоможуть скорегувати роботу та розподілення грошових заходів на майбутнє.

Означені етапи відіграють важливу роль у будь-якій рекламній кампанії, однак особливо важливими вони стають при проведенні рекламних кампаній закладами культури – театрами, музеями тощо.

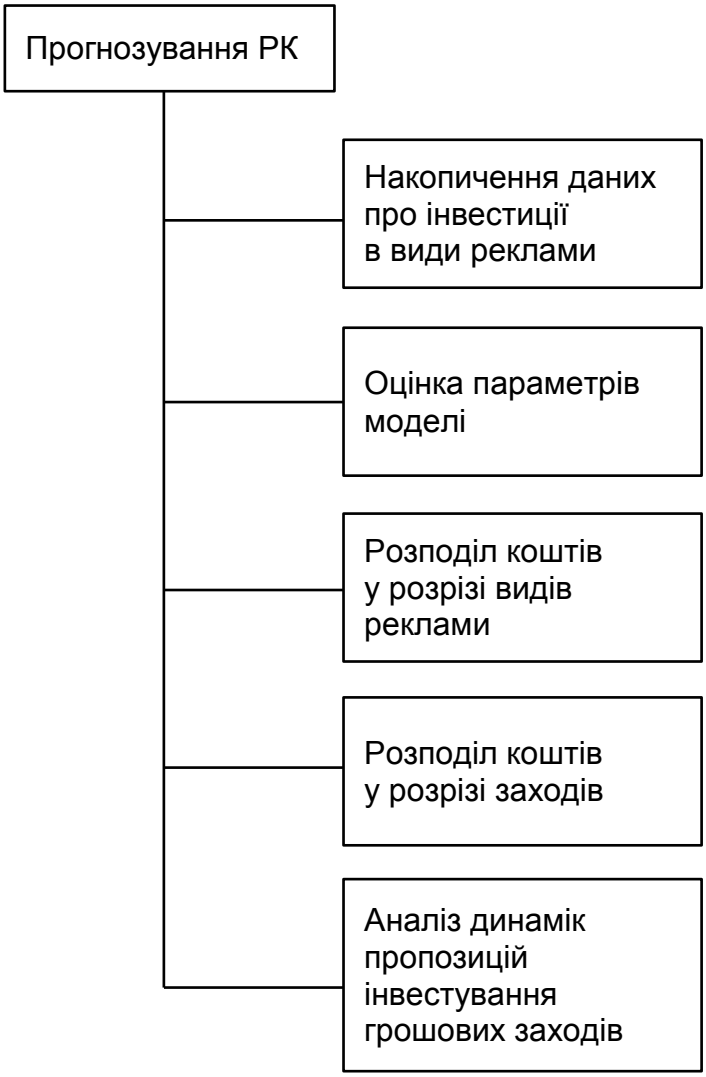


Рис. 12.1. **Дерево функцій процесу "Прогнозування рекламної кампанії"**

Виконання цих етапів дозволить спрогнозувати ефективну рекламну кампанію, результати котрої зможуть контролюватися керівництвом культурно-масового підприємства, а не бути випадковими і непідвласними аналітиці. В цьому випадку на допомогу може прийти математичне моделювання.

12.2. Моделювання проведення рекламної кампанії культурно-масових заходів

Встановлено, що вирішення задачі планування рекламної кампанії складається з двох підзадач: визначення пропорцій розподілу коштів по заходах та визначення пропорцій розподілу коштів по видах реклами.

Для вирішення першої задачі виникає необхідність зберігати історію зміни таких параметрів, як кількість проведених заходів, їх окупність, кількість вкладених коштів у різні види реклами.

Для вирішення другого завдання необхідно мати зібрані і проаналізовані параметри за певний період діяльності в минулому. Запропонована модель, що дозволяє вирішити означені задачі.

Після здобуття Україною незалежності в 1991 році почався новий етап розвитку українського суспільства. Україна стала суверенною демократичною державою.

Головною особливістю сучасного періоду можна вважати його перехідний характер. Можна говорити про те, що в суспільстві склалася нова соціокультурна ситуація, яка характеризується іншими соціально-економічними умовами, формами власності, характером стосунків між людьми, соціальною структурою, системою цінностей. Принципово новий статус у наші дні отримала національна культура.

Для багатьох людей відвідування театрів, музеїв, бібліотек, тим паче різні поїздки стали недоступними.

У зв'язку зі значним скороченням життєвого рівня (за рівнем життя Україна займає 95-те місце в світі, а понад половина населення живе за межею бідності), погіршенням медичного обслуговування, зростанням вартості ліків, ускладненням екологічної обстановки спостерігається збільшення захворюваності, смертності, зниження народжуваності [352].

На сьогоднішній день ситуація в розвитку театрального мистецтва в Україні є одним з представників розвитку мистецтва країни в цілому.

Наявність проблем, що потребують розв'язання, зумовлена цілим комплексом причин як суспільно-історичного, так і організаційно-фінансового характеру.

Причому багато творчих питань, врешті-решт, зводяться саме до скрутного матеріального становища, у якому перебувають заклади культури, до неможливості гнучкого маневру, до закостенілості існуючих структур та умов.

Театральна справа є комплексом заходів, спрямованих на створення, публічне виконання та публічний показ творів театрального мистецтва, їхнє поширення і збереження умов для розвитку театральної творчості, професійної освіти, науки, театральної журналістики, видавничої діяльності з історії, теорії та практики цього виду мистецтва, відповідної музейної та архівної діяльності.

Театральне мистецтво – вид мистецтва, особливістю якого є художнє відображення життя за допомогою сценічної дії акторів перед глядачами.

Нині в Україні діє понад 130 професійних театрів, серед яких національні, драматичні, музично-драматичні театри, театри драми і комедії, юного глядача, ляльок та театри-студії. Середня кількість прем'єр на рік становить від 4 до 6 на кожний театр [244].

Сприяти вирішенню нагальних проблем театру має державна політика у театральній справі, яка відображається у законодавстві. Законодавство України про театри і театральну справу базується на Конституції України і складається з відповідних положень Основ законодавства України про культуру, Цивільного та Господарського кодексів України, законах України "Про гастрольні заходи в Україні", "Про театри і театральну справу", інших нормативно-правових актах.

Особисті немайнові і майнові права авторів та їх правонаступників, пов'язані зі створенням творів літератури і мистецтва (авторське право), права виконавців, виробників фонограм та організацій мовлення (суміжні права) регулюються Законом України "Про авторське право і суміжні права" та іншими нормативно-правовими актами.

Держава регулює відносини в галузі театру і театральної справи шляхом формування державної політики у цій сфері, створення фінансового, матеріально-технічного, кадрового, інформаційного, наукового, нормативно-правового та іншого забезпечення умов діяльності та розвитку театрів [196].

Але окрім держави в процес розвитку культури в Україні мають втручатися і самі організації, що надають послуги зі створення культурно-масових заходів і забезпечувати ефективну рекламну кампанію щодо тих чи інших заходів, які вони проводять. Однак проведений аналіз показав, що, по-перше, наявні системи планування проведення рекламних кампаній не враховують особливості галузі культури, а по-друге, жодна з систем не передбачає врахування того факту, що з часом важливість видів реклами може змінюватися і цей фактор обов'язково повинен бути врахований при плануванні рекламної кампанії.

Таким чином, виникає завдання створення моделі, яка б дозволила прогнозувати подальшу роботу культурно-масової організації і кількість прибутку, яку вона може отримати від своєї діяльності. Це завдання у свою чергу складається з:

- визначення пропорцій розподілу грошових коштів за заходами;
- визначення пропорцій розподілу грошових коштів за видами реклами в розрізі одного культурно-масового заходу;

Тобто рішення завдання планування рекламної кампанії зводиться до побудови двох математичних моделей і вирішення двох задач [236].

Для вирішення першої задачі виникає необхідність зберігати історію динаміки зміни таких параметрів, як кількість проведених заходів, їх окупність, кількість вкладених коштів у створення заходу, а також кількість вкладених коштів у різні види реклами. Для вирішення другого завдання необхідно мати зібрані і проаналізовані параметри за певний період діяльності закладу в минулому.

Визначення пропорцій розподілу грошових коштів за заходами є однією з ключових задач, яка основана на аналізі накопичених даних діяльності підприємства в минулому.

Інакше кажучи, в результаті аналізу необхідно знайти частки розподілу грошових коштів на рекламу кожного заходу.

Необхідна умова вирішення даної задачі:

$$\sum_{i=1}^{s} d_i=1,$$

де d_i – частка вкладення грошових коштів у i-тий захід;

s – кількість заходів.

$$d_i = \frac{L_i}{LS},$$

де L_i– відносна величина, що характеризує відвідуваність i-того заходу;

LS – сумарна відвідуваність усіх заходів.

$$LS = \sum_{i=1}^{m} L_i,$$

$$L_i = GS - G_i$$

де GS – частка приросту глядацького інтересу;

G_i – частка приросту глядацького інтересу до i-того заходу.

Для визначення пропорцій розподілу грошових коштів за видами реклами в розрізі одного культурно-масового заходу виникає необхідність використання одного з методів статистичного аналізу – методу найменших квадратів. Застосування цього методу дозволить на основі даних про об'єм інвестованих грошових заходів у види реклами і отриманого прибутку від цих інвестицій розрахувати пропорції вкладення грошових засобів у види реклами на наступний місяць.

У математичному контексті постановка завдання має такий вигляд:

$$\sum_{n=1}^{m}((a_1 x_{n1} + a_2 x_{n2} + \cdots + a_p x_{np})^2 - b_n^2) \to min,$$

де p – кількість видів реклами;

m – кількість місяців для прогнозування;

$x_{ni}, 1 < i \le p$ – кількість вкладених засобів в i-тий вид реклами, n-того місяця;

b_n – вільні члени, реальний прибуток, отриманий в конкретному місяці.

Необхідно зазначити, що параметри a_i можуть визначатися за заданою кількістю місяців для аналізу. По динаміці зміни параметрів a_i можна простежити рівень важливості певного виду реклами і зробити відповідні висновки щодо необхідності вкладення в нього коштів.

Варто розглянути на прикладі запропонований підхід.

Слід припустити, що є дані щодо обсягів прибутку отриманого театром від показу окремих вистав (табл. 12.1).

Таблиця 12.1

Обсяги отриманого прибутку

Місяць	Назва вистави			Всього
	"Запорожець за Дунаєм"	"Безумний день, або весілля Фігаро"	"Слуга двох панів"	
грудень	5 700	4 800	5 000	15 500
січень	5 900	5 000	5 000	15 900

Слід розрахувати частку приросту глядацького інтересу до першого заходу:

$$G_1 = \frac{5900}{5700} = 1,035.$$

Аналогічно G_2 = 1,042; G_3 = 1,000.

Сумарна частка приросту глядацького інтересу:

$$GS = \sum_{i-1}^{c} G_i = 3,077.$$

де G_i – доля приросту глядацького інтересу до і-го заходу,

c – кількість заходів

$$1 \le i \le c.$$

Слід розрахувати відносну величину відвідуваності першого заходу:

$$L_i = GS - G_i = 3,077 - 1,035 = 2,042.$$

Сумарне значення показників відвідуванності всіх заходів

$$LS = \sum_{i=1}^{c} L_i = 6,154,$$

де L_i – показник відвідуваності і-того заходу,

c – кількість заходів

$$1 \le i \le c.$$

Слід розрахувати коефіцієнти розподілу грошових коштів за заходами.

$$d_1 = \frac{L_1}{LS} = \frac{2,042}{6,154} = 0,332.$$

Таким чином, наявна матриця розрахованих даних (табл. 12.2).

Таблиця 12.2

Розрахунок коефіцієнтів розподілу грошових коштів за заходами на лютий

Коефіцієнти	Назва вистави			Всього
	"Запорожець за Дунаєм"	"Безумний день, або весілля Фігаро"	"Слуга двох панів"	
G_i	1,035	1,042	1,000	3,077
L_i	2,042	2,035	2,077	6,154
d_i	0,332	0,331	0,337	1

На основі розрахованих коефіцієнтів та за наявності даних про об’єм коштів для інвестування в рекламу на лютий (5 000 грн) є можливість розподілити грошові кошти за заходами (табл. 12.3).

"Запорожець за Дунаєм": 5 000 × 0,332 = 1 658,95 грн.

"Безумний день, або весілля Фігаро": 5 000 × 0,331 = 1 653,60 грн.

"Слуга двох панів": 5 000 × 0,337 = 1 687,45 грн.

Аналогічним чином, маючи реальні дані про отриманий прибуток (табл. 12.3) у січні та лютому слід розрахувати розподіл коштів на березень.

А маючи дані за березень – на квітень. Результати розрахунку, за умови, що на рекламу виділяється 5 000 грн на місяць, наведені у табл. 12.4, 12.5.

Таблиця 12.3

Обсяги отриманого прибутку за місяцями

Місяць	Назва вистави			Всього
	"Запорожець за Дунаєм"	"Безумний день, або весілля Фігаро"	"Слуга двох панів"	
Грудень	5 700	4 800	5 000	15 500
Січень	5 900	5 000	5 000	15 900
Лютий	5 100	4 900	5 300	15 300
Березень	5 300	5 200	4 800	15 300
Квітень	5 300	5 500	5 200	16 000

Таблиця 12.4

Розрахунок розподілу грошових коштів за заходами на березень

Коефіцієнти	Назва вистави			Всього
	"Запорожець за Дунаєм"	"Безумний день, або весілля Фігаро"	"Слуга двох панів"	
G_i	0,864	0,980	1,060	2,904
L_i	2,040	1,924	1,844	5,809
d_i	0,351	0,331	0,318	1
	1 755,95	1 656,45	1 587,59	5 000

Таблиця 12.5

Розрахунок розподілу грошових коштів за заходами на квітень

Коефіцієнти	Назва вистави			Всього
	"Запорожець за Дунаєм"	"Безумний день, або весілля Фігаро"	"Слуга двох панів"	
G_i	1,039	1,061	0,906	3,006
L_i	1,967	1,945	2,100	6,012
d_i	0,327	0,323	0,349	1
	1 635,74	1 617,44	1 746,81	5 000

Таким чином, динаміка інвестувань грошових коштів у рекламу певних заходів зображена на рис. 12.2 – 12.8.

Рис. 12.2. **Динаміка інвестування в захід "Запорожець за Дунаєм"**

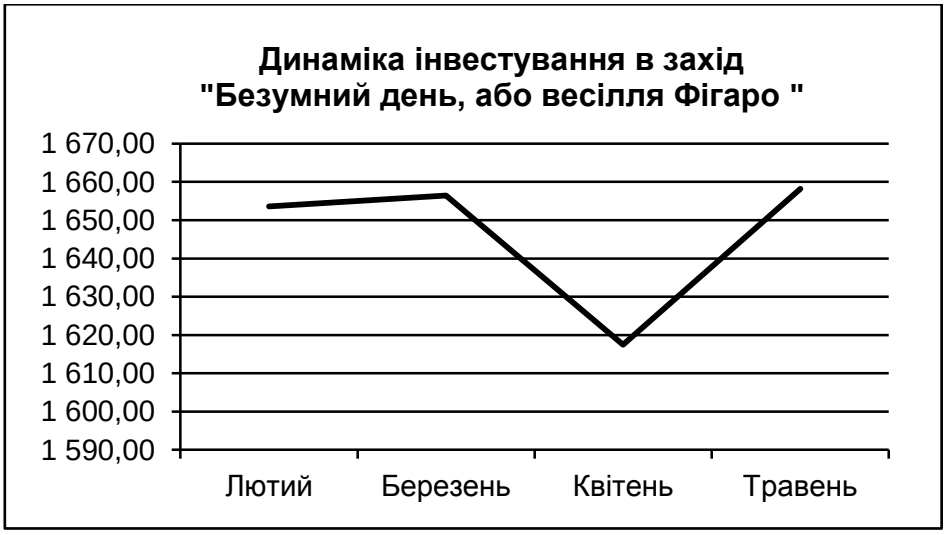


Рис. 12.3. **Динаміка інвестування в захід "Безумний день, або весілля Фігаро"**

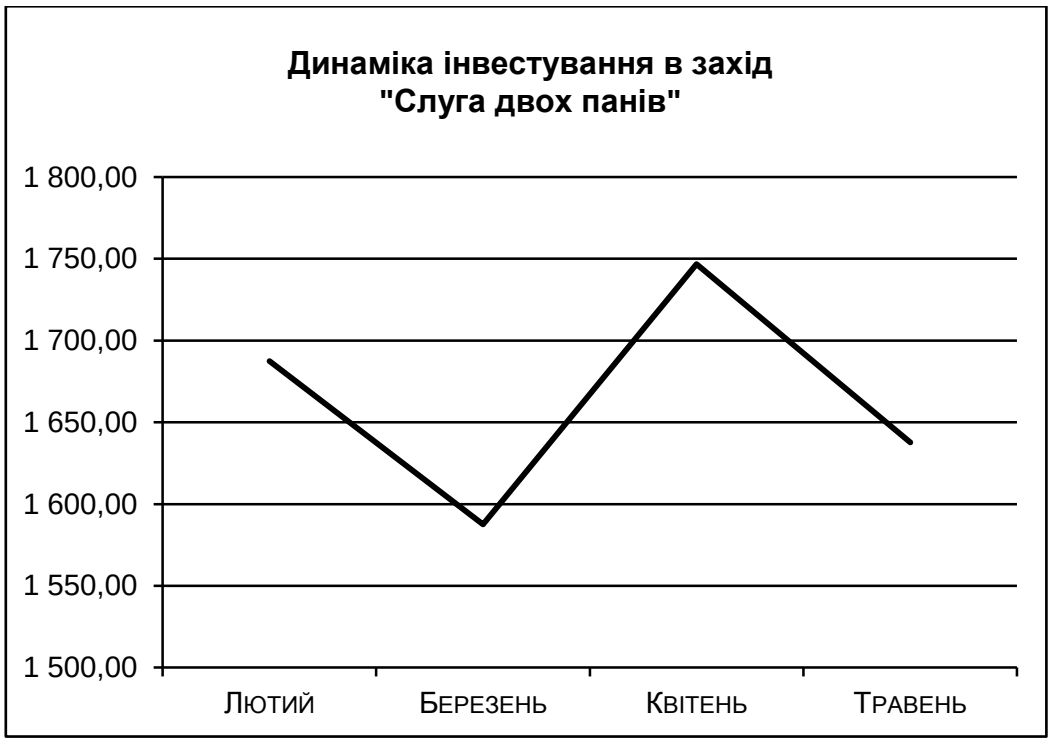


Рис. 12.4. **Динаміка інвестування в захід "Слуга двох панів"**

На основі проведеного аналізу керівництво культурно-масового заходу має можливість зробити висновки щодо стратегії інвестування грошових коштів у заходи в наступному місяці для отримання максимальної відвідуваності і, як результат, максимально можливого прибутку.

Для рішення другої задачі необхідно оперувати раніше накопиченими даними щодо об'єму інвестованих грошових коштів у види реклами та отриманий прибуток.

Наприклад, для наочності можна взяти 4 види реклами: телебачення, Інтернет, радіо та газети та сформувати таблицю такого вигляду (табл. 12.6).

Таблиця 12.6

Інвестиції в види реклами

Місяць	Телебачення	Радіо	Газети	Інтернет	Сума	Прибуток
Грудень	1 600	1 100	1 000	1 300	5 000	15 500
Січень	1 600	1 000	1 300	1 100	5 000	15 900
Лютий	1 100	1 300	1 300	1 300	5 000	15 300

Для більш точного розв'язку, щоб не прив'язуватися до конкретної суми виділених коштів на рекламу, варто знайти частку кожного виду

реклами від загальної суми в розрізі місяця. Результати відображені в табл. 12.7.

Таблиця 12.7

Нормалізовані дані щодо інвестицій у види реклами

Місяць	Телебачення	Радіо	Газети	Інтернет	Сума	Прибуток
Грудень	1 600 / 5 000 = 0,32	0,22	0,2	0,26	1	15 500
Січень	0,32	0,2	0,26	0,22	1	15 900
Лютий	0,22	0,26	0,26	0,26	1	15 300

Для оцінки параметрів функції $f=a_1x_{n1} + a_2x_{n2} + \ldots + a_px_{np}$ *слід* використати пакет Solver Microsoft Excel і отримати розраховані коефіцієнти А розподілу грошових засобів за видами реклами.

Результати відображені в табл. 12.8.

Таблиця 12.8

Коефіцієнти розподілу грошових засобів за видами реклами

Телебачення	Радіо	Газети	Інтернет
15 490,77	405,393	22 214,35	23 118,83

Виходячи з отриманих результатів, слід визначити розмір коштів, які необхідно вкласти у різні види реклами на наступний місяць, тобто березень. Прийнявши за x_i значення середнього відсотку розподілу коштів за попередні місяці, отримаємо оцінку очікуваного прибутку в розрізі видів реклами:

для телебачення: 15 491·(0,32+0,32+0,22)/3 = 4 441;

для радіо: 405·(0,22+0,2+0,26)/3 = 92;

для газет: 22 214·(0,2+0,26+0,26)/3 = 5 331;

для Інтернет: 23 118·(0,26+0,22+0,26)/3 = 5 702.

Сумарний очікуваний прибуток складає 15 556 грн.

Базуючись на отриманому прогнозі, слід розрахувати частку кожного виду реклами у загальному прибутку і розмір коштів на наступний місяць. Результати розрахунку наведені у табл. 12.9.

Таблиця 12.9

Розрахунок коштів за видами реклами

Телебачення	Радіо	Газети	Інтернет	Сума	
4 440,69	91,89	5 331,45	5 702,65	15 566,7	
0,2853	0,0059	0,3425	0,3663	1	Частка у прибутку
1 426,3	29,5	1 712,5	1 831,7	5000	Сума на рекламу

Аналогічним чином після отримання реальних даних за прибутком за березень, на основі січня, лютого та березня варто оцінити значення параметрів a_i для різних видів реклами на квітень і розрахувати об'єм коштів, що необхідно вкласти в таку рекламу.

На рис. 12.5. – 12.8 наведено графіки, що ілюструють динаміку зміни параметрів для різних видів реклами.

Рис. 12.5. **Динаміка зміни коефіцієнта А для телебачення**

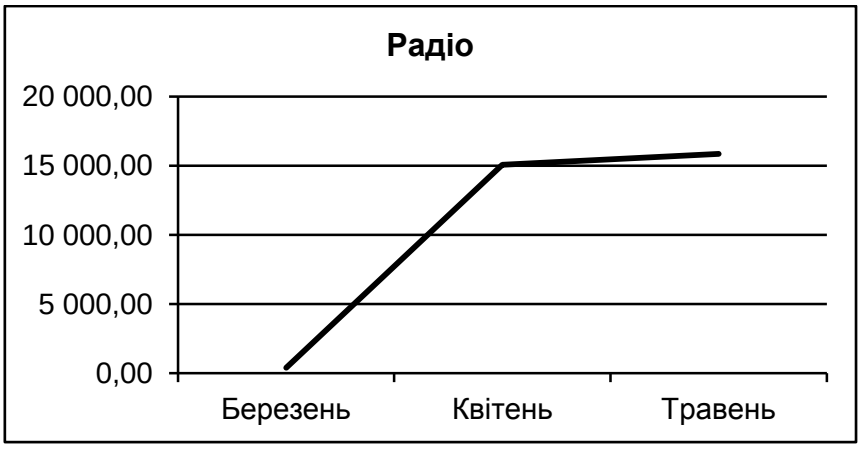


Рис. 12.6. **Динаміка зміни коефіцієнта А для радіо**

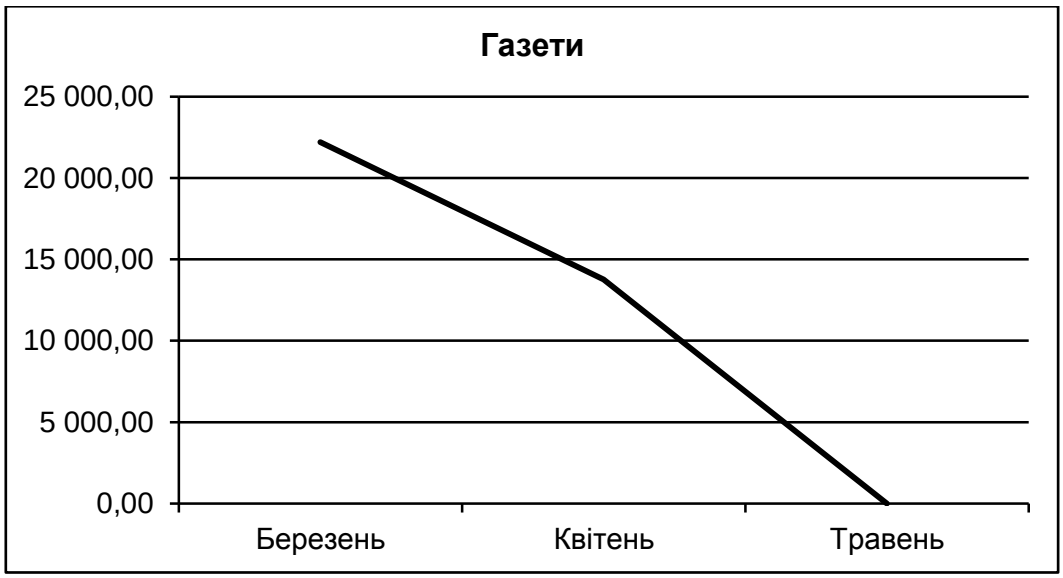


Рис. 12.7. **Динаміка зміни коефіцієнта А для газет**

Рис. 12.8. **Динаміка зміни коефіцієнта А для Інтернету**

З діаграм можна чітко прослідкувати тенденції такого показника, як важливість виду реклами. Для більш точної оцінки параметрів слід базуватися на порівнянні не з попереднім місяцем, а узагальненими даними за деякий попередній період, наприклад квартал.

Таким чином, у результаті проведених досліджень було запропоновано математичну модель, базуючись на якій заклади культури можуть планувати і прогнозувати свою рекламну діяльність.

Висновки

Проведено теоретичний аналіз щодо розкриття сутнісного розуміння таких термінів, як "модель", "моделювання" та "податковий облік". Проведено детальний аналіз податкового обліку на підприємствах та в податкових інспекціях, на основі чого проведено моделювання окремих аспектів цього процесу. На основі проведеного аналізу Програми модернізації державної податкової служби виявлено значне відставання реалізації програми від плану заходів, які були в ній передбачені. Це досить негативно впливає на поліпшення взаємовідносин контролюючих органів та платників податків, а також не дозволяє зменшити частку корумпованих схем у вирішенні проблем бізнесу. Однак можна зазначити і позитивні зрушення в розвитку взаємовідносин між цими суб’єктами в процесі автоматизації функціонування інформаційних систем; цьому сприяє прийняття і активне впровадження положень Податкового кодексу України.

Сучасні інформаційні системи та мережі, використовуючи останні досягнення в розвитку електронних комунікацій і IT-технологій, постійно розширюють спектр надаваних послуг, у тому числі з обслуговування суб’єктів автоматизованих інформаційних систем, забезпечення доступу до різних мультимедійних сервісів і технологій, підтримці користувачів і т. д. У той же час швидке зростання обсягів оброблюваних даних призводить до підвищення жорсткості ймовірносно-часових вимог до основних компонентів інформаційних систем і комунікаційних мереж на всіх етапах інформаційного обміну даними. Проведені дослідження показали, що застосування розроблених крипто-кодових засобів захисту інформації на основі теоретико-кодових схем дозволяє ефективно забезпечити безпеку повідомлень, які передаються, а також протистояти можливим атакам порушника.

Подальший розвиток одержав метод модулярного гешування, що відрізняється від відомих методів відсутністю обмеження на параметри модульної експоненти й введенням ключової залежності вектора ініціалізації. Сформовані функції задовольняють умови строго універсального гешування з відомістю задавання знаходження прообразу або секретного ключа до одного з відомих теоретико-складових завдань. Удосконалена модель відрізняється від відомої (моделі UMAC) застосуванням модулярного гешування на останньому етапі формування MAC, що дозволяє забезпечити високі колізійні властивості строго універсаль-

ного гешування й показники безпеки на рівні сучасних засобів захисту доказової стійкості.

Методи теорії прийняття рішень в умовах визначеності не надають незаперечних рекомендацій щодо остаточного рішення з будь-якої складної проблеми. Вибір критеріїв і методів залежить від важливості вирішуваних завдань, від кваліфікації і відповідальності експертів та ОПР. Підвищення рівня інформованості може бути досягнутим при зверненні ОПР до послуг консультаційної служби, здатної скласти добре обґрунтований прогноз розвитку ситуації, що дозволяє проводити реалізацію такого експерименту за допомогою імітаційного моделювання на основі математичних методів.

Український ринок HRM-систем стрімко розвивається, що обумовлює актуальність проблеми зваженого вибору програмних комплексів для управління персоналом. Одним із ключових етапів у процесі вибору є етап економічного обґрунтування ефективності інвестицій в автоматизацію. Методики та моделі оцінювання ефективності HRM-систем мають ураховувати запропоновані особливі вимоги до HRM-систем, які використовуються для розрахунку таких кількісних показників, як кількість операцій і час, що витрачається користувачем на виконання бізнес-процесу, кількість помилок при розрахунку заробітної плати, кількість вдалих/невдалих співбесід у розрахунку на одиницю часу, відсоток досягнення співробітниками встановлених показників, кількість співробітників HR-департаменту, використання комплексу методів визначення економічної ефективності HRM-систем дозволяє запобігти помилкові управлінські рішення.

Сформульована пропозиція щодо модифікації алгоритму Хаффмана для отримання більшої ефективності при стисненні текстових даних (блоково-статистичний алгоритм) та проведено моделювання з метою оцінки ефективності запропонованого алгоритму для даних з різноманітними законами розподілу частот зустрічаємості символів, які підтверджують, що запропонований блоково-статистичний алгоритм є більш ефективним порівняно з класичним алгоритмом Хаффмана. Для усіх типів текстових даних доцільно розділяти символи тексту на дві групи, приблизно рівні за сумою частот зустрічаємості символів.

Досліджено роботу мереж передачі даних та основних мережних протоколів з точки зору їх корпоративного використання, технології передачі даних, обладнання та його конфігурації. Методом аналізу ієрархій

проведено порівняння за технічними та експлуатаційними параметрами основних апаратно-програмних комунікаційних систем для забезпечення функціонування корпоративної мережі обміну інформацією. Проведено проектування корпоративної інформаційно-комунікаційної системи на базі комплексу Asterisk з урахуванням вимог до технічних характеристик системи та її елементів, забезпечення необхідних функціональних можливостей, вартісних вимог та обмежень.

Вирішено задачу оптимального розподілу споживачів за підприємствами, які пропонують транспортні послуги, з урахуванням параметрів обслуговування, виробничих можливостей надавачів транспортних послуг та вимог клієнтів. Розглянуто питання визначення структури ринку транспортних послуг, для нього обґрунтовано застосування сегментації, класифікації, структуризації, вперше запропоновано метод класифікації за ентропією. Подано теоретико-ігрову модель для визначення структури парку транспортних засобів, що враховує ризики, протидію конкурентів, різноманітні невизначеності. Отримали подальший розвиток принципи та вимоги до програмного забезпечення для комп’ютеризованих систем підтримки прийняття рішень у галузі транспортного обслуговування. Вдосконалено принципи проектування форм і створення інтерфейсів користувача.

Показано, що інформаційні технології дають нові засоби для вдосконалення взаємовідносин бізнеса з клієнтами, зокрема, соціальні мережі. Найбільш перспективним для моделювання процесів, що відбуваються в соціальних мережах є агентне моделювання. Проведено порівняльний аналіз ринку пакетів імітаційного моделювання за різними характеристиками, на підставі якого для моделювання впливу соціальних мереж на лояльність клієнтів був обраний пакет AnyLogic. Подано предметну технологію моделювання, яка включає: моделювання впливу реклами на формування лояльності клієнтів, моделювання з врахуванням впливу спілкування агентів, моделювання повторних покупок та перевірку адекватності моделі. Побудовані модель та здійснено моделювання впливу соціальних мереж на лояльність клієнтів в середовищі пакета AnyLogic.

Вивчено існуючі підходи та методи інформаційного пошуку, зокрема, концептуальні засади семантичної "павутини", проаналізовано засоби інформаційного пошуку в семантичній "павутині". Визначено критерії релевантності, встановлено показники якості інформаційного пошуку, наведено методологію дослідження узагальненої ефективності інформа-

ційного пошуку в мережі Інтернет. Розглянуто практичне використання методики дослідження ефективності інформаційного пошуку та розроблено відповідний програмний засіб. Наведені результати порівняння інформаційного пошуку з використанням традиційних підходів та запропонованого, котрий ґрунтується на семантичному описі інформаційних ресурсів з використанням метаданих.

Прованалізовано організацію навчального процесу вищого навчального закладу. Розглянуто можливі підходи та сучасний стан моделювання елементів навчального процесу та обґрунтовано необхідність використання для цього імітаційного моделювання з використанням математичного апарату Е-мереж. Описано програмну реалізацію системи, виконану на кафедрі інформаційних систем ХНЕУ. Показано приклади її використання для різних елементів навчального процесу. Проведено дослідження моделей окремих видів занять, таких, як лабораторні і самостійні. Доведено можливість використання запропонованого підходу для побудови моделей процесу вивчення окремої навчальної дисципліни та навчального плану в цілому, а також процесів адаптації студентів за курсами.

Обґрунтовано, що ринок послуг вимагає активного використання реклами. Проведено аналіз видів рекламної кампанії та побудовано дерево функцій процесу "Прогнозування рекламної кампанії". Встановлено, що для успіху рекламної кампанії, а особливо у сфері культури, слід мати математичну модель, параметри якої контролюватимуться керівництвом культурних закладів. Вирішення завдання ефективного планування реклами складається з двох підзадач: визначення розподілу грошей за заходами і пропорцій розподілу грошових коштів за видами реклами в аспекті одного культурно-масового заходу. Для вирішення першої задачі необхідно зберігати динаміку змін кількості проведених заходів, окупності, вкладених коштів у захід та його рекламу. Для вирішення другої необхідно мати узагальнені й проаналізовані параметри за певний період діяльності закладу в минулому. Запропонована математична модель вирішує обидві задачі.

Використана література

1. Абдикеев Н. М. Реинжиниринг бизнес-процессов / Н. М. Абдикеев, Т. П. Данько, С. В. Ильдеменов. – М. : ЭКСМО, 2005. – 578 с.

2. Аволио Ф. М. Защита информации на предприятии / Ф. М. Аволио, Г. Шипли // Сети и системы связи. – 2000. − № 8. – С. 91−99.

3. Автоматизированные информациные технологии в налоговой и бюджетной системах : учебн. пособ. для вузов / под ред. проф. А. Г. Титоренко. – М. : ЮНИТИ-ДАНА, 2001. – 191 с.

4. Акофф Р. Искусство решения проблем / Р. Акофф. – М. : Академия, 2007. – 344 с.

5. Алтунин А. Е. Модели и алгоритмы принятия решений в нечетких условиях / А. Е. Алтунин, М. В. Семухин. – Тюмень : Изд. ТГУ, 2000. – 352 с.

6. Андон Ф. И. Semantic web как новая модель информационного пространства интернет / Ф. И. Андон, И. Ю. Гришанова, В. А. Резниченко // Проблеми програмування. – 2008. – № 2–3. – С. 417–430.

7. Андрейчиков А. В. Анализ, синтез, планирование решений в экономике / А. В. Андрейчиков, О. Н. Андрейчикова. – М. : Финансы и статистика, 2002. – 544 с.

8. Анин Б. Ю. Защита компьютерной информации / Б. Ю. Анин. – СПб. : BHV, 2000. – 384 с.

9. Антонов П. Asterisk і телефонні мережі / П. Антонов. – М. : Демос, 1991. – 340 с.

10. Анусов В. М. Сигналізація у мережі зв’язку / В. М. Анусов. – К. : Либідь, 2005. – 302 с.

11. Артюшенко В. М. Цифровое сжатие информации / В. М. Артюшенко, О. И. Шелухин, М. Ю. Афонин. – М. : Дашков и К°, 2004. – 426 с.

12. Асосков А. В. Поточные шифры / А. В. Асосков. – М. : КУДИЦ-ОБРАЗ, 2003. – 334 с.

13. Базы данных. Интеллектуальная обработка информации / В. В. Корнеев, А. Ф. Гареев, С. В. Васютин и др. – М. : Нолидж, 2003. – 400 с.

14. Барабаш О. В. Мережі наступного покоління NGN / О. В. Барабаш. – К. : Еко-Тренд, 2008. – 424 с.

15. Баранов В. В. Процессы принятия управляющих решений, мотивированных интересами / В. В. Баранов. – М. : ФИЗМАТЛИТ, 2005. – 296 с.

16. Беллами Д. К. Цифрова телефонія / Д. К. Беллами. – К. : Еко-Трендз, 2004. – 640 с.

17. Беллман Р. Принятие решений в расплывчатых условиях. Вопросы анализа и процедуры принятия решений / Р. Беллман, Л. Заде. – М. : Мир, 1976. – 215 с.

18. Берлин А. Н. Телекоммуникационные сети и устройства / А. Н. Берлин. — М. : БИНОМ, 2008. – 320 с.

19. Бернет С. Криптография. Официальное руководство RSA Security. RSA Security's Official Guide to Criptographi / С. Бернет, С. Пэйн ; пер. с англ. под ред. А. И. Тихонова. – М. : БИНОМ, 2007. – 381 с.

20. Беспалько В. П. Стандартизация образования: основные идеи и понятия / В. П. Беспалько // Педагогика. – 1993. – № 5. – С. 16–25.

21. Блейхут Р. Теория и практика кодов, контролирующих ошибки / Р. Блейхут ; пер. с англ. – М. : Мир, 1986. – 576 с.

22. Блюмин С. Л. Модели и методы принятия решений в условиях неопределенности / С. Л. Блюмин, И. А. Шуйкова. – Липецк : ЛЭГИ, 2001. – 138 с.

23. Бодров В. И. Математические методы принятия решений / В. И. Бодров, Т. Я. Лазарева, Ю. Ф. Мартемьянов. – Тамбов : ТГТУ, 2004. – 124 с.

24. Бождай А. С. Мережеві технології / А. С. Бождай. – К. : Либідь, 2009. – 346 с.

25. Болотов А. А. Элементарное введение в эллиптическую криптографию: алгебраические и алгоритмические основы / А. А. Болотов, С. Б. Гашков, А. Б. Фролов. – М. : КОМКНИГА, 2006. – 328 с.

26. Борщов А. Б. Практическое агентное моделирование и его место в арсенале аналитика / А. Б. Борщов А. Б. // ИММОД. – 2005. – 2005. – С. 11–24.

27. Боскин О. О. Имитационная модель процесса дистанционного обучения / О. О. Боскин, Н. А. Соколова // Моделирование объектов и систем управления. – 2004. – № 1. – С. 37–42.

28. Бочкарьов О. Ю. Теорія колективної поведінки (Multiagent systems) / О. Ю. Бочкарьов. – Львів : Вид. НУ "Львівська політехніка", 2004. – 56 с.

29. Бурков В. Н. Модели и механизмы теории активных систем в управлении качеством подготовки специалистов / В. Н. Бурков – М. : ИЦ, 1998. – 158 с.

30. Бурцев В. В. Сбытовая и маркетинговая деятельность / В. В. Бурцев. – М. : Экзамен, 2001. – 224 с.

31. Бусин А. А. Преимущества автоматизации процессов бухгалтерского и налогового учета при внедрении интегрированных информационных систем : материалы 12 Международ. научно-практич. конференции ["Новые информационные технологии в образовании: Формирование новой информационной среды образовательного учреждения с использованием технологий "1С"], (Москва, 31 января – 1 февраля 2012 г.) / А. А. Бусин, И. Н. Мутили // М-во образования и науки РФ, Фирма "1С". – М., 2012. – 403 с.

32. Васильев Ю. В. Самоучитель создания локальной сети / Ю. В. Васильев. – СПб. : Триумф, 2008. – 160 с.

33. Васильев Ю. С. Экономика и организация управления вузом / Ю. С. Васильев – СПб. : Изд. "Лань", 2001. – 544 с.

34. Васильев А. Сжатие изображений: вчера, сегодня, завтра / А. Васильев. – Hard'n'Soft. – 2001. – № 4. – С. 117.

35. Ватолин Д. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео / Д. Ватолин, А. Ратушняк. – М. : ДИАЛОГ-МИФИ, 2002. – 384 с.

36. Вентцель Е. С. Исследование операций / Е. С. Вентцель. – М. : Наука, 2001. – 364 с.

37. Вервейко В. Н. Функции хеширования: классификация, характеристика и сравнительный анализ / В. Н. Вервейко, А. И. Пушкарев, Т. В. Цепурит. – Радиотехника: Всеукр. межвед. науч.-техн. сб. 2002. – № 127. – 136 с.

38. Весна М. А. Самоорганизация в студенческой учебной группе / М. А. Весна // Высшее образование в России. – 2003. – № 2. – С. 93– 95.

39. Гаврилов О. А. Працюємо з модемом / О. А. Гаврилов. – К. : Маліп, 2007. – 267 с.

40. Галатенко В. А. Основы информационной безопасности: курс лекций : учебн. пособ. / В. А. Галатенко. – М. : Интернет-Ун-т Информационных Технологий, 2004. – 261 с.

41. Галчинський К. Ю. Комп'ютерні системи у телефонії / К. Ю. Галчинський. – К. : Оскол, 2009. – 210 с.

42. Гарфилд Б. Десять заповедей рекламы / Б. Гарфилд. – СПб. : Питер, 2007. – 256 с.

43. Голубков Е. П. Маркетинговые исследования: теория, методология и практика / Е. П. Голубков. – М. : Финпресс, 1998. – 414 с.

44. Гольдштейн М. П. IP-телефонія / М. П. Гольдштейн, А. В. Пінчук, А. Л. Суховицький – К. : Либідь, 2006. – 346 с.

45. Гольдштейн М. П. IP-телефонія / М. П. Гольдштейн. – К. : Юнайт, 2007. – С. 230–240.

46. Гольдштейн М. П. Call-центри та комп'ютерна телефонія / М. П. Гольдштейн, В. А. Фрейкнман. – Львів : Тебер, 2006. – 476 с.

47. Горальскі В. ADSL / В. Горальскі. – К. : Лоррі, 2005. – 240 с.

48. Горюнов Ю. Ю. Теория и методы принятия решений / Ю. Ю. Горюнов. – Ростов н/Д. : РГУИТП, 2009. – 50 с.

49. Горяинов А. Н. Стоимостные параметры работы автотранспорта в логистической системе / А. Н. Горяинов // Автомобильный транспорт : сборник научных трудов. – Х. – 2002. – Вып. 9. – С. 20–22.

50. Градосельская Г. В. Сетевые измерения в социологии : учебное пособие / Г. В. Градосельская ; под ред. Г. С. Батыгина. – М. : Издательский дом "Новый учебник", 2004. – 248 с.

51. Губанов Д. А. Социальные сети: модели информационного влияния, управления и противоборства / под ред. чл.-корр. РАН Д. А. Новикова // Д. А. Губанов, Д. А. Новиков, А. Г. Чхартишвили. – М. : Издательство Физико-математической литературы, 2010. – 228 с.

52. Давыденко В. А. Моделирование социальных сетей / В. А. Давыденко, Г. Ф. Ромашкина, С. Н. Чуканов // Вестник Тюменского государственного университета. – 2005. – № 1. – С. 68–79.

53. Даниленков А. О. Локальная сеть своими руками / А. О. Даниленков, Ю. В. Васильев. — СПб. : Триумф, 2008. – 320 с.

54. Девянин П. Н. Модели безопасности компьютерных систем : учебн. пособ. для вузов / П. Н. Девянин. – М. : Академия, 2005. – 142 с.

55. Деднев М. А. Защита информации в банковском деле и электронном бизнесе / М. А. Деднев, Д. В. Дыльнов, М. А. Иванов. – М. : КУДИЦ-ОБРАЗ, 2004. – 512 с.

56. Дейт К. Введение в системы баз данных / К. Дейт. – 7-е изд. / К. Дейт. – М. : Вильямс, 2001. – 1072 с.

57. Денисов О. К. Компьютерные сети. Услуги международной связи / О. К. Денисов. – М. : ЭлисЛТД, 2003. – 205 с.

58. Деньжаков А. Ю. Анализ доверия как формализуемой концепции [Текст] / А. Ю. Деньжаков, С. В. Шибанов // Молодой ученый. – 2011. – № 9. – С. 29–33.

59. Джеффри Х. Мур. Экономическое моделирование в MICROSOFT EXCEL / Джеффри Х. Мур, Лари Р. Уэдерфорд. – М. : Вильямс, 2004. – 1024 с.

60. Дилморт М. П. Соціальні мержі. Керівництво з експлуатації / М. П. Дилморт. — Львів : Добра книга, 2010. – 248 с.

61. Диффи У. Защищенность и имитостойкость / У. Диффи, М. Хелльман // Введение в криптографию. – 1979. – № 3 – С. 79–109.

62. Додд З. А. Мір телекомунікації. Огляд технологій / З. А. Додд. – К. : Олімп-бізнес, 2003. – 400с.

63. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты / В. В. Домарев. – М. : DiaSoft, 2002. – 671 с.

64. Домарев В. В. Защита информации и безопасность компьютерных систем / В. В. Домарев. – К. : Издательство ДиаСофт, 1999. – 480 с.

65. Домарев В. В. Защита информации и безопасность компьютерных систем / В. В. Домарев. – К. : ДиаСофт, 2009. – 480 с.

66. Домашев Ф. В. Программирование алгоритмов защиты информации : учебн. пособ. / Ф. В. Домашев. – М. : Нолидж, 2005. – 288 с.

67. Дорохов О. В. Обгрунтування методики класифікації суб'єктів транспортного ринку / О. В. Дорохов, Л. П. Дорохова // Вестн. Харьк. нац. автомоб.-дор. ун-та : сб. науч. тр. – Х., 2003. – Вып. 22. – С. 43–46.

68. Дорохов О. В. Багатокритеріальний розподіл споживачів по центрах транспортного обслуговування / О. В. Дорохов, Є. В. Нагорний // Радіоелектр. і комп'ют. сист.: наук. технічн. журнал Нац. аерокосм. ун-ту ім. М. Е. Жуковського "Харк. авіац. ін-т". – Х., 2004. – № 1(5). – С. 64–68.

69. Дорохов О. В. Методика однопараметричної ідентифікації та сегментації зон обслуговування споживачів / О. В. Дорохов, Є. В. Нагорний, В. І. Вербицький // Вісн. Нац. техн. ун-ту "Харк. політехн. ін-т". – Х., 2003, – № 6, Т. 1. – С. 33–42.

70. Дорохов О. В. Оптимізація та підвищення швидкодії додатків при комп'ютерній реалізації транспортних задач / О. В. Дорохов, В. І. Фастовець // Вестн. Харьк. нац. автомоб. дор. ун-та : Сб. науч. тр. – Х., 2004. – Вып. 24. – С. 81–83.

71. Дружинин В. Н. Когнитивная психология / В. Н. Дружинин, Д. В. Ушаков. – М. : ПЕР СЭ, 2002. – 480 с.

72. Дубров А. М. Моделирование рисковых ситуаций в экономике и бизнесе / А. М. Дубров, Б. А. Лагоша, Е. Ю. Хрусталев ; под ред. Б. А. Лагоши. – М. : Финансы и статистика, 2000. – 176 с.

73. Дуравкин Е. В. Использование аппарата Е-сетей для анализа распределенных программных систем / Е. В. Дуравкин, Амер Таксин Каламех Абу Джаккар // Моделирование объектов и систем управления. — 2005. – № 1. – С. 24–28.

74. Дюбин Г. Н. Введение в прикладную теорию игр / Г. Н. Дюбин, В. Г. Суздаль. – М. : Наука, 1981. – 336 с.

75. Дяконов В. Ю. Matlab. Аналіз, ідентифікація та моделювання систем / В. Ю. Дяконов. – К. : Пітер, 2006. – 448 с.

76. Евсеев С. П. Криптографическое преобразование информации в кодовых криптосистемах на эллиптических кодах для каналов с автоматическим переспросом / С. П. Евсеев / Збірник наукових праць ХУПС. – Х. : ХУПС. – 2007. – Вип. 8(66). – С. 29–32.

77. Евсеев С. П. Несимметричные криптосистемы на ЭК для каналов с автоматическим переспросом / С. П. Евсеев / Збірник наукових праць ХУПС. – Х. : ХУПС. – 2007. – Вип. 5(63). – С. 134–137.

78. Елиферов В. Г. Бизнес-процессы: регламентация и управление / В. Г. Елиферов, В. В. Репин. – М. : ИНФРА-М, 2005. – 319 с.

79. Жданов О. И. Эллиптические кривые: Основы теории и криптографические приложения / О. И. Жданов. – СПб. : Либроком, 2012. – 200 с.

80. Заболотная Г. М. Феномен доверия и его социальные функции / Г. М. Заболотная // Вестник Российского университета Дружбы народов. – 2003. – № 4–5. – С. 79–85.

81. Завгородний В. И. Комплексная защита информации в компьютерных системах : учебн. пособ. для вузов / В. И. Завгородний. – М. : Логос, 2001. – 262 с.

82. Завгородний В. П. Налоги и налоговый контроль в Украине / В. П. Завгородний. – К. : А.С.К., 2003. – 640 с.

83. Защита программ и данных : учебн. пособ. / П. Ю. Белкин, О. О Михальский, А. С. Першаков и др. ; под ред. П. Ю. Белкина. – М. : Радио и связь, 2000. – 188 с.

84. Зелигер Н. Б. Проектирование сетей и систем передачи дискретных сообщений / Н. Б. Зелигер, О. С. Чугреев, Г. Г. Яновский. – М. : Радио и связь, 2010. – 176 с.

85. Зубов А. Ю. Совершенные шифры : учебн. пособ. / А. Ю. Зубов. – М. : ГЕЛИОС АРВ, 2003. – 160 с.

86. Иванов М. А. Криптография. Криптографические методы защиты информации в компьютерных системах и сетях : учебн. пособ. / М. А. Иванов. – М. : КУДИЦ-Образ, 2001. – 368 с.

87. Император 3.1. ЗАО НИЦММиНТ НЕЙРОСПЛАВ. Собственность компании. Самоучитель. – М. : ЭКСМО, 2000. – 188 с.

88. Информационные технологии в кадровом учете и управлении персоналом 2007. Собственность компании. Аналитический обзор российского рынка автоматизированных систем управления персоналом. – М. : Tadviser, 2007. – 81 с.

89. Калянов Г. Н. Моделирование, анализ, реорганизация и автоматизация бизнес-процессов / Г. Н. Калянов. – М. : Финансы и статистика, 2006. – 240 с.

90. Капустин П. Анализ бизнес-процессов организации / П. Капустин, В. Голубев // Право. Экономика. Маркетинг. – 1999. – № 9–10. – С. 17–22.

91. Каскадні схеми захисту інформації на алгеброгеометричних кодах / Ю. В. Стасев, А. А. Кузнецов, В. И. Грабчак и др. Системи озброєння і військова техніка. – Х. : ХУПС. – 2006. – Вип. 1(5). – С. 82–87.

92. Кастельс М. Галактика Интернет / М. Кастельс. – Екатеринбург : У-Фактория, 2004. – 328 с.

93. Катренко А. В. Теорія прийняття рішень : підручник / А. В. Катренко, В. В. Пасічник, В. П. Пасько. – К. : Видавнича група BHV, 2009. – 448 с. : іл.

94. Кашкаров О. П. Нові можливості мобільних телефонів, телефонія, радіозв’язок та інше / О. П. Кашкаров. – К. : Додека XXI, 2007. – 312 с.

95. Кенин А. М. Самоучитель системного администратора / А. М. Кенин. – СПб. : БВХ, 2008. – 560 с.

96. Кірх О. LINUX для професіоналів. Керівництво адміністратора мережі / О. Кірх. – Львів : Огут, 2000. – 368 с.

97. Кнэпп Э. Эллиптические кривые / Э. Кнэпп. – М. : Факториал Пресс, 2004. – 488 с.

98. Колисниченко Д. Ю. Беспроводная сеть дома и в офисе / Д. Ю. Колисниченко. — СПб. : БХВ-Петербург, 2009. – 480 с.

99. Кондратьев В. В. Показываем бизнес-процессы / В. В. Кондратьев, М. Н. Кузнецов. – М. : ЭКСМО, 2008. – 256 с.

100. Кондратьев С. Н. О критериях эффективности графиков совместной работы автомобилей в логистической системе / С. Н. Кондратьев // Автомоб. трансп. : сб. науч. тр. – Х., – 2002. – Вып. 10. – С. 91–93.

101. Конеев И. Р. Информационная безопасность предприятия / И. Р. Конеев, А. В. Беляев. – СПб. : БХВ-Петербург, 2003. – 752 с.

102. Корнеев И. К. Защита информации в офисе : учебник / И. К. Корнеев. – М. : Проспект, 2008. – 333 с.

103. Кофман А. Введение в теорию нечетких множеств / А. Кофман. – М. : Радио и связь, 1982. – 432 с.

104. Краковский Ю. М. Информационная безопасность и защита информации / Ю. М. Краковский. – М. ; Ростов н/Д. : МарТ, 2008. – 287 с.

105. Кричевский Р. Сжатие и поиск информации / Р. Кричевский. – М. : Радио и связь, 1989. – 424 с.

106. Крысин А. В. Информационная безопасность / А. В. Крысин. – М. ; К. : Спаррк: Век+, 2003. – 319 с.

107. Кузнецов А. А. Анализ механизмов обеспечения безопасности банковской информации во внутриплатежных системах коммерческого банка : Матеріали з міжнародної науково-практичної конференції "Безпека та захист інформації в інформаційних і телекомунікаційних системах" / А. А. Кузнецов, О. Г. Король, А. М. Ткачов // Зб. наук. статей "Управління розвитком". − Х. : 2008. – № 6. – С. 28–35.

108. Кузнецов А. А. Исследование протоколов и механизмов защиты информации в компьютерных системах и сетях / А. А. Кузнецов, С. П. Евсеев, Б. П. Томашевский и др. / Збірник наукових праць ХУПС. – Х. : ХУПС. – 2007. – Вип. 2(14). – С. 102–111.

109. Кузнецов А. А. Разработка теоретико-кодовых схем с использованием эллиптических кодов / А. А. Кузнецов, С. П. Евсеев // Системи обробки інформації. – Х. : ХВУ, 2004. – № 5. – С. 127–132.

110. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії : навч. посібн. / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : ХНЕУ, 2010. – 360 с.

111. Кузьмінський А. І. Педагогіка вищої школи : навч. посібн. / А. І. Кузьмінський. – 2-ге вид., стер. – К. : Знання, 2011. – 486 с.

112. Кулябов Д. С. Введение в формальные методы описания бизнес-процессов / Д. С. Кулябов, А. В. Королькова. – М. : РУДН, 2008. – 173 с.

113. Куприянов А. И. Основы защиты информации : учебн. пособ. / А. И. Куприянов. – М. : Академия, 2008. – 256 с.

114. Курицкий Б. Я. Поиск оптимальных решений средствами Excel 7.0 / Б. Я. Курицкий. – СПб. : BHV – Санкт-Петербург, 1997. – 387 с.

115. Курицкий Б. Я. Применение пакетов прикладных программ по экономико-математическим методам в АСУ / Б. Я. Курицкий, Г. П. Алексеенко, Ю. В. Викин. – М. : Статистика, 1980. – 196 с.

116. Кучніков Т. А. Інтернет-телефонія / Т. А. Кучніков. – Львів : Алянс-пресс, 2004. – 128 с.

117. Ландэ Д. В. Интернетика. Навигация в сложных сетях. Модели и алгоритмы / Д. В. Ландэ, А. А. Снарский, И. В. Безсуднов. – М. : Либроком, 2009. – 264 с.

118. Ларичев О. И. Качественные методы принятия решений / О. И. Ларичев, Е. М. Мошкович. – М. : Физматлит, 1996. – 208 с.

119. Ларичев О. И. Теория и методы принятия решений / О. И. Ларичев. – 2-е изд., перераб. и доп. – М. : ЛОГОС, 2002. – 392 с.

120. Ларичев О. И. Теория и методы принятия решений, а также Хроника событий в Волшебных странах / О. И. Ларичев. – М. : ЛОГОС, 2000. – 296 с.

121. Левитин А. Жадные методы: Алгоритм Хаффмана / А. Левитин // Алгоритмы: введение в разработку и анализ. – М. : Вильямс, 2006. – 398 с.

122. Левтеров А. И. Компьютерная реализация задач управления для автотранспортных предприятий / А. И. Левтеров, А. В. Дорохов // Автомоб. трансп. : сб. науч. тр. – Х., 2002. – Вып. 9. – С. 23–25.

123. Леонова Н. М. Параметрически адаптивное управление образовательной деятельностью : монография / под ред. А. Д. Модяева. – М. : МИФИ, 2006. – 116 с.

124. Леонова Н. М. Синтез алгоритмов адаптивного структурно-параметрического управления образовательной деятельностью / Н. М. Леонова ; под ред. А. Д. Модяева. – М. : МИФИ, 2006. – 116 с.

125. Литвак Б. Г. Разработка управленческого решения / Б. Г. Литвак. – М. : Изд. "Дело", 2004. – 392 с.

126. Лодон Дж. Управление информационными системами / Дж. Лодон. – СПб. : Питер, 2005. – 453 с.

127. Лодон Дж. Управление информационными системами / Дж. Лодон ; пер. с англ. ; под ред. Д. Р. Трутнева. – 7-е изд. – СПб. : Питер, 2005. – 912 с.

128. Лоу А. М. Имитационное моделирование / А. М. Лоу, В. Д. Кельтон. – СПб. : Питер, Издательская группа BHV, 2004. – 847 с.

129. Лускатова О. В. Современные проблемы реинжиниринга бизнес-процессов / О. В. Лускатова, М. В. Робертс. – Владимир : Изд. Владим. гос. ун-та, 2011. – 146 с.

130. Лычкина Н. Н. Имитационное моделирование экономических процессов : учебн. пособ. для слушателей программы eMBI / Н. Н. Личкина. – М. : Инфра-М, 2012. – 256 с.

131. Лычкина Н. Н. Компьютерное моделирование социально-экономического развития регионов в системах поддержки принятия решений / Н. Н. Личкина // Банковские технологии. – 2000. – Вып. 9. – С. 60–63.

132. Лычкина Н. Н. Современные тенденции в имитационном моделировании / Н. Н. Лычкина // Вестник университета, серия Информационные системы управления № 2. – М. : ГУУ, 2000. – № 4. – С. 16–22.

133. Лычкина Н. Н. Современные технологии имитационного моделирования и их применение в информационных бизнес-системах / Н. Н. Личкина // ИММОД-2005. – 2005. – С. 25–31.

134. Лычкина Н.Н. Технологические возможности современных систем моделирования / Н. Н. Лычкина // Банковские технологии. – 2000. – Вып. 9. – С. 32–38.

135. Лямец В. И. Системный анализ / В. И. Лямец, А. Д. Тевяшев. – Х. : ХНУРЭ, 2004. – 448 с.

136. Маклаков А. Г. Профессиональный психологический отбор персонала. Теория и практика : учебник для вузов / А. Г. Маклаков. – СПб. : Питер, 2008. – 480 с.

137. Мезенцев К. Н. Моделирование систем в среде AnyLogic 6.4.1 : учебн. пособ. Часть 1 / К. Н. Мезенцев ; под ред. Заслуженного деятеля науки РФ, докт. техн. наук., проф. А. Б. Николаева. — М. : МАДИ, 2011. – 109 с.

138. Мезенцев К. Н. Моделирование систем в среде AnyLogic 6.4.1 : учебн. пособ. Часть 2 / К. Н. Мезенцев ; под ред. Заслуженного деятеля науки РФ, докт. техн. наук., проф. А. Б. Николаева. — М. : МАДИ, 2011. – 103 с.

139. Мельников В. П. Информационная безопасность и защита информации : учебн. пособ. / В. П. Мельников. – М. : Академия, 2008. – 330 с.

140. Минухин С. В. Модели бизнес-процессов для управления процессно ориентированным предприятием / С. В. Минухин, А. Н. Беседовский // Економіка розвитку. – Х. : ХНЕУ, 2005. – № 3. – С. 99–102.

141. Минухин С. В. Моделирование бизнес-процессов в информационной системе предприятия / С. В. Минухин, А. Н. Беседовский // Вестник НТУ "ХПИ". Технический прогресс и эффективность производства. Сборник научных трудов. – Х. : НТУ "ХПИ", 2001. – № 9. – С. 121–125.

142. Миронов А. С. Використання Е-мереж для імітаційного моделювання бізнес-процесів систем масового обслуговування / А. С. Миронов // Міжнародна науково-практична конференція молодих вчених, аспірантів та студентів "Актуальні проблеми науки та освіти молоді: теорія, практика, сучасні рішення", 21–22 квітня 2011 р. : тези доповідей. Том 1. – Х. : ХНЕУ, 2011. – С. 141–143.

143. Миронов А. С. Використання математичного апарату Е-мереж для імітаційного моделювання / А. С. Миронов // Збірник наукових праць студентів специальностей "Інформаційні управляючі системи і технології", "Комп'ютерний еколого-економічний моніторинг". – Х. : ХНЕУ, 2010. – С. 57–58.

144. Михайлов А. В. Компьютерные вирусы и борьба с ними / А. В. Михайлов. – СПб. : Диалог-МИФИ, 2011. – 104 с.

145. Михайлов Д. В. Аутсорсинг. Новая система организации бизнеса / Д. В. Михайлов. – М. : КноРус, 2006. – 145 с.

146. Михеева Т. В. Обзор существующих программных средств имитационного моделирования при исследовании механизмов функционирования и управления производственными системами / Т. В. Михеева // Управление, вычислительная техника и информатика. – 2009. – № 6. – С. 87–90.

147. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / Р. Морелос-Сарагоса. – М. : Техно-сфера, 2006. – 320 с.

148. Мухин В. И. Информационная безопасность компьютерных систем : учебн. пособ. / В. А. Мухин, Ю. А. Щербаков. – М. : Изд. Воен. акад. РВСН, 1999. – 122 с.

149. Мюррей У. Создание переносимых приложений для Windows / У. Мюррей, К. Паппас. – СПб. : БХВ, 1999. – 816 с.

150. Нагорний Є. В. Маршрутизація партіонних перевезень та її комп'ютерна реалізація / Є. В. Нагорний, О. В. Дорохов // Автомоб. трансп. : сб. науч. тр. – Х., 2002. – Вып. 10. – С. 21–23.

151. Нагорний Є. В. Методика вибору ефективної стратегії обслуговування споживачів транспортної продукції / Є. В. Нагориний, О. В. Дорохов // Автомоб. трансп. : сб. науч. тр. – Х., 2002. – Вып. 9. – С. 17–19.

152. Нагорний Є. В. Вибір ефективної стратегії логістичного сервісу споживачів транспортних послуг у фармації / Є. В. Нагориний, О. В. Дорохов, Л. П. Дорохова // Матеріали міжн. наук.-практ. конф. "Здобутки та перспективи розвитку управління фармацевтичними організаціями в умовах ринкової економіки". – Х. : НФаУ. – 2003. – С. 137–142.

153. Нагорний Є. В. Ефективна реалізація інтерфейсу користувача при розробці інформаційних систем транспортного обслуговування / Є. В. Нагорний, А. І. Левтеров, О. В. Дорохов // Автомоб. трансп. : сб. науч. тр. – Х., 2003. – Вып. 12. – С. 11–14.

154. Нагорний Є. В. Засоби перевірки достовірності вводу при комп'ютерній реалізації задач транспортного сервісу / Є. В. Нагорний, А. І. Левтеров, О. В. Дорохов // Пробл. пожежн. безп. : зб. наук. праць. Акад. пожежн. безп. України. – Х., 2003. – Вып. 13. – С. 99–107.

155. Нагорный Е. В. Современное состояние украинского рынка транспортно- экспедиционных услуг и пути его реформирования / Е. В. Нагорный // Вестн. Харьк. нац. автомоб. дор. ун-та : сб. науч. тр. – 2003. – Вып. 22. – С. 39–42.

156. Нанс Б. Комп'ютерні мережі / Б. Нанс. – К. : Бітон, 2007. – 245 с.

157. Нельке М. Учимся принимать решения. Быстро, точно, правильно / М. Нельке. – М. : ОМЕГА-Л, 2007. – 127 с.

158. Нечаев В. И. Элементы криптографии: Основы теории защиты информации : учебн. пособ. / В. И. Нечаев. – М. : Высшая школа, 2004. – 109 с.

159. Ногин В. Д. Принятие решений при многих критериях : учебн.-метод. пособ. / В. Д. Ногин. – СПб. : Изд. "ЮТАС", 2007. – 104 с.

160. Овчинникова Н. Н. Рекламное дело / Н. Н. Овчинникова. – М. : "Дашков и К°", 2008. – 368 с.

161. Оліфер В. Г. Компютерні мережі. Принципи, технології, протоколи / В. Г. Оліфер. – Львів : Олів, 2008. – 230 с.

162. Орехова І. С. Державний контроль у сфері господарської діяльності: адміністративно-правові засади: дис. … кандидата юрид. наук: 12.00.07. / І. С. Орехова – Одеса, 2009. – 211 с.

163. Орлов А. И. Эконометрика / А. И. Орлов. – М. : Экзамен, 2002. – 576 с.

164. Орлов О. А. Повна енциклопедія Інтернету / О. А. Орлов, Н. В. Богданов-Катьков, М. Н. Гор. — К. : АСТ, 2008. – 896 с.

165. Орлов А. И. Нечисловая статистика / А. И. Орлов. – М. : МЗ-Пресс, 2004. – 345 с.

166. Орлов А. И. Основы теории принятия решений / А. И. Орлов. – М. : Финансы и статистика, 2004. – 192 с.

167. Орлов А. И. Принятие решений. Теория и методы разработки управленческих решений : учебн. пособ. / А. И. Орлов. – М. : Март, 2005 – 496 с.

168. Орлова И. В. Экономико-математические методы и модели. Компьютерное моделирование / И. В. Орлова, В. А. Половников. — М. : Вузовский учебник, 2007. — 365 с.

169. Орловский С. А. Проблемы принятия решений при нечеткой исходной информации / С. А. Орловский. – М. : Наука, 1981. – 208 с.

170. Ортинський В. Л. Педагогіка вищої школи : навч. посібн. [для студ. вищ. навч. закл.] / В. Л. Ортинський – К. : Центр учбової літератури, 2009. – 472 с.

171. Основы криптографии : учебн. пособ. / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин и др. – М. : Гелиос АРВ, 2005. – 480 с.

172. Остервальдер А. Построение бизнес-моделей: Настольная книга стратега и новатора / А. Остервальдер, И. Пинье. – М. : Альпина Паблишер, 2011. – 288 с.

173. Павленко Л. А. Методичні рекомендації до виконання самостійної роботи з навчальної дисципліни "Методи та системи підтримки прийняття рішень в управлінні еколого-економічними процесами промислових підприємств" для студентів спеціальності 8.080407 усіх форм навчання / Л. А. Павленко. – Х. : Вид ХНЕУ, 2009. – 36 с.

174. Паринов С. И. К теории сетевой экономики / С. И. Паринов. – Новосибирск : ИЭОПП, СО РАН, 2002. – 168 с.

175. Петров А. Г. Якість обслуговування у мережах IP / А. Г. Петров. – Донецьк : Донтек, 2005. – 205 с.

176. Петров А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров. – М. : Изд. ДМК, 2000. – 445 с.

177. Печенкин В. В. Методы анализа социальных сетей на примере визуализации структуры предпочтений профессий / В. В. Печенкин // Социология: 4М. – 2001. – № 13. – С. 60–75.

178. Податковий кодекс України // Відомості Верховної Ради України. – 2011. – № 13–17.

179. Подиновский В. В. Парето-оптимальные решения многокритериальных задач / В. В. Подиновский, В. Д. Ногин. – М. : Наука, 1982. – 256 с.

180. Положення про організацію навчального процесу в кредитно-модульній системі підготовки фахівців / укл. М. В. Афанасьєв ; [наукове керівництво докт. екон. наук, професора Пономаренка В. С.]. – Х. : Вид. ХНЕУ, 2008. – 244 с.

181. Поляк-Брагинский О. Адміністрування мережі на прикладах / О. Поляк-Брагинський. – Львів : БХВ, 2008. – 432 с.

182. Поляк-Брагинский О. Локальні мережі. Модернізація та пошук помилок / О. Поляк-Брагинський. – Львів : БХВ, 2008. – 432 с.

183. Пономаренко В. С. Механізм прийняття управлінських рішень на підприємстві: процесний підхід : наукове видання / В. С. Пономаренко, С. В. Мінухін, О. М. Беседовський. – Х. : Вид. ХНЕУ, 2005. – 240 с.

184. Поплавская А. Н. Власть дизайна: путь к сердцу потребителя / А. Н. Поплавская – Мн. : Гревцов Паблишер, 2007. – 256 с.

185. Попов В. Б. Основы информационной безопасности. Информационные технологии и право / В. Б. Попов. – М. : 2002. – 248 с.

186. Практика и проблематика моделирования бизнес-процессов / А. Г. Зуева, Б. В. Носков, С. П. Киселев, и др. – М. : АйТи, 2007. – 366 с.

187. Про вищу освіту : Закон України (нова редакція) // Відомості Верховної Ради України (ВВР).– 2002. – № 20. – 134 с.

188. Про електронні документи та електронний документообіг: Закон України / Відомості Верховної Ради. – 2003. – № 36. – С. 275.

189. Про захист інформації в автоматизованих системах : Закон України // Відомості Верховної Ради України. – 2005. – № 26. – С. 347.

190. Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні: указ Президента України від 31 липня 2000 року № 928/2000 // Урядовий кур'єр. – 2000. – № 143. – С. 4.

191. Про зв'язок : Закон України від 16.05.2005 р. № 1280-III // Відомості Верховної Ради України. – 2005. – № 56. – С. 44–45.

192. Про інформацію : Закон України від 13 серпня 2011 року № 32-IV // Відомості Верховної Ради України. – 2011. – № 313. – С. 42.

193. Про концепцію Національної програми інформатизації : Закон України (із змінами, внесеними згідно із Законами № 3421-IV (3421-15) від 09.02.2006, ВВР, 2006, № 22, ст. 199 № 3610-VI (3610-17) від 07.07.2011, ВВР, 2012, № 7, ст. 53) // Голос України (офіційне видання). – 2006. – № 41.

194. Про Національну програму інформатизації : Закон України (із змінами, внесеними згідно із Законами № 2684-III (2684-14) від 13.09.2001,

ВВР, 2002, № 1, ст. 3 № 2289-VI (2289-17) від 01.06.2010, ВВР, 2010, № 33, ст. 471). – Офіційний вісник України (офіційне видання) від 26.03.1998, № 10, стор. 5, стаття 375, код акту 4986/1998.

195. Про положення про порядок здійснення криптографічного захисту інформації в Україні : Указ Президента України від 28 серпня 2009 року № 693/2009 // Президентський вісник. – 2009. – № 6. – С. 131.

196. Про театри і театральну справу: закон України від 31.05.2005 № 2605-IV // Відомості Верховної Ради України. – 2005. – № 26. – С. 350.

197. Пушкарев А. И. Функции хэширования: классификация, характеристика, сравнительный анализ / А. И. Пушкарев, Т. В. Цепурит. – Х. : ХНУРЭ, 2002. – 68 с.

198. Пярин В. А. Безопасность электронного бизнеса / В. А. Пярин. – М. : Гелиос АРВ, 2002. – 429 с.

199. Райхельд Ф. Эффект лояльности: движущие силы экономического роста, прибыли и непреходящей ценности / Ф. Райхельд, Т. Тил. – М. : Вильямс, 2005. – 384 с.

200. Репин В. В. Бизнес-процессы компании: построение, анализ, регламентация / В. В. Репин. – М. : РИА "Стандарты и качество", 2007. – 240 с.

201. Репин В. В. Процессный подход к управлению. Моделирование бизнес-процессов / В. В. Репин, В. Г. Елиферов. – М. : Стандарты и качество, 2004. – 408 с.

202. Робсон М. Реинжиниринг бизнес-процессов: практическое руководство / М. Робсон, Ф. Уллах. – М. : ЮНИТИ-ДАНА, 2003. – 222 с.

203. Романец Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин. – 2-е изд., перераб. и доп. – М. : Радио и связь, 2001. – 376 с.

204. Романов П. В. Методы прикладных социальных исследований : учебн. пособ. / П. В. Романов, Е. Р. Ярская-Смирнова. – [2-е изд., доп.]. – М. : ООО "Вариант", ЦСПГИ, при участии ООО "Норт Медиа", 2008. – 215 с.

205. Росляков А. В. Основи передачі голосових даних мережами IP / А. В. Росляков. – К. : Пресс, 2009. – 309 с.

206. Росс Д. Wi-Fi. Беспроводные сети. Установка. Конфигурирование. Использование / Д. Росс. — СПб. : НТ Пресс, 2006. – 312 с.

207. Ростовцев А. Г. Теоретическая криптография / А. Г. Ростовцев. – СПб. : АНО НПО "Профессионал", 2005. – 480 с.

208. Ротштейн А. П. Интеллектуальные технологии идентификации: нечеткая логика, генетические алгоритмы, нейронные сети / А. П. Ротштейн. – Винница : УНИВЕРСУМ-Винница, 1999. – 320 с.

209. Рябко Б. Я. Основы современной криптографии для специалистов в информационных технологиях : монография / Б. Я. Рябко. – М. : Научный мир, 2004. – 173 с.

210. Саати Т. Аналитическое планирование. Организация систем / Т. Саати, К. Кернс. – М. : Радио и связь, 1991. – 224 с.

211. Сазанов В. М. Социальные сети – публичная сфера. К Солнечной Виртуальности – через пассионарность и интеллектуальность / В. М. Сазанов. – М. : Лабораторія СВМ, 2011. – 223 с.

212. Саморезов В. В. Телекомунікації. Протоколи SIP / В. В. Саморезов. – Л. : Лев, 2008. – 37 с.

213. Северинов А. В. Алгоритм построения укороченных кодов Гоппы / А. В. Северинов // Обработка информации и обеспечение надежности систем управления. – Х. : ХВУ, 1997. – С. 38–41.

214. Северинов А. В. Обеспечение имитозащищенности каналов передачи данных с укороченными кодами Гоппы / А. В. Северинов // Інформаційно-керуючі системи на залізничному транспорті. – Х. : ХарДАЗТ. – 1997. – № 3. – С. 29–30.

215. Селомон Д. Сжатие данных, изображений и звука / Д. Селомон. – М. : Техносфера, 2004. – 368 с.

216. Сергеенко В. Сжатие данных, речи, звука и изображений в телекоммуникационных системах / В. Сергеенко, В. Баринов. – М. : Кудиц-Образ, 2009. – 360 с.

217. Сидельников В. М. Криптография и теория кодирования / В. М. Сидельников. – М. : ФИЗМАТЛИТ, 2008. – 188 с.

218. Сидельников В. М. Криптография и теория кодирования / В. М. Сидельников // Материалы конференции "Московский университет и развитие криптографии в России". – М. : МГУ, 2002. – 22 с.

219. Сидельников В. М. Теория кодирования / В. М. Сидельников. – М. : ФИЗМАТЛИТ, 2008. – 324 с.

220. Скляр Б. О. Цифровий зв’язок / Б. О. Скляр. – Х. : Дельта, 2006. – 256 с.

221. Смехов А. А. Маркетинговые модели транспортного рынка / А. А. Смехов. – М. : Транспорт, 1998. – 120 с.

222. Снетков Н. Н. Имитационное моделирование экономических процессов : учебн.-практ. пособ. / Н. Н. Снетков. – М. : Изд. центр ЕАОИ, 2008. – 228 с.

223. Соколов А. В. Защита от компьютерного терроризма / А. В. Соколов, О. М. Степанюк. – БХВ-Петербург Арлит, 2002. – 496 с.

224. Соколов А. В. Методы информационной защиты объектов и компьютерных сетей / А. В. Соколов. – СПб. : Полигон, 2000. – 269 с.

225. Сословский В. Г. Разработка бизнес-плана предприятия. Методические указания / В. Г. Сословский, Н. А. Куцин. – Х. : Изд. ХГАДТУ, 1996. – 64 с.

226. Сословський В. Г. Визначення структури парку транспортних засобів із застосуванням ігрового підходу / В. Г. Сословський, Є. В. Нагорний, О. В. Дорохов // Вісн. Харк. держ. техн. ун-ту сільськ. госп-ва : зб. наук. праць. – Х., 2004. – Вип. 23. – С. 321–326.

227. Справочник по прикладной статистике. – М. : Финансы и статистика, 1990. – 526 с.

228. Стасев Ю. В. Несимметричные теоретико-кодовые схемы с использованием алгеброгеометрических кодов / Ю. В. Стасев, А. А. Кузнецов / Кибернетика и системный аналіз : международный научно-теоретический журнал. – К. : НАНУ. – 2005. – № 3. – С. 47–57.

229. Степанов Е. А. Информационная безопасность и защита информации : учебн. пособ. / Е. А. Степанов, И. К. Корнеев. – М. : ИНФРА-М, 2001. – 301 с.

230. Столлингс В. Криптография и защита сетей: принципы и практика / В. Столлингс ; пер. с англ. – М. : Вильямс, 2001. – 669 с.

231. Столлінгс В. Криптографія та захист мереж. Принципи та практика / В. Столлінгс. – К. : Вільсон, 2006. – 672 с.

232. Столлінгс В. А. Комп'ютерні мережі, протоколи та технології Інтернета / В. А. Столлінгс. — К. : БХВ, 2005. – 832 с.

233. Суворов М. А. Процессуализация налоговых проверок: проблемы и пути совершенствования / М. А. Суворов. – М. : Наука, 2007. – 271 с.

234. Табачникова М. Б. Сетевой анализ организации : учебн.-метод. пособ. для вузов / М. Б. Табачникова. – Воронеж : Изд.-полигр. центр ВГУ, 2019. – 39 с.

235. Тарасов В. Б. Агенты, многоагентные системы, виртуальные сообщества: стратегическое направление в информатике и искусственном интеллекте / В. Б.Тарасов. – М. : Эдиториал УРСС, 2009. – 47 с.

236. Тарасов О. В. Моделювання процесу проведення рекламних кампаній культурно-масових заходів / О. В. Тарасов, М. А. Бакіров. // Системи обробки інформації. – Х. : ХУПС, 2012. – № 4(102). – С. 68–71.

237. Тарасов О. В. Дослідження ефективності блочно-статистичного методу стиснення інформації / Є. В. Онопко, О. В. Тарасов // Системи обробки інформації. – Х. : ХУПС. – 2012. – № 4(102). – 232 с.

238. Тарасюк Г. М. Планування діяльності підприємства / Г. М. Тарасюк, Л. І. Шваб. – К. : Каравела, 2003. – 432 с.

239. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД СТЗІ 1.1-003-99. − Чинний від 28.04.1999. − К. : Держстандарт України, 1999. – 24 с.

240. Технические методы и средства защиты информации / [Ю. Н. Максимов, В. Г. Сонников, В. Г. Петров и др.]. – СПб. : Полигон, 2000. – 314 с.

241. Товбис Е. М. Информационная система автоматизированного мониторинга самостоятельной работы студентов / Е. М. Товбис // Автореферат диссертации на соискание ученой степени кандидата технических наук. – 2009. – Красноярск. – 22 с.

242. Томпкинса У. Сопряжение датчиков и устройств внедрения данных с компьютерами IBM PC / У. Томпкинса, Дж. Уэбстера. – М. : Мир, 2002. – 402 с.

243. Уайт Т. Чего хочет бизнес от IT: Стратегия эффективного сотрудничества руководителей бизнеса и ИТ-директоров / Т. Уайт ; пер. с англ. А. Поплавская. – Мн : Грецов Букс, 2007. – 256 с.

244. Українська культура та реалізація державної політики в культурній сфері: Аналітичний звіт міністерства культури і туризму за 2005 рік. – К. : Міністерство культури і туризму України, 2006. – 134 с.

245. Уфимцев Ю. С. Методика информационной безопасности : монография / Ю. С. Уфимцев. – М. : Экзамен, 2004. – 542 с.

246. Ушакова И. А. Перспективы интеграции CRM-систем и социальных сетей / И. А. Ушакова, С. А. Панасенко // Системи обробки інформації. – 2011. – № 7. – С.119–120.

247. Ушакова И. А. Проникновение CRM-систем в социальные сети / И. А. Ушакова, С. А. Панасенко // Системи обробки інформації. – 2011. – № 7. – С. 43–48.

248. Ушакова І. О. Моделювання інформаційного впливу соціальних мереж на лояльність клієнтів засобами пакету Anylogic / І. О. Уша-

кова, С. О. Панасенко // Системи обробки інформації. – 2012. – № 4. – С. 76–80.

249. Ушакова І. О. Основи системного аналізу об’єктів та процесів комп’ютеризації: навч. посібн. Частина 1 / І. О. Ушакова. — Х. : Вид. ХНЕУ, 2007. – 212 с.

250. Ушакова І. О. Соціальні мережі як інструментарій взаємовідносин з клієнтами / І. О. Ушакова, С. О. Панасенко // Матеріали міжнародної науково-практичної конференції молодих вчених, аспірантів та студентів "Актуальні проблеми науки та освіти молоді: теорія, практика, сучасні рішення". – Х. : ХНЕУ, 2012. – С. 129 – 131.

251. Уэлстид С. Фракталы и вейвлеты для сжатия изображений в действии / С. Уэлстид. – М. : Триумф, 2003. – 320 с.

252. Халимов Г. З. Обеспечение безопасности каналов передачи данных на основе помехоустойчивых кодов / Г. З. Халимов, А. В. Северинов // Системы управления и связь. – Х. : ХВУ. – 1996. – С. 116–119.

253. Халимов Г. З. Применение помехоустойчивого кодирования для обеспечения безопасности каналов передачи данных / Г. З. Халимов // Труды международной НТК "Передача, обработка и отображение информации" ; под ред. А. В. Королева. – Х. : НАНУ, ПАНИ. – 1994. – С. 28.

254. Комп’ютерні мережі / П. Хамбракен. – К. : Либідь, 2009. – 137 с.

255. Хаммер М. Реинжениринг корпорации: Манифест революции в бизнесе / М. Хаммер, Дж. Чампи ; пер. с англ. – СПб. : Издательство С.-Петербургского университета, 2006. – 332 с.

256. Хант К. TCP/IP. Сетевое администрирование / К. Хант. – СПб. : Символ-Плюс, 2004. – 816 с.

257. Хаулет Т. Защитные средства с открытыми исходными текстами. OPEN SOURCE SECURITY TOOLS: практ. рук. по защитным приложениям : учебн. пособ. / Т. Хаулет ; пер. с англ. В. Галатенко и О. Трофанова ; под ред В. Галатенко. – М. : Интернет-Ун-т Информ. Технологий, 2007. – 607 с.

258. Хиллс М. Т. Программирование для электронных систем коммутации / М. Т. Хиллс. – М. : Связь, 2008. – 238 с.

259. Хорев А. А. Способы и средства защиты информации : учебн. пособ. / А. А. Хорев. – М. : Изд. МО РФ, 1998. – 316 с.

260. Хорев П. Б. Информационная безопасность : учебн. пособ. / П. Б. Хорев. – М. : Издательский центр "Академия", 2010. – 336 с.

261. Цвики Э. Создание защиты в интернете / Э. Цвики. – СПб. : Символ-Плюс, 2002. – 928 с.

262. Чекмарев Ю. В. Локальные вычислительные сети / Ю. В. Чекмарев. – СПб. : ДМК Пресс, 2009. – 200 с.

263. Чернявский Д. И. Моделирование и реинжиниринг бизнес-процессов / Д. И. Чернявский, Д. В. Рудаков. – Омск : Изд. ОмГТУ, 2010. – 84 с.

264. Чмора А. Л. Современная прикладная криптография / А. Л. Чмора. – М., 2002. – 508 с.

265. Чолмарев М. Р. Локальні мережі / М. Р. Чолмарев. – К. : ДМК Пресс, 2009. – 200 с.

266. Чумиков А. Н. Связи с общественностью: Теория и практика : учебн. пособ. / А. Н. Чумиков, М. П. Бочаров. – М. : Дело, 2003. – 496 с.

267. Чураков А. Н. Анализ социальных сетей / А. Н. Чураков. – Социологические исследования (Социс). – 2001. – № 1. – С. 109–121.

268. Шаньгин В. Ф. Компьютерная безопасность ИС : учебн. пособ. / В. Ф. Шаньгин. – М. : "ИНФРА-М", 2008. – 416 с.

269. Шарков Ф. И. Разработка и технологии производства рекламного продукта / Ф. И. Шарков, В. И. Гостенина. – М. : "Дашков и К°", 2007. – 340 с.

270. Шахнович И. Ю. Современные технологии беспроводной связи / И. Ю. Шахнович. — СПб. : Техносфера, 2006. – 288 с.

271. Шашлов С. Азбука сисадміна. Енциклопедія iXBT.com / С. Шашлов. – К., 2008. – 208 с.

272. Шилтон М. Asterisk и Linux: Миссия IP-телефония / М. Шилтон. – М. : Итекс, 2006. – 367 с.

273. Широков Л. А. Базы данных и знаний : учебн. пособ. Ч. 1 / Л. А. Широков. – М. : МГИУ, 2000. – 86 с.

274. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М. : Издательство ТРИУМФ, 2003. – 816 с.

275. Щербаков О. В. Моделювання елементів навчального процесу вищого навчального закладу / О. В. Щербаков, Є. С. Захарова // Збірник наукових праць "Системи обробки інформації". – Х. : ХУПС ім. І. Кожедуба, 2011. Випуск 7 (97). – С. 80–83.

276. Юрасов А. В. Основы электронной коммерции / А. В. Юрасов. – М. : Горячая линия, 2008. – 480 с.

277. Adelman C. A parallel post-secondary universe: the certification system in information technology. – Oslo : Centre for Technology, Innovation and Culture, 2003. – P. 10.

278. Anderson N. IP telephone design and implementation issues / N. Anderson, J. Doherty. – Oxford : UniverPress, 2007. – P. 145.

279. Baeza-Yates R. Modern Information Retrieval: The Concepts and Technology behind Search / R. Baeza-Yates, B. Ribeiro-Neto. – ACM Press, 2011. – 944 p.

280. Bassiouni M. Experiments on Improving the Compression of Special Data Types / M. Bassiouni, A. Mukherjee, N. Tzannes. – Proc. IEEE Data Compression Conference, Snowbird, Utah-April 8–11. – 1991. – P. 433.

281. Bellyte E. Beyond VoIP Protocols / E. Bellyte. – London : Presstes, 2003. – P. 45.

282. Belton K. Cisco IP telephony: planning, design, implementation, operation and optimization / K. Belton. – Paris : LeQuir, 2006. – P. 146.

283. Bierbrauer J. On families of hash function via geometric codes and concatenation / J. Bierbrauer, T. Johansson, G. Kabatianskii // Advances in Cryptology. – CRYPTO 93, Lecture Notes in Computer Science. – 1994. – № 773. – P. 331–342.

284. Blias S. Best Practices for Success / S. Blias. – London : Steven Press, 2011. – P. 45.

285. Brown J. Outsourcing dilemma. The search for competitiveness / J. Brown. – Oxford : Williams, 2004. – P. 45.

286. Cadle J. Business Analysis Techniques: 72 Essential Tools for Success. – Chippenham / J. Cadle, D. Paul, P. Turner / CPI Antony Rowe, 2010. – 280 p.

287. Cannane A. A General-Purpose Compression Scheme for Databases / A. Cannane, H. E. Williams, J. Zobel. – Proc. IEEE Data Compression Conference. – 1999. – 519 p.

288. Carter J. L. Universal classes of hash functions / J. L. Carter, M. N. Wegman / Computer and System Scince. – 1979. – № 18. – P. 143–154.

289. Chen Z. Query Optimization in Compressed Database Systems / Z. Chen, J. Gehrke, F. Korn. – Proc. 2001 ACM-SIGMOD Int. Conf. Management of Data, pp. 271–282, Santa Barbara, CA, May 2001.

290. Clokcer H. Digital Communication / H. Clokcer. – London : Cisco Press, 2005. – P. 203.

291. Collora S. Cisco callmanager best practices / S. Collora. – London : CenterPress, 2003. – P. 306.

292. Cormack G. Data Compression in Database Systems / G. Cormack. – Comm. of ACM, 28(12):1336-1342, December 1985.

293. Donalyd B. IP telephony unveiled / B. Donalyd. – London : Cisco Press, 2007. – P. 98.

294. Duffets D. Asterisk 1.4 for professionals / D. Duffets, K. Karpenter, N. Mildton, I. Plain. – Oxford : Oxford University Press, 2009. – P. 289.

295. Dumpster B. Trixbox Made Easy / B. Dumpster. – Harvard : Harvard University Press, 2010. – P. 405.

296. Elliott M. Buyer's Guide Simulation / M. Elliott. – USA : ГЕЕ Solutions, 2000. – 328 p.

297. Flavio E. Building Telephony Systems with OpenSER / E. Flavio. – London : TechPress, 2007. – P. 267.

298. Focuse R. Dedicated Asterisk PBX server on red hat. Install guide / R. Focuse. – London : TechPress, 2008. – P. 203.

299. Foock T. Securing VoIP Network / T. Foock. – London : Cisco Press, 2005. – P. 145.

300. Gallager R. Variations on a theme by Huffman / R. Gallager. – IEEE Transactions on Information Theory, 24(6):668-674, Nov. 1978.

301. Garrison K. Trixbox 2.6 / K. Garrison. – London : Oxford University Press, 2007. – P. 256.

302. Gazer G. Build your own PBX / G. Gaser. – Oxford : Techo, 2007. – P. 127.

303. Hassoun M. Fundamentals of artificial neural networks / M. Hassoun. – Cambridge : MIT Press, 2001. – P. 310.

304. Hitzler P. Foundations of Semantic Web Technologies / P. Hitzler, M. Krotzsch, S. Rudolph. – Chapman & Hall/CRC, 2009 – 455 p.

305. Kelly T. Administering data centers, servers, storage and voice over IP / T. Kelly. – Oxford : UniPress, 2004. – P. 287.

306. Koorh K. Network Virtualization / K. Koorh. – Oxford : Cisco Press, 2003. – P. 167.

307. Kosko B. Neural networks and fuzzy system. A dynamical systems approach to machine intelligence / B. Kosko. – Englewood : Prentice Hall, 2008. – P. 167.

308. Levison R. Asterisk Open-Source PBX / R. Levison. – Oxford : HallPress, 2005. – P. 304.

309. Lopes F. Towards a Generic Negotiation Model for Intentional Agents: in Proceedings of the IEEE Workshop on Agent-Based Information Systems (London, UK) / F. Lopes, N. Mamede, A. Q. Novais. – CA : IEEE Computer Society Press, 2000. – 1 160 p.

310. McEliece R. J. A Public-Key Criptosystem Based on Algebraic Theory / DGN Progres Report 42-44, Jet Propulsi on Lab. Pasadena, CA. January–February, 1978. – P. 114–116.

311. Meggelen J. Asterisk the future of telephony / J. Meggelen. – New York : OReilly, 2009. – P. 124–345.

312. Moffat A. Coding for compression in full-text retrieval systems / A. Moffat, J. Zobel. – In Proc. IEEE Data Compression Conference, pp. 72–81, Snowbird, Utah, March 1992. IEEE Computer Society Press, Los Alamitos, California.

313. Nash J. Networking Essentials MCSE Study System / J. Nash. – London : IDG Books, 2007. – P. 512.

314. Niederreiter H. Knapsack-Type Cryptosystems and Algebraic Coding Theory / H. Niederreiter / Probl. Control and Inform. Theoty. – 1986. – V. 15. – P. 19–34.

315. Osterwalder A. Business Model Generation / A. Osterwalder, Y. Pigneur. – New Jersey : John Wiley & Sons, Inc., 2010. – 288 p.

316. Peterson M. Asterisk@Home Handbook / M. Peterson. – Oxford : Techs, 2006. – P. 674.

317. Rao T. R. N. Private-key algebraiccoded cryptosystem. Advances in Cryptology / T. R. N. Rao, K. H. Nam. – CRYPTO 86, New York. – N-Y. : Springer. – P. 35–48.

318. Redison S. IMS Multimedia telephony over cellular systems / S. Redison. – London : Cisco Press, 2004. – P. 34.

319. Redmond B. IP telephony cookbook / B. Redmond. – London : InfoPress, 2004. – P. 304.

320. Robar A. FreePBX 2.5 Powerfull telephony / A. Robar. – Paris : LeQuir, 2007. – P. 137.

321. Roth M. Database compression / M. Roth, S. Van Horn. – ACM SIGMOD Record, 22(3):31-39, Sept. 1993.

322. Senio D. Softswitch Architecture for VoIP / D. Senio. – Madrid : Italor, 2007. – P. 453.

323. Sharif B. Trixbox is easy for you / B. Sharif. – New York : Oxifon, 2005. – P. 345.

324. Shih Cl. The Facebook Era: Tapping Online Social Networks to Build Better Products, Reach New Audience, and Sell More Stuff / Cl. Shih. – Prentice Hall, 2009. – 256 p.

325. Simmons G. J. Authentication theory/coding theory in Cryptology / G. J. Simmons// Computer Science. – 1985. – № 96. – P. 411–431.

326. Simons G. J. An impersonation-proof identity verification scheme / G. J. Simons // Computer Science. – 1988. – № 87. – P. 211–215.

327. Spencer M. The Asterisk Handbook / M. Spencer. – London : Digium, 2003. – P. 243.

328. Stair Ralph M. Principles of informations systems: a managerial approach / Stair Ralph M., Reynolds George W. – Seventh edition. – USA : Thomson Course Technnology, 2006. – 758 p.

329. Swam J. J. Simulation Reloaded: Sixth biennial survey of discrete-event software tools / J. J. Swam. – UK : OR/MS Today, 2003. – 257 p.

330. Tekloman R. Asterisk Dialplan Globals / R. Tekloman. – Texas : TUP, 2008. – P. 276.

331. Teksom P. Carrier grade voice over IP / P. Teksom. – Oxford : PressCent, 2005. – P. 340.

332. Termison E. Getting Started. Asterisk / E. Termison. – London : UniPress, 2005. – P. 178.

333. Todd J. Asterisk: a bare-bones VoIP example / J. Todd. – London : TTC, 2003. – P. 245.

334. Todd J. VoIP Services with Asterisk / J. Todd. – Preston : Press-Tess, 2009. – P. 236.

335. Wallace K. Cisco voice over IP / K. Wallace. – London : Preston, 2006. – P. 405.

336. Wallingford T. VoIP hacks / T. Wallingford. – Timelton : Tems-Press, 2007. – P. 304.

337. Webster F. Information technology – a luddite analysis / F. Webster, K. Robins. – Norwood : TechPress, 2010. – P. 23.

338. Willey J. Internet Communications using SIP / J. Willey. – Oxford : Cisco Press, 2008. – P. 298.

339. Willey J. Signaling Telecommunication Networks / J. Willey. – Oxford : Cisco Press, 2005. – P. 230.

340. Zipf G. K. Human Behavior and the Principle of least Effort. / G. K. Zipf // Addison-Wesley. – New York, 1949.

341. Ziv J. A universal algorithm for sequential data compression / J. Ziv, A. Lempel. – IEEE Transactions on Information Theory. – Vol. 23(3). – Pp. 337–343.

342. Ziv J. Compression of individual sequences via variable-rate coding / J. Ziv, A. Lempel. – IEEE Transactions on Information Theory. – Vol. 24(5). – Pp. 530–536.

343. Авдулов П. В. Введение в теорию принятия решений [Электронный ресурс] / П. В. Авдулов. – Режим доступа : http://www.sociolog.in.ua/-view_book.php&id=1687.

344. Блюмин С. Л. Модели и методы принятия решений в условиях неопределенности. – СПб. : ЛЭГИ, 2001. – 138 с. [Электронный ресурс] / С. Л. Блюмин, И. А. Шуйкова. – Режим доступа : http://www.twirpx.com/file/145983.

345. Бондаренко Л. Методика выбора ERP-системы в качестве основы интегрированной системы управления предприятием [Электронный ресурс] // Финансовая газета (Региональный выпуск). – 2005. – № 14. – Режим доступа : http://www.logistics.ru/21/7/4/i20_23802p7.htm.

346. Вертакова Ю. В. Управленческие решения: разработка и выбор. – М. : Кнорус, 2005. – 352 с. [Электронный ресурс] / Ю. В. Вертакова, И. А. Козьева, Э. Н. Кузьбожаев. – Режим доступа : http://www.4tivo.com /bu-siness_finance/18826-vertakova-kozeva-kuzbozhev.html/.

347. Выбор КИС: проблемы и решения [Электронный ресурс]. – Режим доступа : http://soft-expert.ru.

348. Галкин Г. Методы определения экономического эффекта от ИТ-проекта [Электронный ресурс]. – Режим доступа : http://www.iemag.ru/master-class/detail.php?ID=15720.

349. Давыдов А. А. Системная социология: Social Networks Mining / А. А. Давыдов. – М. : ИС РАН, 2009 [Электронный ресурс]. – Режим доступа : http://www.isras.ru/in-dex.php?page_id=1033.

350. Давыдов А. А. Системная социология: анализ мультимедийной информации в Интернете [Электронный ресурс] / А. А. Давыдов. – М. : ИС РАН, 2009. – Режим доступа : http://www.isras.ru/index.php?page_id=988.

351. Домбровская И. Возможности HR-систем: мифы и реальность [Электронный ресурс] / И. Домбровская. – Режим доступа : http://www.hr-zone.net/index.php? mod=articles&go=show&id=1210.

352. Досягнення і проблеми культури України у другій половині XX ст. [Електронний ресурс]. – Режим доступу : http://osvita.ua/vnz/reports/culture/10803/.

353. Дубова Н. Социальная сеть знаний / Н. Дубова // Открытые системы. – 2005. – № 12. – [Электронный ресурс]. – Режим доступа : http://www.osp.ru/os/2005/12/380634/.

354. Еляков А. Д. Современная информационная революция [Электронный ресурс]. – Режим доступа : http://ecsocman.hse.ru/data /653/831/1219/3-Elyakov_29-38.pdf.

355. Жданов Б. Как создать капитал в социальной сети. Часть 1. Facebook – инструмент нетворкинга для накопления социального капитала [Электронный ресурс] / Б. Жданов. – Режим доступа : http://www.manage-ment.com.ua/ims/ims187.html.

356. Жданов Б. Как создать капитал в социальной сети. Часть 2.1. Социальные сети в помощь продажам [Электронный ресурс] / Б. Жданов. – Режим доступа : http://www.management.com.ua/ims/ims191.html.

357. Жданов Б. Как создать капитал в социальной сети. Часть 2.2. Социальные сети для маркетинга, инноваций и рекрутинга [Электронный ресурс] / Б. Жданов. – Режим доступа : http://www.management.com.ua/ims/ims194.html.

358. Завдання та етапи рекламної кампанії [Електронний ресурс]. – Режим доступу : http://crk-knteu.kiev.ua/66359-Zadacha_i_etapy_reklamnoiy_kampa-nii.html.

359. Зайцев М. Г. Методы оптимизации управления и принятия решений : примеры, задачи, кейсы. – М. : Дело, 2008. – 664 с. [Электронный ресурс] / М. Г. Зайцев, С. Е. Варюхин. – Режим доступа : http://institutiones.com/download/books/1834-metody-optimizacii-upravleniya-i-prinyatia-reshenij.html.

360. Иванов О. В. Поддержка процессов управления персоналом с помощью HR-модулей ERP-систем: возможности и преимущества. Intelligent Enterprise, № 6, 2008 [Электронный ресурс]. – Режим доступа : http://www.topsbi.ru/default.asp?artID=1450.

361. Имитационное моделирование с AnyLogic // XJ Technologies [Электронный ресурс]. – Режим доступа : http://www.xjtek.ru/anylogic/why_anylogic/.

362. Инком. HRM. Управление персоналом. Классификация HRM-систем и описание их стандартных функций [Электронный ресурс]. – Режим доступа : http://hrm.incom.ua/content/view/372846/104.

363. Информационный портал CRM.com.ua [Электронный ресурс]. – Режим доступа : www.crm.com.ua.

364. Інтернет в маркетингу [Електронний ресурс]. – Режим доступу : http://www.imanbooks.com /book_240_page_49.

365. Інформація щодо стану реалізації проекту модернізації державної податкової служби України [Електронний ресурс]. – Режим доступу : http://www.rsta.tr.ukrtel.net/News/News_DPA/Arhiv/rik.2006/index.htm.

366. Казимир В. В. Верификация реактивных систем с помощью формул темпоральной логики на E-сетевых моделях [Электронный ресурс] / В. В. Казимир // Математичні машини і системи – 2002. – № 1. – С. 29–40. – Режим доступа : scholar.google.com/scholar_host?q =info:oPo-3SuBRDq0J:scholar.google.com/&hl=ru&as_sdt=2000&output=viewport&pg=31#P32,M1.

367. Как выбрать HRM-систему для компании [Электронный ресурс]. – Режим доступа : http://www.hrmonitor.ru/index.php?p=205&pname=news&news_id=279.

368. Катренко А. В. Моделі та методи формування портфелів IT-проектів. 2010 [Електронний ресурс] / А. В. Катренко, Д. С. Магац. – Режим доступу : http://vlp.com.ua/node/7110.

369. Катренко А. В. Теорія прийняття рішень. 2009 [Електронний ресурс] / А. В. Катренко, В. В. Пасічник. – Режим доступу : http://vlp.com.ua/node/7110.

370. Кеворков В. В. Политика и практика маркетинга на предприятии [Электронный ресурс] / В. В. Кеворков. – Режим доступа : http://www.cfin.ru /marketing/ kevorkov.shtml;

371. Код Хаффмана [Электронный ресурс]. – Режим доступа : http://www.compression.ru/download/articles/huff/simakov_2002_huffcode.html.

372. Код Хаффмана [Электронный ресурс]. – Режим доступа : http://www.codenet.ru/progr/alg/huffcode.php.

373. Колесников С. Что такое КИС и как с ней бороться [Электронный ресурс]. – Режим доступа : http://consulting.ru/econs_wp_3293.

374. Куршакова Н. С. Актуальные вопросы формирования лояльности покупателей и посредников / Н. С. Куршакова // Проблемы современной экономики. – 2010. – № 3 (35) [Электронный ресурс]. – Режим доступа : http://www.m-economy.ru/art.php?nArtId=3266.

375. Кутузов М. Социальные сети как новый информационный канал в Public Relations (на примере Интернет-ресурсов Odnoklassniki.ru и Vkontakte.ru) / М. Кутузов // PR – библиотека Международного пресс-клуба [Электронный ресурс]. – Режим доступа : http://pr-club.com/PR_Lib /Kut-SocSeti.doc.

376. Ленскольд Дж. Маркетинг привлечения и маркетинг удержания клиентов / Дж. Ленскольд [Электронный ресурс]. – Режим доступа :

http://alumni.mgimo.ru/page/blog/club/view_post.seam?userId =41370&postId=43415.

377. Матиас Нельке. Учимся принимать решения [Электронный ресурс] / Нельке Матиас. – Режим доступа : http://www.sociolog.in.ua /view_book.php&id=519.

378. Методи визначення рекламного бюджету компанії [Електронний ресурс]. – Режим доступу : http://www.leosvit.com/art/metody_vyznachennia_reklam-nogo_budzhetu_ kompanii.htm.

379. Мищенко Е. Я. Принятие решений в кризисных ситуациях. – СПб. : Речь, 2008. – 201 с. [Электронный ресурс] / Е. Я. Мищенко. – Режим доступа : http://financepro.ru/management/13656-prinatie-resheniy-v-krizisnyh-biznes-situaciyah-mishenko-e-ya.html.

380. Моделирование систем. Е-сети [Электронный ресурс]. – Режим доступа : www.sardismusic.com/topics/t10r3part1.html.

381. Наказ ДПА № 355 від 27.05.2008 р. Методичні рекомендації щодо порядку організації та проведення перевірок платників податків [Електронний ресурс]. – Режим доступу : http://mir-ekspertiz.info/metodichni-rekomendaci%D1%97-shhodo-poryadku-organizaci%D1%97-ta-provedennya-perevirok-platnikiv-podatkiv/.

382. Організація рекламної діяльності на прикладі підприємства "Діза" [Електронний ресурс]. – Режим доступу : http://crk-knteu.kiev.ua /66380-Organizaciya_reklamnoiy_deyatel_nosti_na_primere_ predpriyatiya_ Diza.html.

383. Оцінка ефективності рекламної кампанії в мережі Інтернет [Електронний ресурс]. – Режим доступу : http://crk-knteu.kiev.ua/66446-Ocenka_effektivnosti_reklamnoiy_kampanii_v_seti_ Internet.html.

384. Паринов С. И. Новые возможности имитационного моделирования социально-экономических систем / С. И. Паринов // Интернет-журнал "Искусственные сообщества". – 2007. № 3–4 [Электронный ресурс]. – Режим доступа : http://www.xjtek.ru/ anylogic/ articles/50/.

385. Перцова Н. Кадровый отчет: эффективность HR-служб [Электронный ресурс] / Н. Перцова. – Режим доступа : http://www.jobs.ua/hr/manager/o_hr_ specialistah/83.

386. Планирование рекламных кампаний в сети интернет – Маркетинг – менеджмент [Электронный ресурс]. – Режим доступа : www.marketing-magazine.ru/about/autor/3/17.

387. Поисковые системы: состав, функции, принцип работы [Электронный ресурс]. – Режим доступа : www.seonews.ru/masterclasses/detail/29814.php.

388. Пономарев А. С. Нечеткие множества в задачах автоматизированного управления и принятия решений. – М. : 2005. – 232 с. [Электронный ресурс] / А. С. Пономарев. – Режим доступа : http://www.kodges.ru/ 32111-nechetkie-mnozestva-v-zadachakh.html.

389. Прохоров А. Социальные сети и интернет / А. Прохоров // КомпьютерПресс. – 2010. – № 10 [Электронный ресурс]. – Режим доступа : http://compress.ru /article.aspx?id=16723&iid=776.

390. Рекламная кампания [Электронный ресурс]. – Режим доступа : http://www.npark.ru/reklamnaya-kampaniya.html.

391. Рекламний менеджмент в загальній концепції управління організації [Електронний ресурс]. – Режим доступу : http://ua-referat.com/Рекламний_менеджмент_в_загальній_концепції_управління_організації.

392. Релевантность [Электронный ресурс]. – Режим доступа : http://www.fru-it.ru/services/text/relevance.php.

393. Российский семинар по оценке методов информационного поиска [Электронный ресурс]. – Режим доступа : http://romip.ru/.

394. Свойства социальных сетей // SD Company [Электронный ресурс]. – Режим доступа : http://www.sd-company.su/article/computers /social.

395. Семантическая поисковая система AskNet [Электронный ресурс]. – Режим доступа : http://asknet.ru/.

396. Скрытый маркетинг. Блог о современных технологиях продвижения [Электронный ресурс]. – Режим доступа : http://www.hid-denmarketing.ru/blog/a/399.

397. Смирнов М. А. Обзор применения методов безущербного сжатия данных в СУБД [Электронный ресурс]. – Режим доступа : http://compression.ru/download/articles/db/smirnov_2003_database_compression_review /index.html.

398. Сорина Г. В. Принятие решений как интеллектуальная деятельность. – М. : "Канон +", "Реабилитация", 2009. – 272 с. [Электронный ресурс] / Г. В. Сорина.– Режим доступа : http://www.twirpx.com/files/ mathematics.

399. Социальная сеть (социология) // Википедия – свободная энциклопедия [Электронный ресурс]. – Режим доступа : http://ru.wiki-pedia.org /wiki/Социальная_сеть_ (социология).

400. Стратегия управления взаимоотношениями с клиентами (CRM) [Электронный ресурс]. – Режим доступа : http://www.intuit.ru/department /itmngt/crm/.

401. Теорія прийняття рішень [Електронний ресурс]. – Режим доступу : http://vlasnasprava.pp.ua/management/3811-skachati-knigu-teoriya-prinyatiya-reshenij.html.

402. Товбис Е. М. Расчет учебной нагрузки с использованием имитационного моделирования на примере дисциплины "Программирование" [Электронный ресурс] / Е. М. Товбис, С. П. Якимов // Наука и образование. Электронный журнал. – 2008, № 9. – Режим доступа : www.technomag.edu.ru/doc/103841.html.

403. Токарчук В. CRM и социальные сети – от тенденций к практическим примерам [Электронный ресурс] / В. Токарчук. – Режим доступа : http://areon.ua/crm-blogs/tokarchuk/197-sm-crm.

404. Толстая Н. Восемь способов оценить эффективность HR-службы [Электронный ресурс] / Н. Толстая. – Режим доступа : http://www.rhr.ru /index/so-vet/tech/11265,0.html.

405. Тынкевич М. А. Экономико-математические методы (Исследование операций) : учебн. пособ. [Электронный ресурс] / М. А. Тынкевич. – Режим доступа : http://vtit.kuzstu.ru/books/shelf/book1.

406. Українська Інтернет-аудиторія [Електронний ресурс]. – Режим доступу : http://e-commerce.com.ua/2011/02/українська-інтернет-аудиторія -за-2010-рі.

407. Федорович Р. Маркетинговий аналіз кон’юнктури ринку. [Електронний ресурс] / Р. Федорович. – Режим доступу : .http://www.nbuv.gov.ua /portal/Soc_Gum/Gev/2009_2/PROBLEMS/GEB_2009_No2-F_Roman_S_Semenyuk-Marketing_analysis_of_mar-ket_conditions__47.pdf.

408. Центр выбора технологий и поставщиков TADVISER [Электронный ресурс]. – Режим доступа : http://www.tadviser.ru.

409. Черноморов Г. А. Теория принятия решений : учебн. пособ. – Рос.гос.техн. ун-т, Новочеркасск, 2002. – 276 с. [Электронный ресурс] / Г. А. Черноморов. – Режим доступа : http://www.kodges.ru/6384-teorija-prinjatija-reshenijj.html.

410. Черноруцкий И. Г. Методы принятия решений. – СПб. : БХВ-Петербург, 2005. – 416 с. [Электронный ресурс] / И. Г. Черноруцкий. – Режим доступа : http://www.stufiles.ru/dir/cat29/subj82/file14112.html.

411. Чичмели И. Как управлять лояльностью клиентов? / И. Чичмели [Электронный ресурс]. – Режим доступа : http://www.e-xecutive.ru/marketing/sales/1367509/.

412. Шатилов М. Инструменты для социальных сетей [Электронный ресурс] / М. Шатилов. – Режим доступа : http://www.osp.ru /os/2008 /04/5114182/.

413. Шевченко Е. Социальные сети в Украине [Электронный ресурс] / Е. Шевченко. — Режим доступа : http://ace.kiev.ua/socialnye-seti-v-ukraine/.

414. Эддоус М. Методы принятия решений. – М. : "Аудит, ЮНИТИ", 2000. – 245 с. [Электронный ресурс] / М. Эддоус. – Режим доступа : http://bankknig.com/raznoe/100333-m.jeddous-metody-prinjatija-reshenijjska-chat.html.

415. Юдин Д. Б. Вычислительные методы теории принятия решений [Электронный ресурс] / Д. Б. Юдин. – Режим доступа : http://arhiv-knig.com/obrazovanie/37474-judin-d.b.-vychislitelnye-metody-teorii.html.

416. Ядыков С. Эффективность информационных систем: докопаться до истины [Электронный ресурс] / С. Ядыков. – Режим доступа : http://vet-riks.ru/info/49-info-3-1.html.

417. Barish S. Passive network analysis / [Electronic recource] S. Barish. – Access mode : http://www.symantec.com/connect /articles/passive-network-analysis

418. Berners-Lee T. The Semantec Web [Electronic resource] / Berners-Lee T., Handler J., Lassila O. – Access mode : www.scientificamerican.com /article.cfm?id=the-semantic-web.

419. Cone Finds that Americans Expect Companies to Have a Presence in Social Media [Electronic recource]. – Access mode : http://www.cone-inc.com/content1182.

420. Description of the DOAP Project [Electronic resource]. – Access mode : https://github.com/edumbill/doap/wiki.

421. Dublin Core Metadata Initiative [Electronic resource]. – Access mode : http://dublincore.org/.

422. Evri Corporate [Electronic resource]. – Access mode : http://www.evri.com/.

423. Forrester Research [Electronic resource]. – Access mode : http://www.forrester.com.

424. Gartner Analysts [Electronic recource]. – Access mode : http://www.gartner.com/0_admin/AnalystCoverageAreas.jsp.

425. Kelly A. Decision making using Game Theory [Electronic resource] / A. Kelly. – Access mode : http://www.getabstract.com/en/summary/ strategy/decision-making-using-game-theory/2560.

426. Official site of firm Palisade. PrecisionTree. – Access mode : http://www.palisade.com.

427. Panorama Consulting Group 2010 ERP Vendor Analysis [Electronic resource]. – Access mode : http://panorama-consulting.com /resource-center/2010-erp-vendor-analysis.

428. Resource Description Framework (RDF): Concepts and Abstract Syntax [Electronic resource]. – Access mode : http://www.w3.org/TR/2004 /REC-rdf-concepts-20040210/.

429. SAP Employee Self-Service & SAP Manager Self-Service [Electronic resource]. – Access mode : http://www.sap.com/uk/solutions/solu-tion-extensions/essmss/index.epx.

430. Semantic Information Mashup [Electronic resource]. – Access mode : http://sig.ma/.

431. Semantically-Interlinked Online Communities [Electronic resource]. – Access mode : http://sioc-project.org/.

432. Simulation Software Survey // Analitics [Electronic recource]. – Access mode : http://www.lionhrtpub.com/orms /surveys/Simula-tion/Simulation.html.

433. Small-world network // Wikipedia, the free encyclopedia [Electronic recource]. – Access mode : http://en.wikipedia.org/wiki/Small-world_network.

434. Swoogle Semantic Web Search Engine [Electronic resource]. – Access mode: http://swoogle.umbc.edu/.

435. The Extended Semantic Web Conference [Electronic resource]. – Access mode : http://2012.eswc-conferences.org/.

436. The Friend of a Friend (FOAF) project [Electronic resource]. – Access mode : http://www.foaf-project.org/.

437. The Semantic Technology & Business Conference [Electronic resource]. – Access mode : http://semtechbizsf2012.semanticweb.com/.

438. The Semantic Web Index [Electronic resource]. – Access mode : http://sindice.com/.

439. What is Social CRM? // The social customer [Electronic recource]. – Access mode : http://thesocialcustomer.com/leighdow /36230/what-social-crm.

НАУКОВЕ ВИДАННЯ

Беседовський Олексій Миколайович
Золотарьова Ірина Олександрівна
Євсеєв Сергій Петрович та ін.

СУЧАСНІ МЕТОДИ ТА МОДЕЛІ ОБРОБКИ ДАНИХ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Монографія

За заг. редакцією **докт. екон. наук, професора Пономаренка В. С.**

Відповідальний за випуск **Пономаренко В. С.**

Відповідальний редактор **Сєдова Л. М.**

Редактор **Бутенко В. О.**

Коректор **Мартовицька-Максимова В. А.**

План 2013 р. Поз. № 107-Н.
Підп. до друку Формат 60 х 90 1/16. Папір MultiCopy. Друк Riso.
Ум.-друк. арк. 33,75. Обл.-вид. арк. 42,19. Тираж прим. Зам. №

Видавець і виготівник – видавництво ХНЕУ ім. С. Кузнеця, 61166, м. Харків, пр. Леніна, 9а

Свідоцтво про внесення до Державного реєстру суб'єктів видавничої справи ***Дк № 481 від 13.06.2001 р.***