Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
комп'ютерно інтегрованих систем і програмної інженерії
(назва факультету)
комп'ютерних систем та мереж
(повна назва кафедри)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту (роботи)

Магістр
(освітній рівень)

на тему: Методи аналізу ітерацій для автоматизації вибору перехідного обладнання з врахуванням вимог безпеки

Виконав: студент (ка) 6 курсу, групи СІІ-61
напряму підготовки (спеціальності) 123
Комп'ютерна інженерія
(шифр і назва напряму підготовки, спеціальності)

(підпис) Тарасата І.Я
(прізвище та ініціали)

Керівник (підпис) Євтух Н.С
(прізвище та ініціали)

Нормоконтроль (підпис) Гнип Є.В
(прізвище та ініціали)

Рецензент (підпис) Гірняк М.В
(прізвище та ініціали)

м. Тернопіль – 2019

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)

Факультет комп'ютерно-інформаційних систем та програмної інженерії

Кафедра комп'ютерних систем та мереж

Освітній рівень Магістр

Напрям підготовки
(шифр і назва)

Спеціальність 123 "Комп'ютерна інженерія"
(шифр і назва)

ЗАТВЕРДЖУЮ

Завідувач кафедри КС

Онуфрійчук Г.М.

«30» 09 2019 р.

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТУ

Гаранюта Андрій Ярославович
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) Методи аналізу ієрархій для автоматизації вибору мережевого обладнання з урахуванням вимог безпеки

Керівник проекту (роботи) Ігрхрегор кафедри КС Свтух Петро Сильвестрович
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом по університету від «27» 09 2019 року №471-85

2. Термін подання студентом проекту (роботи) 26.12.19

3. Вихідні дані до проекту (роботи) Методи аналізу ієрархій для автоматизації вибору мережевого обладнання

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

Розділ 1 проектування мережі з урахуванням вимог; Розділ 2 Постановка задачі багатокритеріального оцінювання та вибору проекта КС; Розділ 3 метод Багатокритеріального вибору архітектури при умові вимог якості; Розділ 4 Обґрунтування економічної ефективності; Розділ 5 Охорона праці та безпека в надзвичайних ситуаціях; Розділ 6 Висновки; перелік посилань; додаток А.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

Вступ
Актуальність теми
Задачі
Моделі вимог
Класифікації вимог через МПП
Послідовність МАІ через
Модифікований МАІ (ММАІ)
Результати порівняння МАІ та ММАІ
Висновки

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата: завдання видав	Підпис, дата: завдання прийняв
Обґрунт. екон. ефект.	Кирич Н.Б.	[signature]	[signature]
Безпека надзвичайних ситуацій	Стоділка, Лягота О.М	[signature]	[signature]
Екологія		[signature] 21.11.19	[signature] 23.12
Охорона праці	Осухівська Г.М.		

7. Дата видачі завдання 30.09.19

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
		30.09.19	Виконав
1	Отримання завдання	30.09.19	Виконав
2	Аналіз завдання	15.10.19	Виконав
3	Написання розділу 1	30.10.19	Виконав
4	Написання розділу 2	20.11.19	Виконав
5	Написання розділу 3	30.11.19	Виконав
6	Обґрунтування економічної ефективності	1.12.19	Виконав
7	Охорона праці та безпека в надзвичайних ситуаціях		
8	Екологія	12.12.19	Виконав
9	Оформлення пояснювальної записки	21.12.19	Виконав
10	Оформлення граф. частини	22.12.19	Виконав
11	Попередній захист	24.12.19	
12	Захист	26.12.19	

Студент [signature] (підпис) Тарапата А.Я (прізвище та ініціали)

Керівник проекту (роботи) [signature] (підпис) Євтух П.С. (прізвище та ініціали)

АНОТАЦІЯ

"Методи аналізу ієрархій для автоматизації вибору мережевого обладнання з врахуванням вимог безпеки ”. // Тарапата Андрій Ярославович // Тернопільський національний технічний університет ім. І.Пулюя, факультет комп’ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних систем та мереж, група СІм-61 // Тернопіль, 2019 // с. –125, рис. –7, табл. –10, джерел –25.

Ключові слова: БАГАТОКРИТЕРІЙНА ОПТИМІЗАЦІЯ, МЕТОД САATI, АЛГОРИТМ ПРОСТОГО ВИБОРУ, QFD, ПРІОРИТЕТ.

У магістерській роботі виконано дослідження способів забезпечення необхідного рівня захищеності комп'ютерних мереж на основі багатокритеріальної оптимізації. Запропоновано використати ідею раннього оцінювання якості програмної архітектури і застосувати її щодо попереднього оцінювання рівня захищеності мережі на етапі її проектування.

В дипломній роботі показано актуальність оцінювання рівня захищеності комп'ютерних мереж з реалізацією різних засобів з метою вибору найбільш придатного. Пропонується спосіб відбору характеристик захищеності для оцінювання інтегрального показника захищеності мережі на основі встановлення їх пріоритетів. Саме оцінювання захищеності може здійснюватися з допомогою методу QFD чи методу аналізу ієрархій (MAI).

Для визначення коефіцієнтів пріоритетності використано обрахунок таких коефіцієнтів з допомогою простого алгоритму вибору. Для цього алгоритму початково визначається ступінь переваги параметрів захищеності мережі один над одним.

ANNOTATION

"Methods of hierarchical analysis for network equipment automatic choice taking into account safety issues " // Diploma paper of Master degree level // Tarapata Andrii Yaroslavovych // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Computer Systems and Networks Department // Ternopil, 2019 // p. –125, Fig. –7, Tables –10, Refence. –25.

Key words: SECURITY, COMPUTER NETWORK, ANALITICAL HIERARCHIC PROCESS, OPTIMIZATION.

The investigation of computer networks security assurance is carried out at the master degree paper. The main method for investigation is multicriteria optimization. The idea for early assessment of software architecture quality is offered for assessment of network security on the stage of its design.

The relevance of assessing the level of security of computer networks is shown in the thesis work with the implementation of various tools in order to choose the most suitable. A method for selecting security features is proposed for estimating the integral value of network security based on their prioritization. Security assessment can be done using the QFD method or analytical hierarchy process (AHP).

To determine the coefficients of priority, the calculation of such coefficients using a simple selection algorithm is used. For this algorithm, the degree of supremacy of network security parameters is determined.

ЗМІСТ

ВСТУП

Актуальність теми. Сучасні комп'ютерні мережі (КМ) характеризуються високим рівнем інтегрованості функціональних можливостей, підтримкою взаємодії декількох апаратних та програмних платформ, часто з використанням принципів розподіленості та паралельної роботи користувачів. Цей факт обумовлює високу складність проектованих систем. Не зважаючи на ріст рівня складності, вимоги до якості сервісів, котрі надаються цими системами, не знижуються. Однією з вимог до сервісів, які надаються через КМ, є безпека даних.

Контроль за безпекою інформації у КМ на сьогоднішній час – це не просто побажання замовників, а досить часто необхідність. Отже, розробка методів та засобів комп'ютерної безпеки взагалі та безпеки КМ зокрема є актуальною задачею при проектуванні комп'ютерних мереж.

Мета роботи. Метою роботи є розробка методів і засобів проектування комп'ютерних мереж з врахуванням вимог безпеки інформації.

Для досягнення вказаної мети в рамках дипломної роботи було сформульовано та розв’язано наступні **задачі:**

– дослідити сучасний стан технологій проектування КМ з врахуванням вимог захищеності;

– розробити модель для оцінювання рівня захисту КМ та метод її проектування;

– розробити метод порівняльного оцінювання проектів КМ на основі моделі багатокритеріальної ієрархічної оптимізації;

– дослідити ефективність модифікованого методу аналізу ієрархій в задачі оптимізації архітектури ПС.

Об’єкт дослідження: процеси забезпечення, контролю та управління безпекою у комп'ютерних мережах.

Предмет дослідження: методи та засоби проектування КМ, які забезпечують встановлений рівень захищеності даних у КМ.

Методи дослідження. Для досягнення мети дипломної роботи використовувались:

– методи узагальнення та аналізу – при проведенні огляду стану проектування КМ з врахуванням показників захищеності;

– формалізації та математичного моделювання – при розробці методу визначення показників рівня захищеності КМ та при вирішенні задачі вибору проектного рішення;

– методи багатокритеріальної ієрархічної оптимізації для оцінювання альтернативних проектів.

Наукова новизна отриманих результатів. Наукова новизна полягає у вирішенні задачі забезпечення захищеності КМ на етапі проектування. При цьому було отримано такі результати:

– запропоновано модель показників захищеності КМ;

– запропоновано метод оцінювання альтернативних проектів КМ на основі моделі багатокритеріальної ієрархічної оптимізації.

Практичне значення отриманих результатів. Всі розроблені методи можуть бути доведені до практичного впровадження у складі системи підтримки прийняття рішень (СППР) конструктора КМ. Така СППР дозволить реалізувати процес управління захищеністю КМ на етапі проектування архітектури шляхом розробки вимог якості до КМ, оцінювання та вибору найкращого з альтернативних проектів по визначеній множині критеріїв захищеності, можливості оперативної корекції оцінок при зміні вимог якості. А це дозволить підвищити якість проекту та зменшити ризик невідповідності виконаних проектів вимогам замовника.

Апробація результатів та особистий внесок здобувача. Основні положення роботи доповідались, розглядались та обговорювались на наукових

конференціях Тернопільського національного технічного університету. Результати дипломної роботи опубліковані у тезах студентської наукової конференції, яка проводились у ТНТУ.

Структура роботи. Робота складається з розрахунково-пояснювальної записки та графічної частини. Розрахунково-пояснювальна записка складається з вступу, 5 частин, висновків, переліку посилань та додатків. Обсяг розрахунково-пояснювальної записки – 125 арк. формату А4.

РОЗДІЛ 1
ПРОЕКТУВАННЯ МЕРЕЖ З ВРАХУВАННЯМ ВИМОГ БЕЗПЕКИ

Поняття інформаційних технологій (IT) включає в себе широкий обсяг дисциплін і сфер діяльності і стосується технічних засобів обробки і передачі даних (чи інформації).

В англійській мові поняття безпеки IT має два значення. Поняття функціональної безпеки (англ. safety) означає, що система коректно і у повному обсязі реалізує ті і лише ті цілі, що відповідають намірам її власника тобто функціонує відповідно до існуючих вимог. Поняття власне інформаційної безпеки (англ. security) стосується безпечності процесу технічної обробки інформації і є властивістю функціонально безпечної системи. Така система повинна унеможливлювати несанкціонований доступ до даних та запобігати їхній втраті у разі виникнення збоїв.

Говорячи про інформаційну безпеку, часто мають на увазі інформаційну безпеку в найзагальнішому сенсі, як комплекс заходів, покликаний зменшити число ймовірних шкідливих сценаріїв чи розмір збитків, яких може зазнати підприємство у разі розголошення конфіденційної інформації. З цієї точки зору інформаційна безпека – це економічний параметр, який повинен враховуватися у роботі підприємства, а інформацію (або дані) можна розглядати як певний товар або цінність, що підлягає захисту, а відтак вона має бути доступною лише для авторизованих користувачів чи програм.

Інформаційна безпека (information security) – збереження конфіденційності, цілісності та доступності інформації; крім того, можуть враховуватися інші властивості, такі, як автентичність, відстежуваність, неспростовність та надійність.

Інформаційні системи можна розділити на три частини: програмне забезпечення, апаратне забезпечення та комунікації з метою цільового застосування (як механізму захисту і попередження) стандартів інформаційної безпеки. Самі механізми захисту реалізуються на трьох рівнях або шарах: фізичному, особистісному та організаційному. По суті, реалізація політик і процедур безпеки покликана надавати інформацію адміністраторам, користувачам і операторам про те як правильно використовувати готові рішення для підтримки безпеки.

1.1. Модель характеристик безпеки у комп'ютерних мережах

1.1.1. Загальна характеристика системи безпеки. Рівні захисту мережевих систем

Захист даних є однією з головних проблем комп'ютерної мережі, оскільки перевагою мережі є доступ до спільних даних та пристроїв, а це зумовлює можливість несанкціонованого доступу до даних.

Безпека даних це захист ресурсів мережі від руйнування та захист даних від випадкового чи навмисного розголошення, а також від неправомірних змін.

Гарантувати безпеку даних покликаний адміністратор мережі. У великих мережах з цією метою передбачені спеціальні посади (security officers). Для гарантування безпеки даних розробляють багаторівневу систему захисту:

– вбудовані засоби захисту – програмно-системні (паролі, права доступу);

– фізичні засоби захисту – замки, двері, охорона, сигналізація тощо;

– адміністративний контроль – організаційні заходи, накази адміністрації;

– законодавство та соціальне оточення – закони про захист авторських та майнових прав, нетерпимість до комп'ютерного піратства.

Рівні захисту інформаційних систем.

Міністерство оборони США у книзі "Критерії оцінки безпеки комп'ютерів", (Оранжева книга), визначило сім рівнів безпеки комп'ютерних та мережевих систем. Ця розробка стала загальноприйнятою в світі для класифікації ступеня захищеності системи. Визначено такі рівні захисту:

– D – рівень мінімального захисту (Minimal Protection). Зарезервовано для систем, які за іншими рівнями не гарантують потрібного рівня безпеки;

– C1 – рівень вибіркового захисту (Discretionary Protection). Дає змогу користувачам застосовувати обмеження доступу для захисту приватної інформації;

– C2 – рівень керованого доступу (Controlled Access Protection). Містить вимоги рівня C1, а також захист процесу реєстрації у системі, облік подій захисту, ізоляцію ресурсів різних процесів;

– B1 – рівень захисту за категоріями (Labeled Protection). До вимог рівня C2 додається можливість захисту окремих файлів, записів у файлах, інших об'єктів системи спеціальними позначками безпеки, що зберігаються разом з цими об'єктами. Вважають, що подолати такий захист може добре підготовлений хакер, а звичайний користувач – ні;

– B2 – рівень структурованого захисту (Structured Protection). До вимог рівня B1 додається повний захист усіх ресурсів системи прямо чи посередньо доступних користувачу. Вважають, що хакери не зможуть проникнути у систему з таким захистом;

– B3 – рівень доменів безпеки (Security Domains). До вимог рівня B2 додається явна специфікація користувачів, яким заборонено доступ до певних ресурсів, повніша реєстрація потенційно небезпечних подій. Вважають, що навіть досвідчені програмісти не в стані подолати систему з таким рівнем безпеки;

– A1 – рівень верифікованої розробки (Verified Design). Повний захист інформації. Специфіковані та верифіковані механізми захисту. Вважають, що у систему з таким рівнем захисту без дозволу не може проникнути ніхто (навіть спеціалісти спецслужб).

1.1.2. Персональна ідентифікація

У деяких системах (наприклад, банківських чи податкових) потрібна ідентифікація не користувача, а фізичної особи. Розрізнюють кілька способів такої ідентифікації.

За персональними фізичними ознаками (біометрія). Знімають відбиток пальця, або геометрію руки, сітківку ока, зіницю, риси обличчя, а потім аналізують. Інший спосіб: система пропонує повторити певну кількість випадково вибраних слів та аналізує особливості голосу.

За предметом, який особа-користувач носить з собою. Таким предметом може бути спеціальний значок, магнітна картка з кодом. Цей спосіб є дешевим, проте ненадійним, предмет можна підробити, вкрасти тощо.

За тим, що особа повинна знати або пам'ятати. Треба пам'ятати пароль або правильно відповісти на низку запитань. Цей метод найдешевший і найпоширеніший, однак ненадійний (пароль можна підібрати, відповіді вгадати).

1.1.3. Надання права на доступ, автентифікація і реєстрація підключень

Безпека використання мережі забезпечується шляхом надання права на доступ, автентифікації і реєстрації підключень.

Процес ідентифікації користувача називається автентифікацією. Стандартний метод автентифікації – використання імені користувача і пароля як попередня призначена пара ідентифікаторів, які користувач повинен ввести у відповідь на запит системи для діставання доступу до мережевих засобів. При цій, найбільш простій, формі автентифікації ідентифікатор користувача і пароль передаються по мережі відкритим текстом (тобто не в зашифрованому вигляді). Сам процес автентифікації – порівняння переданої пари ідентифікаторів із записами таблиці, що знаходиться на сервері, – виконується відповідно до протоколу автентифікації по паролю (Password Authentication Protocol, PAP). Записи, що зберігаються, зашифровані, на відміну від передаваної пари ідентифікаторів, і це є слабкою стороною даного методу автентифікації.

Більш вдосконалена система запит-відповідь функціонує відповідно до протоколу автентифікації за запитом при встановленні зв'язку (Challenge Handshake Authentication Protocol, CHAP). Згідно цьому протоколу, агент автентифікації (ПЗ, що знаходиться на сервері) передає користувачеві ключ, за допомогою якого той шифрує своє ім'я і пароль і пересилає цю інформацію назад на сервер. Авторизація – процеснадання користувачеві права доступу до засобів системи, під час якого ім'я користувача і призначений йому пароль записуються в спеціальну таблицю системи.

Широко поширена система, що забезпечує високий рівень захисту при автентифікації, система запит-відповідь, в якій використовуються смарт-карти.

Регіструючи спроби доступу до мережі, можна легко визначити, чи не намагався неавторизований користувач проникнути у систему, а також дізнатися, чи не забув свій пароль хто-небудь з співробітників.

Блокування доступу. В багатьох організаціях як ідентифікатори користувачів вказувалися їх ініціали і прізвища. Зловмисникові, щоб спробувати проникнути в систему, досить було дізнатися такі. Розробники ПЗ створили програму блокування доступу до системи. Дуже часто ПЗ, що виконує блокування доступу, дозволяє задати ще один поріг: цим порогом визначається час, протягом якого система буде заблокована.

Важливим поняттям проблематики захисту даних у мережах є розпізнавання.

Розпізнавання – це гарантування, що інформація (пакет) надійшла від законного джерела законному одержувачу.

Справді, однією з найпоширеніших практик зловмисників у мережах є перехоплення пакетів та підміна їх своїми або скерування їх іншому адресату. Тому всі сучасні мережеві протоколи, зазвичай, оснащені засобами розпізнавання. Одним з механізмів розпізнавання пакетів є розміщення у відправника та одержувача однакових генераторів псевдовипадкових чисел. Кожен пакет позначають псевдовипадковим числом, яке порівнюється з таким же числом одержувача.

Аналогічне завдання виконує електронний підпис – послідовність байтів, які формують спеціальними алгоритмами та автентичність яких можна перевірити.

Для розпізнавання використовують окремі сервери, які видають електронні сертифікати. Сервери сертифікації застосовують у всіх достатньо потужних операційних системах.

Одним з найвідоміших вирішень є система централізованого розпізнавання Kerberos (вона реалізована програмним шляхом та сумісна з усіма типами систем. Працює система у клієнт-серверній парадигмі. Вона складається з програм-клієнтів, розміщених на робочих станціях користувачів, та серверних програм. Є три типи серверних програм: сервер розпізнавання, сервер надання дозволів та сервер адміністрування. У процесі розпізнавання клієнта беруть участь перші два з цих серверів. Кожен сервер має свою сферу дії, визначену змістом його бази даних користувачів).

Для вимірювання точності розпізнавання використовують два показники: відсоток хибного розпізнавання (False Acceptance Rate (FAR)) та відсоток хибного нерозпізнавання (False Rejection Rate (FRR)).

1.1.4. Захист мережі з використанням брандмауерів та серверів-посередників

Первинне значення терміну брандмауер (firewall) – це стіна у будівлі, зроблена з вогнетривких та незаймистих матеріалів, яка може перешкодити поширенню пожежі. У комп'ютерній мережі брандмауер – це комп'ютер з програмною системою, який встановлюють на межі мережі і який перепускає тільки авторизовані певним чином пакети.

Найчастіше брандмауери захищають внутрішню корпоративну мережу від зазіхань із зовнішньої мережі. Однак їх можна використовувати для фільтрування вихідної інформації, обмеження доступу користувачів внутрішньої мережі назовні.

Сервери-посередники (proxy-server). Інколи функції брандмауера в складних системах розподілені між власне брандмауерами та серверами-посередниками. Брандмауер захищає мережу від зовнішнього впливу. Він фільтрує кадри канального рівня, розпізнає сеанс, який відкриває зовнішній користувач. Сервер-посередник контролює та обмежує вихід внутрішнього користувача назовні, а також часто є його представником. Функції сервера-посередника: приховування адреси внутрішніх станцій, подаючи всю мережу назовні як один комп'ютер з адресою сервера; кешування популярних web-сторінок, файлів, так що користувачі не змушені звертатися до зовнішньої мережі. Популярну інформацію сервер оновлює автоматично з визначеною періодичністю.

Класифікація брандмауерів. Брандмауери застосовують різні алгоритми фільтрування, вони мають різні ступені захисту та вартість. Для класифікації брандмауерів їхню роботу описують з використанням еталонної моделі OSI.

Розрізняють:

– брандмауери з фільтруванням пакетів (packet filtering firewall; працюють на канальному, мережевому рівнях);

– шлюзи сеансового рівня (circuit level gateway; працюють на сеансовому рівні, розпізнають сеанс);

– шлюзи рівня застосувань (application level gateway; фільтрують інформацію за застосуваннями);

– брандмауери експертного рівня (stateful inspection farewall; виконують функції брандмауерів усіх нижчих рівнів).

Зазвичай, чим вищий рівень роботи брандмауера, тим більший рівень захисту він забезпечує.

Брандмауери з фільтруванням пакетів працюють разом з апаратним або програмним маршрутизатором. Вони аналізують зміст IP-заголовків пакетів і на підставі інформації у них та своєї таблиці правил й ухвалюють рішення про проходження пакета чи його відкидання. Найчастіше інформацією, на підставі якої ухвалюють рішення про проходження пакета, є його повна адресна

інформація, інформації про протокол та застосування, номери портів одержувача та відправника. Якщо пакет не задовольняє жодного з правил, то діє правило "за замовчуванням". Воно найчастіше відкидає пакет. Конкретна конфігурація правил залежить від політики організації. Брандмауери генерують невелику затримку передавання повідомлень. Часто функції фільтрування пакетів інтегрують у маршрутизаторах. Водночас рівень захисту у таких брандмауерів незначний – зловмисник може підмінити адресну частину IP-пакета.

Шлюзи сеансового рівня розпізнають учасників сеансу. Процедури перевірки виконують тільки на початку сеансу. Після того, як автентичність клієнта та сервера підтверджена, такий шлюз просто копіює пакети, не виконуючи фільтрування. Шлюзи сеансового рівня підтримують таблицю діючих сеансів і, коли сеанс завершується, знищують відповідний запис. Копіювання пакетів виконують спеціальні програми, які називають канальними посередниками (pipe proxies). Шлюзи сеансового рівня можуть виконувати і функцію сервера-посередника, який відображає внутрішні адреси локальної мережі в одну (фактично адресу брандмауера). Для пакетів, що надходять у зворотному напрямі, виконується зворотна операція. Отже, адресний простір мережі захищено – зовнішній користувач не бачить внутрішніх адрес. Однак такі шлюзи не забезпечують достатнього захисту і тому, зазвичай, не є окремим продуктом, їх постачають разом зі шлюзами рівня застосувань.

Шлюзи рівня застосувань. Застосуванням відповідають спеціальні програми-посередники. Вони можуть виконувати фільтрування на рівні застосувань. Кожне застосування може мати свого посередника. На відміну від посередників у шлюзах сеансового рівня, посередники рівня застосувань аналізують пакети на рівні застосувань. Наприклад, посередник застосування FTP може заборонити використання команди put для заборони передавання інформації на свій сервер.

Брандмауери експертного рівня поєднують риси всіх попередніх систем. Вони виконують фільтрування пакетів на канальному рівні, розпізнають сеанс

як шлюзи сеансового рівня і мають змогу аналізувати й фільтрувати пакети за ознаками рівня застосувань. На відміну від брандмауерів рівня застосувань, які фактично передають інформацію між двома розірваними ланками передавання клієнт-шлюз та шлюз-зовнішній комп'ютер і спричинюють значну затримку в передаванні інформації, брандмауери експертного рівня налагоджують пряме сполучення між розпізнаним клієнтом та сервером. Для фільтрування потоку використовують спеціальні шаблони, евристичні правила, порівняння зі зразками, інші методи з арсеналу експертних систем. Брандмауери експертного рівня забезпечують найвищий рівень захисту та високі параметри продуктивності.

Захист мережі за допомогою брандмауерів.

Брандмауер зазвичай встановлюється між маршрутизатором і мережею, яку захищають, і є комп'ютером з двома мережевимиі адаптерами. Один адаптер підключений до концентратора так званої демілітаризованої мережі (DMZ), інший – до концентратора мережі, яку захищають. Брандмауер зазвичай підключають, аби через нього проходив увесь трафік "Інтернет – мережа, яку захищають". Важливо відмітити, що, оскільки доступ до DMZ-концентратору мають тільки маршрутизатор і брандмауер, весь обмін даними з Інтернетом проходить через брандмауер.

Програмним забезпеченням брандмауера здійснюється: перевірка вмісту пакету, виконання проксі-служб, шифрування, автентифікація і генерування попереджень. Для перевірки підозрілого трафіку (наприклад, неодноразових спроб підключення до мережі) проводиться аналіз вмісту пакетів з однаковою IP-адресою пункту призначення. Далі дії залежать від конфігурації брандмауера: або відкидаються всі подальші підозрілі пакети, або про цю ситуацію повідомляється адміністратор брандмауера.

Проксі-служба є посередником між хостом, що запрошує службу, і самою службою і застосовується з такими протоколами, як FTP, Telnet. Брандмауер обробляє запити на з'єднання, а це означає, що він функціонує в якості проксі-

служби. Багато проксі-служб FTP дозволяють задіяти або відключати певні FTP-команди.

1.1.5. Захищені з’єднання та віртуальні приватні мережі

Одним із недоліків базового стека протоколів мережі Internet є відсутність криптографічного захисту та автентифікації передавань. Водночас такий захист потрібний у роботі корпоративних мереж, особливо для об'єднання мереж філій з головною мережею, а також для зовнішнього доступу у мережу з окремих комп'ютерів. Завдання захисту можна вирішити шляхом побудови окремої приватної мережі корпорації. Використання Internet є дешевою альтернативою побудові приватних захищених мереж.

Для забезпечення захисту передавань через Internet розроблено велику кількість різноманітних протоколів, які розміщені на декількох рівнях, починаючи з прикладного і закінчуючи канальним. Можливості та обмеження окремих протоколів залежать від протокольного рівня, до якого вони належать. Наприклад, захищені протоколи прикладного рівня пов'язані з конкретним прикладним протоколом, і з іншими протоколами не працюють. Отже, сполучення інших протоколів є незахищеними.

Протоколи сеансового та рівня відображення надають сервіс всім прикладним протоколам, однак застосування, що працюють з ними, все одно доводиться переписувати, проставляючи звертання до захищеного протоколу, що незручно. Протоколи мережного рівня не потребують переписування застосувань і тому, напевно, найзручніші. Захищені протоколи канального рівня, відповідно, пов'язані з мережевими технологіями канального рівня, їх використовують для вирішення обмеженого кола завдань, таких як захист віддаленого доступу до корпоративної мережі.

Розглянемо головні протокольні вирішення, які використовують для створення захищених сполучень.

1. Протокол SSL (Secure Socket Layer – рівень захищених сокетів). Щоб забезпечити можливість використовувати в операціях купівлі-продажу в

мережі, корпорацією Netscape був розроблений протокол передачі закритих даних між web-серверами і web-браузерами – протокол SSL. SSL є протоколом рівня відображення, він надає протоколам прикладного рівня сервіс зі створення захищених застосувань. Цей протокол використовує протокольний стек TCP/IP. Відкритою реалізацією SSL є протокол TLS (Transport Layer Security- безпека транспортного рівня).По протоколу SSL відкритий ключ передається браузером через SSL-з'єднання. Потім він використовується для отримання з сервера секретного ключа, за допомогою якого шифруються дані. Протокол SSL підтримується всіма найбільш популярними браузерами. Якщо для звернення до web-сторінки потрібне SSL-підключення, її URL починається з префікса https://, а не http://.

Протокол SSL вирішує три завдання:

– розпізнавання сервера на запит клієнта. Це особливо актуально, якщо клієнт передає конфіденційну інформацію, наприклад, номер кредитної картки;

– розпізнавання клієнта на запит сервера;

– захищене, зашифроване сполучення.

Складається SSL з двох протоколів: record protocol (визначає формати даних, які використовують для передавання) та handshake protocol (використовує record-протокол у фазі прив'язання сеансу). Під час обміну повідомленнями між клієнтом та сервером відбувається таке: розпізнавання сервера; сервер та клієнт обирають криптографічні алгоритми, які вони обидва підтримують; розпізнавання клієнта для сервера (необов'язково); визначення зашифрованого SSL-сполучення. Вибір алгоритму шифрування залежить від багатьох чинників. Наприклад, можна використовувати такі методи, як 3DES, AES, MD5, RSA, SHA.

Другим протоколом, що визначає порядок захищеної передачі даних через Web, є захищений HTTP – S-HTTP.

2. Протокол S-HTTP (Secure HTTP), RFC 2660, є розширенням до HTTP. На відміну від SSL, яким передбачається створення безпечного з'єднання між клієнтом і сервером, S-HTTP призначений для передачі індивідуальних

повідомлень Цей протокол створює захищені канали на прикладному рівні, даючи змогу шифрувати повідомлення. Він пов'язаний з HTTP та кожне http-повідомлення шифрує окремо.

Повідомлення S-HTTP складається з трьох частин: HTTP-повідомлення та криптографічних вимог відправника й одержувача. Відправник використовує відомі йому вимоги відправника та одержувача для шифрування повідомлення, а одержувач–для його дешифрування.

S-HTTP не потребує отримання відкритого ключа клієнтом і використовує тільки метод роботи з симетричними ключами. Це дуже важливо, тому що уможливлює надсилання запиту клієнтом без попереднього отримання відкритого ключа (спонтанну комунікацію). Використання захищеного протоколу відображене у заголовках запиту та статусу відповіді. Водночас S-HTTP є достатньо гнучким та може застосовувати багато різноманітних механізмів шифрування й розпізнавання. Протокол S-HTTP передбачає попередню домовленість між відправником та одержувачем про параметри захищеного сполучення. Ще однією перевагою S-HTTP є змога використання електронного підпису. Можливе передавання і без шифрування, однак з підписуванням.

3. Протоколи IPSec – це набір відкритих стандартів для організації захищеного передавання в мережах TCP/IP на мережевому рівні протоколу. Комплекс протоколів гарантує цілісність (незмінність даних), автентичність (дані надійшли від автентифікованого адресата); конфіденційність (не було несанкціонованого доступу до даних). IPSec, як і багато інших популярних технологій захисту даних, створює двопунктове захищене сполучення (тунель) між відправником та одержувачем даних.

4. Протокол PPTP (Point-to-Point Tunneling Protocol), розробки ф. Microsoft, кадри канального рівня під час передавання через Internet інкапсулюють у кадри IP. На боці одержувача відбувається зворотний процес. Виникає враження, що між учасниками обміну налагоджується пряме канальне сполучення, яке зазвичай можливе тільки в межах локальної мережі. Таке

сполучення назвали тунелем. Технологія тунелювання є основою створення віртуальних приватних мереж (Virtual Private Networks (VPN)) – це двопунктові сполучення, які налагоджують у межах комутованої мережі. Вони подібне до призначеного каналу або тунелю, який прокладають через багато проміжних пристроїв. Передавання даних цим тунелем автентифікують та шифрують. VPN створюють для вирішення двох завдань: віддаленого сполучення з корпоративною мережею; сполучення двох локальних мереж. PPTP використовує на транспортному рівні протокол TCP, так що фактично PPTP-тунель є TCP-сполученням.

Побічним ефектом від налагодження тунелю канального рівня є те, що через такий тунель можна передавати пакети мереж, які не підтримують протоколи TCP/IP (наприклад, пакети IPX, Appletalk та ін.). Справді, вихідний пакет канального рівня PPTP може містити довільний пакет мережного рівня. Коли цей пакет дійшов до адресата через мережу TCP/IP, його розпаковують, і мережевий пакет надходить для опрацювання у внутрішній корпоративній мережі. Отже, через Internet можна мати доступ у мережу, яка працює з іншим протокольним стеком.

5. Протокол L2TP. Недоліком PPTP є підтримка його головно в продуктах однієї ф. Microsoft. Корпорація Cisco розробила аналогічний стандарт L2TP (Layer 2 Tunneling Protocol) на базі L2F (Layer 2 Forwarding. За функційними можливостями L2TP наближений до PPTP: він також створює двопунктовий тунель канального рівня від комп'ютера користувача до сервера корпоративної мережі через Internet. Як і PPTP, L2TP забезпечує розпізнавання у разі налагодження каналу, однак не потребує обов'язкового шифрування. На відміну від PPTP, пакети L2TP інкапсулюють у пакети UDP. Для транспортування пакетів можна використовувати інші мережі (ATM, Frame Relay).

1.1.6. Шифрування даних

При передачі інформації застосовуються два методи шифрування даних: з використанням секретного ключа і з використанням відкритого ключа. В

першому випадку відправник і одержувач виконують шифрування і розшифровку повідомлення за допомогою одного і того ж ключа, в другому – із застосуванням двох ключів: відкритого, який відомий кожному і служить для шифрування даних, і секретного, відомого тільки одержувачеві повідомлення. При розшифруванні повідомлення виконуються складні математичні обчислення, в яких беруть участь обидва ключі.

В обох системах для шифрування і розшифровки даних застосовується операція додавання по модулю 2. Шифрування повідомлення виконується таким чином: спочатку з використанням ключа генерується псевдовипадковий потік даних, який потім складається по модулю 2 з відкритим текстом. Той же ключ використовується одержувачем повідомлення для його розшифровки.

З таблиці 1.1 видно, що при обміні даними виконується наступна послідовність дій: на передавачі для отримання потоку зашифрованих даних генерується псевдовипадковий рядок (PN-дані), який потім складається по модулю 2 з відкритим текстом. На приймачі за допомогою того ж ключа генеруються ті ж PN-дані, які складаються по модулю 2 з отриманими зашифрованими даними для отримання відкритого тексту.

Таблиця 1.1

Шифрування і розшифровка даних

Шифрування	Код
Відкритий текст (дані, що підлягають шифруванню)	10110110
PN-дані, що згенерували за допомогою ключа	01101101
Зашифровані дані	11011011
Розшифровка	Код
Зашифровані дані	11011011
PN-дані, що згенерували за допомогою ключа	01101101
Відкритий текст (розшифровані дані)	10110110

Головні проблеми системи шифрування з використанням секретного ключа пов'язані з адмініструванням і розподілом ключів. Оскільки обидві сторони, що беруть участь в обміні даними, використовують однаковий ключ, існує вірогідність того, що із збільшенням числа користувачів, що беруть участь в обміні, ключ перестане бути таємним. Крім того, великі проблеми виникають при адмініструванні і розподілі секретних ключів, оскільки для кожної пари (відправник і одержувач) потрібний свій секретний ключ. Внаслідок цих причин система шифрування з використанням секретного ключа не набула широкого поширення в середовищі World Wide Web. У системі з використанням відкритого ключа будь-який користувач, звертаючись на захищений web-вузол, отримує відкритий ключ, за допомогою якого шифрує свої дані і відправляє їх на вузол, де вони будуть розшифровані із застосуванням секретного ключа, який відомий тільки на цьому вузлі.

Системи з використанням секретного ключа називають також системами симетричної криптографії, оскільки для шифрування і розшифровки даних використовується один і той же ключ. Такі системи вважаються відносно нескладними в роботі і не вимагають виконання великого об'єму обчислень. Недоліки – проблеми, пов'язані з адмініструванням і розподілом ключів. Кожен ключ потрібно якимсь способом передати одній або обом сторонам, що беруть участь в обміні даними. Системи шифрування з використанням відкритого ключа позбавлені проблем, пов'язаних з розповсюдженням ключа (відкритий ключ доступний для всіх), проте, як це нерідко буває, вирішення однієї проблеми породжує іншу. У цих системах при розшифровці повідомлень виконуються дуже складні математичні обчислення, де задіяні обидва ключі, як відкритий, так і секретний, що вимагає наявність на комп'ютері одержувача достатньо потужного процесора. В деяких випадках використовуються обидві системи – відкритий ключ застосовується для передачі другій стороні секретного ключа, за допомогою якого потім шифруються передавані дані.

1.1.7. Цифрові сертифікати

Щоб упевнитися в тому, що користувач протилежної сторони дійсно є тим, за кого він себе видає, була розроблена система цифрових сертифікатів і організована служба, що поширює ці сертифікати; її назва – інфраструктура відкритих ключів (Public Key Infrastructure, PKI).

Цифровий сертифікат, що додається до передаваного повідомлення, призначений для посвідчення «достовірності» користувача або організації, що відправляють повідомлення, а також для надання одержувачеві інформації, яка буде використана ним при відправці відповіді. Цифровий сертифікат є тільки «посвідченням особи» відправника, але не дозволом на виконання яких-небудь дій.

Користувач (або організація), бажаючий передати зашифроване повідомлення, звертається до сервера сертифікатів (Certification Authority, CA). Сервер CA видає йому зашифрований цифровий сертифікат, в якому міститься відкритий ключ і додаткова інформація. Одержувач повідомлення також повинен звернутися до сервера сертифікатів і отримати відкритий ключ для розшифровки цифрового сертифікату, доданого до повідомлення. Це дає можливість одержувачеві упевнитися, що отриманий цифровий сертифікат є справжнім. Крім того, йому видається відкритий ключ відправника повідомлення.

CA можна розглядати як посередника, який дозволяє переконатися, що на протилежній стороні знаходиться саме той користувач, який потрібен. Поширеним стандартом видачі цифрових сертифікатів є ITU-T X.509.

1.1.8. Захист з використанням маршрутизаторів

Головною функцією, що виконується маршрутизаторами, була і залишається передача пакетів з однієї мережі в іншу. Але оскільки одна з цих мереж може бути приватною, а інша, скажімо, Інтернетом, маршрутизатори виступають в ролі першої лінії оборони, захищаючи дані закритої мережі.

Будь-який користувач, що має доступ до Інтернету, здатний проникнути в корпоративну мережу. Таким користувачем може бути потенційний покупець товарів, пропонованих через Інтернет, або просто цікава людина. Але, на жаль, це може бути і користувач, що намагається проникнути в корпоративну мережу з певною метою, їх саме прийнято називати хакерами. Для захисту корпоративних мереж застосовуються різні методи і використовуються різні типи мережного обладнання. Одним з таких методів захисту є обробка списку доступу, що виконується на маршрутизаторі.

Списки доступу.

Список доступу ACL (Access Control List) містить декілька операторів, призначених для управління потоком пакетів, які приходять на порт маршрутизатора. Більшість виробників маршрутизаторів підтримують два типи списків доступу: стандартний і розширений.

Стандартні списки доступу. У стандартному, або базисному, списку доступу є один або більше операторів, що складаються з IP-адреси джерела і ключового слова permit або deny. Під час вступу пакету на порт маршрутизатора, де задіяна функція захисту за списком доступу, перевіряється IP-адреса джерела. Якщо вона співпадає з адресою, що міститься в операторові списку доступу, і в цьому операторові вказано ключове слово permit, маршрутизатор пропускає пакет в мережу, що захищається. Але якщо в операторові вказано ключове слово deny, пакет відкидається.

У маршрутизаторах Cisco стандартний список доступу має наступний формат: access-list номер_списку {permit/deny} IP-адреса маска_адреси. Номером списку може бути будь-яке значення з діапазону від 1 до 99, що ідентифікує групу операторів, що належать одному списку доступу. Маска адреси, що складається з 32 біт, вказаних в десятковому вигляді, служить як спеціальний оператор, що ідентифікує конкретну IP-адресу або групу адрес. На відміну від маски підмережі значення бітів маски адреси трактуються протилежним чином. Тобто біти, що мають значення 0, повинні співпадати з

бітами, що знаходяться на цих же позиціях в адресі, що перевіряється, а біти, що мають значення 1, можуть не співпадати.

Приклад використання стандартних списків доступу. Припустимо, що мережа організації підключена до Інтернету в двох географічно віддалених пунктах (тобто мережа організації складається з двох віддалених мереж А і Б). Якщо мережа А має адресу 205.131.195.0, то, для того, щоб мережа Б могла отримувати пакети тільки з мережі А, на її маршрутизаторі повинен бути наступний список доступу: access- list I permit 205.131.195.0 0.0.0.255.

У цьому операторові маска адреси виглядає так: 0.0.0.255. Як вже згадувалося вище, значення 0 указують, що біти адреси відповідних позицій повинні співпадати, а значенням 1 можуть відповідати як одиниці, так і нулі. Отже, оскільки в масці адреси перші 24 біта мають значення 0, маршрутизатор пропустить в мережу Б тільки ті пакети, адреса мережі яких в точності співпадатиме з IP-адресою, вказаною в списку доступу (205.131.195.0), тобто тільки пакети мережі А. Останній байт маски має в десятковому вигляді значення 255, що відповідає запису 11111111 в бітовому виді. Себто, маршрутизатор пропустить в мережу Б пакети, відправлені будь-яким комп'ютером мережі А.

Слід зазначити одну важливу деталь, що відноситься до цього прикладу, – оператор дозволяє прийняти пакети, що поступають з мережі 205.131.195.0, проте тут немає жодного оператора, який би забороняв маршрутизатору пропускати певні пакети. Більшість маршрутизаторів, у тому числі і Cisco, конфігуровані так, що в їх списках доступу забороняється пропускати всі пакети, окрім тих, які явно визначені в операторах з ключовим словом permit. Тобто можна вважати, що в списках доступу після операторів permit слідує нескінченна послідовність «прихованих» операторів deny.

Розглянемо ще приклад. Припустимо, що потрібно пропускати в мережу тільки пакети, що відправляються хостом, IP-адреса якого 205.131.195.12. Для цього указують в списку доступу наступного оператора: access-list I permit 205.131.195.12 0.0.0.0. Замість цієї послідовності нулів і крапок можна

скористатися ключовим словом host. Іншими словами, попередній оператор може бути записаний так: access-list I permit host 205.131.195.12.

Розширені списки доступу надають додаткові можливості при фільтрації пакетів. Вони забезпечують фільтрацію на основі як IP-адреси відправника, так і IP-адреси одержувача, фільтрацію на основі номера порту протоколу (IP, ICMP, TCP, UDP) тощо. Загальний формат розширених списків Cisco виглядає так: access-list номер__списка {permit/deny} (протокол) адреса відправника маска_адреси [порт відправника] адреса_отримувача маска_адреси [порт отримувача] [додаткові^параметри].

Номер розширеного списку доступу може бути представлений значенням з діапазону від 100 до 199. Як і в стандартному списку доступу, номер розширеного списку ідентифікує тип списку, а також оператори, з яких він складається. У будь-який момент часу для перевірки пакетів, що поступають на один порт маршрутизатора, може використовуватися тільки один список доступу, проте можна створити декілька списків доступу і застосовувати їх в міру необхідності. Крім того, для потоків пакетів, що входять і виходять через один інтерфейс, можна застосовувати різні списки доступу.

Приклад використання розширеного списку IP-доступу. Припустимо, що мережа організації має IP-адресу 205.121.175.0; в мережі розташовані web-сервер з IP-адресою 205.121.175.10 і telnet-сервер з IP-адресою 205.121.175.14. Адміністратор прагне дозволити всім користувачам мережі з IP-адресами 205.131.195.0 звертатися до web-серверу, а доступ до telnet-серверу треба надати тільки адміністраторові, комп'ютер якого має IP-адресу 205.131.195.007. Для виконання такого непростого сценарію необхідно створити наступний розширений список доступу:

– access-list 101 permit 205.131.195.0 0.0.0.255 host 205.121.175.10
– access-list 101 permit host 205.131.195.7 host 205.121.175.14

Перший оператор списку доступу дозволяє будь-якому хосту мережі 205.131.195.0 звертатися до хосту (web-серверу) мережі, IP-адреса якого – 205.121.175.10. Згідно другому операторові, для того, щоб пакет був

пропущений в мережу, IP-адреса його джерела повинна бути рівною 205.131.195.7, а IP-адреса пункту призначення – 204.121.175.14. Пакети з будь-якими іншими адресами джерел і пунктів призначення будуть відкинуті.

Методика обробки операторів списку доступу. При перевірці пакету оператори списку доступу обробляються послідовно зверху вниз до першої відповідності вмісту заголовка пакету параметрам оператора списку доступу. Після виявлення збігу пакет або пропускається в мережу, або відкидається. Тому дуже важливо при створенні списку доступу враховувати не тільки зміст операторів, але і порядок їх перерахування

Списки доступу на маршрутизаторах, на жаль, не завжди ефективні. Існує можливість імітувати з'єднання і тим самим подолати бар'єр, встановлений за допомогою списку доступу. З таким методом злому можна боротися, заборонивши, наприклад, пропуск всіх пакетів, але це рівносильне відключенню від Інтернету. Крім того, при фільтрації пакетів за допомогою списків доступу не перевіряється їх вміст. Це означає, що хто-небудь може спробувати проникнути в закриту призначену для користувача групу на сервері шляхом послідовного перебору різних паролів. Дана технологія злому називається атакою із словником. Для подолання подібних проблем були розроблені пристрої мережного захисту ще одного типу – брандмауери (підрозділ 13.4).

Однією з функцій брандмауера, є вибіркове шифрування, що дозволяє шифрувати тільки ті дані, які на шляху до пункту призначення проходять через певні мережі, залишаючи інші дані незашифрованими. Використовуючи вибіркове шифрування і автентифікацію, можна створити логічний тунель, що з'єднує віддалені мережі організації через Інтернет. Створювані таким чином VPN стали альтернативою дорогим виділеним лініям. Детальніше технологію VPN розглянемо у наступному розділі.

1.2. Процес проектування комп'ютерних мереж з врахуванням вимог безпеки

При створенні комп'ютерної мережі розробник спільно з замовником визначає набір вимог до цієї системи. Для реалізації всіх необхідних функцій створюється каркас системи, елементами котрого будуть вузли, що реалізують певні функції. При чому для реалізації однієї і тієї ж вимоги можуть використовуватись різні типові рішення. Таким чином, система може бути реалізована багатьма способами, що приводить до появи певної кількості альтернативних проектних рішень.

Проектування високоякісної архітектури мережі з потрібним рівнем захищеності – це дослідницький процес для знаходження оптимальної комбінації, яка відповідає вимогам зацікавлених сторін. Цей дослідницький процес являє собою покроковий процес, під час якого інженер оцінює варіанти проектних рішень по відношенню до атрибутів захищеності, і отримує оптимізований проект, який відповідає вимогам зацікавлених сторін з мінімальними затратами. В процесі проектування повинні задовольнятись функціональні вимоги і вимоги якості. Прийняті проектні рішення мають вирішальний вплив на успіх будь-якого проекту програмного забезпечення. Потрібно мати структурований спосіб досягнення компромісів між різними варіантами проектних рішень з точки зору вимог до якості, так щоб розроблені системи програмного забезпечення були більше пристосовані для вирішення своїх завдань.

Процес проектування архітектури комп'ютерної системи (КС) з врахуванням показників якості включає декілька етапів:

– визначення вимог до КС, як функціональних, так і вимог якості, яке виконується на основі аналізу потреб всіх зацікавлених сторін.

Також необхідно визначити відносну важливість атрибутів якості. Після цього необхідно провести комунікацію вимог якості до КС на вимоги якості до проектної пропозиції.

– вибір альтернативних проектних рішень.

На основі аналізу вимог створюються альтернативні проектні рішення, які в подальшому будуть розглядатись для пошуку кращого з них. Кожен варіант проектного рішення повинен бути оцінений і порівняний з іншими. Архітектор повинен при цьому враховувати те, що альтернативи по різному впливають на реалізацію атрибутів якості, а атрибути, у свою чергу, мають різну відносну важливість. Оскільки вимоги до КС можуть змінюватись як в процесі проектування, так і під час експлуатації, то будуть змінюватись і пріоритети атрибутів, що може вплинути на порядок ранжування альтернатив. Це також необхідно враховувати при виборі варіантів рішення.

1.3. Методи комунікації вимог до захищеності мережі на вимоги до її проекту

Оскільки проект комп'ютерної мережі є моделлю реального інженерного рішення, то формулювання вимог захищеності до неї повинно виконуватись з врахуванням того, що прийняті проектні рішення в значній мірі визначать якість створюваної на їх проектів комп'ютерної мережі. Тобто вимоги якості до проекту безпосередньо повинні визначатись вимогами якості до готової мережі.

У цій роботі характеристики захищеності проекту мережі вибрано на основі аналізу предметної області. Потім кожна характеристика описувалась атрибутами, перелік яких визначається предметною областю.

У цій роботі пропонується загальна методика отримання характеристик захищеності мережі на основі загальної моделі її захищеності, оскільки для різних предметних областей різні характеристики захищеності мають різні значення важливості та різний вплив на реалізацію проекту мережі. Як згадувалось вище, реалізовані у проекті показники захищеності мережі визначають захищеність проектованої мережі загалом. Тому потрібно мати технологію комунікації характеристик захищеності проекту на характеристики

захищеності готової мережі. В якості такої технології пропонується застосовувати метод QFD (Quality Function Deployment) [1].

Метод QFD передбачає побудову так званого "будинку якості", який умовно показаний на рис0.

Цей метод був створений з метою отримання специфікації вимог до системи на основі вимог користувача. Зліва в будинку якості записуються вимоги користувача, а зверху – множина вимог до системи, сформульованих у технічних термінах. Елементами будинку якості a_{ij} є числа, що показують ступінь залежності кожного елементу верхнього рядка від елементів лівого стовпця. Разом ці числа становлять матрицю взаємозалежностей (або кореляційну матрицю). Значення a_{ij} вибирається з множини {0; 3; 6; 9} і відповідно показує міру залежності: 0 – елементи незалежні один від одного, 9 – елемент стовпця повністю задається елементом відповідного рядка. "Дах" будинку якості відображає взаємозв'язки між елементами множини вимог до системи і позначки в ньому показують міру взаємозалежності: ⊙ – сильно негативний зв'язок (покращення одного параметру веде до погіршення іншого), ○ негативний зв'язок, × – позитивний зв'язок, # – сильно позитивний зв'язок.

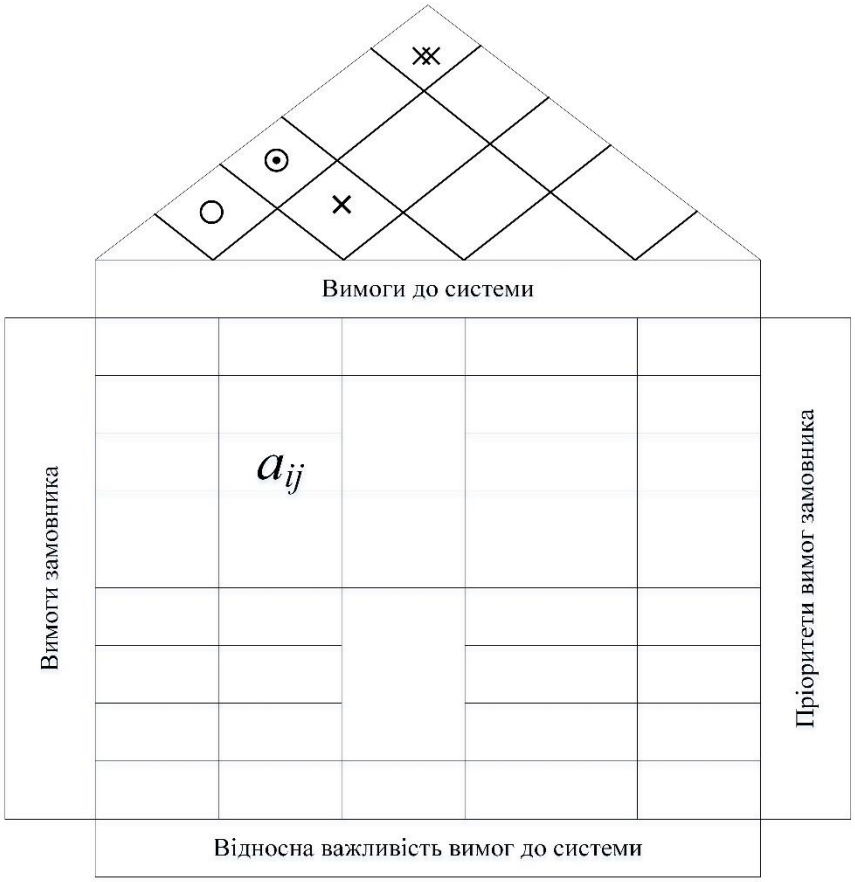

Рис. 1.1. "Будинок якості" методу QFD

Після заповнення кореляційної матриці експертами на основі пріоритетів вимог користувача (правий стовпець) обчислюються відносні важливості вимог до системи як сума добутків елементів матриці та пріоритетів вимог користувача.

Спрощену версію "будинку якості" пропонується використати у цій роботі для виділення найважливіших характеристик захищеності проектованої мережі з усієї множини характеристик (атрибутів) захищеності. Тут використовується лише частина "будинку якості", яка містить кореляційну матрицю.

У випадку розробки проекту мережі справа у будинку якості записуються характеристики захищеності системи $H_j^{ПС}$, а зверху – характеристики захищеності для конкретного проектного рішення H_i^A (див. рис0).

	…	H_i^A	…	
		⋮		
$H_j^{ПС}$	…	a_{ij}	…	$p_j^{ПС}$
		⋮		
		w_i^A		

Рис. 1.2. "Дім якості" для вибору характеристик якості архітектури

У клітинках таблиці дому якості експерти розставляють значення a_{ij}, які відображають ступінь впливу кожної характеристики якості архітектури на кожну характеристику захищеності мережі a_{ij}.

Використовуючи алгоритм простого вибору [2], для кожної характеристики (підхарактеристики) захищеності мережі $H_j^{ПС}$ визначаються її пріоритети $p_j^{ПС}$. Згідно цього алгоритму, початково визначимо ступінь переваги підхарактеристик захищеності мережі одна над одною. Для цього скористаємось транзитивною шкалою при основі 2. Тобто слабка перевага позначатиметься коефіцієнтом 2, сильна – 4, дуже сильна – 8 та абсолютна перевага – 16 і більше. Пронумеруємо показники якості у використанні в порядку зростання.

Тоді, до прикладу, коефіцієнт $\alpha_{2,1}=2$ означатиме, що показник з номером 2 за своєю значимістю вдвічі переважає показник з номером 1. Таким чином, через опитування експертів встановлюються всі значення коефіцієнтів переважання показників захищеності мережі один над одним. Потім цей вектор нормується до одиниці.

Останнім кроком буде обрахунок коефіцієнту важливості (ваги) кожної характеристики захищеності, реалізований у конкретній альтернативі проекту, для даної предметної області згідно формули:

$$w_i^A = \sum_j a_{ij} \cdot p_j^{ПС} . \quad (1.1)$$

Якщо наступним кроком задати нижню порогову межу $w_{пор.}$ для розрахованих значень ваг характеристик захищеності у альтернативному проекті, то можна таким чином "відсікти" малозначимі характеристики:

$$\{w_i^s\} \in \{w_i^{ПС}\} > w_{пор.}, \quad (1.2)$$

де $\{w_i^s\}$ – множина критеріїв захищеності, на основі яких проводитиметься її порівняльне оцінювання.

Цей крок на наступних стадіях проектування системи дозволить значно скоротити часові, людські та матеріальні ресурси, оскільки не доведеться затрачати сили на реалізацію всіх характеристик захищеності, а лише на найбільш значимі в контексті розроблюваного проекту.

Встановлена таким чином множина критеріїв захищеності дасть можливість отримати інтегральну оцінку кожного з альтернативних проектів на основі обрахованих ваг критеріїв захищеності та знаходження найкращого варіанту проекту комп'ютерної мережі.

1.3.2. Загальний аналіз проекту мережі і прийняття рішення

Використовуючи результати попереднього етапу, спеціаліст з комп'ютерних мереж обирає найкращий варіант з точки зору задоволення всіх вимог захищеності. Якщо такого варіанта проекту немає, то досліджується конфлікти між критеріями захищеності і будуються області компромісів, на основі аналізу яких обирається рішення.

Приведемо короткий огляд існуючих методів оцінювання і вибору проектних рішень мережі з аналізом повноти реалізації в них наведених вище етапів.

1.3.3. Методи на основі сценаріїв

Існує раннє і пізнє оцінювання. Раннє оцінювання використовується тоді, коли ще не створено реальної мережі або її моделей. Таке оцінювання базується на досвіді розробників та логічному обґрунтуванні, оскільки відсутні артефакти, які дають змогу імітувати роботу мережі. Методи, які реалізують раннє оцінювання, базуються на сценаріях. Вони були розроблені для оцінювання архітектурних рішень програмних систем, але принципи, закладені у них, можуть використатись і на етапі проектування мереж. Приклад такого сценарію описано далі у цьому підрозділі.

До цих методів належать наступні: SAAM і ATAM [3]. В методі SAAM для коректного порівняння проектних рішень, що розглядаються, запропоновано аналізувати їх у трьох аспектах, а саме: функціональність, структура та розміщення. На основі пріоритетів зацікавлених сторін визначаються критерії якості. Для перевірки задоволення кожного атрибута якості розробляється сценарій і проводиться оцінка рівня задоволення даного атрибуту варіантом архітектури.

1.3.4. Метод аналізу компромісних архітектурних рішень ATAM

Метод ATAM подібний до SAAM, але в ньому на основі аналізу сценаріїв для відібраних архітектур проводиться оцінка ризиків задоволення атрибутів якості. Оцінку ризиків проводить група експертів, яка також ранжує альтернативні варіанти за рівнем ризику і визначає так звані точки чутливості у компонентах чи зв’язках архітектури, також аналізуються компроміси між критеріями якості.

Методи ATAM і SAAM поєднані єдиною концепцією і часто використовуються в сукупності.

При використанні сценаріїв для оцінювання якості архітектурного рішення складаються певні сценарії: на основі варіантів використання, сценарії росту чи дослідні сценарії [3]. Перший тип сценаріїв ілюструють роботу системи у штатних умовах. Сценарії росту відображають реакцію системи на можливу зміну самої системи, а дослідні сценарії використовуються для оцінювання в нештатних ситуаціях.

Наприклад, сценарій на основі варіантів використання: віддалений користувач затребував звіт з бази даних через WEB в період пікового навантаження та отримав його через 5 секунд. Сценарій росту: добавити новий сервер даних для зменшення затримки у попередньому сценарії до 2,5 секунди. Дослідний сценарій: половина серверів відключається під час нормальних умов роботи без впливу на доступність системи в цілому.

Як видно, кожен із сценаріїв може відбуватись при певних умовах і містить стимул, об'єкт впливу, реакцію системи на стимул та величину, котра змінюється під час виконання сценарію. Для виконання оцінювання системи на основі сценарію мають бути визначені її архітектурні рішення, встановлені вимоги від різних зацікавлених сторін та побудоване дерево характеристик якості, подібне до зображеного на рисунку 0 [3].

Дерево характеристик якості у якості кореня містить інтегральну характеристику якості (корисність). Далі, як правило, характеристики продуктивності, модифікованості та інші, виділені в [4], становлять наступний рівень дерева. Потім кожна характеристика розбивається на підхарактеристики, перелік яких визначається предметною областю. Наприклад, продуктивність може містити підхарактеристики "Латентність даних" та "Пропускна здатність". На цьому рівні підхарактеристики виділяються таким чином, щоби їм вже можна було надати пріоритети. Далі підхарактеристики розбиваються на конкретні атрибути. Наприклад, "Латентність даних" може бути представлена атрибутами "Мінімізація затримки збереження даних у БД" чи "Доставка відео в режимі реального часу" з наступним можливим вказанням конкретних значень цих атрибутів у вигляді листків дерева.

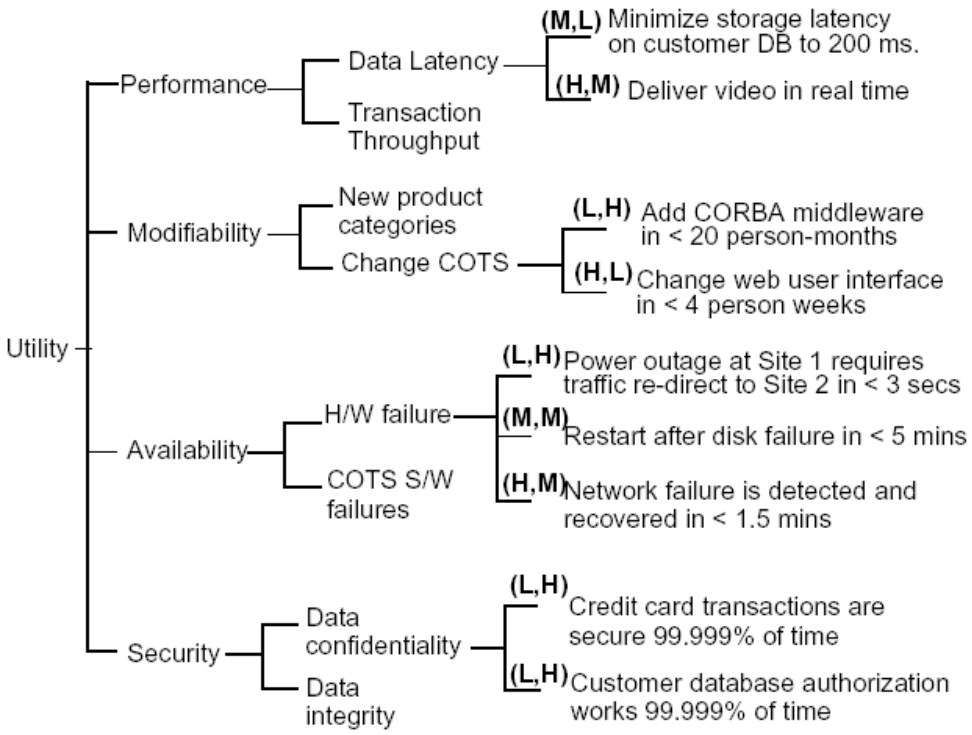

Рис. 1.3. Приклад дерева характеристик якості

Пріоритети присвоюються саме листкам дерева з використанням шкали H (High – Високий), M (Medium – Середній), L (Low – Низький). Присвоюється два значення пріоритетів кожному листкові: перше для відображення важливості вузла для успішної реалізації системи, а другий – для відображення того, наскільки легким розробники вбачають реалізацію даного атрибуту. Наприклад "Мінімізація затримки збереження даних у БД" має пріоритети (M,L), що означає середню важливість цього атрибуту для всієї системи та низький рівень ризику для його реалізації (тобто його буде просто забезпечити).

Далі представники різних зацікавлених сторін розробляють сценарії для оцінювання системи. Результатом цих сценаріїв є визначення ризиків того, які з характеристик якості будуть не відповідати поставленим вимогам, а також визначення чутливих точок (елементів системи), для котрих доведеться приймати рішення про компроміси між конфліктуючими характеристиками якості. На основі цих даних обирається певне проектне рішення.

Для кожної з характеристик захищеності мережі можна розробити і запропонувати загальні сценарії оцінювання. Ці сценарії спочатку потрібно

перетворити із загального вигляду у системно-орієнтований, тобто у такий, що відображає специфіку предметної області, для котрої проектується мережа.

Однією з переваг загальних сценаріїв полягає в тому, що вони дозволяють налагодити спілкування зацікавлених осіб, оскільки вони використовують різні терміни для позначення одних і тих же понять та явищ. Це особливо важливо при прийнятті компромісних рішень.

При створенні системно-орієнтованих сценаріїв на основі загальних для кожної складової сценарію вибираються конкретні елементи з можливим вказанням потрібних значень цих елементів.

Для методики оцінювання на основі сценаріїв у [3] пропонується використовувати шаблон, показаний у таблиці 1.2. Описи ризиків, чутливих до компромісів точок системи для кожного архітектурного рішення в такій таблиці не вказуються, а виносяться окремо.

Таблиця 1.2

Шаблон для оцінювання проекту мережі з використанням методу ATAM

<table>
<tr><td>Сценарій
Атрибут
Середовище
Стимул
Реакція системи</td><td colspan="3">Короткий опис сценарію
Назва атрибуту якості архітектури для оцінювання
Опис умов роботи системи (штатні, нештатні)
Що впливає на рівень захищеності
Відповідь системи на вплив в плані зміни атрибуту захищеності, який розглядається</td></tr>
<tr><td>Проектне рішення</td><td>Ризик</td><td>Чутливість</td><td>Компроміс</td></tr>
<tr><td>Список проектних рішень</td><td>Посилання на опис ризику</td><td>Посилання на опис чутливої точки (елементу)</td><td>Посилання на компроміс між атрибутами</td></tr>
<tr><td colspan="4">Обґрунтування
Обґрунтування вибору проектного рішення
Зображення проекту
Діаграма (топологія) вибраного проектного рішення</td></tr>
</table>

Всі етапи методу ATAM та їх вплив на кінцеві продукти оцінки показано у таблиці 0 [4].

Таблиця 1.3

Залежність операцій та продуктів ATAM

Операції	Формування вимог по атрибутах якості з розставленими пріоритетами	Каталог застосовуваних архітектурних методик	Аналітичні питання, що стосуються конкретних методик та атрибутів якості	Відображення архітектурних методик на атрибути якості	Ризиковані та неризиковані рішення	Точки чутливості та точки компромісу
1. Презентація ATAM						
2. Презентація комерційних факторів	*a				*b	
3. Презентація архітектури		**			*c	*d
4. Виявлення проектних методик		**	**		*e	*f
5. Складання дерева корисності атрибутів	**					
6. Аналіз проектних методик		*g	**	**	**	**
7. Мозковий штурм та розподіл сценаріїв по пріоритетах	**					
8. Аналіз проектних методик		*	**	**	**	**
9. Презентація результатів						

Пояснення до таблиці:

* – операція діє на результат напряму;

** – операція діє на результат опосередковано;

a – під час встановлення комерційних факторів викладається перший, найзагальніший опис архітектури;

b – під час презентації комерційних факторів можуть оголошуватись раніше виявлені чи постійні ризики, котрі підлягають фіксації;

c – у презентації архітектор може встановити додаткові ризики;

d – в презентації архітектор може виявити додаткові точки чутливості чи компроміси;

e – стандартні супутні ризики характерні для багатьох архітектурних методик;

f – багатьом архітектурним методикам властиві стандартні супутні варіанти чутливості та компроміси між атрибутами якості;

g – під час розгляду аналітичних операцій можливе виявлення нових архітектурних методик, не помічених під час операції 4 (таблиця 0). В такому випадку формулюються нові методико-орієнтовані питання.

Слід зазначити, що процес оцінювання архітектури КС з використанням методу ATAM – досить трудомісткий процес, який вимагає залучення значної кількості експертів та вимагає суттєвих часових ресурсів. Приблизний обсяг людських та часових ресурсів, потрібних на виконання етапів методу, показано у таблиці 0 [4].

Як видно з загального опису методу, вимоги якості до архітектури в даних методах визначаються експертами, формальні методи не використовуються. Тому має місце суттєвий вплив суб’єктивних факторів і відсутні методи автоматизації цих процесів.

Таблиця 1.4

Етапи ATAM та їх характеристики

Етап	Операції	Учасники	Середня тривалість
0	Встановлення партнерських відносин та підготовка	Керівництво групи оцінки та основні відповідальні за проект особи	Може тривати декілька тижнів
1	Оцінка	Група оцінки та основні відповідальні за проект особи	1 день з наступною перервою від 2-х до 3-х тижнів
2	Оцінка (продовження)	Група оцінки, відповідальні за проект особи і зацікавлені особи	2 дні
3	Доопрацювання	Група оцінки та замовник оцінки	1 тиждень

Аналіз проектних рішень відбувається послідовно по одному атрибуту якості, при виборі варіанта архітектури не використовуються методи оптимізації. Рівень автоматизації процесів низький через недостатнє використання формальних методів.

1.3.5. Метод аналізу вартості та ефективності CBAM

Метод ATAM відображає технологічну сторону проектування мережі і не враховує того фактору, що більшість компромісів здійснюються з врахування економічних факторів. Основним з них є вигоди, котрі може принести те чи інше проектне рішення.

Для спрощення прийняття рішень економічного характеру був розроблений метод економічного моделювання мережі, орієнтований на аналіз варіантів їх проектів – метод аналізу вартості та ефективності (Cost Benefit Analysis Method, CBAM). Він базується на ATAM та забезпечує моделювання затрат та вигод, пов'язаних з прийняттям архітектурно-проектних рішень та сприяє їх оптимізації. Вигоди представляються у вигляді величини ROI (Return of Investments – повернення інвестицій).

Для обґрунтованого вибору рішення в методі SAAM/ATAM вибрані альтернативні проекти аналізуються на ефективність витрат методом CBAM

[5]. Цей метод забезпечує економічний аналіз КС, який базується на вибраних в попередніх методах варіантах архітектури та сценаріях моделювання.

Експерти призначають оцінки критеріям якості в балах від 1 до 100 і ранжують архітектури за значенням, яке ці архітектурні рішення забезпечують для атрибуту якості. Оцінка кожного варіанта архітектури обчислюється за формулою (1.3).

$$B(A_i) = \sum_{j=\overline{1,K}} \left(Cost_{i,j} \cdot Q_j\right) \; i = \overline{1,n}. \tag{1.3}$$

Тут $Cost_{i,j}$ – вага і-ї архітектури відносно j-го атрибута;

Q_j – пріоритет j-го атрибута.

Під час оцінювання проекту мережі згідно методики CBAM виконують наступні етапи [6].

1. Критичний аналіз сценаріїв. Цей етап проводиться в рамках ATAM. Зацікавлені сторони можуть також генерувати нові сценарії. Пріоритети розставляються відповідно з потенціалом сценаріїв в контексті виконання комерційних задач системи. За результатами виконання етапу залишається приблизно третина сценаріїв.

2. Уточнення сценаріїв. Уточняються сценарії, відібрані на першому етапі. Основна увага приділяється значенням стимул-реакція. Для кожного сценарію встановлюється найгірший, найкращий та бажаний рівень реакції атрибуту якості.

3. Розстановка сценаріїв відповідно до пріоритетів. Кожній зацікавленій особі виділяється однакова кількість голосів, яку потрібно розподілити між сценаріями на основі бажаних значень їх реакції. Після підрахунку голосів залишається приблизно половина сценаріїв. Сценарію з найвищим рангом присвоюється вага 1 і, відштовхуючись від цього значення, встановлюються значення ваг для решти сценаріїв. Саме ці значення потім використовуються для обчислення загальної вигоди від проектного рішення. Також на цьому етапі

встановлюється перелік атрибутів якості, які зацікавлені сторони вважають значимими.

4. Встановлення корисності. Тут визначаються значення корисності всіх рівнів реакції (найкраще, найгірше, поточне та бажане) атрибуту якості.

5. Розробка для сценаріїв архітектурних рішень та встановлення їх бажаних рівнів реакції атрибуту якості. Оскільки кожне проектне рішення впливає на декілька сценаріїв, то розрахунки виконують для кожного сценарію.

6. Визначення корисності очікуваних реактивних рівнів атрибуту якості.

7. Розрахунок загальної вигоди ROI, отриманої від проектного рішення згідно (1.3).

8. Відбір проектних рішень з врахуванням ROI, а також обмеження по часу та вартості.

9. Інтуїтивне підтвердження результатів.

Метод забезпечує оцінку затрат на реалізацію кожної альтернативи і дає можливість обчислити показник бажаності як відношення прибутку до затрат. На основі отриманих даних проводиться вибір кращого рішення.

Метод CBAM використовує архітектурні рішення і атрибути якості, отримані із SAAM/ATAM, і забезпечує лише оцінку рішень, тобто фактично реалізує третій і частково четвертий етапи проектування архітектури.

Часто виникають задачі створення КС на базі існуючої шляхом перепроектування для задоволення нових вимог якості. Для вирішення таких задач було створено метод реінжинірингу архітектури КС на основі сценаріїв SSAR (Scenario-based Software Architecture Reengineering) [*7*], який є сукупністю чотирьох методів оцінки проектів відносно атрибутів якості:

– оцінка на основі сценаріїв;
– моделювання;
– математичне моделювання;
– оцінка на базі практичного досвіду.

При використанні SSAR обирається один із методів, але основним є метод оцінювання на основі сценаріїв. Цей метод подібний до того, що реалізується в SAAM.

При використанні моделювання основні компоненти КС реалізуються в коді, а інші моделюються комп'ютером, утворюючи виконувану систему.

При використанні математичного моделювання характеристики якості КС оцінюються за допомогою математичних моделей операцій, на яких ці характеристики реалізуються.

Оцінювання на базі практичного досвіду дає можливість виявити дефекти проектних рішень та проблеми, які необхідно усунути.

Метод SSAR не містить процедур вибору альтернативних проектів, а також виявлення конфліктів і пошук компромісів між атрибутами якості. Оцінювання проводиться послідовно по кожному атрибуту якості без використання процедури оптимізації. Спільним недоліком розглянутих методів є послідовне оцінювання архітектури по одному параметру, що робить процес вибору трудомістким і неформалізованим

З проведеного аналізу слідує, що методи оцінювання проектів базуються в основному на експертній інформації. При цьому широко використовуються знання та досвід проектувальників. Тому для підвищення ефективності цих методів необхідно використовувати їх у складі експертної системи, в якій знання формалізовані в базі знань, а процеси введення та обробки експертної інформації автоматизовані з допомогою апаратно-програмної платформи.

1.4. Використання методу аналізу ієрархій для оцінювання якості проекту КС

Поява робіт, в яких було використано процедуру аналізу ієрархій, дозволив значно покращити процес вибору обладнання для реалізації необхідного рівня захищеності мережі і формалізувати його по аналогії, як це запропоновано у роботах [*8*], [9].

В методі AHP (Analytical Hierarchy Process) використовується порівняльне оцінювання альтернатив стосовно реалізації атрибутів якості. Він дає змогу визначити відносні ваги альтернатив по кожному атрибуту якості і проранжувати їх. За призначеними зацікавленими сторонами пріоритетами атрибутів якості обчислюється їх усереднене значення і визначаються ваги альтернатив відносно сукупності атрибутів якості.

Отримані відносні оцінки альтернатив можуть використовуватись для аналізу конфліктів між атрибутами якості і пошуку компромісного рішення.

Перевагами методу SAHP є оцінювання альтернатив по всіх атрибутах якості, оптимізація рішень та досить високий рівень формалізації, що дає змогу автоматизувати процес.

Як було відзначено раніше, для вибору найкращого проекту КС з множини альтернативних необхідно отримати їх оцінки відносно реалізації критеріїв якості. Але, оскільки якість проект КС визначальним чином впливає на якість реалізованої мережі, існує залежність між показниками якості проектного рішення та КС і ця залежність є ієрархічною, де на вершині міститься інтегральний показник якості КС, далі – проміжні рівні (критерії якості КС, критерії якості альтернативного проекту), а на найнижчому рівні розташовані проектні альтернативи.

Для розв'язання такого типу задач використовується метод аналізу ієрархій Сааті [*10*]. Суть методу полягає в тому, що для побудованої ієрархії на кожному рівні визначаються ваги елементів відносно їх впливу на елемент наступного рівня. Для цього будується матриця парних порівнянь для кожного з нижчих рівнів, по одній матриці для кожного елемента рівня, який примикає зверху. Парні порівняння проводяться в термінах домінування одного з елементів над іншим.

Детальний аналіз цього методу буде приведено у далі у цій дисертаційній роботі. Зараз же варто зазначити, що при значній кількості альтернатив неузгодженості коефіцієнтів матриці парних порівнянь є досить суттєвими (20 – 30%), що не дозволяє отримати прийнятне рішення. Для зменшення

неузгодженості при великій кількості альтернатив та/або критеріїв порівняння автор методу [*10*] пропонує розбивати кожен рівень ієрархії на кластери, об'єднуючи у них споріднені за певною ознакою елементи та оцінювати вплив на елемент наступного рівня ієрархії цілого кластеру. При все ще надто великій кількості кластерів (більше 9) пропонується згрупувати кластери у ще загальніші групи. При визначенні ваг кожного з кластерів потім розв'язується задача визначення ваг складових цього кластеру і так далі, аж поки не будуть отримані значення ваг для початкової множини альтернатив. Очевидно, що в цьому випадку доведеться виконувати значний обсяг обчислень, що може суттєво позначитись на продуктивності системи, яка реалізовуватиме розв'язок задачі оптимального вибору на основі методу аналізу ієрархій, а також групування в кластери проводиться експертами, що є непростою задачею і вносить свої похибки.

РОЗДІЛ 2
ПОСТАНОВКА ЗАДАЧІ БАГАТОКРИТЕРІАЛЬНОГО ОЦІНЮВАННЯ ТА ВИБОРУ ПРОЕКТУ КС З ВРАХУВАННЯМ ХАРАКТЕРИСТИК ЗАХИСТУ

Як зазначалось у вище, може бути запропоновано декілька альтернативних проектів комп'ютерних мереж, які будуть задовольняти функціональним вимогам та вимогам захищеності. Компоновка альтернативних проектів для аналізу і оцінювання здійснюється, як правило, з готових рішень (патернів) проектування за розробленими технологіями. У розгляд може включатись і проекти існуючої мережі при проведенні її реінжинірингу. Задачею інженера є вибір з наявної множини проектів такого, який буде найкраще задовольняти вимогам якості, в тому числі і захисту даних. Схематично процес оцінювання та вибору проекту мережі подано на рис. 2.1.

Тут представлено такі рівні характеристик якості:

$K_i^1, i = \overline{1,m1}$ – критерії якості мережі;

$K_i^2, i = \overline{1,m2}$ – критерії якості проекту мережі;

$A_i, i = \overline{1,n}$ – альтернативні проекти.

Набір характеристик для оцінки якості проекту комп'ютерної мережі $\{K_i^1\}$ визначається на основі сформульованих замовником вимог. А набір критеріїв $\{K_i^2\}$ отримуємо через відображення $\{K_i^1\}$ на якість мережі методом Quality Function Deployment (QFD) або іншим.

Треба обрати рішення, яке буде оптимізувати сукупність критеріїв $\{K_i^1\}$, $\{K_i^2\}$. Це задача мультикритерійної оптимізації на ієрархічній структурі.

Розв'язок сформульованої задачі будемо через імплементацію такої послідовності кроків.

1. Визначимо оцінки альтернатив по кожному з характеристик якості. Для цього можна скористатись одним із методів, порівняльний аналіз яких здійснено далі у наступних підрозділах.

2. Визначити оцінки альтернатив по сукупності критеріїв захищеності, а коли це неможливо з достатньою точністю, то визначити порядок ранжування альтернатив.

3. На основі аналізу отриманих на попередніх етапах оцінок та аналізу компромісів і чутливості рішень до зміни вимог якості здійснюємо вибір кращої альтернативи.

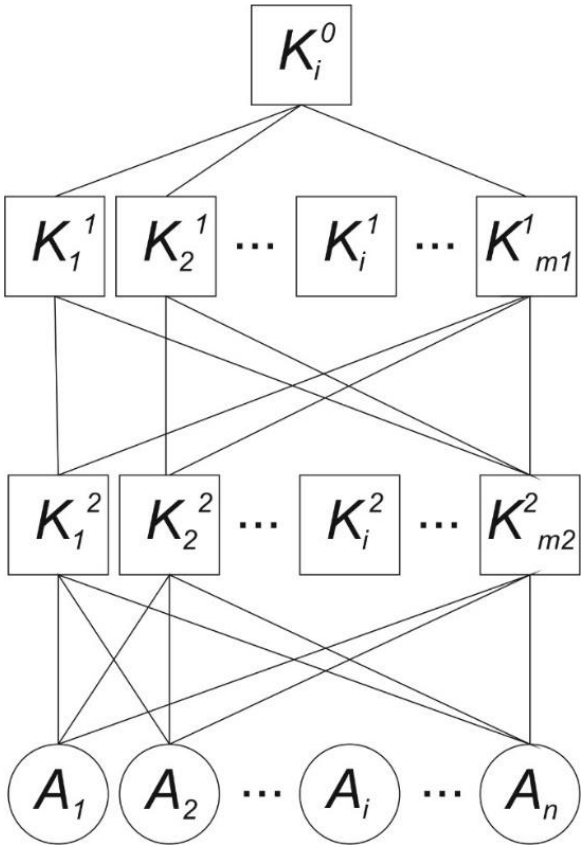

Рис. 2.1. Ієрархічне подання задачі вибору та оцінювання проекту мережі

Тут слід відмітити, що оцінювання проектів здійснюється на ранніх етапах проектування, коли відносно створюваної мережі визначені лиш вимоги. Визначити абсолютні значення характеристик якості для альтернатив з достатньою достовірністю неможливо на цьому етапі, і тому будемо визначати порівняльні оцінки.

Для оцінювання альтернатив по множині характеристик якості розроблено ряд методів, які мають свої переваги і недоліки. Для

обґрунтованого вибору найбільш ефективного, для вирішення поставленої задачі, приведемо результати аналізу цих методів.

Огляд мультикритеріальних методів оцінювання

В процесі вирішення більшості задач вироблення рішень виникає потреба враховувати велику кількість альтернатив і критеріїв. Розглянемо основні методи вироблення рішень для випадку мультикритерійної оптимізації. У процесі мультикритеріального оцінювання та вибору альтернатив розв'язуються такі задачі:

1. Порівняльне оцінювання.
2. Впорядкування альтернатив (ранжування).
3. Вибір найкращої альтернативи.

З допомогою деяких методів вироблення мультикритерійних рішень можна тільки вирішити завдання ранжування альтернативних проектів. Вони дозволяють отримати впорядковану множину альтернативних варіантів рішень (ординальні оцінки). Ці методи не дають можливість визначити відносні оцінки критеріїв у кількісній формі. Розглянемо деякі з них.

Метод ЗАПРОС

Метод ЗАПРОС (Замкнуті Процедури у Опорних Ситуаціях) [11], [12] ґрунтується на ідеї перевірки незалежності критеріїв та заміщення приростень оцінок за одними характеристиками приростеннями оцінок за іншими. Метод ЗАПРОС дозволяє вирішити лише завдання ранжування альтернативних проектів, яке зводиться до упорядкування в межах єдиної шкали множини допустимих кортежів оцінок за прийнятими якісними характеристиками. Спочатку треба ранжувати різні значення оцінок, виражені природною мовою, за кожним якісним критерієм. Далі визначити кінцеву множину допустимих кортежів оцінок, що є декартовим добутком множин значень оцінок за кожним критерієм; потім ранжувати кортежі в межах підмножини кортежів, які

розрізняються оцінками тільки за одним критерієм. Кортежі, що мають виключно кращі та гірші значення оцінок за всіма характеристиками, називають замкненими процедурами у опорних ситуаціях. ОПР (особа, яка виробляє рішення) для визначення переваг пред'являється пара кортежів (r_i, r_j). У кортежі r_i оцінки за всіма характеристиками, за винятком *i*-го, збігаються з оцінками в опорній ситуації (тобто найкращими або найгіршими), в ситуації r_j те саме простежується щодо оцінок за критерієм c_j. Особі, яка приймає рішення пропонується визначити, який з кортежів на її думку є кращим. Інакше кажучи, їй пропонується виконати заміщення прирощення оцінки за критерієм c_i, який відповідає заміні найкращого (найгіршого) значення оцінки за цим критерієм значенням оцінки з r_i, прирощенням, яке відповідає заміні найкращого (найгіршого) значення оцінки за критерієм c_j, значенням оцінки з r_j. Результат порівняння альтернатив із кортежами (r_i, r_j) дозволяє побудувати єдину шкалу для подання оцінок за характеристиками c_i, c_j. Після цього здійснюється впорядкування у межах цієї шкали множини кортежів оцінок за досліджуваними характеристиками. Перевагою методу ЗАПРОС є те, що метод дозволяє ранжувати альтернативи за суб'єктивними вербальними оцінками з урахуванням важливості критеріїв, що дуже важливо для задач мультикритеріального вибору.

Цей метод належить до групи методів, які використовують числові ваги критеріїв, але не використовують функції цінності, замість якої будується вирішальне правило у вигляді бінарного відношення, яке дозволяє виділити підмножину з вхідної сукупності.

Метод ELECTRE

Метод ELECTRE [11], [13] полягає в тому, що критеріям $c_1, c_2, \ldots, c_\mu$ оцінювання альтернатив присвоюються коефіцієнти важливості $v_1, v_2, \ldots, v_\mu$.

Для кожної пари альтернатив (A_i, A_j) обчислюють Індекс незгоди $d(A_i, A_j)$ та індекс згоди $v(A_i, A_j)$. Індекс згоди визначають так:

$$v(A_i, A_j) = \sum_{c_h \in C_{ij}^+} w_h \Big/ \sum_{u=1}^{\mu} w_u ,$$

де $v(A_i, A_j)$– індекс згоди пари альтернатив (A_i, A_j);

C_{ij}^+ – підмножина критеріїв, за якими альтернатива A_i не поступається альтернативі A_j;

c_h – критерій з підмножини C_{ij}^+;

μ – кількість критеріїв;

w_h, w_u – коефіцієнти відносної важливості критеріїв c_h і c_u відповідно.

Індекс незгоди обчислюють за такою формулою:

$$d(A_i, A_j) = \begin{cases} 0, \text{ якщо } C_{ij}^- = \varnothing; \\ \underset{c_h \in C_{ij}^-}{Max}\left[w_h \left| e_h(A_i) - e_h(A_j) \right|\right] \Big/ d_h, \text{ якщо } C_{ij}^- \neq \varnothing, \end{cases}$$

де $d(A_i, A_j)$ – індекс незгоди пари альтернатив (A_i, A_j);

C_{ij}^- – підмножина критеріїв, за якими альтернатива A_i поступається альтернативі A_j;

c_h – критерій з підмножини C_{ij}^-;

w_h – коефіцієнт відносної важливості критерію c_h;

$e_h(A_i), e_h(A_j)$ – оцінки альтернатив A_i, A_j за критерієм c_h відповідно;

$d_h = \underset{A_i, A_j \in A}{Max}\left[w_h \left| e_h(A_i) - e_h(A_j) \right|\right]$.

Набір значень індексів згоди і незгоди дає можливість отримати підсумкове ранжування альтернативних проектів. Пропонується наступне

правило порівняння: альтернатива A_i перевершує альтернативу A_j, коли $v(A_i, A_j) \geq p$, а $d(A_i, A_j) \leq q$, де p, q – порогові значення, визначені ОПР. Це правило порівняння спрощує проблему виділення підмножини серед альтернативних проектів, що містять найкращу альтернативу, проте не дозволяє вирішити завдання їх повного впорядкування.

Методи ЗАПРОС і ELECTRE дозволяють вирішити лише завдання ранжування альтернативних проектів, таким чином більш загальна задача знаходження кількісних оцінок відносної корисності альтернатив за допомогою даних методів нерозв'язна. Слід зауважити, що метод ELECTRE не дозволяє вирішити задачу повного впорядкування альтернатив.

Методи вироблення рішень, які базуються на використанні функції цінності

Розглянемо методи, які ґрунтуються на використанні функції цінності. Вони базуються на отриманні "системи цінності" особи, яка приймає рішення, у процесі діалогу з нею.

Далі ця інформація використовується для побудови функції цінності, значення якої враховується при прийнятті рішення. Ця група методів дозволяє для завдань мультикритеріального вибору отримати багатовимірну функцію цінності (корисності), максимальне значення якої відповідає варіанту, якому віддається найбільша перевага.

Найчастіше використовується функція лінійної згортки, при цьому вибір функції в багатьох випадках проводиться необґрунтовано. Серед таких методів найбільш широко використовуваними є метод простого адитивного зважування (ПАЗ), метод мультиплікативного експоненціального зважування (МЕЗ).

Метод простого адитивного зважування (ПАЗ) [11] дозволяє розв'язати задачу знаходження кількісних оцінок відносної корисності альтернатив. Альтернативи ранжуються відповідно до зростання сум s_j:

$$s_i = \sum_{j=1}^{\mu} w_j r_{ij} ,$$

де s_i – сума оцінок r_{ij} альтернатив за характеристиками, з ваговими коефіцієнтами w_j відносної їх важливості;

μ – кількість критеріїв оцінки;

r_{ij} – оцінки за характеристиками;

w_j – коефіцієнти відносної важливості цих критеріїв.

Метод мультиплікативного експоненціального зважування (МЕЗ) [11] відрізняється від ПАЗ лише тим, що альтернативи ранжуються відповідно до величин добутків оцінок за різними характеристиками:

$$p_i = \prod_{j=1}^{\mu} r_{ij}^{w_j} ,$$

де p_i – величина добутків степенів оцінок за характеристиками для кожного *i*-го проекту;

μ – кількість критеріїв;

r_{ij} – оцінки за характеристиками;

w_j – коефіцієнти відносної важливості критеріїв.

Використання методу аналізу ієрархій

"Метод аналізу ієрархій" (MAI) Сааті [10] в даний час найбільш часто застосовується для розв'язування задач мультикритеріального вибору. Основними етапами MAI є:

1. Сформулювати задачу.

2. Побудувати ієрархію з проміжними рівнями (критерії, які задають наступні рівні). Найнижчий рівень є, як правило, самими альтернативами (рис. 2.2).

У представленій на рис.0 задачі маємо m альтернатив $A_1,\ldots,A_m$ і s рівнів критеріїв $E_j^i, i=\overline{1,s},\ j=\overline{1,m_i}$.

3. Скласти набір матриць попарних порівнянь (МПП) для кожного з нижніх рівнів – по одній матриці для кожного елемента батьківського рівня. Парні порівняння проводяться в термінах домінування одного з елементів над іншим. Число b_{ij} задається експертом і показує, у скільки разів вага об'єкта A_i більша від об'єкта A_j відносно заданої цілі (критерію), $b_{ij}=\dfrac{1}{b_{ji}}$, на головній діагоналі МПП стоять одиниці. МПП (суджень) є позитивною, квадратною та обернено симетричною. Шкалою для виконання попарних порівнянь є найбільш часто використовувана дев'ятибальна шкала, запропонована Т. Сааті. Для отримання кожної матриці потрібно $\dfrac{n(n-1)}{2}$ суджень, де n – це кількість порівнюваних елементів.

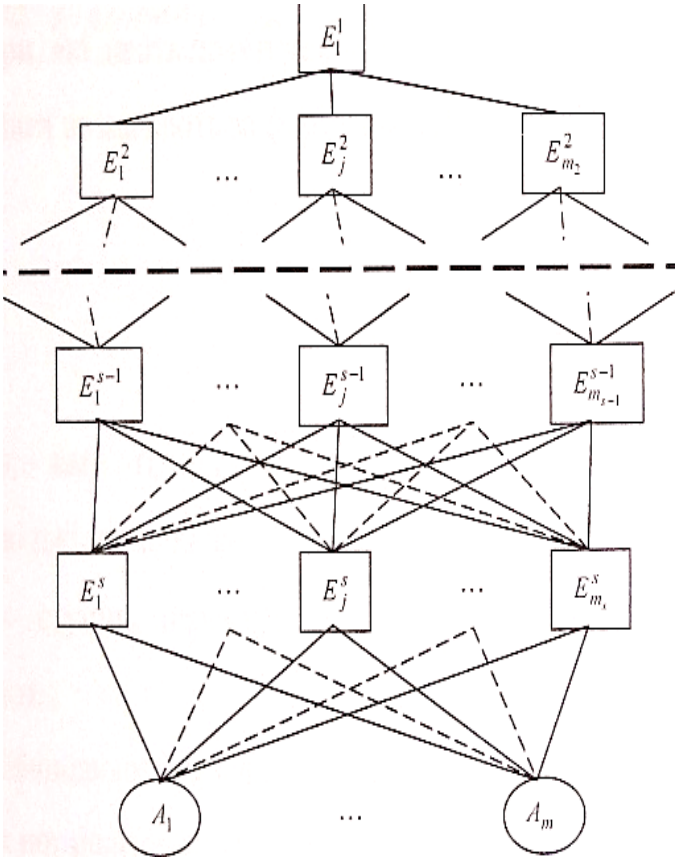

Рис. 2.2. Приклад ієрархічного представлення задачі вироблення рішень

4. Визначити ваги $w_i, i=\overline{1,n}$ об'єктів $A_i, i=\overline{1,n}$ через знаходження вектора. Як відомо, знаходження власного вектора матриці є вкрай трудомісткою обчислювальною процедурою. Наближені значення ваг можна отримати за співвідношеннями 0:

$$w_i = \frac{\sqrt[n]{\prod_{j=1}^{n} b_{ij}}}{\sum_{i=1}^{n}\left(\sqrt[n]{\prod_{j=1}^{n} b_{ij}}\right)} \text{ або } w_i = \frac{1}{n}\sum_{j=1}^{n}\frac{b_{ij}}{\sum_{j=1}^{n} b_{ij}},$$

де w_i – вага *i*-го об'єкта;

n – кількість порівнюваних об'єктів;

b_{ij} – ступінь переваги *i*-го об'єкта на *j*-м об'єктом щодо заданої мети (критерію). В подальшому це позначення у віх формулах має такий же зміст.

5. Визначити узгодженість матриць попарних порівнянь. Для цього знаходять наближене значення $\lambda_{\max}$ за рахунок обчислення вектор-стовпця $B\overline{w}$ з подальшим підсумовуванням його елементів [14]. Відомо, що для повністю узгодженої МПП $\lambda_{\max} = n$, а для неузгодженої матриці завжди $\lambda_{\max} \geq n$. Т. Сааті запропонував як показник ступеня узгодженості елементів МПП використовувати величину індексу узгодженості $I_u = \frac{\lambda_{\max} - n}{n-1}$ та відношення узгодженості $I_0 = \frac{I_u}{M(I_u)}$, де $\lambda_{\max} = \sum_{i=1}^{n}\left(x_i \times \sum_{k=1}^{n} b_{ik}\right)$ – максимальне значення власного вектору, $M(I_u)$ – середнє значення I_u, обчислене для великої кількості випадковим чином згенерованих МПП у фундаментальній шкалі. Значення $M(I_u)$ можна обчислити за такою формулою:

$$M(I_u) = \frac{1{,}98 \cdot (n-2)}{n},$$

n – розмірність МПП.

Слід зазначити, що $M(I_u)$ збільшувалися зі збільшенням порядку МПП.

У праці [15] рекомендовано вважати ваги достовірними, коли $I_u < 10\%$ (деколи для критичних випадків не перевищує 20%).

6. Виконати синтез ваг, починаючи від другого рівня вниз. Для цього, як зазначено у праці [11], локальні ваги перемножують на вагу відповідного критерію на вищому рівні й підсумовують за кожним елементом відповідно до критеріїв, на які впливає цей елемент. Це дає складову вагу того елемента, який потім використовують для зважування локальних ваг елементів, порівнюваних відносно нього як критерію і розміщених на рівень нижче. Процедура триває до найнижчого рівня.

7. Визначити узгодженість усієї ієрархії. Згідно з працею [15], процес полягає в тому, що індекс узгодженості, отриманий з МПП, множать на пріоритет властивості, щодо якого здійснено порівняння, і до цього числа додають аналогічні результати для всієї ієрархії. Потім цю величину порівнюють із відповідним індексом, який отримано як сума випадково сформованих індексів, зважених за допомогою відповідних пріоритетів. Відношення має міститися в околі 0,10.

Необхідно відзначити, що проблема узгодженості ієрархії для МАІ є найбільш критичною, тому коли в результаті розв'язування задачі отримані ваги виявляються неузгодженими, то потрібен повторний перегляд експертом (ОПР) усіх своїх оцінок.

Таким чином, за допомогою методів ПАЗ, МЕЗ і МАІ можна вирішити як задачу ранжирування альтернатив, так і задачу знаходження кількісних оцінок відносної корисності альтернатив. Згідно з працею [11] ПАЗ і МАІ дають більш точні результати. Обидва методи є простими в реалізації та завдяки цьому широко використовуються на практиці, при цьому слід зазначити, що метод ПАЗ має недостатнє теоретичне обґрунтування, у той час як МАІ є повністю теоретично обґрунтованим методом.

Застосування MAI для оцінювання захищеності проекту мережі

Метод аналіз ієрархій було використано для оцінювання якості програмного забезпечення в ряді робіт [16]. Аналогічні підходи пропонується дослідити для попереднього оцінювання рівня захищеності комп'ютерних мереж на основі оцінювання проектних рішень для неї.

Так, в роботі [16] детально розглянуто застосування MAI для отримання порівняльних оцінок проектів мереже відносно реалізації кожного з характеристик якості. Послідовність кроків у застосуванні MAI до задачі оцінювання систематизована і викладена у вигляді детальної технології. Аналогічний підхід можна використати і для оцінювання загального рівня захищеності комп'ютерної мережі.

Оскільки в MAI в якості вхідної інформації є елементи МПП, які виставляються експертами, то виникають неузгодженості в їх оцінках. Для підвищення достовірності отриманих оцінок в [16] запропоновано обчислювати нормалізовані значення по множині проектів і по множині характеристик якості та знаходити усереднене значення відхилення оцінок. При перевищенні відхиленням встановленої норми пропонується проводити повторно всю процедуру від заповнення МПП до обчислення вагових множників проектних рішень. Це може значно збільшити об’єм роботи експертів без гарантії отримати прийнятний результат.

Для отримання оцінок проектних рішень по множині показників якості пропонується використовувати метод скалярної згортки, для чого треба слід мати значення для пріоритетів характеристик якості, що є також непростою задачею. Оскільки призначення пріоритетів критеріїв здійснюється по такому ж алгоритму, що і визначення ваг альтернатив, в розв'язок вноситься додаткове джерело похибок.

Варта уваги також робота [17], в якій розглядається задача проектування архітектури розподіленої системи з врахуванням характеристик якості методом аналізу ієрархій. В ній було проведено аналіз проектних рішень проекту GB [18], виділено п’ять типів з них, потім було проведено порівняльне оцінювання

цих рішень методом аналізу ієрархій. Після нормалізації оцінок була проведена оптимізація і вибір найкращого розв'язку. Проведені достатньо масштабні дослідження для альтернатив проекту GB показали ефективність MAI при рішенні подібних задач.

Однак MAI Сааті має такі обмеження:

1. МПП мають бути узгодженими, проте реальні МПП зазвичай не є повністю узгодженими внаслідок можливих протиріч у проявах властивостей об'єктів, а також можливого впливу на експертів різних психофізіологічних факторів. Відзначимо, що відхилення $\lambda_{\max}$ від n є мірою узгодженості МПП (для повністю узгодженої МПП $\lambda_{\max} = n$, а для неузгодженої матриці завжди $\lambda_{\max} \geq n$). Як зазначено у праці [10], зміни в елементах b_{ij} МПП (помилки експертів) призводять до зміни $\lambda_{\max}$, тобто до росту неузгодженості МПП.

2. МПП мають бути малої розмірності. Ця вимога випливає з вимоги узгодженості МПП. Також слід зазначити, що згідно з дослідженнями, проведеними Міллером [19], людина не може оперувати більше, ніж 7 ± 2 об'єктами.

3. Елементи попарно мають бути порівнянними за дев'ятибальною шкалою, запропонованою Т. Сааті. Він стверджує при цьому, що така шкала обумовлена можливістю порівняння співрозмірні величини [10].

В. Тоценко у праці [20] детально розглядає методи поліпшення узгодженості МПП, які ґрунтуються на отриманні уточнювальної інформації від експерта.

Існують методи отримання формально повністю узгодженої МПП. Найбільш загальні результати в цьому напрямі отримав В.Д. Ногін, котрий у праці [21] запропонував спрощений варіант методу аналізу ієрархій, особливістю якого є те, що матриця попарних порівнянь будується на основі елементів базисного набору. Базисним набором елементів МПП називають мінімальний (за кількістю) визначальний набір. Деякий набір елементів МПП, розміщених вище від головної діагоналі, є визначальним, коли на його основі за

допомогою виразів $b_{ij} = \frac{1}{b_{ij}}, i = \overline{1,n}\ j = \overline{1,n};\ b_{ij} \cdot b_{jk} = b_{ik},\ i = \overline{1,n},\ j = \overline{1,n}, k = \overline{1,n},$ де b_{ij} – ступінь переваги *i*-го об'єкта над *j*-м об'єктом відносно заданої цілі (критерію); *n* – кількість порівнюваних об'єктів, можна однозначно обчислити всі інші елементи МПП.

Розглянемо базисний набір $b_{12}, b_{23}, \ldots, b_{n-1,n}$. Йому відповідає така схема "послідовного порівняння": з наявного набору об'єктів обирається один певний об'єкт, якому присвоюється перший номер. Для нього для подальшого порівняння підбирається інший об'єкт, якому присвоюється другий номер. У результаті порівняння стає відомим елемент b_{12}, а решту елементів обчислюється аналогічно. Формула для послідовного обчислення всіх інших елементів МПП, розміщених вище головної діагоналі, на основі базисного набору $b_{12}, b_{23}, \ldots, b_{n-1,n}$ має такий вигляд:

$$b_{ij} = b_{i,j-1} \cdot b_{j-1,j}, \quad (i = 1, \ldots, n-2;\ j = 1, \ldots, n;\ i < j-1),$$

де *n* – кількість порівнюваних об'єктів.

Компоненти вагового вектора (ненормованого) *w* можна знайти у вигляді добутку за формулою:

$$w_k = b_{k,k+1} \cdot b_{k+1,k+2} \cdot \ldots \cdot b_{n-1,n}\ (k = 1,2,\ldots,n-1), \quad w_n = 1,$$

де w_k – компонента вагового вектора $w, k = \overline{1,n-1};$

n – кількість порівнюваних об'єктів.

Далі здійснюється нормування компонентів вагового вектора.

Отже, цей метод використовує для знаходження ваг не всю інформацію, яка міститься в емпіричній МПП, що призводить до зниження достовірності одержуваного розв'язку.

Модифікований МАІ

Професором Павловим А.А. в роботі [22] було можна модифікувати звичайний МАІ для розв'язування задач мультикритеріального вибору при неузгоджених матрицях попарних порівнянь. Основна ідея модифікації полягає у визначенні ваг альтернатив з умови мінімізації міри неузгодженості МПП. Наведемо постановку деяких з цих задач та застосування цього підходу до задачі мультикритеріального оцінювання та вибору структури КС.

Коли матриця попарних порівнянь є повністю узгодженою, то:

$$\frac{w_i}{w_j} = b_{ij},\ w_i = b_{ij} w_j \quad \forall b_{ij} \in B,$$

де w_i – вага *i*-го об'єкта;

B – набір коефіцієнтів $b_{ij}, i, j = \overline{1,n}$ МПП.

В якості ступеня узгодженості значень $\frac{w_i}{w_j}$ і b_{ij} можна використовувати один з наступних виразів:

$$\left(w_i - b_{ij} w_j\right)^2 \text{ або } \left|w_i - b_{ij} w_j\right|;$$

$$\frac{1}{b_{ij}^2}\left(\frac{w_i}{w_j} - b_{ij}\right)^2 \text{ або } \frac{1}{b_{ij}^2}\left|\frac{w_i}{w_j} - b_{ij}\right|.$$

В залежності від постановки задачі розглядається декілька моделей оптимізації.

Модель 1 [22].

Для випадку мінімізації інтегральної міри узгодженості отриманого розв'язку $w_i^*, i=\overline{1,n}$, $\sum\limits_{(ij)\in|B|}\sum\left|w_i^* - b_{ij}w_j^*\right|$ модель оптимізації матиме наступний вигляд:

$$\min \sum_{(ij)\in|B|}\sum\left(y_{ij}^+ + y_{ij}^-\right)$$

$$\begin{aligned} &w_i - \underset{(i,j)\in|B|}{b_{ij}w_j} = y_{ij}^+ - y_{ij}^-,\ y_{ij}^+ \geq 0,\ y_{ij}^- \geq 0 \\ &w_i \geq a \geq 1, \quad i=\overline{1,n}, \end{aligned}$$

де $w_i, i=\overline{1,n}, \quad y_{ij}^+, y_{ij}^-, \forall(i,j)\in|B|$ – це змінні, потрібні для формування задачі лінійного програмування (ЗЛП).

Модель 2 [22].

Для мінімізації максимальної величини неузгодженості розв'язку модель оптимізації буде наступною:

$$\min \sum_{(ij)\in|A|}\sum y_{ij}\ .$$

$$\begin{aligned} &-y_{ij} \leq w_i - \underset{(i,j)\in|B|}{b_{ij}w_j} \leq y_{ij},\ y_{ij} \geq 0 \\ &w_i \geq a \geq 1, \quad i=\overline{1,n}, \end{aligned}$$

де $w_i, i=\overline{1,n}, \quad y_{ij}, \forall(i,j)\in|B|$ – це змінні, потрібні для формування ЗЛП.

Інші позначення мають такий же зміст, що і в попередній моделі 0, 0.

Оптимальному вирішенню задача ЛП 0, 0 відповідають ваги $w_i^*, i=\overline{1,n}$, на яких досягається мінімум $\sum\limits_{(ij)\in|B|}\sum\left|w_i^* - b_{ij}w_j^*\right|$.

Модель 3 [22].

Для випадку, коли критерієм оптимальності є мінімум виразу $\max\limits_{\forall(i,j)\in|B|}\left|w_i^* - b_{ij}w_j\right|$, модель оптимізації має вигляд

$$\min\ y$$

$$-y \le w_i - b_{ij}w_j \le y$$
$$(i,j)\in|A|$$

$$w_i \ge a \ge 1, \quad i=\overline{1,n},\ y \ge 0,$$

де $w_i, i=\overline{1,n}, \quad y$ – це змінні, потрібні для формування ЗЛП;

$|A|$ – набір пар (ij), кожна з яких є індексом всіх $b_{ij} \in B$;

B – набір коефіцієнтів $b_{ij},\ i, j=\overline{1,n}$ МПП;

a – задане число, $a \ge 1$;

n – кількість порівнюваних об'єктів.

Модель 4, допустимо узгодженого розв'язку [22].

$$\min \sum_{(ij)} \sum_{\in|A|} \left(y_{ij}^+ + y_{ij}^-\right)$$

$$-t_{don} b_{ij} w_j \le w_i - b_{ij}w_j \le t_{don} b_{ij} w_j,$$
$$(i,j)\in|A|$$
$$w_i - b_{ij}w_j = y_{ij}^+ - y_{ij}^-,\ y_{ij}^+ \ge 0, y_{ij}^- \ge 0,$$
$$w_i \ge a \ge 1, \quad i=\overline{1,n},$$

де $w_i, i=\overline{1,n}, \quad y_{ij}, \forall(i,j)\in A$ – це змінні, потрібні для формування ЗЛП;

t_{don} – задане граничне число.

Задача 0, 0 може не мати розв'язку, оскільки обмеження можуть бути несумісними. У цьому разі можна або збільшити значення t_{don}, або скористатися

іншою моделлю за умови, що число $t = \max\left\{\frac{y^0}{b_{ij} w_j^*}\right\}$ може бути прийнято як допустимий коефіцієнт узгодженості розв'язку задачі 0, 0.

Для оцінювання узгодженості знайдених ваг пропонується використовувати
коефіцієнти узгодженості [22]:

$$K\left(w_i^*\right) = \frac{1}{n-1} \sum_{\substack{j=1 \\ j \neq i}}^{n} \frac{1}{b_{ij}} \left| \frac{w_i^*}{w_j^*} - b_{ij} \right|.$$

Коли для деякого j, b_{ij}<1 то відповідний доданок змінюється на $\frac{1}{b_{ji}} \left| \frac{w_j^*}{w_i^*} - b_{ji} \right|$, тобто коефіцієнт узгодженості $K\left(w_i^*\right)$ для w_i^* визначається за b_{ij}≥1. $K\left(w_i^*\right)$ мають належати деякому заданому допустимому інтервалу узгодженості, інакше приймається w_i^*=0. Також пропонується використовувати критерії оцінювання знайденого набору ваг за коефіцієнтами узгодженості:

$$M_1 = \sum_{i=1}^{n} K\left(w_i^*\right)$$

$$M_2 = \max_{i,\, i=\overline{1,n}} K\left(w_i^*\right)$$

Після застосування моделей оптимізації та вибору кращого розв'язку обрані ваги $w_1^*, \ldots, w_n^*$ або безпосередньо беруть участь у наступних етапах MAI, або нормуються, при цьому нормування можливе декількома способами [22], зокрема:

1. Звичайне нормування виду

$$\hat{w}_i^* = \frac{w_i^*}{\sum_{j=1}^{n} w_j^*}, i = \overline{1,n}, \text{ тоді } \sum_{i=1}^{n} \hat{w}_i^* = 1,$$

де $\hat{w}_i^*, i = \overline{1,n}$ – нормовані знайдені ваги об'єктів;

$w_i^*, i = \overline{1,n}$ – знайдені ваги об'єктів;

n – кількість порівнюваних об'єктів.

2. Нормування за коефіцієнтами узгодженості $K(w_i^*)$:

$$\hat{w}_i^* = \frac{\frac{w_j^*}{K(w_i^*)}}{\sum_{j=1}^{n} \frac{w_j^*}{K(w_i^*)}} = \frac{w_j^*}{K(w_i^*) \sum_{j=1}^{n} \frac{w_j^*}{K(w_i^*)}}, \quad i = \overline{1,n}, \quad \sum_{i=1}^{n} \hat{w}_i^* = 1$$

де $\hat{w}_i^*, i = \overline{1,n}$ – нормовані знайдені ваги об'єктів;

$w_i^*, i = \overline{1,n}$ – знайдені ваги об'єктів;

$K(w_i^*)$ – коефіцієнти узгодженості вагових коефіцієнтів;

n – кількість порівнюваних об'єктів.

Застосування ММАІ до задачі оцінювання загального рівня захищеності проекту комп'ютерної мережі

Як відмічалось в попередньому пункті застосування МАІ забезпечує коректне рішення при невеликій кількості альтернатив ($n \leq 7 \pm 2$). При цьому індекс узгодженості не перевищує визначену межу $I_0 \leq 0{,}1$. При збільшенні розмірності задачі $n > 9$ індекс узгодженості збільшується і може перевищувати межу $I_0 > 0{,}1$. В цьому випадку відносні оцінки альтернатив будуть містити похибки, які призведуть до неправильного ранжування пропонованих альтернативних проектів і вибору варіанта, що є не найкращий. Було проведено дослідження по порівнянню методів МАІ та ММАІ при збільшенні розмірності МПП в задачі кількісного вибору варіантів альтернативних проектів.

Для зміни міри узгодженості розв'язку задачі кількісного вибору варіантів альтернативних проектів з застосуванням ММАІ скористаємось моделлю оптимізації, визначеної виразами 0, 0.

Для оцінки узгодженості отриманих рішень будемо використовувати наступні показники: коефіцієнт узгодженості M_1, визначений формулою 0, а також міру узгодженості M_2, визначеної формулою 0.

Були проведені дослідження ефективності методу обчислення вагових множників згідно моделі допустимого узгодженого розв'язку 4, яка приводить до задачі оптимізації 0, 0 для отримання оцінок альтернативних проектів ПС при неузгоджених матрицях $B\{b_{ij}\}$.

При цьому, для певних значень межі неузгодженості $t_{доп}$ було імітовано похибки, які допускають експерти при заповненні МПП через отримання випадкових значень як відхилень матриці $B\{b_{ij}\}$ і шукались вагові коефіцієнти $w_i^*, i=\overline{1,n}$ стандартним і модифікованим МАІ.

Після цього обчислювались коефіцієнти та міри узгодженості 0, 0 для результатів, отриманих обома методами. Було проведено дослідження впливу похибок неузгодженості МПП на ранжування альтернативних проектів.

Дослідження проводилось для різної кількості альтернативних проектів, які оцінювались відносно наступних характеристик якості:

1. Стійкість паролів.
2. Шифрування.
3. Продуктивність.
4. Вартість.
5. Затрати на розробку.
6. Масштабованість.
7. Легкість встановлення.

По кожному з критеріїв формувалась матриця $B^s\{b_{ij}^s\},\ i,j=\overline{1,n}, s=\overline{1,7}$, де b_{ij}^s показує, наскільки *i*-та альтернатива переважає *j*-ту по реалізації *s*-го критерію. При чому, матриці задавались ідеально узгодженими. Потім

моделювались помилки експертів шляхом генерування випадкових величин K_{ij} в інтервалі $K_{ij} \in [-0{,}5 \cdot t_{доп} + 0{,}5 \cdot t_{доп}]$ з певним кроком Δt, і елементи матриці $B^s\{b_{ij}^s\}$ визначались за формулою:

$$b_{ij}^{s*} = b_{ij}^s + K_{ij} \cdot b_{ij}^s$$

Для отриманих матриць $B^{s*}\{b_{ij}^{s*}\}$ визначались набори вагових множників $\{w_i^s\}, i = \overline{1,n}, s = \overline{1,7}$ стандартним МАІ і як розв'язок задачі 0, 0. Після цього обчислювались міри узгодженості M_1 і M_2, які усереднювались по множині характеристик якості.

На рисунку 2.3 зображена залежність значення критерію M_1 від величини інтервалу, з якого вибирався K_{ij} для обох методів для випадку 15 альтернатив.

Як можна побачити на графіку, ММАІ дає набагато кращі результати для M_1, ніж МАІ без модифікації. Так, вже при похибках в матриці $B^{s*}\{b_{ij}^{s*}\}$ в межах $t_{доп}$=0,15 ММАІ зменшив міру неузгодженості на 20 відсотків порівняно з немодифікованим.

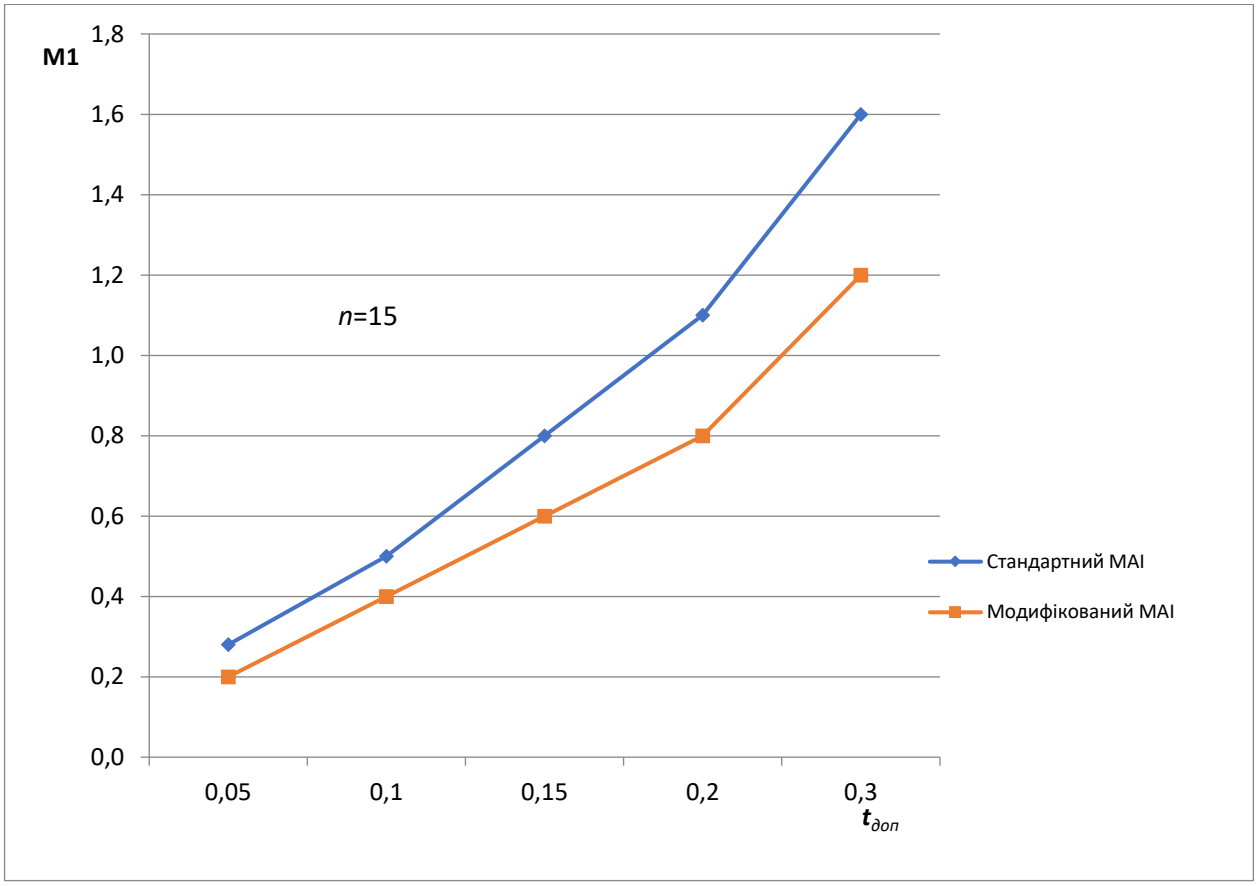

Рис. 2.3. Графік залежності критерію M_1 від похибок

На рисунку 2.4 показані графіки залежності величини міри узгодженості M_2 від інтервалу, на якому моделювались збурення матриці. З графіка видно, що за критерієм M_2 із збільшенням $t_{доп}$ переваги модифікованого MAI збільшуються і при $t_{доп}$ = 0,25 значення критерію M_2 майже на 30 відсотків менше, ніж для стандартного.

З графіків також видно, що зростання значень критеріїв неузгодженості рішень для стандартного MAI більшt від такого зростання для модифікованого, що свідчить про меншу нестійкість модифікованого MAI. Важливим також є дослідження впливу похибок визначення вагових множників $\{w_i\}$, викликаних неузгодженостями в МПП, на впорядкування альтернатив $\{A_i\}$ як за окремими характеристиками якості, так і за їх сукупністю. Для цього по узгоджених матрицях попарних порівнянь $B^s\{b_{ij}^s\}$; $i, j = \overline{1,n}$; $s = \overline{1,m2}$ знаходились набори множників $\{w_i^s\}$ і альтернативи ранжувались за значеннями $\{w_i^s\}$ по кожному

критерію. Таким чином, отримали впорядковані множини $\{A_{is}, K_{is}^{s}\}$, $s=\overline{1,m2}$, $is \in J_s$ – впорядкована за значеннями вагових множників набір номерів проектів. Після цього, згідно описаної вище методики, моделювались помилки експертів та визначались $\{w_i^*\}$ і проводилось повторне ранжування $\{A_{is}\}$.

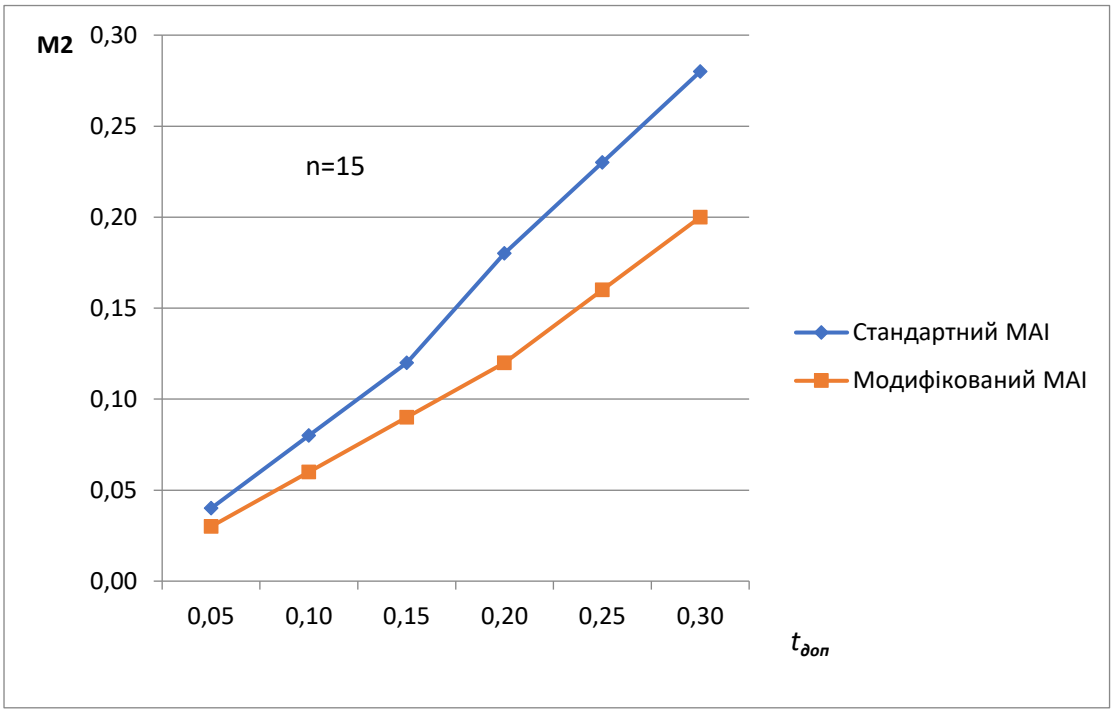

Рис.2.4. Залежність критерію M_2 від інтервалу похибок

Розрахунки показали, що відбувалась зміна ранжування при близьких значеннях $\{w_i\}$ вже при границі неузгодженості $t_{доп}$<0,1.

Застосування модифікованого алгоритму дозволить забезпечити стійкість отриманого розв'язку при більших значеннях неузгодженостей МПП і таким чином розширити межі застосування MAI.

Для впорядкування (сортування, ранжування) альтернатив по множині критеріїв слід визначити їх пріоритети. Це можна зробити або безпосереднім присвоєнням значень пріоритетів експертами, або обчисленням їх методом попарних порівнянь. Другий варіант є кращим, оскільки дозволяє зменшити

вплив суб’єктивних чинників на результат. Для цього експертами заповнюється матриця попарних порівнянь $B^s\{b_{ij}^s\}$, де величина b_{ij}^s визначає, на скільки вплив підхарактеристики захищеності мережі K_i^2 переважає вплив критерію K_j^2 на реалізацію загального рівня захищеності K_s^1. Застосувавши ММАІ, отримаємо набори пріоритетів критеріїв захищеності проекту мережі $\{p_i^{1s}\}$, $i=\overline{1,m2}$, $s=\overline{1,m1}$. Тоді вага альтернативного розв'язку A_i відносно реалізації підхарактеристики захищеності K_s^1 визначатиметься за формулою:

$$J_i^{1s}=\sum_{j=1}^{m2} p_j^{1s}\cdot w_i^j,\quad i=\overline{1,n},\quad s=\overline{1,m1},$$

де w_i^j – вагові множники альтернативних проектів, визначені на попередньому етапі.

Тепер можна проводити ранжування альтернативних проектів $\{A_i\}$ за величиною $\{J_i^s\}$ для кожного $s=\overline{1,m1}$.

Коли потрібно проранжувати альтернативи відносно глобальної показника захищеності, то слід отримати числові значення для пріоритетів кожного критеріїю захищеності $\{p_i^2\}$, $i=\overline{1,m1}$, застосувавши модифіковану процедуру МАІ.

Тепер встановимо ваги альтернативних проектів для наступного обчислення глобального критерію якості, обчисливши такий показник:

$$J_i^0=\sum_{s=1}^{m1} J_i^{1s}\cdot p_s^2,\quad i=\overline{1,n}.$$

З приведених результатів досліджень видно, що зміна порядку ранжування альтернативних проектів може відбуватись як через похибки у визначенні w_j^i, так і через зміну пріоритетів $\{p_j\}$. Тому, при виборі оптимального варіанту проекту необхідно проводити відповідні дослідження,

які показали, що коли рахувати вагові множники в MAI стандартним методом, то це може бути причиною невірних рішень для більшої за 9 кількості варіантів та характеристик для вибору. MMAI суттєво зменшує неузгодженості рішень, навіть при суттєвих значеннях коефіцієнту неузгодженості для МПП.

Аналіз результатів дозволяє зробити висновок, що ріст критерію неузгодженості M_1 збільшується із ростом похибок МПП. А тому є потреба додатково аналізувати отриманий порядок альтернатив і інтегрально і за окремими характеристиками [23].

Отже, застосування MMAI разом із згаданими заходами зменшить міру впливу помилок експертів при парних порівняннях та уразливість MAI до таких помилок, і, як наслідок, підвищити якість розв'язку задачі кількісного вибору варіантів альтернативних проектів для загального показника якості і, що є предметом цієї роботи, для критерія захищеності.

Дослідження чутливості ранжування альтернативних проектів та аналіз компромісів при прийнятті мультикритеріальних рішень

Більшість методів оцінювання інтегрального показника за певною характеристикою включають оцінку по окремих критеріях та інтегральне оцінювання по всій сукупності критеріїв [16, 17, 23]. Причому інтегральне оцінювання проводиться обчисленням функції цінності у вигляді лінійної згортки частинних критеріїв. Для цього призначаються ваги характеристик якості експертними методами.

Але при виборі розв'язку виникають ряд проблем пов’язаних з неточностями визначення вагових множників, особливо коли значення деяких ваг для різних альтернатив близькі. При цьому також треба враховувати можливість внесення змін до специфікації вимог захищеності і якості загалом у процесі проектування, які приведуть до зміни значень пріоритетів критеріїв. А це приведе до зміни порядку ранжування альтернативних проектів і в кінцевому підсумку до зміни розв'язку стосовно остаточного вибору для одного

з варіантів проектів. Також використання інтегрального критерію для вибору розв'язку приховує допущені компроміси між конкуруючими характеристиками.

Тому для обов'язкового врахування можливих змін у вимогах та вибору рішення, яке буде найстійкіше до таких змін, необхідно дослідити чутливість розв'язку, а також можливі компроміси між характеристиками захищеності.

Питання чутливості рішень до похибок та аналізу компромісів в задачі оцінювання та вибору архітектури ПС було вперше підняте в роботі [23], але там не запропоновано методу дослідження цієї проблеми. Це пояснюється тим що більшість використовуваних методів аналізу архітектур, таких як ATAM, та інші сценарно-орієнтовані методи не є кількісними. Пропонується застосувати цю ідею для оцінювання захищеності комп'ютерних мереж.

Для дослідження цих проблем може бути використаний один з методів оцінювання ПА. Це метод, подібний до CBAM (Cost Benefit Analysis Method) та MAI. В методі CBAM замовники можуть надати залежності альтернативних проектів від вимог якості, використовуючи функцію відгуку корисності, а потім виконати числові розрахунки для оцінювання альтернатив і вибору найкращого варіанта [5, 23]. Однак, як зазначається у [4], отримати у замовників функцію відгуку корисності досить складно, тому застосування CBAM для вирішення цієї задачі є проблематичним.

Іншим, більш перспективним, методом є MAI, який дає можливість отримати оцінки альтернатив відносно всіх характеристик якості і, використовуючи лінійну згортку критеріїв, отримати оцінки по їх сукупності. Це дозволяє провести ранжування альтернативних проектів і вибрати найкраще відносно отриманих оцінок розв'язку. Однак, як відмічалось раніше, при застосуванні MAI використовуються експертні оцінки при парних порівняннях, а також при призначенні пріоритетів критеріям якості. Це може привести до помилок при прийнятті рішень, особливо коли оцінки альтернатив мало відрізняються. Також використання інтегрального показника приховує

взаємозв'язки між характеристиками якості і міру прийнятого компромісу між ними при призначенні ваг критеріям.

Розглянемо тепер чутливість рішень, отриманих з застосуванням MAI, до зміни пріоритетів характеристик якості.

Нехай ми маємо ваги альтернативних проектів по реалізації критеріїв захищеності $\{w_i^s\}$ та проранжовані (впорядковані) проектні пропозиції $\{A_i\}$, отримані MAI. Наведемо формулу для визначення мінімального відхилення абсолютного значення для вагового коефіцієнту атрибуту P_s, таку, що порядок A_i та A_j зміниться:

$$D'_{s,i,j} = \frac{\left|J_i - J_j\right|}{\left|w_i^s - w_j^s\right|} \cdot \frac{100}{P_s}$$

Тут $D'_{s,i,j}\left(s = \overline{1,m2};\, i, j = \overline{1,n},\, i \neq j\right)$ – мінімальна зміна величини пріоритету P_s критерію якості K_s, яка змінює порядок сусідніх альтернатив A_i та A_j на зворотній. Мінімальне значення $D'_{s,i,j}$ показує, що пріоритет P_s для певного конкретного атрибуту K_s є критичним стосовно внесення змін до оцінок в парних порівняннях. Це рівняння можна також використати у випадку зміни вимог до ПС у процесі проектування, яке може привести до зміни пріоритетів для кожної характеристики якості.

Для кожного атрибуту (характеристики) якості проекту можлива наявність декількох значень $D'_{s,i,j}$, які можуть спричинити зміну порядку слідування сусідніх альтернатив. Найчутливіше і найкритичніше рішення відповідає найменшому значенню $D'_{s,i,j}$. Тому при прийнятті рішення можливо більш доцільно вибрати не найкращий розв'язок по критерію якості, але той, для якого $D'_{s,i,j}\left(s = \overline{1,m2};\, i, j = \overline{1,n},\, i \neq j\right)$ не буде критичним до зміни пріоритету критерію.

Таблиця 2.1 містить мінімальні значення *D*, що можуть змінити порядок ранжування (впорядкування) альтернативних проектів, значення яких знайдені відповідно до 0.

Мінімальні зміни значень пріоритетів для атрибутів якості, що спричиняють змінив у порядку ранжування

Атрибут якості	Альтернатива *i*	Альтернатива *j*	Найменша зміна
Продуктивність	PROJ1	PROJ2	9,4
Вартість	PROJ1	PROJ2	5,1
Затрати на розробку	PROJ1	PROJ2	3,1
Портативність	PROJ1	PROJ2	2,4
Легкість установки	PROJ1	PROJ2	13,5
Масштабованість	PROJ2	PROJ3	5,7
Модифікованість	PROJ2	PROJ1	3,9

Числа в таблиці – це відсотки змін від абсолютної величини ваги окремого атрибута якості. Як бачимо з таблиці, портативність – це атрибут, найбільш чутливий до змін.

Таким чином, аналіз чутливості дозволяє визначити допустимі межі для змін ваг у числових значення атрибутів якості, коли міняються вимоги. Коли зміни пріоритетів виконуються в рамках цих меж, поточний порядок альтернатив залишається без змін.

РОЗДІЛ 3
МЕТОД БАГАТОКРИТЕРІАЛЬНОГО ВИБОРУ АРХІТЕКТУРИ ПРИ ЗМІНІ ВИМОГ ЯКОСТІ

Внесення змін в проект, при зміні вимог, в тому числі і вимог захищеності, здійснюється шляхом оцінювання існуючого проекту і порівняння його якісних характеристик з альтернативами. Причому, в якості альтернатив можуть розглядатися стандартні рішення, в які можуть вноситись необхідні коригування.

Оскільки зміна вимог якості приводить також до зміни пріоритетів характеристик якості, то врахувати ці зміни при виборі варіанта проекту мережі можна шляхом коригування властивостей тих альтернатив, які можуть розглядатися як найбільш прийнятні.

Розглянемо підхід до отримання рішення мультикритеріального вибору проекту мережі на основі інформації про порівнянність критеріїв за важливістю і проведення необхідної коригування оцінок при зміні вимог до КС.

Оперативне корегування альтернатив з заміщення і компенсування

Задача перерахунку чи коригування для отриманої оцінки з'являється, коли експерти надають перевагу певному варіантові A_i, хоча він за деякими характеристиками не є найкращий. Виникає задача покращити оцінки за цими характеристиками за рахунок зменшенняза іншими, але так, щоб оцінки альтернативи A_i за всіма характеристиками були не гірші за інші.

Така ситуація є типовою при проектуванні мереж, коли бажана структура відома, а корегування критеріїв може здійснюватися шляхом підбору стандартних функціональних компонентів [18].

До розв’язування цієї задачі можна застосувати аксіоматичний підхід В. Подіновського [24], який полягає в попарному заміщенні критеріїв. Критерії K_r і K_s є порівняними за заміщенням, коли для деякої альтернативи A_i

можлива компенсація за перевагою будь-якої зміни критерію K_r зміною критерію K_s.

Тобто, коли A_i^p – це альтернатива, яка заміщує A_i шляхом коригування K_r і компенсування K_s, то їх значення після корекції будуть

$$\overline{K}_r^{ip} = \overline{K}_r^i - \delta_r,\ \overline{K}_s^{ip} = \overline{K}_s^i + \delta_{si},\ \delta_{si} = f\left(r, s, \overline{K}, \delta_r\right),$$

де $\overline{K}$ – вектор скалярних критеріїв.

Подамо співвідношення для компенсування з заміщенням для множини компонентів вектора $\overline{K}^i$ для вибраного серед інших проекту A_i, який ми хочемо зробити кращим за A_j:

$$\delta\overline{K}_r^{ir_z} = C_r^{ir_z} \cdot \delta K_r^i,\ r_z \in R_i^2(r),\ r \in R_i^1,$$

де $\delta\overline{K}_r^{ir_z}$ – можливе зменшення компоненти $\overline{K}_r^i$ з метою збільшення $\overline{K}_{r_z}^i$;

R_i^1 – набір індексів r, для яких $\overline{K}_r^{iz} > \overline{K}_r^j,\ j = \overline{1,n};\ i \neq j$;

$R_i^2(r)$ – задана для R_i^1 набір індексів, така, що компоненти $\overline{K}_r^i, r \in R_i^1$ можуть бути вибрані для заміщення компонентів $\overline{K}_s^i, s \in R_i^2(r)$;

$C_r^{ir_z}$ –коефіцієнти пропорційності, задані попередньо.

Компоненти вектору $\overline{K}^i$ після заміщення задаються такими співвідношеннями:

$$\overline{K}_r^{ip} = \overline{K}_r^i - \sum_{r_z \in R_i^2(r)} C_r^{ir_z} \cdot \delta\overline{K}_{r_z}^i,\quad r \in R_i^1;$$

$$\overline{K}_r^{ip} = \overline{K}_{r_z}^i + \sum_{r \in R_i^1} \sum_{r_z \in R_i^2(r)} \delta\overline{K}_{r_z},\quad r_z \in s, s \overline{\in} R_i^1, r_z \in R_i^2(r).$$

О.А. Павловим в роботі [25] сформульовані задачі оптимізації заміщення 0, які зводяться до задач ЛП. Математичні моделі задач оптимізації залежать від стратегії вироблення рішень. З метою отримання Парето-оптимальної моделі вираз для оптимізації буде , як показано в наступній формулі:

$$\max\left\{\sum_{r\in R_r^1} d_r + \sum_{s\overline{\in} R_j^1} d_s\right\} = \max\{y\}$$

з обмеженнями:

$$d_r, d_s \geq 0, r \in L_j^1, s \overline{\in} R_j^1$$

$$\overline{K}_r^j - \sum_{r_z \in R_j^2(r)} \delta \overline{K}_r^{jr_z} \geq \max_i \left(\delta \overline{K}_r^i\right) + d_r, i \in \overline{1,n}, i \neq j, r \in R_j^1$$

$$\overline{K}_s^j + \sum_{r\in R_j^1} \sum_{r_z \in R_j^2(r)} \frac{1}{d_r^{jr_z}} \delta \overline{K}_r^{jr_z} \geq \max_i \left(\overline{K}_s^i\right) + d_s, \quad i = \overline{1,n}, i \neq j, r \overline{\in} R_j^1, r_z = s,$$

$$\exists r, s \in R_j^2(r);$$

$$\sum_{r_z \in L_j^2(r)} \delta \overline{K}_r^{ir_z} \leq b_{K_r^j}, \quad j \neq i, r \in R_j^1, r_z = s.$$

Змінними тут є $\delta K_r^{jr_z}, d_r, d_s$.

Після ряду математичних трансформацій для розв’язування задачі використовується звичайний симплекс-метод.

Метод коригування альтернатив на практиці

Розглянемо застосування даного підходу для розв'язування практичної задачі заміщення. Маємо три альтернативні варіанти проектів мережі, якість яких оцінюється п'ятьма характеристиками. Задача полягає в тому, щоби відкоригувати характеристики однієї з альтернатив таким чином, щоб вона стала найкращою.

Числові значення оцінок проектних альтернатив, отриманих з застосуванням модифікованого MAI, наведені в таблиці 0.

Числові оцінки проектів мережі, отриманих з застосуванням MMAI

Критерії	Альтернатива		
	A_1	A_2	A_3
K_1	0,56	0,22	0,22
K_2	0,33	0,33	0,33
K_3	0,21	0,36	0,43
K_4	0,22	0,44	0,33
K_5	0,57	0,14	0,29

Необхідно відкоригувати оцінки альтернативи A_1 так, щоби за всіма характеристиками вона була не гірша, ніж дві інші.

Тут набір $L_i^1 \to \left(\forall l \in L_i^l, \overline{K}_l^i > \overline{K}_l^j, i \neq j\right) \in \{1;5\}$, а відповідно $L_i^2 = \{3;4\}$. Тому задача полягає в тому, щоби за рахунок зменшення оцінок по першому і п'ятому критеріях збільшити оцінки по третьому і четвертому, але так, щоб вони лишились не гірші, ніж по двох інших альтернативах. Оскільки максимальна оцінка по першому критерію по другій та третій альтернативах 0,22 і по п'ятому критерію теж 0,22. Тобто ці обмеження мають вигляд

$$0{,}56 - \left(\Delta\overline{K}_{13} + \Delta\overline{K}_{14}\right) \geq 0{,}22 \pm 1 \cdot y;$$
$$0{,}57 - \left(\Delta\overline{K}_{53} + \Delta\overline{K}_{54}\right) \geq 0{,}22 \pm 0{,}8 \cdot y.$$

Обмеження того, щоб оцінки по третьому та четвертому критеріях, по котрих здійснюється корегування, були не гірші, ніж по двох інших альтернативах, має вигляд:

$$0{,}21 + \left(1{,}6 \cdot \Delta\overline{K}_{13} + 1{,}3 \cdot \Delta\overline{K}_{53}\right) \geq 0{,}43 + 0{,}5 \cdot y;$$
$$0{,}22 + \left(2{,}5 \cdot \Delta\overline{K}_{14} + 2 \cdot \Delta\overline{K}_{54}\right) \geq 0{,}33 + 0{,}6 \cdot y.$$

Коефіцієнти заміщення C_l^{ilm} – введені експертами, виходячи з важливості критеріїв.

Обмеження на максимальну зміну оцінок по першому та п'ятому критеріях мають вигляд:

$$\Delta\overline{K}_{13} + \Delta\overline{K}_{14} \le 0{,}34;$$
$$\Delta\overline{K}_{53} + \Delta\overline{K}_{54} \le 0{,}28.$$

В результаті розв'язування задачі оптимізації з введеними обмеженнями отримаємо:

$$\Delta K_{13} = 0{,}12;\ \Delta K_{14} = 1{,}11;$$
$$\Delta K_{53} = 0{,}18;\ \Delta K_{54} = 0;\ y = 0{,}13.$$

Таким чином в перших трьох розділах сформульована задача вибору структури КС з набору попередньо запропонованих проектів у вигляді мультикритеріального вироблення рішень з моделлю у вигляді ієрархії.

Задачу розв'язуємо у два етапи. На першому з них знаходяться оцінки альтернатив по кожному критерію якості, а на другому – на основі отриманих оцінок здійснюється вибір найкращої альтернативи.

Приведені результати аналізу методів мультикритеріального вироблення рішень, з якого зроблено висновок, що найбільш прийнятним методом, в даному випадку є MAI Сааті. Однак його застосування обмежене невеликою кількістю альтернатив і критеріїв ($n \le 7 \pm 2$). Для розширення меж коректного застосування MAI використано оптимізаційний метод обчислення (визначення) ваг альтернатив, який базується на використанні моделей мінімізації неузгодженостей МПП, розроблений О.А.Павловим та його учнями.

Були проведені дослідження ефективності MMAI в даній задачі, які показали, що застосування MMAI дозволяє отримувати достовірні результати при значно більшій кількості альтернатив ($n \le 45$) і критеріїв. При дослідженні для МПП різної розмірності знаходились ваги альтернатив з застосуванням MAI та MMAI. Імітувалась неузгодженість МПП внесенням випадкових відхилень в значення елементів МПП. Отримані результати показали, що MMAI більш стійкий до неузгодженостей МПП ніж звичайний MAI, що також підтвердили результати експериментальних досліджень про можливість його

застосування для задач оцінювання зі значно більшою кількістю альтернатив чи критеріїв ($n \leq 45$).

Приведені також результати практичного застосування MMAI для розв'язування задачі мультикритеріального оцінювання та вибору проекту мережі. Отримані оцінки альтернатив, як по кожному критерію, так і по їх сукупності, за результатами яких можна обрати найкращий варіант проекту.

Було виконано також аналіз чутливості методу MMAI для впорядкування альтернативних проектів до зміни вимог то до змін їх пріоритетів. Цей механізм дозволить оцінити допустимі інтервали змін пріоритетів вимог, для яких не потрібно наново перераховувати оцінки альтернативних проектів.

Було проаналізовано також адаптивний метод вибору проекту мережі для випадку зміни вимог до проекту і оцінки потреби нового розрахунку показника захищеності. Метод передбачає обрахунок та співставлення для порівняння оцінок різних проектів мереж та коригування цих оцінок "на льоту", щоби оперативно врахувати зміни у вимогах. Тут використовується MMAI, а для коригування отриманих кількісних оцінок проектів мереж – метод попарного заміщення Подіновського В.В. Для розв'язування задачі оптимального заміщення використовуємо математичний апарат ЛП.

РОЗДІЛ 4

ОБҐРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ

Метою цього розділу дипломної роботи є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності від розробки, а також прийняття рішення щодо подальшого розвитку і впровадження або ж недоцільність впровадження відповідної розробки.

Передбачається, що описаний в роботі підхід буде імплементовано у вигляді спеціальної програмної СППР. Розробка такого продукту вимагатиме певних затрат. Тому розрахуємо ці затрати. Для здійснення оцінки потрібно зробити розрахунки трудомісткості кожної операції.

4.1. Визначення стадій технологічного процесу та загальної тривалості проведення НДР

Витрати часу по окремих операціях технологічного процесу відображені в таблиці 4.1.

Таблиця 4.1

Операції технологічного процесу та час їх виконання

	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
.	Витрати праці на підготовку опису задачі	інженер	9
.	Витрати праці на розробку проекту	інженер	18
	Витрати праці на розробку структури	інжен	11

.	системи	ер	
.	Витрати праці на створення системи по вибраному проекту та структурі	інжен ер	74
.	Витрати праці на підготовку документації	інжен ер	15
.	Витрати праці на відлагодження роботи зпроектованої системи при комплексній відладці	інжен ер	42
Разом			169

Загальні затрати на дипломний проект становить 169 годин.

4.2. Визначення витрат на оплату праці та відрахувань на соціальні заходи

Відповідно до Закону України “Про оплату праці” заробітна плата – це “винагорода, обчислена, як правило, у грошовому виразі, яку власник або уповноважений ним орган виплачує працівникові за виконану ним роботу”.

Розмір заробітної плати залежить від складності та умов виконуваної роботи, професійно-ділових якостей працівника, результатів його праці та господарської діяльності підприємства. Заробітна плата складається з основної та додаткової оплати праці.

Основна заробітна плата нараховується на виконану роботу за тарифними ставками, відрядними розцінками чи посадовими окладами і не залежить від результатів господарської діяльності підприємства.

Додаткова заробітна плата – це складова заробітної плати працівників, до якої включають витрати на оплату праці, не пов’язані з виплатами за фактично відпрацьований час. Нараховують додаткову заробітну плату залежно від досягнутих і запланованих показників, умов виробництва, кваліфікації

виконавців. Джерелом додаткової оплати праці є фонд матеріального стимулювання, який створюється за рахунок прибутку.

При розрахунку заробітної плати кількість робочих днів у місяці слід в середньому приймати – 24,5 дні/міс., або ж 196 год./міс. (тривалість робочого дня – 8 год.).

Місячний оклад кожного працівника слід враховувати згідно існуючих на даний час тарифних окладів. Згідно закону України «Про Державний бюджет України на 2018 рік», зокрема Статтею восьмою мінімальна заробітна плата у погодинному розмірі встановлена у розмірі 22,41 грн. Рекомендовані тарифні ставки: керівник дипломної роботи – 30,00...50,00 грн./год., інженер – 22,41...30,00 грн./год., консультант – 22,41...30,00 грн./год., технік – 22,41...30,00 грн./год., лаборант – 22,41...25,00 грн./год.

Основна заробітна плата розраховується за формулою:

$$З_{осн.} = Т_с \cdot К_г \, , \tag{4.1}$$

де $Т_с$ – тарифна ставка, грн.;

$К_г$ – кількість відпрацьованих годин.

Оскільки всі види робіт в даному проекті виконує інженер, то основна заробітна плата буде розраховуватись тільки за однією формулою

$$З_{осн.} = 30 \cdot 169 = 5070 \text{ грн.}$$

Додаткова заробітна плата становить 10–15 % від суми основної заробітної плати.

$$З_{дод.} = З_{осн.} \cdot К_{допл.}, \tag{4.2}$$

де $К_{допл.}$ – коефіцієнт додаткових виплат працівникам, 0,1–0,15 (візьмемо його рівним 0,15).

$$З_{дод.} = 5070 \cdot 0,15 = 760,50 \text{ грн.}$$

Звідси загальні витрати на оплату праці ($В_{о.п.}$) визначаються за формулою:

$$В_{о.п.} = З_{осн.} + З_{дод.}. \quad (4.3)$$

$В_{о.п.}$=5070+760,50 = 5830,50 грн.

Крім того, слід визначити відрахування на соціальні заходи:

1) ЄСВ + ПДФО 22 %;
2) військовий збір – 1,5 %.

У сумі зазначені відрахування становлять 23,5 %.

Отже, сума відрахувань на соціальні заходи буде становити:

$$В_{с.з.} = Ф_{оп} \cdot 0,235, \quad (4.4)$$

де $Ф_{ОП}$ – фонд оплати праці, грн.

$$В_{с.з.} = 5830,5 \cdot 0,235 = 1370,05 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

Таблиця 4.2

Зведені розрахунки витрат на оплату праці

/п	Категорія працівників	Основна заробітна плата, грн.			Додаткова заробітна плата, грн.	Нарахув. на ФОП, грн.	Всього витрати на оплату праці, грн. 6= 3+4+5
		Тарифна ставка, грн.	К-сть відпрацьов. год.	Фактично нарах. з/пл., грн.			
	Б	1	2	3	4	5	6
	інженер	30	169	5070	760,5	1370,05	7200,55

Загальні витрати на оплату праці становить 7200,55 грн.

4.3. Розрахунок матеріальних витрат

Матеріальні витрати визначаються як добуток кількості витрачених матеріалів та їх ціни:

$$M_{Bi} = q_i \cdot p_i, \quad (4.5)$$

де: q_i – кількість витраченого матеріалу i-го виду;

p_i – ціна матеріалу i-го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$З_{м.в.} = \sum M_{Bi}. \quad (4.6)$$

Проведені розрахунки занесемо у таблицю 4.3. Для розробки ПЗ передбачається покупка Microsoft Visual Studio Professional 2017, вартість якого на сьогодні становить 74400 грн.

Таблиця 4.3

Зведені розрахунки матеріальних витрат

Найменування матеріальних ресурсів	Одиниця виміру	Норма витрат	Ціна за одиницю, грн	Затрати матеріалів, грн	Транс-портно-заготівельні витрати, грн	Загальна сума витрат на матеріа-ли, грн
1. Основні матеріали						
Програмне забезпечення	комп.	1	74400,00	74400,00	–	74400,00
2. Допоміжні матеріали						
Папір формату А4	шт.	200	0,18	36	–	36
Разом:						74436,00

Загальні матеріальні затрати становлять 74436,00 гривень.

4.4. Розрахунок витрат на електроенергію

Затрати на електроенергію 1-ці обладнання визначаються за формулою:

$$З_е = W \cdot T \cdot S \,, \qquad (4.7)$$

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Вартість кіловат-години електроенергії слід приймати згідно існуючих на даний час тарифів. Отже, 1 кВт з ПДВ коштує 2,42 грн.

Потужність комп'ютера для створення проекту – 550 Вт, кількість годин роботи обладнання згідно таблиці 4.1 – 169 годин.

Тоді, $З_е = 0{,}55 \cdot 169 \cdot 2{,}42 = 224{,}94$ грн.

4.5. Розрахунок суми амортизаційних відрахувань

Характерною особливістю застосування основних фондів у процесі виробництва є їх відновлення. Для відновлення засобів праці у натуральному виразі необхідне їх відшкодування у вартісній формі, яке здійснюється шляхом амортизації.

Амортизація – це процес перенесення вартості основних фондів на вартість новоствореної продукції з метою їх повного відновлення.

Комп'ютери та оргтехніка належать до четвертої групи основних фондів. Для цієї групи річна норма амортизації дорівнює 60 % (квартальна – 15 %).

Для визначення амортизаційних відрахувань застосовуємо формулу:

$$A = \frac{Б_В \cdot Н_А}{100\%}, \qquad (4.8)$$

де A – амортизаційні відрахування за звітний період, грн.;

$Б_В$ – балансова вартість групи основних фондів на початок звітного періоду, грн.;

$Н_А$ – норма амортизації, %.

Для даного проекту засобом розробки є комп'ютер. Його сума становить 7335 грн. Отже, амортизаційні відрахування будуть рівні:

$$A = \frac{7335 \cdot 5\%}{100\%} = 366{,}75 \text{ грн.}$$

Оскільки робота виконувалась 169 годин, то амортизаційні відрахування будуть становити:

$$A = \frac{366{,}75 \cdot 169}{150} = 413{,}21 \text{грн.}$$

4.6. Обчислення накладних витрат

Накладні витрати пов'язані з обслуговуванням виробництва, утриманням апарату управління спілкою та створення необхідних умов праці.

В залежності від організаційно-правової форми діяльності господарюючого суб'єкта, накладні витрати можуть становити 20 – 60 % від суми основної та додаткової заробітної плати працівників.

$$H_в = B_{о.п.} \cdot 0{,}2 \ldots 0{,}6 \,, \qquad (4.9)$$

де H_B – накладні витрати.

Отже, накладні витрати:

H_B = 5830,5· 0,2 = 1166,10 грн.

4.7. Складання кошторису витрат та визначення собівартості НДР

Результати проведених вище розрахунків зведемо у таблицю 4.4.

Собівартість (C_B) проекту розрахуємо за формулою:

$$C_в = B_{о.п.} + B_{с.з.} + З_{м.в.} + З_в + A + H_в. \qquad (4.10)$$

Отже, собівартість проекту дорівнює:

$C_в$ = 5830,50 + 370,05 + 74436 + 224,94 + 413,21 + 1166,10 = 82440,80 грн.

Таблиця 4.4

Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до загальної суми
Витрати на оплату праці (основну і додаткову заробітну плату)	5830,5	7,1%
Відрахування на соціальні заходи	370,05	0,4%
Матеріальні витрати	74436	90,3%
Витрати на електроенергію	224,94	0,3%
Амортизаційні відрахування	413,21	0,5%
Накладні витрати	1166,1	1,4%
Собівартість	82440,8	100,0%

4.8. Розрахунок ціни проекту

Ціну НДР можна визначити за формулою:

$$Ц = \frac{C_B \cdot (1 + P_{рен}) + K \cdot B_{н.і.}}{K} \cdot (1 + ПДВ), \qquad (4.11)$$

де $P_{рен.}$ – рівень рентабельності, 30 %;

K – кількість замовлень, од. (встановлюється лише при розробці програмного продукту та мікропроцесорних систем);

$B_{н.і.}$ – вартість носія інформації, грн. (встановлюється лише при розробці програмного продукту);

ПДВ – ставка податку на додану вартість, (20 %).

Оскільки розробка є прикладною, і використовуватиметься тільки для одного підприємства, то для розрахунку ціни не потрібно вказувати коефіцієнти K та $B_{i.н}$, оскільки їх в даному випадку не потрібно.

Тоді, формула для обчислення ціни розробки буде мати вигляд:

$$Ц = C_B \cdot (1 + P_{рен}) \cdot (1 + ПДВ). \quad (4.12)$$

Звідси ціна на проект складе:

Ц = C_B · (1+0,3)(1+0,2) = 128607,65 грн.

4.9. Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва – це узагальнене і повне відображення кінцевих результатів використання робочої сили, засобів та предметів праці на підприємстві за певний проміжок часу.

Економічна ефективність (E_p) полягає у відношенні результату виробництва до затрачених ресурсів:

$$E_p = П / C_B, \quad (4.13)$$

де $П$ – прибуток;

C_B – собівартість.

Плановий прибуток ($П_{пл}$) знаходимо за формулою:

$$П_{пл} = Ц - C_B. \quad (4.14)$$

Розраховуємо плановий прибуток:

$П_{пл}$ = 128607,65 – 82440,8 = 46166,85 грн.

Отже, формула для визначення економічної ефективності набуде вигляду:

$$E_р = \frac{П_{пл}}{Св} . \quad (4.15)$$

Тоді, $E_р$ = 46166,85 / 82440,8 = 0,56

Поряд із економічною ефективністю розраховують термін окупності капітальних вкладень ($T_р$):

$$T_р = 1/ E_р , \quad (4.16)$$

Термін окупності дорівнює:

$T_р$ = 1/0,56 = 1,8 роки.

В цьому розділі дипломної роботи було розраховано основні техніко-економічні показники проекту (див. таблицю 4.5).

Розраховане значення економічної ефективності становить 0,42 що є високим значенням.

Так само нормальним є термін окупності. Для даного продукту він становить 2,4 роки.

Таблиця 4.5

Техніко-економічні показники НДР

/п	Показник	Значення
	Собівартість, грн.	82440,8

.		
.	Плановий прибуток, грн.	46166,85
.	Ціна, грн.	128607,65
.	Економічна ефективність	0,56
.	Термін окупності, рік	1,8

Отже, даний проект може бути впроваджений та мати подальший розвиток, оскільки він є економічно вигідним за всіма основними техніко-економічними показниками.

РОЗДІЛ 5

ОХОРОНА ПРАЦІ ТА БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ

5.1. Загальні вимоги законодавства з охорони праці в галузі інформаційних технологій

Правову основу охорони праці становить Конституція України як за своїми юридичними особливостями, так і своїми принципами, тобто юридично вираженими об'єктивними закономірностями організації і функції соціально-економічної, політичної, духовної сфер суспільства, правового положення особи.

Конституційні норми, з одного боку, закладають суть безпеки (норми-принципи), а з іншого, – вказують на цілі подальшого розвитку і реалізацію правового забезпечення безпеки життєдіяльності (норми-програми, норми-завдання, норми-зобов'язання).

Реалізація і розвиток основних конституційних положень, які регламентують суспільні правовідносини, безпосередніми суб'єктами яких є особа і держава, здійснюється за допомогою як чинних фундаментальних нормативно-правових актів, так і спеціальних (Кодексів України про працю, Закону "Про охорону навколишнього природного середовища" та ін.)

Поруч з нормативними актами, які прийняті вищим законодавчим органом держави, для встановлення взаємозв'язків, усунення програм, а в ряді випадків і реалізації окремих правових норм або їх елементів, до правової бази безпеки життєдіяльності належать спеціальні акти, розроблені за дорученням виконавчих державних органів усіх рівнів (Кабінет Міністрів, Міністерства, Державні Комітети та ін.).

Так, наприклад, "Положення...", які розвивають Закон України Про охорону праці, діляться на звичайні "Положення" і "Типові положення". Тут держава розподілила питання своєї прерогативи стосовно розробки

нормативних актів і прерогативи своїх повноважень стосовно контролю, "правового простору" у вигляді нормативних актів підприємств.

З іншого боку, формуючи систему "Типових положень" держава на сьогоднішній день ліквідує прогалини в чинному законодавстві, узгоджує взаємозв'язки між суб'єктами правовідносин, створює юридичну базу для удосконалення і розвинення "правового поля" підприємств.

Кожний нормативно-правовий документ має свою структуру, яка визначає собою ідею систематизації відповідно зі своїм рівнем, метою та завданнями. Відповідно до цього в кожному нормативному акті є елементи, що відповідальні за зовнішній його зв'язок і створення передумов для відповідного розвинення за рахунок розробки нижчих нормативно-законодавчих актів. Сама структура нормативного акту формує відповідні внутрішні зв'язки.

Основними систематизуючими ланками нормативних актів безпеки життєдіяльності (які за ієрархією знаходяться нижче законів) є встановлення взаємовідносин в галузі виробництва, в межах дії небезпечного фактора (в тому числі і факторів довкілля), а також відносно управління основних технологій безпеки життєдіяльності (розслідування нещасних випадків, навчання, організації робіт та ін.).

Узагальнюючими ланками систематизації на рівні держави є національна ідея, взаємовідносини в суспільстві, соціально-економічне і політичне становище держави, можливості сприймання і використання законодавчих актів з боку споживачів та ін.

5.2. Розрахунок освітленості робочого місця експерта з якості програмного забезпечення

Належне освітлення необхідне для виконання більшості задач користувача персонального комп'ютера, в тому числі і експерта з якості програмного забезпечення. Для того, щоб спланувати раціональну систему освітлення, враховується специфіка робочого завдання, для якого створюється

система освітлення, швидкість і точність, з якою це робоче завдання повинне виконуватися, тривалість його виконання і різні зміни в умовах виконання робітників.

Приміщення, у якому знаходиться робоче місце, має наступні характеристики:

– довжина приміщення 16 м;

– ширина приміщення 6 м;

– висота 4 м;

– кількість вікон 3;

– кількість робочих місць 3;

– біла стеля, блідо-зелені стіни, підлога обтягнута лінолеумом зеленого кольору.

У приміщенні, де знаходиться робоче місце, використовується змішане освітлення, тобто сполучення природного і штучного освітлення.

У якості природного – бічне освітлення через вікна. Штучне освітлення використовується при недостатньому природному освітленні.

Розрахунок його здійснюється по методу світлового потоку з врахуванням потоку, відбитого від стін і стелі.

Нормами для даних робіт встановлена необхідна освітленість робочого місця Ен = 300 лк. Загальний світловий потік визначається за формулою:

$$F_{заг} = \frac{E_н \cdot S \cdot z1 \cdot z2}{V}, \qquad (5.1)$$

де $E_н$ – нормована освітленість ($E_н$ = 300 лк);

S – площа приміщення;

z1 – коефіцієнт, що враховує старіння ламп і забруднення світильників (z1 = 1,5);

z2 – коефіцієнт, що враховує нерівномірність освітлення приміщення (z2 = 1,1);

V – коефіцієнт використання світлового потоку; визначається в залежності від коефіцієнтів відбивання від стін, стелі, робочих поверхонь, типів світильників і геометрії приміщення.

Площа приміщення S = A*B = 16*6 = 96 м^2.

– коефіцієнт відбивання побіленої стелі $R_п$ = 70%;

– коефіцієнт відбивання від стін, пофарбованих у світлий колір $R_{ст}$ = 50%;

– коефіцієнт відбивання від підлоги, покритого лінолеумом темного кольору $R_р$ = 10%;

– індекс приміщення $i = \frac{A*B}{h*(A+B)} = \frac{16*6}{4*(16+6)} = 1{,}1$.

Знайдений коефіцієнт V = 0,34.

За формулою (3.1) визначаємо загальний світловий потік

$$F_{заг} = \frac{300*96*1{,}1*1{,}5}{0{,}34} = 139764 \text{ лм.}$$

Для організації загального штучного освітлення виберемо лампи типу ЛБ40. Люмінесцентні лампи мають ряд переваг перед лампами накалювання: їхній спектр ближче до природного; вони мають велику економічність (більша світловіддача) і термін служби у 10-12 раз більший.

Поряд з цим вони мають і недоліки: їхня робота супроводжується іноді шумом; гірше працюють при низьких температурах; не можна використовувати у вибухонебезпечних приміщеннях.

Для нашого приміщення люмінесцентні лампи підходять. Світловий потік однієї лампи ЛБ40 складає не менш $F_л$ = 2810 лм. Число N ламп, необхідних для організації загального освітлення визначається наступним чином:

$$N = \frac{F_{заг}}{F_л} = \frac{139764}{2810} = 50 \text{ шт.}$$

Як світильники вибираємо ПВЛ-1, 2*40 Вт. Таким чином, щоб забезпечити світловий потік $F_{заг}$ = 139764 лм треба використати 25 світильників по 2 лампи ЛБ40 у кожному.

Електрична потужність однієї лампи $W_л$ = 40 Вт. Потужність всієї освітлювальної системи:

$W_{заг} = W_л * N = 40*50 = 2000$ Вт.

Зі зробленого в даному розділі розрахунку випливає, що для нормальної роботи користувача робочого місця необхідне загальне освітлення приміщення зі світловим потоком 139764 лм, для чого необхідна наявність 25 світильників типу ПВЛ-1 з двома лампами типу ЛБ40. Крім того рекомендується використовувати ряд спеціальних заходів захисту від шкідливих факторів екрана дисплея, наприклад, використання занавісок на вікнах.

5.3. Зміст безпеки життєдіяльності

Безпека життєдіяльності – одна з наймолодших наук, яка спрямована на вирішення основної проблеми сучасного суспільства України – збереження здоров'я населення.

За змістом дисципліна "Безпека життєдіяльності" формує світогляд майбутнього фахівця, який у своїй повсякденній праці повинен створювати передумови запобігання нещасним випадкам, захворюванням та усуненням негативного впливу шкідливостей на здоров'я людини в умовах виконання виробничих завдань, її існування в побуті та різних за характером надзвичайних ситуаціях.

Виникнення дисципліни "Безпека життєдіяльності" історично пов'язане з багатьма об'єктивними аспектами розвитку суспільства:

1)необхідністю створення передумов соціального захисту;

2)державним завданням зі здійснення кроку вперед щодо

запобігання високому рівню захворюваності, травматизму, аваріям, катастрофам на новій якісній основі в галузях політики, правовому забезпеченні, науково-освітній діяльності, матеріально-економічному забезпеченні тощо;

3)розбудовою єдиної глобальної системи освіти на базі ступеневої підготовки фахівців;

4)відбудовою бази для всіх дисциплін, що вирішують питання "людського фактора".

Дисципліна "Безпека життєдіяльності" встановлює зміст регулювання зв'язків між природою та людиною. Жодне існуюче суспільство не може розвиватися без споживання. З метою задоволення своїх потреб люди організовують свою господарчу діяльність. Основою цієї діяльності є виробництво. Цілі розвитку виробництва в різних суспільствах мають великі розбіжності. Але якими б не були ті цілі і принципи суспільного розвитку, виникнення суперечок між людиною і природою, між виробництвом і природними екологічними системами неминуче. Мова може йти тільки про різну глибину цих суперечок і про різні шляхи їх вирішення. Це – діалектика взаємодії суспільства та людини.

Нормативна дисципліна "Безпека життєдіяльності" становить фундамент для розвитку інших дисциплін циклу, що розглядають "людський фактор" (інженерну екологію, охорону праці, цивільну оборону та інші), а також — спеціальні дисципліни, які розвивають її положення в рамках проектних, технологічних, конструкторських, організаційних та інших рішень щодо запобігання небезпечних умов життєдіяльності.

5.4. Дії населення в надзвичайних ситуаціях (пожежа)

Якщо виникла пожежа, відлік часу йде на секунди, тому необхідно заздалегідь знати, де і які засоби пожежогасіння розміщуються та як ними користуватися.

Під час пожежі остерігайтеся: високої температури, задимленості та загазованості, обвалу конструкцій будинків і споруд, вибухів технологічного обладнання і приладів, падіння обгорілих дерев і провалів. Небезпечно входити в зону задимлення.

Заходи щодо рятування потерпілих з будинків, які горять, та під час гасіння пожежі:

– перед тим, як увійти у приміщення, що горить, накрийтесь мокрою ковдрою, будь-яким одягом чи щільною тканиною;

– відчиняйте обережно двері в задимлене приміщення, щоб уникнути спалахування від великого притоку свіжого повітря;

– в дуже задимленому приміщенні рухайтесь поповзом або пригинаючись; для захисту від чадного газу необхідно дихати через зволожену тканину; насамперед рятуйте дітей, інвалідів та старих людей;

– пам’ятайте, що маленькі діти від страху часто ховаються під ліжко, в шафу та забиваються у куток;

– виходити із осередку пожежі необхідно в той бік, звідки віє вітер;

– побачивши людину, на якій горить одяг, зваліть її на землю та швидко накиньте пальто, плащ або будь-яку ковдру чи покривало (бажано зволожену) і щільно притисніть до тіла, за необхідності викличте медичну допомогу;

– якщо загорівся ваш одяг, падайте на землю і перевертайтесь, щоб збити полум'я, ні в якому разі не біжіть – це ще більше роздмухує вогонь;

– під час гасіння пожежі використовуйте вогнегасники, пожежні гідранти, а також воду, пісок, землю, кошму, ковдри та інші засоби, пристосовані для гасіння вогню;

– бензин, гас, органічні масла та розчинники, що загорілися, гасіть тільки з допомогою пристосованих видів вогнегасників, засипайте піском або ґрунтом, а якщо осередок пожежі невеликий, накрийте його азбестовим чи брезентовим покривалом, зволоженою тканиною чи одягом;

– якщо горить електричне обладнання або проводка, вимкніть рубильник, вимикач або електричні пробки, а потім починайте гасити вогонь.

Дії, якщо пожежа застала у приміщенні:

– ви прокинулись від шуму пожежі і запаху диму, не сідайте в ліжку, а скотіться з нього на підлогу;

– повзіть підлогою під хмарою диму до дверей вашого приміщення, але не відчиняйте їх відразу;

– обережно доторкніться до дверей тильним боком долоні, якщо двері не гарячі, то обережно відчиніть їх та швидко виходьте;

– якщо двері гарячі – не відчиняйте їх, дим та полум'я не дозволять вам вийти;

– щільно зачиніть двері, а всі щілини і отвори заткніть будь- якою тканиною, щоб уникнути подальшого проникнення диму, та повертайтесь поповзом у глибину приміщення і вживайте заходи для порятунку;

– присядьте, глибоко вдихніть повітря, відчиніть вікно, висуньтеся та кричіть: "Допоможіть, пожежа!";

– ви не в змозі відчинити вікно – розбийте віконне скло твердим предметом та зверніть увагу людей, які можуть викликати пожежну команду;

– якщо ви вибрались через двері, зачиніть їх і поповзом рухайтесь до виходу із приміщення;

– обов'язково зачиніть за собою всі двері;

– під час пожежі заборонено користуватися ліфтами;

– якщо ви перебуваєте у висотному будинку, не біжіть вниз крізь вогнище, а користуйтеся можливістю врятуватися на даху будівлі.

У всіх випадках, якщо ви маєте змогу, зателефонуйте "01" і викличте пожежну команду.

Пожежі в лісах, стелах та на торфовищах.

Такі масові пожежі можуть виникати в спеку та при посухах від ударів блискавки, необережного поводження з вогнем, очищення поверхні землі випалюванням сухої трави та з інших причин. Вони можуть викликати

загорання будівель в населених пунктах, дерев'яних мостів, дерев'яних стовпів ліній електромереж та зв'язку, складів нафтопродуктів та інших матеріалів, що горять, а також ураження людей та тварин.

Дії, якщо ви опинилися в осередку пожежі:

– не панікуйте та не приймайте поспішних, необдуманих рішень;

– не тікайте від полум'я, що швидко наближається, у протилежний від вогню бік, а рухайтесь крайкою полум'я проти вітру, закривши голову і обличчя одягом;

– з небезпечної зони, до якої наближається полум'я, виходьте швидко, перпендикулярно напряму поширення вогню;

– якщо втекти від пожежі неможливо, то вийдіть на відкриту місцевість або галявину, ввійдіть у водойму або накрийтесь мокрим одягом і дихайте повітрям, що над самою поверхнею землі, – воно тут менш задимлене, рот і ніс при цьому прикривайте одягом чи шматком будь-якої тканини;

– гасити полум'я невеликих низових пожеж можна, забиваючи його гілками листяних порід дерев, заливаючи водою, закидаючи вологим ґрунтом та затоптуючи ногами;

– під час гасіння пожежі не відходьте далеко від доріг та просік, не упускайте з виду інших учасників гасіння пожежі, підтримуйте з ними зв'язок з допомогою голосу;

– будьте обережні в місцях горіння високих дерев, вони можуть упасти та травмувати вас;

– особливо будьте обережні у місцях торф'яних пожеж, ввжайте, що там можуть створюватися глибокі вирви, тому рухайтеся, за можливості, перевіряючи палицею глибину шару, що вигорів;

– після виходу із осередку пожежі повідомте місцеву адміністрацію та пожежну службу про місце, розміри та характер пожежі.

Якщо людина знає правила поводження під час пожежі, то вона в змозі не лише вистояти за будь-яких обставин і врятувати своє життя, а й надати

допомогу в рятуванні інших людей та врятувати матеріальні цінності від вогню.

РОЗДІЛ 6

ЕКОЛОГІЯ

6.1. Зниження енергоємності та енергозбереження

Енергоефективність та енергозбереження є пріоритетними напрямами енергетичної політики більшості країн світу. Це обумовлено вичерпанням невідновлювальних паливно-енергетичних ресурсів, відсутністю реальних альтернатив їх заміни, наявністю ризиків при їх виробництві і транспортуванні. В останній час ці чинники набувають все більшого значення у зв'язку із загальною нестабільністю у регіонах видобутку паливно-енергетичних ресурсів (ПЕР), напругою на паливно-ресурсних ринках та несприятливими прогнозами щодо подальшого зростання цін на енергоресурси. Розвинені країни світу, у першу чергу, країни ЄС, які вже досягли значних успіхів у вирішенні проблем енергоефективності, продовжують пошук нових джерел енергозабезпечення та розробку заходів щодо енергозбереження, що є позитивним прикладом для України.

З огляду на ситуацію, що сьогодні складається, вирішення цих проблем буде відбуватися в умовах загальної нестабільності в світі, у тому числі і на паливно-ресурсних ринках, несприятливих прогнозів щодо подальшого зростання цін на енергоресурси та незначних іноземних інвестицій у вітчизняну економіку.

Досвід розвинутих країн і власний досвід України вказує на необхідність державного регулювання процесами енергозбереження та проведення цілеспрямованої державної політики. Тільки держава шляхом виваженої законодавчої, гнучкої цінової, тарифної та податкової політики може забезпечити дієздатність фінансового механізму енергозбереження.

Основними принципами такої політики повинні стати:

– пріоритет підвищення ефективності використання паливно-енергетичних ресурсів над зростанням обсягів їх видобутку й виробництва теплової та електричної енергії;

– відповідність політики загальним ринковим перетворенням в країні;

– пріоритетність забезпечення безпеки здоров'я людини, соціально-побутових умов її життя, охорони навколишнього середовища переробці та використанні паливно-енергетичних ресурсів та (або) енергії;

– здійснення державного регулювання у сфері енергозбереження, в першу чергу, контролю виконання законів, нормативів та прийнятих рішень;

– необхідність економічної підтримки енергозбереження, стимулювання використання відновлювальних джерел енергії;

– обов'язковість вірогідного обліку паливно-енергетичних ресурсів, що виробляються та споживаються;

– системний підхід в енергозбереженні;

– реалізація інформаційної, освітньої та науково-дослідницької діяльності у сфері енергозбереження.

З результатів розрахунків проведених на базі прогнозних даних проекту енергетичної стратегії України до 2030 року виходить, що в країні за рахунок енергозбереження до 2020 року можна досягти економії енергоносіїв у загальному обсязі порядку 470 млн. т у.п., що відповідає зменшенню витрат на їх імпорт близько 38 млрд. дол.

Чиста економія (із врахуванням витрат на енергозбереження) може скласти у 2020 році близько 15 млрд. дол. Такі переваги відповідають зниженню енергоємності ВВП більш ніж у 4,8 рази.

Інші переваги енергозбереження складаються у зменшенні техногенного навантаження на навколишнє середовище: зменшення обсягів викидів CO_2 у 2020 році може досягти 207 млн. т, що поліпшить умови життя населення країни, а також забезпечить можливість торгувати квотами і одержувати

додаткові дивіденди на впровадження новітніх технологій і взагалі на соціально-економічний розвиток країни.

Крім того, енергозбереження в енергетиці дозволить зекономити у 2020 році близько 323 млрд. кВт год. електроенергії, що дозволить не вводити в експлуатацію електрогенеруючих потужностей у 37 ГВт і зменшити потреби в інвестиціях для галузі на 74 млрд. дол.

Таким чином, проведення нової політики енергозбереження забезпечить для країни такі дивіденди:

1. Знизяться обсяги необхідного імпорту енергоносіїв (це особливо важливо, бо при зростанні економіки потреби в енергоносіях будуть зростати).

2. За рахунок економії коштів на імпорті енергоносіїв з'явиться можливість оновлення основних фондів та впровадження нових технологій.

3. Технологічне переоснащення виробництв призведе до зменшення обсягів шкідливих викидів у навколишнє середовище (це взагалі є дуже важливим при нинішній екологічній ситуації в країні, окрім того при відповідному розвитку подій може з'явитися можливість торгівлі квотами).

4. Підвищиться конкурентоспроможність вітчизняних товарів, бо зменшиться частка енергії в собівартості продукції.

5. Буде відбуватися відстрочка термінів вичерпання вітчизняних не відновлювальних енергоносіїв

6. З'являться також інші переваги, що пов'язані із соціальними стандартами, з поліпшенням міжнародного іміджу країни.

Все це дасть додаткові можливості країні щодо досягнення європейського рівня соціально-економічного розвитку і забезпечення у прогнозований період її повноправного членства у європейському співтоваристві.

Забезпечення енергетичної безпеки є одним із найбільш важливим питань, які визначають можливість сталого розвитку суспільства в країнах світу в тому числі і в Україні. Проблема забезпечення енергетичної безпеки стоїть в центрі уваги енергетичної політики майже для всіх країн світу.

Енергетична безпека держави – це стан готовності паливно-енергетичного комплексу країни щодо максимально надійного, технічно безпечного, екологічно прийнятного, економічно ефективного та обґрунтовано достатнього енергозабезпечення економіки держави й населення, а також щодо гарантованого забезпечення можливості керівництва держави у формуванні і здійсненні політики захисту національних інтересів у сфері енергетики без зовнішнього і внутрішнього тиску.

Виходячи з такого визначення енергетичної безпеки можна виділити наступні її складові: енергозабезпечення, енергетичну незалежность, екологічну прийнятність та соціальну стабільність. Необхідно зазначити, що характер поділу на складові є дещо умовним, тому деякі механізми та стратегічні пріоритети забезпечення енергетичної безпеки будуть загальними для різних її складових. Це цілком зрозуміло в зв'язку із багатоплановістю самого поняття енергетичної безпеки, тісним зв'язком та взаємним впливом різних її складових.

На сучасному етапі основними реальними та потенційними загрозами енергетичній безпеці України є неефективність використання паливно-енергетичних ресурсів, відсутність активної політики енергозбереження, недостатні темпи диверсифікації джерел постачання енергоносіїв, низький рівень екологічної прийнятності енергетичного виробництва та соціальні конфлікти в сфері енергетичного виробництва та енергопостачання населення.

Сучасний стан енергетичної безпеки в Україні є незадовільним. Однією із основних причин цього є низька ефективність виробництва, транспортування та споживання ПЕР, відсутність активної політики енергозбереження в країні. Вплив заходів енергоефективності на енергетичну безпеку є багатоплановим та значним, що позначається на стані енергетичної безпеки з усіх її складових.

6.1.1. Складова енергозабезпечення

Не визиває сумнівів що визначальним фактором впливу на цю складову буде рівень енергоємності споживання. Необхідність стабільного, максимально надійного та якісного забезпечення енергетичними ресурсами потреб

національного господарства і населення як головної складової енергетичної безпеки залежить від реалізації цілої низки заходів з підвищення енергетичної ефективності.

Як показують результати розрахунків, динаміка росту показника енергозабезпечення на період до 2020 року спостерігається для всіх варіантів, в яких реалізуються заходи щодо енергозбереження. Ці заходи дозволяють значно (у 2,5-4 рази) підвищити рівень показника енергозабезпечення.

6.1.2. Складова енергетичної незалежності

Україна є енергодифіцитною державою яка на сьогодні лише на половину задовольняє потреби в паливі та енергії, що є негативним чинником впливу на її енергетичну безпеку. Головними чинниками, які впливають на енергетичну незалежність є відносний рівень імпорту енергоносіїв та рівень його диверсифікації. Зниження рівня енергетичної залежності як складової енергетичної безпеки залежить, в першу чергу, від заходів щодо зменшення частки загального імпорту паливно-енергетичних ресурсів, яке повинно здійснюватися за рахунок збільшення рівня та ефективності власного виробництва ПЕР та за рахунок підвищення ефективності їх використання.

Враховуючи можливості країни щодо нарощування власного видобутку ПЕР і нарощування потужностей ПЕК та існуючий значний потенціал енергозбереження особлива увага повинна приділятися заходам енергоефективності. При цьому головним механізмом для запобігання можливому зростанню собівартості власного видобутку (виробництва) енергоносіїв повинно бути технологічне переозброєння галузі за рахунок впровадження інновацій.

Аналіз результатів розрахунків впливу різних варіантів розвитку ПЕК України показує на їх значну залежність саме від рівня енергетичної ефективності.

Так у варіанті збереження енергоємності на рівні 2000р., як показують розрахунки, буде спостерігатися зменшення показника імпорту з часом, що

пояснюється ростом частки імпорту нафти і газу пов'язане зі зростанням економіки і таким же зростанням енергоспоживання, а також обмеженими можливостями власного видобутку цих енергоносіїв та прогнозованим зростанням цін на імпортовані ПЕР. Економічне ж зростання дає більше можливостей для диверсифікації постачання енергоносіїв які імпортуються, що позитивно позначається на показнику монопольного імпорту, який зростає практично для всіх розглянутих варіантів.

Зменшення енергоємності ВВП, як показують результати розрахунків на всьому розглянутому періоді часу (2000-2020р.р.), дозволяє значно підвищити значення показників енергетичної незалежності. Це відбувається за рахунок зменшення енергетичних потреб економіки в результаті впровадження енергозберігаючих заходів. До того ж, ці енергоносії є більш дорогими відносно вугілля, частка ж власного видобутку якого в Україні зостається великою на весь розглянутий період часу.

6.1.3. Складова екологічної прийнятності

Складна екологічна ситуація в Україні, яка зумовлена значною мірою шкідливими викидами підприємств традиційної енергетики також вимагає широкого впровадження енергозберігаючих заходів. Існує певна залежність між послідовним проведенням політики підвищення енергоефективності (реалізацією енергозберігаючих заходів) у всіх сферах національного господарства та охороною навколишнього середовища (позитивним впливом на довкілля). Ефективне енергоспоживання в галузях економіки та населенням зменшить загальне використання енергоресурсів, що відповідно, призведе до зменшення забруднення довкілля, зокрема, до скорочення викидів в атмосферу антропогенних газів, що виникають у промислових процесах виробництва енергоносіїв. Покращенню екологічного стану довкілля будуть також сприяти впровадження енергоефективних технологій, устаткування, обладнання, побутових енергетичних пристроїв; використання нетрадиційних поновлюваних джерел енергії, альтернативних видів палива, що забезпечать

економію або заміщення енергоресурсів, технології видобутку, виробництва та використання яких є екологічно неприйнятними. Тому при плануванні і проведенні політики енергозбереження та підвищення енергоефективності виробництва в Україні необхідно поєднувати ці питання з проблемами екології в єдину державну політику розвитку економіки держави.

Енергозберігаючі заходи повинні мати позитивний екологічний вплив на довкілля і, навпаки, при оцінці витрат на зменшення шкідливих викидів необхідно враховувати економічні вигоди від енергозбереження, тобто окупність цих витрат.

Для оцінки екологічної прийнятності енергетичного виробництва використано показники, які враховують рівень викидів у відносному вигляді у порівнянні з викидами у 1990р. (прийнятими Україною за Кіотською згодою) та вартість ліквідації наслідків від впливу основних забруднювачів (SO2, NO2, золи і парникових газів). Результати розрахунків показують, що рівень екологічної прийнятності зменшується з часом для всіх варіантів крім варіанту де рівень енергоємності ВВП поступово наближається до рівня енергоємності розвинутих країн. Для базового варіанту економічного розвитку, який був прийнятий у проекті “Енергетичної стратегії...2030р...” це зниження є незначним на ~ 5% у 2020 році, а для варіанту де енергоємність ВВП залишається на рівні 2000 р. – дуже значним, що пояснюється як темпами нарощування виробництва і споживання електроенергії, так і темпами введення обладнання для уловлювання забруднювачів. Варіант підвищення енергетичної ефективності є превалюючим, бо веде до зменшення виробництва електроенергії для потреб економіки і майже пропорціонального зменшення викидів парникових газів, які у вартості викидів дають найбільший вклад, але найменше піддаються очищенню. Інші забруднювачі можуть очищуватись більш ефективно. Зростання економіки дає більше можливостей для оновлення обладнання електростанцій та впровадження технологій очищення шкідливих викидів, таких як: SO_2, NO_2 та попіл.

Загалом реалізація енергоефективних варіантів дозволить значно збільшити значення показника екологічної прийнятності відносно варіанту незмінної енергоємності, в тім, тільки варіант де енергоємність ВВП поступово наближається до рівня розвинутих країн дає можливість забезпечити збільшення рівня екологічної прийнятності у 2020 році відносно рівня 2000 року.

6.1.4. Складова соціальної стабільності

Енергозбереження є довгостроковою, стратегічно важливою складовою державної політики, яка містить значні резерви впливу на соціально-економічні перетворення в країні, а тобто на соціальну стабільність в суспільстві.

Соціальний фактор є достатньо значущим в забезпеченні енергетичної безпеки, навіть у відносно благополучних економічно розвинутих країнах. Проблеми виникнення загроз енергетичної безпеки в цих країнах пов'язуються, в першу чергу, із зростаючим попитом на бензин та ціновою політикою щодо нього. Ця ситуація змушує країни змінювати політику управління попитом, зокрема політику підвищення енергетичної ефективності [3].

В Україні соціальні загрози, пов'язані з енергетичною сферою, є гострішими, що пояснюється як значною кількістю факторів впливу на них, так і економічним становищем в країні, яке ще не дозволяє ефективно зменшувати рівень цих загроз.

Серед найбільш значущих факторів впливу слід відзначити: значний рівень енергетичної складової в собівартості продукції, низька платоспроможність населення, в тому числі, щодо енергетичних послуг, а також екологічний фактор. В самій енергетичній галузі факторами впливу є: невиплата заробітної плати, зростання рівня безробіття, аварії та травматизм на виробництві (особливо у вугільній галузі). Можна зробити припущення, що внаслідок економічного зростання в країні, вплив зазначених факторів в енергетичній галузі буде значно зменшуватися. Заходи найбільш ефективного використання енергоресурсів (реалізація найбільших обсягів потенціалу

енергозбереження) за рахунок впровадження новітніх технологічних процесів та інноваційних перетворень будуть найкраще сприяти покращенню екології, умов та охорони праці, зниженню травматизму та смертності на виробництві.

Значний вплив на рівень соціальної напруги, пов'язаний з цінами на енергоресурси (що прямо пов'язано із споживчими цінами) буде залишатися ще достатньо довго у термін часу, що розглядається. Значні коливання цін на нафту у світі будуть збільшувати економічні ризики, що буде позначатися і на соціальній сфері.

Для стимулювання виконання накреслених заходів з енергозбереження та зниження витрат необхідні стабілізація фінансового стану підприємств енергетичної галузі і відповідна тарифна стратегія, яка передбачала би врахування фактичних витрат за постачання енергії споживачам, відсутність перехресних субсидій і бартерних взаєморозрахунків, мінімізацію комерційних втрат, механізми подолання неплатежів, соціальні інтереси споживачів енергії.

Для ілюстрації розглянемо показник, який характеризує співвідношення вартості енергетичних ресурсів (яка є також складовою собівартості цін для споживачів) та рівня заробітної плати в Україні відносно цих показників для країн ЄС. Ці результати є ще одним із аргументів на користь підвищення рівня енергетичної ефективності, що значно впливає на рівень соціальної стабільності, особливо в період 2015-2020 рр.

Таким чином, необхідність сталого енергопостачання населення і економіки країни, зниження рівня енергетичної залежності, зниження техногенного навантаження на довкілля, зниження соціальної напруги у сфері енергетики, загальне підвищення рівня енергетичної безпеки України потребують вирішення проблем, пов'язаних з низькою енергетичною ефективністю економіки країни, значними витратами суспільства на своє енергозабезпечення. Тобто, реалізація заходів енергетичної ефективності, покликаних забезпечити реалізацію одних із головних задач енергетичної стратегії держави, є переважним фактором підвищення рівня енергетичної безпеки України.

Різні фактори впливу (економічні, екологічні, соціальні) рівня енергетичної ефективності на енергетичну безпеку, які були розглянуті вище, хоча і в різному ступені, але однозначно показують на позитивну роль підвищення рівня енергетичної ефективності в забезпеченні енергетичної безпеки країни.

6.2. Організаційні форми, види і способи статистичного спостереження

Форми спостереження. У статистичний практиці застосовують дві організаційні форми спостереження: звітність і спеціально організовані статистичні спостереження.

Звітність — це форма статистичного спостереження, при якій статистичні дані надходять у статистичні органи від підприємств і установ у вигляді обов'язкових і таких, що мають юридичну силу звітів про їх роботу.

Звітність підприємств, установ та організацій є поки що основним джерелом статистичної інформації. У ній передбачається система твердо регламентованих показників, які характеризують діяльність підприємств, установ та організацій. Зміст звіту, форма і термін подання також встановлюється вищим статистичним органом. Звітність складають на основі документів первинного оперативно-технічного і бухгалтерського обліку. Вірогідність гарантується також юридичною відповідальністю керівників підзвітних підприємств та організацій.

Перелік усіх форм із зазначенням їх реквізитів називають табелем звітності. За різними ознаками статистичну звітність поділяють на окремі види. Насамперед розрізняють типову і спеціалізовану звітність:

– типова звітність має єдину форму і зміст для всіх підприємств окремої галузі або всього народного господарства.

– спеціалізована звітність властива тим підприємствам чи окремим виробництвам, що мають свої специфічні особливості.

За періодичністю подання звітність буває тижнева, двотижнева, місячна, квартальна, різна; за способом подання термінова (телеграфна) і поштова. Вид звітності впливає на техніку збору і зведення статистичної інформації. Удосконалення статистичної звітності на сучасному етапі відбувається у напрямі скасування термінової звітності та скорочення кількості поштових звітів.

За порядком проходження звітність поділяють на централізовану і децентралізовану:

– централізована звітність проходить через систему державної статистики, де обробляється і передається відповідним органам управління;

– децентралізована опрацьовується у відповідних міністерствах чи відомствах, а зведення подають статистичним органам.

Другою за значенням організаційною формою спостереження є спеціально організоване статистичне спостереження. Застосовують його у випадках, коли не можна застосувати звітність або складати звітність нераціонально; коли необхідно детально вивчити явище поряд з вивченням його у формі звітності або потрібно перевірити вірогідність даних звітності.

Спеціально організоване статистичне спостереження поєднує в собі такі організаційні форми: а) перепис, б) суцільне і несуцільне обстеження.

Види і способи спостереження. Різноманітність соціально-економічних явищ потребує різних видів спостереження. Різновид спостереження визначається ознакою групування: охватом одиниць сукупності, часом проведення, способом одержання статистичних даних.

За охватом одиниць сукупності спостереження поділяють на суцільне і несуцільне:

– при суцільному спостереженні обстеженню і реєстрації підлягають усі без винятку елементи сукупності; прикладами суцільного спостереження є статистична звітність, яку складають і подають державні і кооперативні підприємства чи установи, а також перепис населення;

– при несуцільному спостереженні обліку підлягають не всі елементи сукупності, наприклад обстеження бюджетів населення.

Несуцільні спостереження поділяють на такі види: спостереження основного масиву, вибіркове, монографічне і анкетне:

– спостереження основного масиву охоплює переважну частину елементів сукупності, обсяг значень істотної ознаки у яких визначає розмір явища. Цей метод використовують при вивчені екологічного стану регіонів.

– при вибірковому спостереженні також обстежуються не всі елементи сукупності, а певна, випадково відібрана їх частина. Таке спостереження застосовують для вивчення якості природних сфер, екологічного стану НПС, забрудненості об'єктів середовища тощо;

– монографічне спостереження передбачає детальне обстеження лише окремих типових елементів сукупності. До цього вдаються з метою поглибленого вивчення тих сторін екологічних явищ, які не були висвітлені масовим обстеженням;

– анкетні спостереження розповсюджені в соціальних і демографічних, при вивчені громадської думки щодо різноманітних соціальних питань, таких як умови праці і відпочинку, житлові умови, організація громадського харчування тощо. Це відносно дешевший вид спостереження, але менш точний, оскільки відповіді на питання анкети дають переважно зацікавлені особи.

За часом проведення статистичне спостереження поділяють на поточне, періодичне і одноразове:

– поточне спостереження полягає в безперервній реєстрації фактів по мірі їх виникнення. Так здійснюється облік викидів шкідливих речовин в атмосферне повітря, природні водойми, ґрунти;

– періодичне спостереження проводиться регулярно, здебільшого через рівні проміжки часу;

– одноразове спостереження проводять епізодично з метою вирішення певних соціально-економічних завдань. Прикладом є обстеження при аварійних та інших надзвичайних ситуаціях.

За способом одержання статистичних даних виділяють: безпосередній облік фактів, документальний облік і опитування респондентів:

– безпосередній облік фактів передбачає безпосередній огляд, перелік, вимірювання, зважування тощо. Так проводять інвентаризацію викидів на підприємствах;

– документальний облік ґрунтується на даних різноманітних документів первинного обліку. Найбільш широкого вжитку він набув при складанні статистичної звітності, екологічних паспортів, паспортів забруднюючих речовин тощо;

– опитування респондентів це таке спостереження, при якому відповіді на питання формуляра записують зі слів респондента. Опитування буває експедиційне, само реєстрація, кореспондентське і анкетне:

– при експедиційному опитуванні спеціально підготовлені реєстратори заповнюють формуляри спостереження і одночасно перевіряють правдивість відповідей на питання;

– само реєстрація це опитування, при якому респонденти самі заповнюють статистичні формуляри. Працівники статистичних органів лише інструктують їх і перевіряють повноту та правильність одержаних відомостей;

– кореспондентське опитування здійснюють спеціальні дописувачі, які заповнюють формуляри згідно з інструкцією і передають відомості статистичним органам;

– при анкетному опитуванні анкети респондентам вручають особисто або висилають поштою. Опитування може проводитись також у формі інтерв'ю. Це спосіб допускає довільність відповідей респондентів на поставлені питання, з'ясування їх думок.

Різноманітність екологічних явищ, їх специфіка, особливості статистичного вимірювання потребують поєднання зазначених способів і видів спостереження.

ВИСНОВОК

У магістерській роботі виконано дослідження способів забезпечення необхідного рівня захищеності комп'ютерних мереж на основі багатокритерійної оптимізації.

Основні наукові та практичні результати полягають в наступному.

1. Проведено аналіз наукових публікацій, стандартів та практичних рішень в області проектування комп'ютерних мереж та багатокритерійної оптимізації, результатом чого обґрунтовано актуальність теми та методів забезпечення необхідного рівня захищеності комп'ютерних мереж.

2. Розроблено модель атрибутів захищеності комп'ютерної мережі шляхом виконання комунікації вимог до власне мережі на вимоги до її проекту з використанням методу QFD.

3. Розроблено метод порівняльного оцінювання проектних архітектурних рішень в рамках предметної області як розв'язок задачі багатокритеріальної ієрархічної оптимізації з використанням модифікованого методу аналізу ієрархій.

4. Виконано порівняння стандартного та модифікованого методу аналізу ієрархій при порівняльному рівня захищеності проектів мережі, оцінено стійкість рішення задачі вибору альтернативного проекту.

ПЕРЕЛІК ПОСИЛАНЬ

1. Akao, Y., ed. (1990). Quality Function Deployment, Productivity Press, Cambridge MA.
2. Черноруцкий И.Г. Методы принятия решений / Черноруцкий И.Г. – СПб. БХВ-Петербург. – 2005. – 416 с.
3. Kazman, R. ATAM^{SM}: Method for Architecture Evaluation / Rick Kazman, Mark Klein, Paul Clements. – Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, August 2000. – CMU/SEI-2000-TR-004, ADA377385. – 83 p.
4. Bass, L. Software architecture in practice : 2nd edition / Len Bass, Paul Clements, Rick Kazman. – Boston, MA: Addison-Wesley Professional, 2003. – 528 p. – ISBN 0321154959.
5. Kazman, R. Quantifying the costs and benefits of architectural decision / Kazman, R., Asundi, J., and Klein // Proceedings of the 23rd International Conference on Software Engineering (ICSE), 2001. – Pp. 297 – 306.
6. Nord, Robert. Integrating the Architecture Tradeoff Analysis Method (ATAM) with the Cost Benefit Analysis Method (CBAM) [Електронний ресурс] / Robert Nord, Mario R. Barbacci, Paul C. Clements, Rick Kazman, Mark H. Klein, Liam O'Brien, James E. Tomayko // tech. report CMU/SEI-2003-TN-038, Software Eng. Inst., Carnegie Mellon Univ., 2003, Software Engineering Institute. http://www.sei.cmu.edu/reports/03tn038.pdf
7. Bengtsson, Perolof Architecture-level modifiability analysis (ALMA)/ Perolof Bengtsson, Nico H. Lassing, Jan Bosch, Hans van Vliet // Journal of Systems and Software. – 2004. – Vol. 69, No. 1-2. – Pp. 129-147.
8. Харченко О.Г. Метод багатокритеріальної оптимізації програмної архітектури на основі аналізу компромісів / Харченко О.Г., Боднарчук І.О., Галай І.О. // Інженерія програмного забезпечення. – 2012. – № 3–4 (11–12). – С. 5–11.

9. Harchenko, A. Stability of the Solutions of the Optimization Problem of Software Systems Architecture. // A. Harchenko, I. Bodnarchuk, I. Halay / Proceeding of VIIth International Scientific and Technical Conference CSIT 2012. Lviv. 2012. – Pp. 47–48.
10. Саати Т. Принятие решений. Метод анализа иерархий / Tomas Saaty; пер. с англ. Р.Г. Вачнадзе. – М.: Радио и связь, 1993. – 278 с.
11. Дэвид Г. Метод парных сравнений / Дэвид Г.; пер. с англ. Н. Космарской и Д. Шмерлинга под ред. Ю. Адлера. – Цр Статистика, 1978. – 144 с.
12. Ginzberg M.J., Stohr E.A. Decision Support Systems: Issues and Perspectives. // Processes and Tools for Decision Support. / Ed. by H.G. Sol. – Amsterdam: North-Holland Publ. Co., 1983. – Pp. 9 – 31.
13. Alter S.L. Decision support systems: current practice and continuing challenges / S.L. Alter - Reading, Mass.: Addison-Wesley Pub., 1980. – 316 p.
14. Зайченко Ю. П. Нечеткие модели и методы в интеллектуальных системах: [учебное пособие для студентов высших учебных заведений] / Ю. П. Зайченко. – К.: "Издательский дом "Слово", 2008. – 344 с.
15. Бир Ст. Кибернетика и управление производством / Бир Ст. - М.: Наука, 1965. – 391 с.
16. M. Svahnberg, C. Wholin, and L. Lundberg. A Quality-Driven Decision-Support Method for Identifying Software Architecture Candidates. // Int. Journal of Software Engineering and Knowledge Engineering, 2003. 13(5): pp. 547-573.
17. Tariq Al-Naeem, Ian Gorton, Muhammad Ali Babar, Fethi A. Rabhi, Boualem Benatallah. A quality driven systematic approach for architecting distributed software application, In Proceedings of the 27th International Conference on Software Engineering St. Louis, 2005, pp. 244 – 253.
18. Gorton I. Architecting in the Face of Uncertainty: An Experience Report. Proc. / I. Gorton, J. Haack // ICSE '04 Proceedings of the 26th International

Conference on Software Engineering, – Edinburgh, Scotland, 2004. – Pp. 543-551.

19. Миллер Г. Магическое число семь плюс или минус два. О некоторых пределах нашей способности перерабатывать информацию. // Инженерная психология. – М.: Прогресс, 1964, – С. 192-225.
20. Totsenko V.G. Method of Paired Comparisons Using Feedback with Expert/ Totsenko V.G., Tsyganok V.V. // J. Of Automation and Information Sciences. – 1999. – 31, № 9. – Pp. 86 – 97.
21. Ногин В.Д. Упрощенный вариант метода анализа иерархий на основе нелинейной свертки критериев / Ногин В.Д. // Журнал вычислительной математики и математической физики. – М.: Наука, 2004. – т. 44. – № 7. – с. 1259 – 1268.
22. Павлов А.А. Математические модели оптимизации для нахождения весов объектов в методе парных сравнений. Павлов А.А, Лищук Е.И., Кут В.И. // Системні дослідження та інформаційні технології. – К.: ІПСА, – 2007. №2. – С. 13 – 21.
23. Dobrica, L. A survey on software architecture analysis methods / L. Dobrica, E. Niemela // IEEE Transactions on Software Engineering. – Volume 28. – Issue 7, NJ, USA: IEEE Press Piscataway – July, 2002. – Pp. 638-653.
24. Подиновский В. В. Введение в теорию важности критериев в многокритериальных задачах принятия решений / Подиновский В. В. – М.: Физматлит, 2007. – 64 с.
25. Павлов О.А. Оперативные алгоритмы принятия решений в иерархической системе Саати, основанные на замещении критериев / Павлов О.А., Ліщук К.І. // Вісник НТУУ “КПІ”. Інформатика, управління та обчислювальна техніка. К.: “ВЕК+”, 2008. – № 48. – с. 78 – 81.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

VII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ »

11–12 **грудня** 2019 **року**

ТЕРНОПІЛЬ
2019

УДК 004.7
А. **Тарапата, М. Іваник**
Тернопільський національний технічний університет імені Івана Пулюя

ВИКОРИСТАННЯ МЕТОДУ АНАЛІЗУ ІЄРАРХІЙ ДЛЯ ОЦІНЮВАННЯ ЯКОСТІ ПРОЕКТУ КОМП`ЮТЕРНИХ МЕРЕЖ

UDC 004.7
A. Tarapata, M. Ivanyk
(Ternopil Ivan Puluj National Technical University, Ukraine)

ANALITICAL HIERARCHIC PROCESS FOR QUALITY ASSESSMENT IN COMPUTER NETWORKS DESIGN

Поява робіт, в яких було використано аналіз ієрархій, дозволив значно покращити процес вибору обладнання для реалізації необхідного рівня захищеності мережі і формалізувати його по аналогії, як це запропоновано у роботах [1], [2]. В методі AHP (Analytical Hierarchy Process) використовується порівняльне оцінювання альтернатив стосовно реалізації атрибутів якості. Він дає змогу визначити відносні ваги альтернатив по кожному атрибуту якості і проранжувати їх.

За призначеними зацікавленими сторонами пріоритетами атрибутів якості обчислюється їх усереднене значення і визначаються ваги альтернатив відносно сукупності атрибутів якості. Перевагами методу AHP є оцінювання альтернатив по всіх атрибутах якості, оптимізація рішень та досить високий рівень формалізації, що дає змогу автоматизувати процес.

Як було відзначено раніше, для вибору найкращого проекту комп'ютерної мережі (КМ) з множини альтернативних необхідно отримати їх оцінки відносно реалізації критеріїв якості. Але, оскільки якість проект КМ визначальним чином впливає на якість реалізованої мережі, існує ієрархічна залежність між показниками якості проектного рішення та КМ, де на вершині міститься інтегральний показник якості, далі – проміжні рівні (критерії якості КМ), а на найнижчому рівні розташовані проектні альтернативи.

Для розв'язання такого типу задач використовується метод аналізу ієрархій Сааті [3]. Суть методу полягає в тому, що для побудованої ієрархії на кожному рівні визначаються ваги елементів відносно їх впливу на елемент наступного рівня. Для цього будується матриця парних порівнянь для кожного з нижчих рівнів, по одній матриці для кожного елемента рівня, який примикає зверху. Парні порівняння проводяться в термінах домінування одного з елементів над іншим.

Варто зазначити, що при значній кількості альтернатив неузгодженості коефіцієнтів матриці парних порівнянь є досить суттєвими (20 – 30%), що не дозволяє отримати прийнятне рішення.

Для зменшення неузгодженості при великій кількості альтернатив та/або критеріїв порівняння автор методу [3] пропонує розбивати кожен рівень ієрархії на кластери. Очевидно, що в цьому випадку доведеться виконувати значний обсяг обчислень, що може суттєво позначитись на продуктивності системи, а також групування в кластери проводиться експертами, що є непростою задачею і вносить свої похибки.

Література

1. Харченко О. Г. Метод багатокритеріальної оптимізації програмної архітектури на основі аналізу компромісів / Харченко О. Г., Боднарчук І. О., Галай І. О. // Інженерія програмного забезпечення. – 2012. – № 3–4 (11–12). – С. 5–11.
2. Harchenko, A. Stability of the Solutions of the Optimization Problem of Software Systems Architecture. // A. Harchenko, I. Bodnarchuk, I. Halay / Proceeding of VIIth International Scientific and Technical Conference CSIT 2012. Lviv. 2012. – Pp. 47–48.
3. Саати Т. Принятие решений. Метод анализа иерархий / Tomas Saaty; пер. с англ. Р. Г. Вачнадзе. – М.: Радио и связь, 1993. – 278 с.

УДК 004.7
А. **Тарапата, А. Гулик**
Тернопільський національний технічний університет імені Івана Пулюя

ВИКОРИСТАННЯ МОДЕЛЕЙ ЯКОСТІ ДЛЯ РОЗРОБКИ ВИМОГ

UDC 004.7
A. Tarapata, A. Hulyk
(Ternopil Ivan Puluj National Technical University, Ukraine)

REQUIREMENTS ENGINEERING ON THE BASE OF QUALITY MODELS

Питання розробки вимог якості до інформаційних систем (ІС) на програмному рівні на основі моделей якості розглядались в ряді публікацій [1], [2]. Тут розглядаються моделі трьох категорій якості, а саме якості у використанні, зовнішньої та внутрішньої якості.

На основі моделі якості у використанні розробляються загальні вимоги якості користувача або замовника. Модель вимог якості у використанні ІС можна представити у вигляді [3]

$$V_{use} = \{H^u_i, A^u_{ik}, C^u_{ik}, M^u_{ik}\},\ N_u, K = 1,S_i\ , \qquad (1)$$

тут H_{ui} – характеристика якості у використанні;
A_{uik} – атрибут характеристики якості;
C_{uik} – обмеження на значення атрибута;
$\underline{M_{uik}}$ – метрика атрибута.

Характеристики і метрики підбираються із стандарту [4], а атрибути і обмеження із вимог користувача та аналізу предметної області.

Вимоги зовнішньої якості представляються у вигляді структури моделі зовнішньої якості і інтерпретуються як вимоги до ІС в цілому, в тому числі і до архітектури. Ці вимоги записуються у вигляді

$$V_{ex} = \{H^e_i, \mathit{П}^e_{ik}, A^e_{ik}, C^e_{ik}, M^e_{ik}\},\quad N_e, K = 1,R_i \qquad (3.2)$$

тут H^e_i - характеристики;
$\mathit{П}^e_{ik}$ - підхарактеристики зовнішньої якості;
A^e_{ik}, C^e_{ik}, M^e_{ik} - атрибути, обмеження та метрики відповідно.

Комунікація (трасування) вимог якості (1) на структуру вимог (2) виконується з використанням методу SQFD [3]. На основі отриманих вимог зовнішньої якості формулюються вимоги якості до системи.

.

Література

1. Glenn E., Krasner and Stephen T.Pope. A cookbook for using the model-view controller user interface paradigm in Smalltalk – 80. Jornal of Object-Orient Programming 1 (3): 26-49, August 1998.
2. Фаулер М. Архитектура корпоративных программных приложений: Пер. с англ. – М.: Издательский дом «Вильямс», 2004. – 544 с.
3. Харченко О. Розробка та керування вимогами до програмного забезпечення на основі моделі якості / О. Харченко, В. Яцишин – Вісник ТДТУ – 2009. Том 14. №1. – с. 201-207.
4. ISO/IEC 12207:2008. Systems and software engineering – Software life cycle processes. – 123 p.