Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кібербезпеки
(повна назва кафедри)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломної роботи

магістр
(освітній рівень)

на тему: **Розробка методу вибору активного устаткування для досягнення заданого рівня захищеності мережі**

Виконав: студент 6 курсу, групи СБм-61
спеціальності 125 «Кібербезпека»
(шифр і назва спеціальності)

_____ Іваник М.С..
(підпис) (прізвище та ініціали)

Керівник _____ Александер М.Б..
(підпис) (прізвище та ініціали)

Нормоконтроль _____ Кареліна О.В.
(підпис) (прізвище та ініціали)

Рецензент _____ _____
(підпис) (прізвище та ініціали)

м. Тернопіль – 2019

РЕФЕРАТ

"Розробка методу вибору активного устаткування для досягнення заданого рівня захищеності мережі". // Іваник Максим Сергійович // Тернопільський національний технічний університет ім. І.Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2019 // с. – , рис. – , табл. – , ілюстр. – , джерел – .

Ключові слова: БАГАТОКРИТЕРІЙНА ОПТИМІЗАЦІЯ, МЕТОД САТІ, 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

" Development of a method of active facilities choice to reach the necessary level of network security " // Diploma paper of Master degree level // Ivanyk Maksym Serhiyovytch // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Cybersecurity Department // Ternopil, 2019 // p. – , Fig. – , Tables – , Posters – 7, 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;

– запропоновно 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.

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 (ріре 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 інкапсулюює 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 рис1.1–.

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.

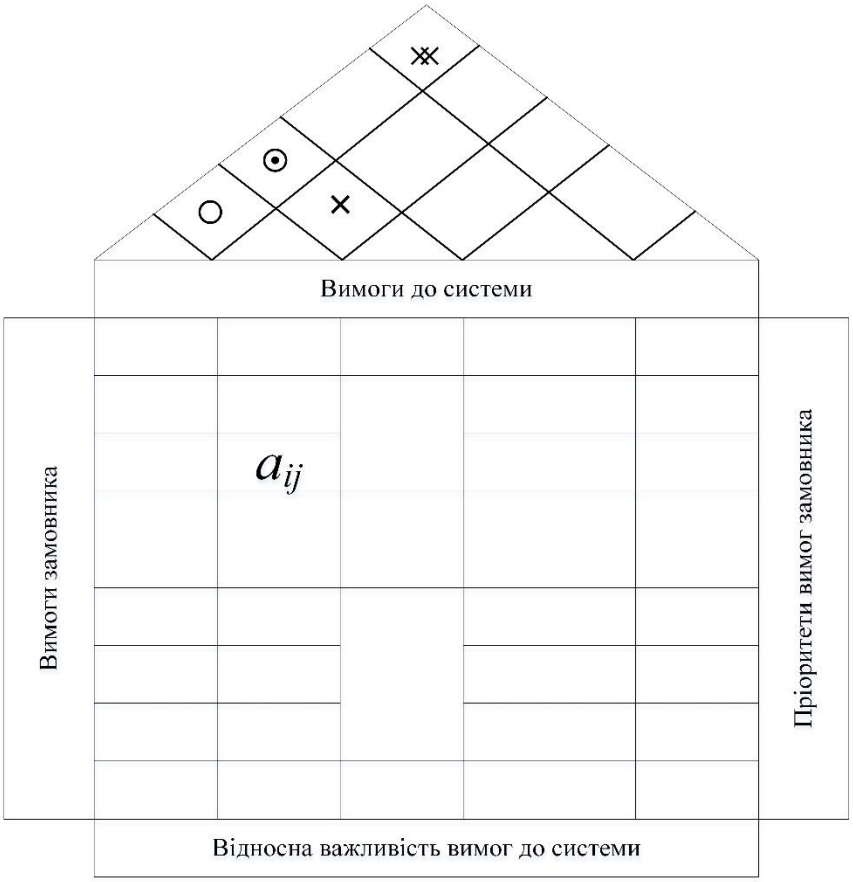

Рисунок 1.1 – "Будинок якості" методу QFD

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. рис1.2–).

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

Рисунок 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:

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

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 1.3– [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.

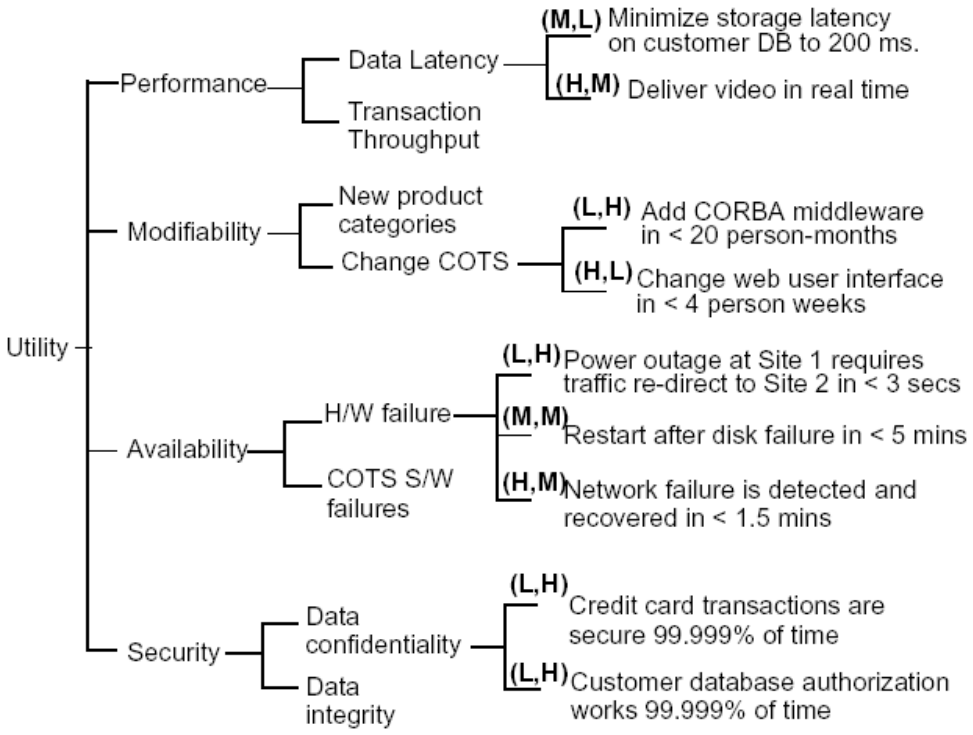

Рисунок 1.3 – Приклад дерева характеристик якості

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 1.3– [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 1.3–). 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 1.4– [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).

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

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.

2 ПОСТАНОВКА ЗАДАЧІ БАГАТОКРИТЕРІАЛЬНОГО ОЦІНЮВАННЯ ТА ВИБОРУ АРХІТЕКТУРИ 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 сформованої множини альтернатив ту, яка буде найкраще задовольняти вимогам якості, в тому числі і захисту даних. Схема процедури оцінювання якості та вибору проекту мережі представлена на рисунку 2.1.

Тут представлено такі рівні критеріїв 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 проектні рішення.

Множина критеріїв якості мережі $\{K_i^1\}$ визначається на основі сформульованих замовником вимог. А множина критеріїв $\{K_i^2\}$визначається шляхом комунікації $\{K_i^1\}$ на якість архітектури застосуванням технології QFD або інших методів, поданих вище.

Необхідно вибрати таке архітектурне рішення, яке б оптимізувало сукупність критеріїв $\{K_i^1\}$, $\{K_i^2\}$. Це задача багатокритеріальної ієрархічної оптимізації.

Рішення поставленої задачі будемо виконувати декількома послідовними діями.

1. На першому кроці визначимо оцінки альтернатив по кожному з критеріїв 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 якщо 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.

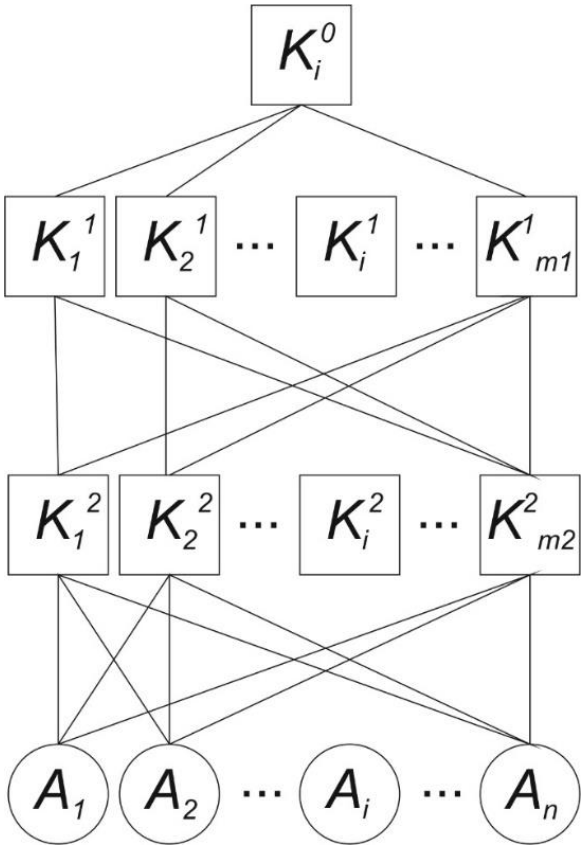

Рисунок 2.1 – Структурна схема задачі оцінювання та вибору ПА

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

Для оцінювання альтернатив по множині критеріїв якості розроблено ряд методів, які мають свої переваги і недоліки. Для обґрунтованого вибору найбільш ефективного, для вирішення поставленої задачі, приведемо результати аналізу цих методів.

2.1 Огляд багатокритеріальних методів оцінювання, та прийняття рішень

В процесі вирішення більшості задач прийняття рішень виникає потреба враховувати велику кількість альтернатив і критеріїв. Розглянемо основні багатокритеріальні методи прийняття рішень. У процесі багатокритеріального оцінювання альтернатив вирішуються такі завдання:

1. Порівняльне оцінювання альтернатив.
2. Ранжування альтернатив.
3. Вибір найкращої альтернативи.

Ряд багатокритеріальних методів прийняття рішень дозволяють лише вирішити завдання ранжування альтернатив. 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.

2.1.1 Метод ЗАПРОС

Метод ЗАПРОС (Замкнуті Процедури у Опорних Ситуаціях) [11], [12] ґрунтується на ідеї перевірки незалежності критеріїв та заміщення прирощень оцінок за одними критеріями прирощеннями оцінок за іншими. Метод ЗАПРОС дозволяє вирішити лише завдання ранжування альтернатив, яке зводиться до упорядкування в межах єдиної шкали множини допустимих кортежів оцінок за прийнятими якісними критеріями. 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 критеріями, називають замкненими процедурами у опорних ситуаціях. ОПР (особа, яка приймає рішення) для визначення переваг пред'являється пара кортежів (r_i, r_j). У кортежі r_i оцінки за всіма критеріями, 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 критеріями c_i, c_j. Після цього виконується впорядкування у межах цієї шкали множини кортежів оцінок за досліджуваними критеріями. Перевагою методу ЗАПРОС є те, що метод дозволяє ранжувати альтернативи за суб'єктивними вербальними оцінками з урахуванням важливості критеріїв, що дуже важливо для задач багатокритеріального 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.

2.1.2 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:

$$v(A_i, A_j) = \sum_{c_h \in C_{ij}^+} w_h \Big/ \sum_{u=1}^{\mu} w_u , \qquad (2.1)$$

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 оцінки альтернатив;

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

Індекс незгоди обчислюють за такою формулою:

$$d(A_i, A_j) = \begin{cases} 0, \text{ якщо } C_{ij}^- = \varnothing; \\ \underset{c_h \in C_{ij}^-}{Max}\left[w_h \left| e_h(A_i) - e_h(A_j) \right|\right] \Big/ d_h, \text{ якщо } C_{ij}^- \neq \varnothing, \end{cases} \quad (2.2)$$

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;

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

Множина значень індексів згоди і незгоди дає можливість отримати підсумкове ранжування альтернатив. Пропонується наступне правило порівняння: альтернатива A_i перевершує альтернативу A_j, якщо $v(A_i, A_j) \geq p$, а $d(A_i, A_j) \leq q$, де p, q – порогові значення, визначені ОПР. Це правило порівняння спрощує проблему виділення підмножини альтернатив, що містять найкращу альтернативу, проте не дозволяє вирішити завдання їх повного впорядкування.

Методи ЗАПРОС і ELECTRE дозволяють вирішити лише завдання ранжування альтернатив, 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.

2.1.3 Методи прийняття 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 багатокритеріального 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:

$$s_i = \sum_{j=1}^{\mu} w_j r_{ij} \,, \tag{2.3}$$

де s_i – сума оцінок r_{ij} альтернатив за критеріями, зважених коефіцієнтами w_j відносної важливості цих критеріїв;

μ – кількість критеріїв оцінки альтернатив;

r_{ij} – оцінки альтернатив за критеріями;

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 ступенів оцінок альтернатив за різними критеріями:

$$p_i = \prod_{j=1}^{\mu} r_{ij}^{w_j} \,, \tag{2.4}$$

де p_i – величина добутків степенів оцінок альтернатив за критеріями;

μ – кількість критеріїв оцінки альтернатив;

r_{ij} – оцінки альтернатив за критеріями;

w_j – коефіцієнти відносної важливості цих критеріїв.

2.1.4 Метод аналізу ієрархій Сааті

Метод аналізу ієрархій (МАІ) Сааті [10] в даний час найбільш часто використовується для вирішення задач багатокритеріального вибору. Основними етапами МАІ є:

1. Сформулювати проблему і виявити, що необхідно визначити.
2. Побудувати ієрархію, починаючи з вершини (цілі – з погляду управління), через проміжні рівні (критерії, від яких залежать наступні рівні) до найнижчого рівня, який зазвичай є переліком альтернатив (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. Побудувати множину матриць парних порівнянь для кожного з нижніх рівнів – по одній матриці для кожного елемента рівня, який примикає зверху. 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), $b_{ij}=\frac{1}{b_{ji}}$, на головній діагоналі матриці парних порівнянь стоять одиниці. Матриця парних порівнянь (суджень) є позитивною, квадратною та обернено симетричною. Шкалою для виконання парних порівнянь є найбільш часто використовувана дев'ятибальна шкала, запропонована Т. Сааті. Для отримання кожної матриці потрібно $\frac{n(n-1)}{2}$ суджень, де n – це кількість порівнюваних елементів.

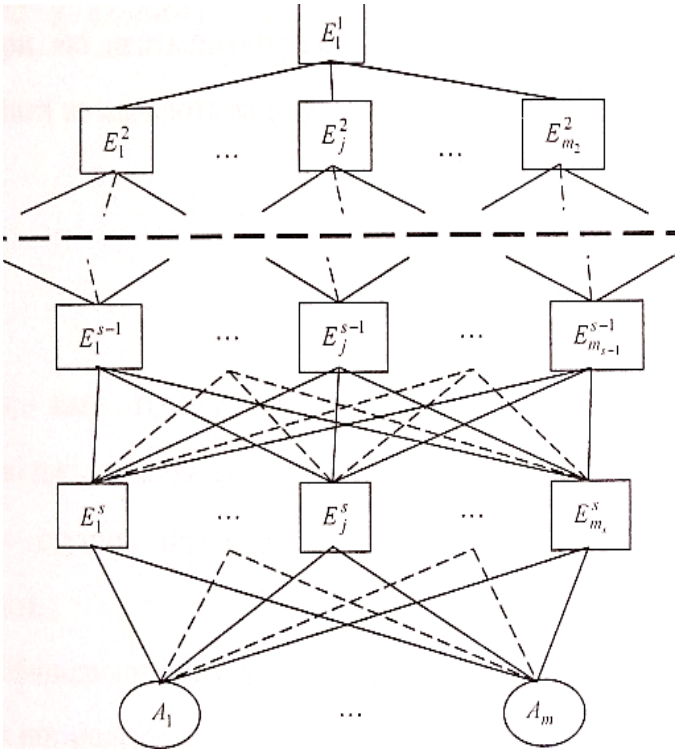

Рисунок 2.2 – Приклад ієрархічного представлення задачі прийняття рішень

4. Визначити ваги $w_i, i=\overline{1,n}$ об'єктів $A_i, i=\overline{1,n}$ методом власного вектора. Як відомо, знаходження власного вектора матриці є вкрай трудомісткою обчислювальною процедурою. Наближені значення ваг можна отримати за співвідношеннями (2.5):

$$w_i = \frac{\sqrt[n]{\prod_{j=1}^{n} b_{ij}}}{\sum_{i=1}^{n}\left(\sqrt[n]{\prod_{j=1}^{n} b_{ij}}\right)} \text{ або } w_i = \frac{1}{n}\sum_{j=1}^{n}\frac{b_{ij}}{\sum_{j=1}^{n} b_{ij}}, \qquad (2.5)$$

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 парних 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 матриці парних порівнянь $\lambda_{\max} = n$, а для неузгодженої матриці завжди $\lambda_{\max} \geq n$. Т. Сааті запропонував як показник ступеня узгодженості елементів матриці парних порівнянь 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 матриць парних порівнянь у фундаментальній шкалі. Значення $M(I_u)$ можна обчислити за такою формулою:

$$M(I_u) = \frac{1{,}98 \cdot (n-2)}{n}, \qquad (2.6)$$

n – розмірність матриці парних порівнянь.

Слід зазначити, що $M(I_u)$ збільшувалися зі збільшенням порядку матриці парних порівнянь.

У праці [15] рекомендовано вважати ваги достовірними, якщо $I_u < 0{,}10$ (у крайньому разі не перевищує 0,20).

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 матриці парних порівнянь, 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 MAI є найбільш критичною, тому якщо в результаті вирішення 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 застосовуються на практиці, при цьому слід зазначити, що метод ПАЗ має недостатнє теоретичне обґрунтування, у той час як МАІ є повністю теоретично обґрунтованим методом.

2.1.5 Застосування МАІ 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 МАІ для отримання порівняльних оцінок альтернативних проектів відносно реалізації кожного з критеріїв якості. Послідовність кроків у застосуванні МАІ 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 МАІ в якості вхідної інформації є елементи матриці парних порівнянь, 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 критеріїв якості та знаходити усереднене значення відхилення оцінок. При перевищенні відхиленням встановленої норми пропонується проводити повторно всю процедуру від заповнення матриці парних порівнянь 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 визначити пріоритети критеріїв якості, що є також непростою задачею. Оскільки

призначення пріоритетів критеріїв виконується по такому ж алгоритму, що і визначення ваг альтернатив, в рішення вноситься додаткове джерело похибок.

Варта уваги також робота [17], в якій розглядається задача проектування архітектури розподіленої системи з врахуванням критеріїв 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 рішення. Проведені достатньо масштабні дослідження для альтернатив проекту GB показали ефективність MAI при рішенні подібних задач.

Однак метод аналізу ієрархій Сааті має такі обмеження:

1. Матриці парних порівнянь мають бути узгодженими, проте реальні матриці парних порівнянь 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 матриці парних порівнянь (для повністю узгодженої матриці парних порівнянь $\lambda_{\max} = n$, а для неузгодженої матриці завжди $\lambda_{\max} \geq n$). Як зазначено у праці [10], зміни в елементах b_{ij} матриці парних порівнянь (помилки експертів) призводять до зміни $\lambda_{\max}$, тобто до зменшення узгодженості матриці парних порівнянь.

2. Матриці парних порівнянь мають бути малої розмірності. Ця вимога випливає з вимоги узгодженості матриць парних порівнянь. 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 матриці парних порівнянь, які ґрунтуються на отриманні уточнювальної інформації від експерта.

Існують методи отримання формально повністю узгодженої матриці парних порівнянь. 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 парних порівнянь будується на основі елементів базисного набору. Базисним набором елементів матриці парних порівнянь називають мінімальний (за кількістю) визначальний набір. Деякий набір елементів матриці парних порівнянь, розміщених вище від головної діагоналі, є визначальним, якщо 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 матриці парних порівнянь.

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 матриці парних порівнянь, розміщених вище головної діагоналі, на основі базисного набору $b_{12}, b_{23}, \ldots, b_{n-1,n}$ має такий вигляд:

$$b_{ij} = b_{i,j-1} \cdot b_{j-1,j}, \quad (i = 1, \ldots, n-2;\ j = 1, \ldots, n;\ i < j-1), \tag{2.7}$$

де *n* – кількість порівнюваних об'єктів.

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

$$w_k = b_{k,k+1} \cdot b_{k+1,k+2} \cdot \ldots \cdot b_{n-1,n}\ (k = 1,2,\ldots,n-1), \quad w_n = 1, \tag{2.8}$$

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

n – кількість порівнюваних об'єктів.

Далі виконується нормування компонентів вагового вектора.

Отже, цей метод використовує для знаходження ваг не всю інформацію, яка міститься в емпіричній матриці парних порівнянь, що призводить до зниження достовірності одержуваного рішення.

2.1.6 Модифікований метод аналізу ієрархій

Професором Павловим А.А. в роботі [22] було запропоновано модифікацію методу аналізу ієрархій для розв'язування задач багатокритеріального вибору при неузгоджених матрицях парних порівнянь. Основна ідея модифікації полягає у визначенні ваг альтернатив з умови мінімізації міри неузгодженості матриці парних порівнянь. Наведемо постановку деяких з цих задач та застосування цього підходу до задачі багатокритеріального оцінювання та вибору архітектури ПС.

Якщо матриця парних порівнянь є повністю узгодженою, то:

$$\frac{w_i}{w_j} = b_{ij},\ w_i = b_{ij} w_j \quad \forall b_{ij} \in B, \tag{2.9}$$

де w_i – вага *i*-го об'єкта;

B – множина коефіцієнтів $b_{ij}, i, j = \overline{1,n}$ матриці парних порівнянь.

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

$$\left(w_i - b_{ij} w_j\right)^2 \text{ або } \left|w_i - b_{ij} w_j\right|; \tag{2.10}$$

$$\frac{1}{b_{ij}^2}\left(\frac{w_i}{w_j} - b_{ij}\right)^2 \text{ або } \frac{1}{b_{ij}^2}\left|\frac{w_i}{w_j} - b_{ij}\right|. \tag{2.11}$$

В залежності від постановки задачі розглядається декілька моделей оптимізації.

Модель 1 [22].

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

$$\min \sum_{(ij)\in|B|}\sum \left(y_{ij}^+ + y_{ij}^-\right) \tag{2.12}$$

$$\begin{aligned} &w_i - b_{ij} w_j = y_{ij}^+ - y_{ij}^-,\ y_{ij}^+ \geq 0,\ y_{ij}^- \geq 0 \\ &\underset{(i,j)\in|B|}{} \\ &w_i \geq a \geq 1, \quad i = \overline{1,n}, \end{aligned} \tag{2.13}$$

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

Модель 2 [22].

Для мінімізації максимальної величини неузгодженості рішення модель оптимізації буде наступною:

$$\min \sum_{(ij)\in|A|}\sum y_{ij} \,. \tag{2.14}$$

$$\begin{gathered} -y_{ij} \le w_i - b_{ij} w_j \le y_{ij},\ y_{ij} \ge 0 \\ {\scriptstyle (i,j)\in|B|} \\ w_i \ge a \ge 1, \quad i=\overline{1,n}, \end{gathered} \tag{2.15}$$

де $w_i, i=\overline{1,n}, \quad y_{ij}, \forall(i,j)\in|B|$ – змінні задачі лінійного програмування.

Інші позначення мають такий же зміст, що і в попередній моделі (2.12), (2.13).

Оптимальному вирішенню задачі лінійного програмування (2.14), (2.15) відповідають ваги $w_i^*, i=\overline{1,n},$ на яких досягається мінімум $\sum_{(ij)\in|B|}\sum\left|w_i^* - b_{ij} w_j^*\right|$.

Модель 3 [22].

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

$$\min\ y \tag{2.16}$$

$$\begin{gathered} -y \le w_i - b_{ij} w_j \le y \\ {\scriptstyle (i,j)\in|A|} \\ w_i \ge a \ge 1, \quad i=\overline{1,n},\ y \ge 0, \end{gathered} \tag{2.17}$$

де $w_i, i=\overline{1,n}, \quad y$ – змінні задачі лінійного програмування;

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

B – множина коефіцієнтів $b_{ij},\ i, j=\overline{1,n}$ матриці парних порівнянь;

a – задане число, $a \ge 1$;

n – кількість порівнюваних об'єктів.

Модель 4, допустимо узгодженого рішення [22].

$$\min \sum_{(ij)\in|A|}\sum\left(y_{ij}^{+} + y_{ij}^{-}\right) \tag{2.18}$$

$$
\begin{aligned}
&-t_{\partial on} b_{ij} w_j \le w_i - b_{ij} w_j \le t_{\partial on} b_{ij} w_j, \\
&\underset{(i,j)\in|A|}{} \\
&w_i - b_{ij} w_j = y_{ij}^{+} - y_{ij}^{-},\ y_{ij}^{+} \ge 0, y_{ij}^{-} \ge 0, \\
&w_i \ge a \ge 1, \quad i = \overline{1,n},
\end{aligned}
\tag{2.19}
$$

де $w_i, i = \overline{1,n}, \quad y_{ij}, \forall (i,j) \in A$ – змінні задачі лінійного програмування;

$t_{\partial on}$ – задане граничне число.

Задача (2.18), (2.19) може не мати рішення, оскільки обмеження можуть бути несумісними. У цьому разі можна або збільшити значення $t_{\partial on}$, або скористатися іншою моделлю за умови, що число $t = \max\left\{\dfrac{y^0}{b_{ij} w_j^*}\right\}$ може бути прийнято як допустимий коефіцієнт узгодженості рішення задачі (2.18), (2.19).

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

$$
K(w_i^*) = \frac{1}{n-1} \sum_{\substack{j=1 \\ j \ne i}}^{n} \frac{1}{b_{ij}} \left| \frac{w_i^*}{w_j^*} - b_{ij} \right|. \tag{2.20}
$$

Якщо для деякого j, b_{ij}<1 то відповідний доданок змінюється на $\dfrac{1}{b_{ji}} \left| \dfrac{w_j^*}{w_i^*} - b_{ji} \right|$,

тобто коефіцієнт узгодженості $K(w_i^*)$ для w_i^* визначається за $b_{ij} \ge 1$. $K(w_i^*)$ мають належати деякому заданому допустимому інтервалу узгодженості, інакше приймається w_i^*=0. Також пропонується використовувати критерії оцінювання знайденого набору ваг за коефіцієнтами узгодженості:

$$
M_1 = \sum_{i=1}^{n} K(w_i^*) \tag{2.21}
$$

$$
M_2 = \max_{i,\ i=\overline{1,n}} K(w_i^*) \tag{2.22}
$$

Після застосування моделей оптимізації та вибору кращого рішення 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

$$\hat{w}_i^* = \frac{w_i^*}{\sum_{j=1}^{n} w_j^*},\ i=\overline{1,n},\ \text{тоді}\ \sum_{i=1}^{n}\hat{w}_i^* = 1, \tag{2.23}$$

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 $K(w_i^*)$:

$$\hat{w}_i^* = \frac{\frac{w_j^*}{K(w_i^*)}}{\sum_{j=1}^{n}\frac{w_j^*}{K(w_i^*)}} = \frac{w_j^*}{K(w_i^*)\sum_{j=1}^{n}\frac{w_j^*}{K(w_i^*)}},\quad i=\overline{1,n},\quad \sum_{i=1}^{n}\hat{w}_i^* = 1 \tag{2.24}$$

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.

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

Як відмічалось в попередньому пункті використання МАІ забезпечує коректне рішення при невеликій кількості альтернатив ($n \leq 7\pm2$). 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 альтернатив і вибору не найкращого варіанта. Було проведено дослідження по порівнянню методів МАІ та ММАІ при збільшенні розмірності МПП в задачі оцінювання альтернатив.

Для можливості змінювати ступінь узгодженості рішення задачі оцінювання альтернатив з використанням ММАІ скористаємось моделлю оптимізації, визначеної виразами (2.18), (2.19).

Для оцінки узгодженості отриманих рішень будемо використовувати наступні показники: коефіцієнт узгодженості M_1, визначений формулою (2.21), а також міру узгодженості M_2, визначеної формулою (2.22).

Були проведені дослідження ефективності методу обчислення вагових множників згідно моделі допустимого узгодженого рішення 4, яка приводить до задачі оптимізації (2.18), (2.19) для отримання оцінок альтернативних проектів ПС при неузгоджених матрицях $B\{b_{ij}\}$.

При цьому, для заданих значень порогу неузгодженості $t_{доп}$ моделювались похибки експертів при визначенні елементів МПП шляхом генерування випадкових збурень матриці $B\{b_{ij}\}$ і знаходились вагові множники $w_i^*, i=\overline{1,n}$ стандартним і модифікованим МАІ.

Після цього обчислювались коефіцієнти та міри узгодженості (2.21), (2.22) для результатів, отриманих обома методами. Було проведено дослідження впливу похибок неузгодженості матриці парних порівнянь на ранжування альтернатив.

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

$$b_{ij}^{s*} = b_{ij}^s + K_{ij} \cdot b_{ij}^s \qquad (2.25)$$

Для отриманих матриць $B^{s*}\{b_{ij}^{s*}\}$ визначались набори вагових множників $\{w_i^s\}, i=\overline{1,n}, s=\overline{1,7}$ стандартним MAI і як рішення задачі (2.18), (2.19). Після цього обчислювались міри узгодженості M_1 і M_2, які усереднювались по множині критеріїв якості.

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

Як видно з графіка, модифікований MAI дає значно кращі результати за критерієм M_1, ніж стандартний. Так, вже при похибках в матриці $B^{s*}\{b_{ij}^{s*}\}$ в межах $t_{доп}$=0,15 модифікований MAI дав на 20 відсотків менше значення міри неузгодженості рішення, ніж стандартний.

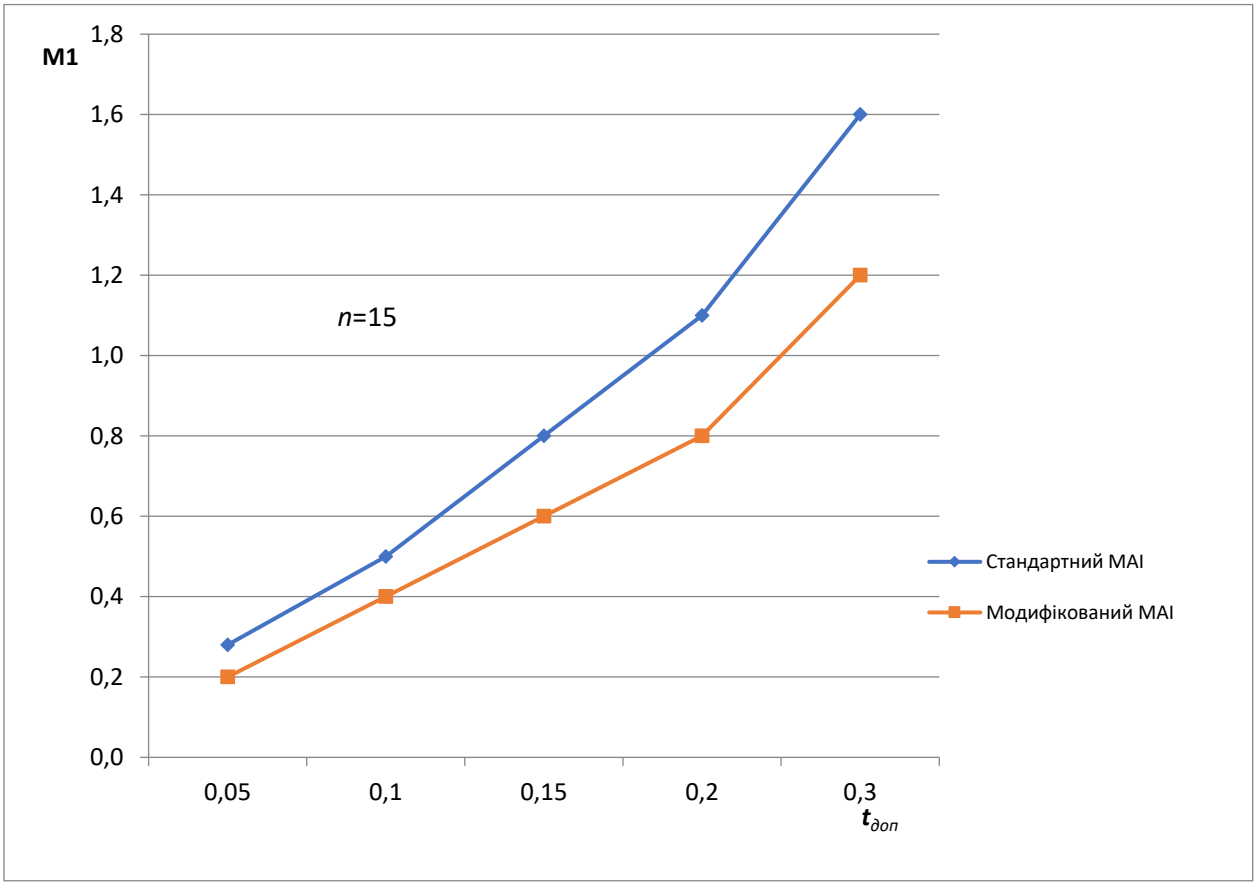

Рисунок 2.3 – Залежність критерію M_1 від інтервалу похибок

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.

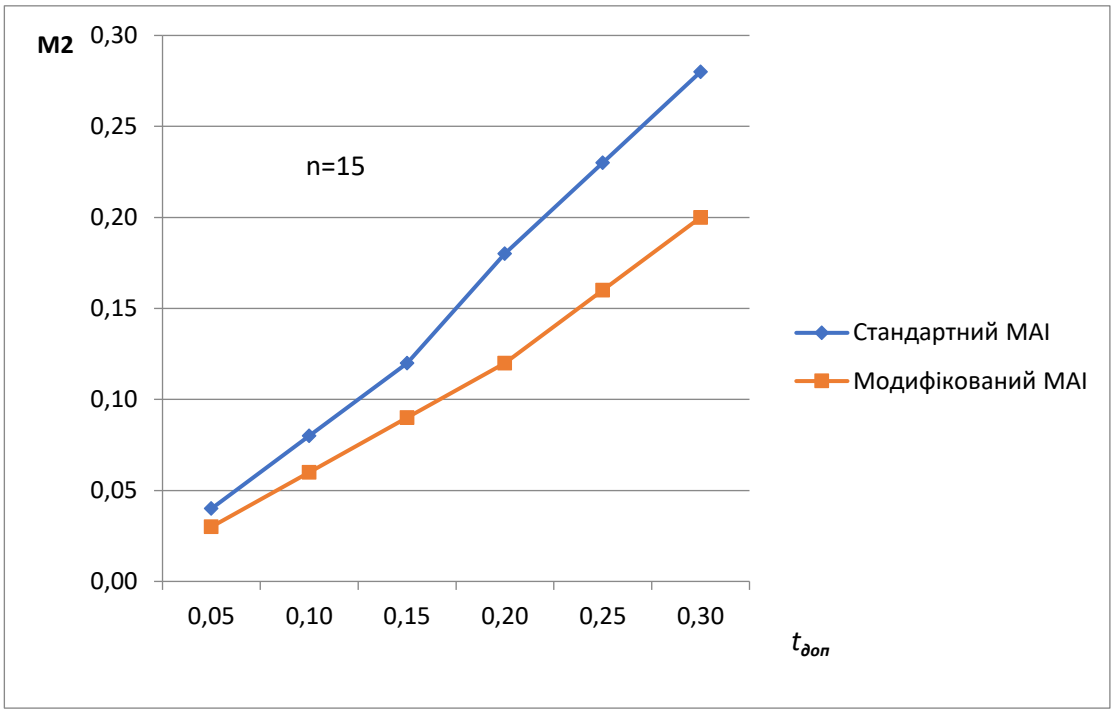

Рисунок 2.4 – Залежність критерію M_2 від інтервалу похибок

З графіків також видно, що градієнт зростання значень критеріїв неузгодженості рішень для стандартного MAI більший, ніж для модифікованого, що свідчить про меншу нестійкість модифікованого MAI.

Важливим також є дослідження впливу похибок визначення вагових множників $\{w_i\}$, викликаних неузгодженостями в матриці парних порівнянь, на ранжування альтернатив $\{A_i\}$ як за окремими критеріями якості, так і за їх сукупністю. Для цього по узгоджених матрицях парних 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 множина номерів проектів. Після цього, згідно описаної вище методики, моделювались помилки експертів та визначались $\{w_i^*\}$ і проводилось повторне ранжування $\{A_{is}\}$.

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 рішення при більших значеннях неузгодженостей матриці парних порівнянь і таким чином розширити межі застосування MAI.

Для ранжування альтернатив по множині критеріїв необхідно визначити їх пріоритети. Це можна зробити або безпосереднім присвоєнням значень пріоритетів експертами, або обчисленням їх методом парних порівнянь. Другий варіант є кращим, оскільки дозволяє зменшити вплив суб'єктивних чинників на результат. Для цього експертами заповнюється матриця парних 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 модифікований MAI, отримаємо набори пріоритетів критеріїв захищеності проекту мережі $\{p_i^{1s}\}$, $i=\overline{1,m2}$, $s=\overline{1,m1}$. Тоді вага альтернативної архітектури A_i відносно реалізації підхарактеристики захищеності K_s^1 визначатиметься за формулою:

$$J_i^{1s}=\sum_{j=1}^{m2} p_j^{1s}\cdot w_i^j,\quad i=\overline{1,n},\quad s=\overline{1,m1}, \tag{2.26}$$

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

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

Якщо потрібно провести ранжування альтернатив відносно глобальної показника захищеності, то необхідно визначити пріоритети критеріїв захищеності $\{p_i^2\}$, $i=\overline{1,m1}$, застосувавши модифіковану процедуру MAI.

Визначити ваги альтернатив відносно реалізації глобального критерію можна за значеннями показника:

$$J_i^0=\sum_{s=1}^{m1} J_i^{1s}\cdot p_s^2,\quad i=\overline{1,n}. \tag{2.27}$$

З приведених результатів досліджень видно, що зміна порядку ранжування альтернатив 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.

Проведені дослідження показали, що використання стандартного алгоритму обчислення вагових множників в МАІ в задачі оптимізації рівня захищеності мережі може привести до прийняття невірних рішень у випадку значної кількості альтернатив. Застосування модифікованої процедури в МАІ дозволяє суттєво зменшити неузгодженості рішень, навіть при значних неузгодженостях матриці парних порівнянь. Так, для використовуваних критеріїв неузгодженості застосування модифікованого алгоритму забезпечило в деяких випадках зменшення значень критеріїв від 20 до 30 відсотків.

Аналіз результатів показав також, що градієнт росту критерію неузгодженості M_1 збільшується із збільшенням похибок матриць парних порівнянь, тобто отримане в МАІ рішення є нестійким до цих похибок. Тому необхідно проводити додатковий аналіз отриманих ранжувань альтернатив, як за сукупністю критеріїв так і за окремими критеріями, а при необхідності – будувати області компромісів [23]. Корисним також є узгодження пріоритетів різних категорій фахівців при визначенні ваг критеріїв (підхарактеристик) захищеності.

Таким чином, застосування модифікованого алгоритму в МАІ, а також виконання перерахованих вище заходів дозволить зменшити вплив похибок парних порівнянь, а також нестійкість МАІ до цих похибок, і, таким чином, покращити якість рішень задачі оцінювання альтернативних проектів по кожному з критеріїв захищеності а також по їх сукупності.

2.3 Дослідження чутливості ранжування альтернативних проектів та аналіз компромісів при прийнятті багатокритеріальних 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 критеріїв якості експертними методами.

Але при виборі рішення 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 зміни вимог якості 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 рішення по вибору остаточного варіанту. Також використання інтегрального критерію для вибору рішення приховує прийняті компроміси між конкуруючими критеріями.

Тому для врахування можливих змін вимог та вибору найбільш стійкого до цих змін рішення по вибору проекту мережі, необхідно дослідити чутливість рішення, а також можливі компроміси між критеріями захищеності.

Питання чутливості рішень до похибок та аналізу компромісів в задачі оцінювання та вибору архітектур 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 критеріїв якості і, використовуючи лінійну згортку критеріїв, отримати оцінки по їх сукупності. Це дозволяє провести ранжування альтернатив і вибрати найкраще відносно отриманих оцінок рішення. 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 критеріями якості і міру прийнятого компромісу між ними при призначенні ваг критеріям.

Розглянемо тепер чутливість рішень, отриманих з використанням MAI, до зміни пріоритетів критеріїв якості.

Нехай ми маємо ваги альтернатив по реалізації критеріїв захищеності $\{w_i^s\}$ та проранжовані архітектурні альтернативи $\{A_i\}$, отримані методом аналізу ієрархій. Наведемо формулу для визначення мінімальної зміни абсолютної величини ваги атрибуту якості P_s, таку, що порядок слідування A_i та A_j поміняється на протилежний:

$$D'_{s,i,j} = \frac{\left|J_i - J_j\right|}{\left|w_i^s - w_j^s\right|} \cdot \frac{100}{P_s} \qquad (2.28)$$

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 слідування сусідніх альтернатив A_i та A_j на зворотній. Найменше значення $D'_{s,i,j}$ показує, що пріоритет P_s атрибуту K_s є критичним до змін оцінок в парних порівняннях. Це рівняння можна також використати у випадку зміни вимог до ПС у процесі проектування, яке може привести до зміни пріоритетів відносно критеріїв якості.

Для кожного атрибуту якості 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 найкраще по критерію якості рішення, а те, 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.

В таблиці 2.1 показані найменші значення D, що можуть привести до зміни ранжування альтернатив, обчислені по (2.28).

Таблиця 2.1– Найменша зміна пріоритетів атрибутів якості для зміни 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 представлені у відсотках від абсолютної величини ваги атрибута якості. Як бачимо з таблиці, портативність має другий найменший пріоритет серед атрибутів захищеності і, в той же час цей атрибут найчутливіший до змін.

Таким чином, аналіз чутливості дозволяє визначити межі змін пріоритетів ваг атрибутів якості при зміні вимог. Якщо зміни пріоритетів виконуються в рамках цих меж, поточний порядок ранжування альтернатив залишається без змін.

3 МЕТОД БАГАТОКРИТЕРІАЛЬНОГО ВИБОРУ АРХІТЕКТУРИ ПРИ ЗМІНІ ВИМОГ ЯКОСТІ

Внесення змін в проект, для врахування зміни вимог якості, виконується шляхом оцінювання існуючого проекту і порівняння його якісних характеристик з альтернативами. Причому, в якості альтернатив можуть розглядатися стандартні рішення, в які можуть вноситись необхідні корекції.

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

Розглянемо підхід до отримання рішення багатокритеріального вибору проекту мережі на основі інформації про порівнянність критеріїв за важливістю і проведення необхідної корекції оцінок, для врахування зміни вимог якості до КС.

3.1 Оперативне корегування альтернатив з використанням заміщення і компенсації

Задача корегування оцінок альтернатив виникає тоді, коли експерти і архітектор при виборі проекту надають перевагу певній альтернативі A_i, хоча вона за деякими критеріями має не найкращі оцінки. Ставиться задача збільшити оцінки за цими критеріями за рахунок зменшення за іншими, але так, щоб оцінки альтернативи A_i за всіма критеріями 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, якщо для деякої альтернативи A_i можлива компенсація за перевагою будь-якої зміни критерію K_r зміною критерію K_s.

Тобто, якщо A_i^p – це альтернатива, яка заміщує A_i шляхом корекції K_r і компенсації K_s, то їх скореговані значення будуть

$$\overline{K}_r^{ip} = \overline{K}_r^i - \delta_r, \ \overline{K}_s^{ip} = \overline{K}_s^i + \delta_{si}, \ \delta_{si} = f\left(r, s, \overline{K}, \delta_r\right), \tag{3.1}$$

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

Запишемо співвідношення для компенсації при заміщенні для множини компонент вектору $\overline{K}^i$ альтернативи A_i, яку ми хочемо зробити кращою за A_j:

$$\delta\overline{K}_r^{ir_z} = C_r^{ir_z} \cdot \delta K_r^i, \ r_z \in R_i^2(r), \ r \in R_i^1, \tag{3.2}$$

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 – множина 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 множина індексів, така, що компоненти $\overline{K}_r^i, r \in R_i^1$ можуть брати участь у заміщенні компонентів $\overline{K}_s^i, s \in R_i^2(r)$;

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

Компоненти вектору $\overline{K}^i$ після заміщення визначаються наступними співвідношеннями:

$$\begin{aligned} &\overline{K}_r^{ip} = \overline{K}_r^i - \sum_{r_z \in R_i^2(r)} C_r^{ir_z} \cdot \delta\overline{K}_{r_z}^i, \quad r \in R_i^1; \\ &\overline{K}_r^{ip} = \overline{K}_{r_z}^i + \sum_{r \in R_i^1} \sum_{r_z \in R_i^2(r)} \delta\overline{K}_{r_z}, \quad r_z \in s, s \overline{\in} R_i^1, r_z \in R_i^2(r). \end{aligned} \tag{3.3}$$

О.А. Павловим в роботі [25] сформульовані задачі оптимізації заміщення (3.3), які зводяться до задач лінійного програмування. Математичні моделі задач оптимізації залежать від стратегії прийняття рішень. Для Парето-оптимальної стратегії модель оптимізації буде такою:

$$\max\left\{\sum_{r \in R_r^1} d_r + \sum_{s \overline{\in} R_j^1} d_s\right\} = \max\{y\} \tag{3.4}$$

при обмеженнях:

$$\begin{aligned} &d_r, d_s \geq 0, r \in L_j^1, s \overline{\in} R_j^1 \\ &\overline{K}_r^j - \sum_{r_z \in R_j^2(r)} \delta\overline{K}_r^{jr_z} \geq \max_i\left(\delta\overline{K}_r^i\right) + d_r, i \in \overline{1,n}, i \neq j, r \in R_j^1 \end{aligned} \tag{3.5}$$

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

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

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

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

Після деяких перетворень для розв'язування задачі застосовується стандартний симплекс-метод.

3.2 Застосування методу корекції альтернатив

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

Числові значення оцінок проектних альтернатив, отриманих з використанням модифікованого MAI, наведені в таблиці 3.1.

Таблиця 3.1 – Числові значення оцінок проектів мережі, отриманих з використанням модифікованого MAI

Критерії	**Архітектура**		
	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 критеріями вона була не гірша, ніж дві інші.

Тут множина $L_i^1 \to \left(\forall l \in L_i^l, \overline{K}_l^i > \overline{K}_l^j, i\neq j\right) \in \{1;5\}$, 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

$$\begin{aligned} 0{,}56 - \left(\Delta\overline{K}_{13} + \Delta\overline{K}_{14}\right) \geq 0{,}22 \pm 1 \cdot y; \\ 0{,}57 - \left(\Delta\overline{K}_{53} + \Delta\overline{K}_{54}\right) \geq 0{,}22 \pm 0{,}8 \cdot y. \end{aligned} \quad (3.6)$$

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

$$\begin{aligned} 0{,}21 + \left(1{,}6 \cdot \Delta\overline{K}_{13} + 1{,}3 \cdot \Delta\overline{K}_{53}\right) \geq 0{,}43 + 0{,}5 \cdot y; \\ 0{,}22 + \left(2{,}5 \cdot \Delta\overline{K}_{14} + 2 \cdot \Delta\overline{K}_{54}\right) \geq 0{,}33 + 0{,}6 \cdot y. \end{aligned} \quad (3.7)$$

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

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

$$\begin{aligned} \Delta\overline{K}_{13} + \Delta\overline{K}_{14} \leq 0{,}34; \\ \Delta\overline{K}_{53} + \Delta\overline{K}_{54} \leq 0{,}28. \end{aligned} \quad (3.8)$$

В результаті вирішення задачі оптимізації з введеними обмеженнями отримаємо:

$$\begin{aligned} \Delta K_{13} = 0{,}12;\ \Delta K_{14} = 1{,}11; \\ \Delta K_{53} = 0{,}18;\ \Delta K_{54} = 0;\ y = 0{,}13. \end{aligned} \quad (3.9)$$

Таким чином в перших трьох розділах сформульована задача вибору архітектури ПС з множини альтернатив, як задачі багатокритеріального прийняття рішень на ієрархічній структурі.

Розв'язування задачі виконується в 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 багатокритеріального прийняття рішень, з якого зроблено висновок, що найбільш прийнятним методом, в даному випадку є метод аналізу ієрархій Сааті. Однак його застосування обмежене невеликою кількістю альтернатив і критеріїв ($n \leq 7 \pm 2$). Для розширення меж коректного застосування MAI використано оптимізаційний метод обчислення

(визначення) ваг альтернатив, який базується на використанні моделей мінімізації неузгодженостей матриці парних порівнянь, розроблений О.А.Павловим та його учнями.

Були проведені дослідження ефективності ММАІ в даній задачі, які показали, що використання ММАІ дозволяє отримувати достовірні результати при значно більшій кількості альтернатив ($n \leq 45$) і критеріїв. При дослідженні для матриць парних порівнянь різної розмірності знаходились ваги альтернатив з використанням МАІ та ММАІ. Моделювались похибки неузгодженості матриці парних порівнянь внесенням випадкових збурень в значення коефіцієнтів МПП. Отримані результати показали, що ММАІ більш стійкий до неузгодженостей МПП ніж стандартний МАІ, 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 ММАІ для вирішення задачі багатокритеріального 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.

Були також проведені дослідження чутливості, отриманого застосуванням ММАІ ранжування альтернатив, до зміни вимог, а також до зміни пріоритетів критеріїв захищеності. Отримані результати дозволяють визначити інтервали можливих змін пріоритетів, які не приводять до зміни ранжування альтернатив.

Також розглядається адаптивний метод вибору проекту мережі при зміні вимог. Метод включає обчислення порівняльних оцінок альтернатив і оперативну корекцію оцінок, для врахування зміни вимог. Порівняльні оцінки альтернатив визначаються модифікованим методом аналізу ієрархій, а для корекції оцінок використовується метод попарного заміщення В.В. Подіновського, який полягає в компенсації за перевагою зміни критеріїв. Для оптимізації заміщення використовуються моделі лінійного програмування.

4 СПЕЦІАЛЬНА ЧАСТИНА

4.1 Використання програми NetCracker для моделювання мереж

Фірма-виробник цього продукту – NetCracker Technology, платформа – Windows.

NetCracker дозволяє створювати модель мережі практично будь-якого масштабу – від локальної на декілька користувачів до рівня регіону. Програма легко настроюється і відносна проста у використанні завдяки дружньому призначеному для користувача інтерфейсу і використанню технології "drag and drop".

NetCracker має велику базу даних, яка містить інформацію про близько 5000 різнотипних пристроїв: повторювачах, концетраторах, комутаторах, мережевих адаптерах, серверах різних виробників. Також є відомості про навантаження, що створюється різним програмним забезпеченням. База даних легко оновлювана через інтернет з сервера виробника.

Кожен пристрій описується набором властивостей, які детально описують такі дані, як затримка, швидкість передачі, фільтрації і перенаправлення пакетів, використовувані протоколи, тип портів, їх доступність, опис інтерфейсної карти і так далі. Апаратне і програмне забезпечення в сукупності дозволяє описувати різноманітну мережеву архітектуру: клієнт-сервер, VLAN (віртуальна локальна мережа), intranet, безпровідні мережі та ін.

Мережеве навантаження може бути описане звичайним потоком даних, або потоком голосової і відеоінформації. Для завдання цього навантаження вимагається вказати станцію-відправник, станцію-отримувач і вид трафіку: розмір пакетів, час очікування між їх передачами, закон зміни цих величин, можливо також визначити використовуваний протокол високого рівня: SMTP,

POP3, FTP, HTTP, CAD/CAM client – server, Database client – server, File client – server, Voice over IP, peer to peer та ін. Під час імітування навантаження кожен клас заявок наочно показується як серія прямокутників певного кольору, що рухаються. Напрям, швидкість рух і проміжки між ними приблизно показують основні характеристки трафіку.

NetCracker має розвинені засоби генерації звітів. Як правило, швидкий звіт, що включає дані по завантаженню усіх вузлів мережі, с допомогою спеціального майстра можна зробити за 1-2 хвилини, з можливістю експорту в HTML-файл.

NetCracker має таку корисну можливість, як розрив і відновлення зв'язків між мережевими пристроями. Це дозволяє промоделювати різні сценарії розриву з'єднань, перевантаження сервера, перевантаження каналу та ін. Ця можливість надзвичайно важлива для адміністратора мережі, оскільки робить можливим моделювання мережі не лише в нормальному режимі, але і в режимі виходу з ладу її окремих елементів.

Достоїнства і недоліки програми моделювання NetCracker зручно продемонструвати на конкретному прикладі. Побудуємо невелику локальну мережу, що складається з одного клієнта, сервера і комутатора між ними (рисунок 4.1). Хоча робоча станція, що виступає клієнтом, тут одна, є можливість задати одночасно декілька класів заявок, генерованих клієнтом і оброблюваних сервером. Це імітує роботу в мережі одночасно декількох клієнтів.

Рисунок 4.1 – Модель локальної мережі в NetCracker Professional

Для побудови вказаної конфігурації були виконані наступні дії:

– З бази цих пристроїв були вибрані Ethernet Workstation, Ethernet Switch і Ethernet Server і "перетягнуті" на робоче поле. У цих пристроях вже передбачається наявність мережевого адаптера Ethernet, тому добавдять його вручну не потрібно.

– Створені зв'язки між клієнтом і комутатором, а також між комутатором і сервером. У властивостях каналу вказувався тип кабелю (вита пара), його довжина і максимальна швидкість передачі (10 Мбіт/с).

– Створені профілі робочих навантажень, які були потім додані в якості трафіку між клієнтом і сервером : 4 класи заявки з розміром пакету 50 байт і 2 класи з розміром пакету 1500 байт, часом підготовки і обробки 2 мс. Виведені індикатори використання каналів передачі і швидкості обробки в клієнтові і сервері.

Після завершення роботи імітації були отримані результати, показані на рисунку 4.2.

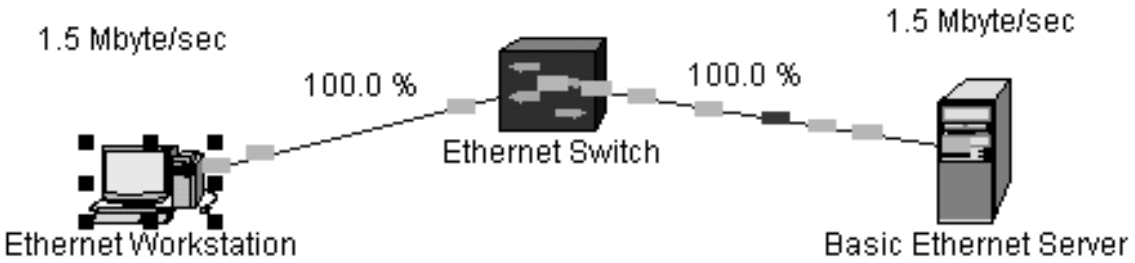

Рисунок 4.2 – Відображення результату моделювання локальної мережі

Цей приклад наочно показує недосконаліть застосованої моделі мережі Ethernet. Ніколи коефіцієнт використання моноканалу не може досягати 100 %. По-перше, метод доступу до середовища CSMA/CD стає неефективним при завантаженості більше 50-60%. З її збільшенням вище цієї цифри, поточна пропускна здатність практично не збільшується.

По-друге, обов'язкові часові інтервали між пакетами також знижують пропускну здатність.

NetCracker враховує тільки максимальну пропускну здатність моноканалу. Моделювання функціонування протоколу Ethernet спрощене до крайності.

По суті, розрахунок поточної пропускної здатності моноканалу зводиться до простої формули:

$$U = \max(Q_{max}, Q_{gen})/Q_{max} * 100\ \%, \qquad (4.1)$$

де U – коефіцієнт використання моноканалу;

Qmax – максимальна пропускна здатність без урахування витрат на очікування між передачею пакетів, біт/с;

Q_{gen} – пропускна здатність, затребувана від моноканалу станцією, біт/с;

$Q_{gen} = \Sigma Q_i (Q_i)$ – навантаження від кожного класу заявки, біт/с.

Примітивність використаної моделі мережі стала розплатою за багаті можливості по моделюванню найрізноманітнішої мережевої архітектури.

Не вникаючи в подробиці функціонування, легко представити цілий сегмент мережі як область, яка просто сполучається з іншими пристроями через канали зв'язку із заданою пропускною здатністю і заданою завантаженістю.

Такою ж областю може бути і окрема робоча станція, і ціла регіональна мережа.

4.2 Опис можливостей програми КОМПАС для побудови креслень при проектуванні комп'ютерних мереж

КОМПАС – це сімейство систем автоматизованого проектування з можливостями оформлення проектної і конструкторської документації згідно із стандартами серії ЄСКД і СПДС. Розробляється російською компанією "АСКОН".

Система орієнтована на підтримку стандартів ЄСКД і СПДС.

КОМПАС здатний автоматично генерувати асоціативні види тривимірних моделей (у тому числі розрізи, перерізи, місцеві розрізи, місцеві види, види по стрілці, види з розривом). Усі вони асоційовані з моделлю: зміни в моделі призводять до зміни зображення на кресленні.

Стандартні види автоматично будуються в проекційному зв'язку. Дані в основному написі креслення (позначення, найменування, маса) синхронізуються з даними з тривимірної моделі.

Існує велика кількість додаткових бібліотек до системи КОМПАС, що автоматизують різні спеціалізовані завдання. Наприклад, бібліотека стандартних виробів дозволяє додавати вже готові стандартні деталі в тривимірні складки (кріпильні вироби, підшипники, елементи трубопроводів, шпонки, ущільнення), а також графічні позначення стандартних елементів на креслення (позначення отворів), надаючи можливість завдання їх параметрів.

КОМПАС існує в декількох версіях:

– КОМПАС-графік.
– КОМПАС-СПДС.
– КОМПАС-3D.
– КОМПАС-3D LT.

Можливості кожної з версії представлені в таблиці 4.1.

Таблиця 4.1 – Порівняння продуктів сімейства КОМПАС

Функція	КОМПАС-графік	КОМПАС-СПДС	КОМПАС-3D	КОМПАС-3D LT
Можливість комерційного використання	Так	Так	Так	Ні
Створення креслень будь-якої складності	Так	Так	Так	Так
Тривимірне моделювання деталей	Ні	Ні	Так	Так
Тривимірне моделювання складок	Ні	Ні	Так	Ні
Поверхневе моделювання	Ні	Ні	Так	Так
Створення текстових документів	Так	Так	Так	Ні
Створення специфікацій	Так	Ні	Так	Ні
Імпорт DXF і DWG	Так	Так	Так	Так
Імпорт 3D-форматов	Ні	Ні	Так	Обмежені можливості
Експорт документів в інші системи	Так	Так	Так	Ні

КОМПАС-графік може використовуватися як повністю інтегрований в КОМПАС-3D модуль роботи з кресленнями і ескізами, так і в якості самостійного продукту, що повністю закриває завдання 2D-проектирования і випуску документації. А КОМПАС-3D LT є втіленою некомерційною версією КОМПАС-3D.

Для проектування комп’ютерних мереж потрібні лише засоби 2D-креслення, тому КОМПАС-графік може в повному ступені задовольняти необхідним вимогам.

КОМПАС-графік дозволяє в швидкісному режимі випускати креслення виробів, схеми, специфікації, різні текстові документи, таблиці, інструкції і інші документи. Гнучкість налаштування системи і велика кількість прикладних

бібліотек і застосувань для КОМПАС-графік дозволяють закрити практично усі завдання користувача, пов'язані з випуском технічної документації.

Система КОМПАС-графік надає щонайширші можливості автоматизації проектно-конструкторских робіт в різних галузях промисловості. Він успішно використовується в машинобудівному проектуванні, при проектно-будівельних роботах, складанні різних планів і схем.

КОМПАС має ряд недоліків. Він не підтримує відкриття і редагування створених в пізніших версіях застосування проектів більше ранніми. Також є проблема сумісності версії LT з повнофункціональною версією.

Ці факти змушують використати одну версію програми на усіх етапах виробництва, що на великих підприємствах може викликати деякі утруднення.

КОМПАС на відміну від AutoCAD не містить засобу для розрахунку міцності, динаміки, кінематики модельованого об'єкту. Проте це не є великим мінусом програми, оскільки при проектуванні комп’ютерних мереж подібні компоненти не використовуються.

5 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 програмного продукту для мобільної платформи. Розробка такого продукту вимагатиме певних затрат. Тому розрахуємо ці затрати.

Для здійснення оцінки потрібно зробити розрахунки трудомісткості кожної операції.

5.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР

Витрати часу по окремих операціях технологічного процесу відображені в таблиці 5.1.

Таблиця 5.1 – Операції технологічного процесу та час їх виконання

№	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1.	Витрати праці на підготовку опису задачі	інженер	10
2.	Витрати праці на розробку проекту	інженер	15
3.	Витрати праці на розробку структури системи	інженер	10
4.	Витрати праці на створення системи по вибраному проекту та структурі	інженер	75
5.	Витрати праці на підготовку документації	інженер	15
6.	Витрати праці на відлагодження роботи зпроектованої системи при комплексній відладці	інженер	40
Разом			165

Загальні затрати на дипломний проект становить 165 годин.

5.2 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:

$$З_{осн.} = Т_с \cdot К_г \,, \qquad (5.1)$$

де T_c – тарифна ставка, грн.;

$K_г$ – кількість відпрацьованих годин.

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

$$З_{осн.} = 30 \cdot 165 = 4950 \text{ грн.}$$

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

$$З_{дод.} = З_{осн.} \cdot К_{допл.}, \quad (5.2)$$

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

$$З_{дод.} = 4950 \cdot 0,15 = 742,50 \text{ грн.}$$

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

$$В_{о.п.} = З_{осн.} + З_{дод.}. \quad (5.3)$$

$В_{о.п.}$=4950+742,50 = 5692,50 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:

$$В_{с.з.} = Ф_{оп} \cdot 0,235, \quad (5.4)$$

де $Ф_{ОП}$ – фонд оплати праці, грн.

$$B_{с.з.} = 5692{,}50 \cdot \ 0{,}235 = 1337{,}74 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 5.2.

Таблиця 5.2 – Зведені розрахунки витрат на оплату праці

№ п/п	Категорія працівник-ків	Основна заробітна плата, грн.			Додаткова заробітна плата, грн.	Нарахув. на $Ф_{ОП}$, грн.	Всього витрати на оплату праці, грн. *6=3+4+5*
		Тарифна ставка, грн.	К-сть відпра-цьов. год.	Фактично нарах. з/пл., грн.			
А	Б	1	2	3	4	5	6
1	інженер	30	165	4950	742,50	1337,74	7030,24

Загальні витрати на оплату праці становить 7030,24 грн.

5.3 Розрахунок матеріальних витрат

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

$$M_{Bi} = q_i \cdot p_i, \qquad (5.5)$$

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

p_i – ціна матеріалу *i*-го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$З_{м.в.} = \sum M_{Bi}. \qquad (5.6)$$

Проведені розрахунки занесемо у таблицю 5.3. Для розробки ПЗ передбачається покупка Visual Studio Team Foundation Server CAL SNGL LicSAPk OLP NL UsrCAL 2017, вартість якого на сьогодні становить 19400 грн.

Таблиця 5.3 – Зведені розрахунки матеріальних витрат

Найменування матеріальних ресурсів	Одиниця виміру	Норма витрат	Ціна за одиницю, грн	Затрати матеріалів, грн	Транс-портно-заготівель-ні витрати, грн	Загальна сума витрат на матеріа-ли, грн
1. Основні матеріали						
Програмне забезпечення	комп.	1	19400,00	19400,00	–	19400,00
2. Допоміжні матеріали						
Папір формату А4	шт.	200	0,18	36	–	36
Разом:						19436,00

Загальні матеріальні затрати становлять 19436,00 гривень.

5.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1-ці обладнання визначаються за формулою:

$$З_е = W \cdot T \cdot S \,, \qquad (5.7)$$

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 5.1 – 165 годин.

Тоді, $З_е = 0{,}55 \cdot 175 \cdot 2{,}42 = 219{,}62$ грн.

5.5 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:

$$A = \frac{Б_В \cdot Н_А}{100\%}, \qquad (5.8)$$

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 17400 грн. Отже, амортизаційні відрахування будуть рівні:

$$A = 17400 \cdot 5\% / 100\% = 870{,}00 \text{ грн.}$$

Оскільки робота виконувалась 165 годин, то амортизаційні відрахування будуть становити:

$$A = 870{,}00 \cdot 175 / 150 = 1015{,}00 \text{ грн.}$$

5.6 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.

$$H_в = B_{о.п.} \cdot 0{,}2 \ldots 0{,}6 \,, \qquad (5.9)$$

де H_B – накладні витрати.

Отже, накладні витрати:

H_B = 5692,00 · 0,2 = 1138,50 грн.

5.7 Складання кошторису витрат та визначення собівартості НДР

Результати проведених вище розрахунків зведемо у таблицю 5.4.

Таблиця 5.4 – Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до загальної суми
Витрати на оплату праці (основну і додаткову заробітну плату)	5692,50	19,7%
Відрахування на соціальні заходи	1337,74	4,6%
Матеріальні витрати	19436,00	67,4%
Витрати на електроенергію	219,62	0,8%
Амортизаційні відрахування	1015,00	3,5%
Накладні витрати	1138,50	3,9%
Собівартість	28839,35	100,0%

Собівартість (C_B) проекту розрахуємо за формулою:

$$C_в = B_{о.п.} + B_{с.з.} + З_{м.в.} + З_в + А + Н_в. \qquad (5.10)$$

Отже, собівартість проекту дорівнює:

$C_в$ = 5692,50 + 1337,74 + 19436 + 219,62 + 1015,00 + 1138,50 = 28839,35 грн.

5.8 Розрахунок ціни проекту

Ціну НДР можна визначити за формулою:

$$Ц = \frac{C_B \cdot (1 + P_{рен}) + K \cdot B_{н.і.}}{K} \cdot (1 + ПДВ), \quad (5.11)$$

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 $B_{і.н}$, оскільки їх в даному випадку не потрібно.

Тоді, формула для обчислення ціни розробки буде мати вигляд:

$$Ц = C_B \cdot (1 + P_{рен}) \cdot (1 + ПДВ). \quad (5.12)$$

Звідси ціна на проект складе:

Ц = C_B · (1+0,3)(1+0,2) = 44989,39 грн.

5.9 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 ($E_р$) полягає у відношенні результату виробництва до затрачених ресурсів:

$$E_р = П / C_B, \quad (5.13)$$

де $П$ – прибуток;

$С_В$ – собівартість.

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

$$П_{пл} = Ц - С_В . \quad (5.14)$$

Розраховуємо плановий прибуток:

$П_{пл}$ = 44989,39 – 28839,35 = 16150,04 грн.

Отже, формула для визначення економічної ефективності набуде вигляду:

$$E_р = \frac{П_{пл}}{Св} . \quad (5.15)$$

Тоді, $E_р$ = 16150,04 / 28839,35 = 0,56

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

$$Т_р = 1/ E_р , \quad (5.16)$$

Термін окупності дорівнює:

$Т_р$ = 1/0,56 = 1,8 роки.

В цьому розділі дипломної роботи було розраховано основні техніко-економічні показники проекту (див. таблицю 5.5).

Розраховане значення економічної ефективності становить 0,56 що є високим значенням.

Так само нормальним є термін окупності. Для даного продукту він становить 1,8 роки.

Таблиця 5.5 – Техніко-економічні показники НДР

№ п/п	Показник	Значення
1.	Собівартість, грн.	28839,35
2.	Плановий прибуток, грн.	16115,04
3.	Ціна, грн.	44989,39
4.	Економічна ефективність	0,56
5.	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.

РОЗІДЛ 6
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

6.1 Предмет та зміст безпеки життєдіяльності

Середовище існування – оточуюче людину середовище, яке обумовлене сукупністю діючих на цей час факторів – природного, суспільного, матеріального, духовного та іншого характеру. Основними властивостями цих факторів є їх здатність впливати на діяльність людини, її здоров'я та нащадків. Характер впливу, що реалізується, може бути безпосереднім, побічним, негайним чи віддаленим.

Метою вивчення дисципліни «Безпека життєдіяльності» є:

− підготовка людини до повноцінного життя в суспільстві, що динамічно змінюється;

− формування загальних системних уявлень;

− формування знань з питань методичного забезпечення в галузі обґрунтування рішень безпеки і їх здійснення в практиці сільськогосподарського виробництва.

Об'єктом вивчення дисципліни "Безпека життєдіяльності" є людина. Основними її потребами є:

1) фізіологічні;
2) особиста безпека;
3) соціальні;
4) престиж;
5) духовні.

Головним завданням досягнення особистої безпеки є гармонізація цієї потреби з потребами суспільства і держави.

БЖД – це наукова дисципліна, що вивчає небезпеку і захист від неї.

Мета БЖД – досягнення безпеки людини в місці існування. Безпека людини визначається відсутністю виробничих і невиробничих аварій, стихійних і інших природних лих, небезпечних чинників, що викликають травми або різке погіршення здоров'я, шкідливих чинників, що викликають захворювання людини і котрі знижують його працездатність.

До предметів вивчення БЖД можна віднести фізіологічні і психологічні можливості людини з погляду БЖД, формування безпечних умов і їх оптимізації тощо.

Досягнення гармонізації на базі загальної безпеки дає змогу скласти основу до реалізації всього комплексу потреб людини і забезпечити стабілізацію її психічного стану за рахунок відчуття особистої захищеності індивіда і суспільства від загроз, створених навколишнім середовищем.

Безпека діяльності людини – це сукупність:

− властивостей навколишнього середовища, які не завдають шкоди людині в процесі її діяльності;

− якостей людини та заходів і засобів, які запобігають можливій шкоді її здоров'ю.

Виходячи з визначеної сукупності, основним завданням дисципліни є розробка системи, що забезпечує безпеку життєдіяльності людини, суспільства та держави.

Структура вивчення безпеки життєдіяльності пов'язана з логікою встановлення безпеки. В основу системи встановлення безпеки кладуться теоретичні основи дисципліни, які в формулюються у вигляді відповідних елементів, та передумови, які сформовані у вигляді теоретичних основ (чи їх елементів). Цей розділ забезпечує встановлення змісту і розв'язання проблем в безпеці життєдіяльності, в питаннях наявності небезпек, взаємодії їх з людиною, наслідки розвитку негараздів, формування стабільних комфортних умов.

6.2 Аналіз умов праці розробника програмного забезпечення

6.2.1 Загальна характеристика умов праці

В приміщенні бухгалтерії підприємства є місця для роботи трьох чоловік. Розміри приміщення наведені у таблиці 6.2.

Згідно СН-245-71, на одного працюючого об'єм приміщення повинен складати не менше 19,5 м^2, а площа – не менше 6 м^2.

Число працюючих у приміщенні Np=3.

Таким чином, на кожного працюючого виходить приблизно 22,6 м^3 і 6,6 м^2, отже, усі вимоги тут дотримані.

Таблиця 6.2 – Розміри приміщення

l	довжина	5 м
d	ширина	4 м
h	висота	3,4 м
S_0	площа	20 м^2
V_0	об'єм	68 м^3

Далі, відповідно до норм, повинні дотримуватися:

– ширина основних проходів, не менше: – 1200 мм

– ширина допоміжних проходів, не менше: – 700 мм

– відстань між двома столами, якщо між ними є стілець, не менше: – 1300 мм

У розглянутому приміщенні:

– ширина основних проходів: – 2000 мм

– відстань між двома комп'ютерами у ряді: – 1500 мм

Отже, норми виконуються.

6.2.2 Повітряне середовище

Шляхом провітрювання і центральної системи опалення у приміщенні бухгалтерії завжди підтримується:

– стабільна температура повітря , що становить 25 °С;

– відносна вологість повітря 55 %.

При зниженні тиску погіршується відвід тепла від елементів ЕОМ, знижуються ізоляційні властивості повітря. Показники об’єму і площі приміщення на одного працюючого відповідають нормативним значенням.

Роботи, що проводяться в бухгалтерії відносяться до легких фізичних робіт групи 1а, відповідно до ГОСТ 12.1.005-88, тому що вони проходять сидячи і не вимагають фізичного навантаження, проводяться при нормальних метеорологічних умовах і не викликають забруднення одягу і рук. Витрати енергії не перевищують 172 Дж/с (155 Ккал/год).

У таблиці 6.3 і 6.4 наведені норми температури, відносної вологості і швидкості руху повітря на робочих місцях відповідно ГОСТ 12.1.005-88, що встановлює норми виробничого мікроклімату. Дані приведені для приміщень з незначним надлишком явного тепла (до 20 Ккал/год $м^3$) для виконання легких робіт.

Таблиця 6.3 – Норми температури, відносної вологості і швидкості руху повітря на постійних робочих місцях

Період року	Норми	Температура повітря t, ^{0}C	Відносна вологість, %	Швидкість руху повітря, м/с
холодний	оптим.	20-22	30-60	менше ніж 0,2
	доп.	17-22	менше 75	менше ніж 0,3
теплий	оптим.	20-25	30-60	0,2-0,3
	доп.	менше ніж 28	менше ніж 80*	0,3-0,5
* - у теплий період року припустима відносна вологість повітря для всіх приміщень і категорій робіт має значення, приведені в таблиці 6.4				

Таблиця 6.4 - Відносна вологість повітря в теплий період року

Температура повітря,	28	27	26	25	2	<=
Відносна вологість, %	>=	60	65	70	7	75

Основними джерелами тепла в приміщенні є:

- сонячна радіація;
- система опалення;
- люди, що працюють у приміщенні;
- устаткування.

У таблиці 6.5 наведені дані вимірювання в приміщенні ОЦ у місяці грудні.

Таблиця 6.5 – Результати виміру параметрів мікроклімату в приміщенні бухгалтерії

Температура повітря t, °C	20 – 25
Відносна вологість, %	50 – 60
Швидкість руху повітря, м/с	0,2

Як видно з таблиці 6.5, у розглянутому приміщенні значення параметрів мікроклімату відповідають нормативним. Стабільність цих параметрів підтримується загальною системою утеплення і кондиціонування повітря.

6.2.3 Освітлення

У приміщенні бухгалтерії використовується природне і штучне освітлення. Природне освітлення здійснюється за допомогою двох вікон загальною площею S=7,5 м^2, що забезпечує коефіцієнт природної освітленості Е=1,5%. Це відповідає СНиП І-4-79.

Штучне освітлення в бухгалтерії здійснюється системою загального рівномірного освітлення, що реалізована на основі люмінесцентних ламп типу ЛДЦ-40-1, які мають наступні параметри:

- висока світловіддача;
- тривалий термін служби;

– мала яскравість освітлювальної поверхні;

– близькість спеціального складу до природного освітлення.

Робота за монітором ПЕОМ по розряду зорових робіт відноситься до III типу (роботи високої точності з розміром об'єкта 0,2–0,4 мм). При загальному освітленні, освітленість робочого місця повинна складати від 200 до 400 лк.

При штучному освітленні нормуються наступні параметри:

- *E* (лк) – найменша припустима освітленість;
- *M* – показник дискомфорту;
- *Кп* (%) – коефіцієнт пульсації освітлення.

Перевіримо відповідність фактичних параметрів штучного освітлення в приміщенні нормам. Номінальний світловий потік лампи білого свічення ЛДЦ-40-1: *Фл* = 3120 лм.

У приміщенні застосовуються світильники, у яких встановлені дві лампи. Висоту підвіски світильника визначимо по формулі:

$$h = H - h_C - h_P - h_П, \quad (6.1)$$

де:

H – висота приміщення, м.;

h_C – висота світильника, м.;

$h_П$ – відстань від стелі до підвіски, м.;

h_P – висота робочої поверхні, м.;

Для розглянутого приміщення:

H = 3,4 м,

h_C = 0,15 м,

$h_П$ – 0 м, (підвісу немає)

h_P = 0,8 м.

Ззвідси *h* = 3,4 – 0,15 – 0,8 = 2,45м.

Світильники розташовані в 2 ряди. Висота підвіски світильників складає 2,45 метра відносно підлоги, відстань між рядами 1 м, відстань від ряду до стіни 1,5 метра. Приміщення має наступні габарити:

- довжина *A* = 5 метрів;
- ширина *B* = 4 метрів.

Визначимо освітленість у робочій точці. Для розрахунку загальної рівномірної освітленості при горизонтальній робочій поверхні використовуємо метод коефіцієнта використання світлового потоку.

Розрахункова формула для світлового потоку світильника має такий вигляд:

$$Фл = \frac{E \cdot Кз \cdot S \cdot Z}{N \cdot n}, \qquad (6.2)$$

де N - кількість світильників у приміщенні, $N = 3 \cdot 2 = 6$;

n - коефіцієнт використання світлового потоку;

$Фл$ - світловий потік ламп;

$Кз$ - коефіцієнт запасу, $Кз = 1{,}5$;

Z - коефіцієнт нерівномірності;

S - площа приміщення;

E - освітленість, створювана усіма світильниками.

Звідси одержуємо формулу для розрахунку освітленості на робочому місці :

$$E = \frac{Фл \cdot N \cdot n}{Кз \cdot S \cdot Z} \qquad (6.3)$$

Коефіцієнт використання світлового потоку залежить від:

- ККД кривої розподілу сили світла світильника;
- коефіцієнта відбивання стелі $R_П$ і стін $R_С$,;
- висоти підвісу світильників $h_П$;
- показника приміщення i:

$$i = \frac{A \cdot B}{h \cdot (A + B)} \quad . \qquad (6.4)$$

$i = (5 \bullet 4) / (2{,}45 \bullet (5 + 4)) = 0{,}408$

Стеля і стіни пофарбовані в білий колір.

Приймаємо:

$R_П$ = 50%

$R_{С,}$ = 30%.

Звідси:

n = 31%.

$$E = \frac{(3120 \cdot 2) \cdot 6 \cdot 0{,}31}{20 \cdot 1{,}1 \cdot 1{,}5} = 352 лк$$

Так як по розряду зорової роботи робота за дисплеєм ПЕОМ відноситься до III типу (високої точності, розмір об'єкта 0.2-14 мм), то при загальному висвітленні освітленість робочого місця повинна складати від 200 до 400 лк, рекомендована освітленість при роботі з дисплеєм ПЕОМ складає 200 лк, а при сполученні роботи з документами 400 лк. Фактична освітленість на робочому місці складає 352 лк.

Таким чином для роботи з дисплеєм цілком достатньо існуючих джерел світла, однак робота з документами повинна вестися при природному освітленні, або за допомогою додаткових місцевих джерел освітлення.

7 ЕКОЛОГІЯ

7.1 Сталий розвиток як парадигма суспільного зростання

На думку багатьох вчених, що займаються розробкою концепції розвитку, головним пріоритетом повинний стати розгляд цілісного еколого-економічного підходу до економічного зростання, зміни техногенного типу розвитку на сталий. Необхідні зміна існуючої економічної парадигми, нові концепції збалансованого і стійкого розвитку для запобігання глобальному і локальних екологічних криз

Питання сталого екологічного розвитку є дуже актуальними для України, яка нині переживає глибоку еколого-економічну кризу. Це викликано тим, що тривалий час домінував принцип — одержання максимальної вигоди при мінімальних затратах.

При цьому мали місце неузгодженість темпів економічного розвитку і вимог екологічної безпеки, домінування природомістких галузей з високою питомою вагою ресусо- і енергомістких застарілих технологій, сировинна орієнтація експорту, мілітаризація виробництва, відсутність культури праці та споживання тощо.

Все це привело до формування техногенного типу економічного розвитку. І, як наслідок, нині антропогенне навантаження на природу наближається (а в деяких регіонах України наблизилося) до граничної межі її екологічної стійкості. За нею починаються кризові та катастрофічні зміни в природі, що негативно впливає на життєдіяльність людини і суспільства.

Під техногенним тилом розвитку слід розуміти природоємкісний (природоруйнуючий) тип розвитку, що базується на використанні штучних засобів виробництва, створених без урахування екологічних обмежень.

Характерними рисами такого розвитку є швидке і виснажуюче використання невідновлюваних видів природних ресурсів (передусім корисних копалин) і надмірна експлуатація відновлюваних ресурсів (ґрунту, лісів і ін.) з швидкістю, що перевищує можливості їх відтворювання і відновлення.

При цьому наноситься значний економічний збиток, що є вартісною оцінкою деградації природних ресурсів і забруднення навколишнього середовища внаслідок людської діяльності.

Для техногенного типу економічного розвитку притаманні значні зовнішні ефекти. У природокористуванні їх можна охарактеризувати як негативні еколого-економічні наслідки економічної діяльності, які не приймаються до уваги суб'єктами цієї діяльності.

Будь яка країна, що стала на шлях науково-технічного прогресу та широкомасштабного використання його результатів, вже не може і не повинна ігнорувати такі об'єктивні чинники, як вичерпаність багатьох природних ресурсів, насамперед невідтворювальних і невідновлюваних, вразливість навколишнього середовища, екологічну стійкість та екологічну місткість довкілля, межі його екологічної міцності і опірності щодо негативних і шкідливих антропогенних впливів тощо.

Всі ці чинники необхідно всебічно враховувати в господарській діяльності і при визначенні темпів та масштабів соціально-економічного розвитку на майбутнє. Цей розвиток має бути врівноваженим і адекватним екологічній ситуації, узгоджуватися з природничими законами. А це можливо тільки за умови, що виробниче господарська діяльність суспільства ґрунтуватиметься на концепції сталого екологічного розвитку.

Зараз в літературі є більше за 60 визначень сталого розвитку. Найбільш поширене визначення, дане в доповіді комісії Брундтланд: сталий розвиток -це такий розвиток, який задовольняє потреби теперішнього часу, але не ставить під загрозу здатність майбутніх поколінь задовольняти свої власні потреби. Воно містить два ключових поняття:

– поняття потреб, зокрема потреб, необхідних для існування найбідніших верств населення, які повинні бут" предметом першорядного пріоритету;

– поняття обмежень, зумовлених станом технології і організацією суспільства, що накладаються на здатність навколишнього середовища задовольняти нинішні і майбутні потреби.

Є і більш короткі визначення сталого розвитку, що відображають його окремі важливі економічні аспекти. Серед таких визначень можна виділити наступні:

– розвиток, який не покладає додаткові витрати на наступні покоління;

– розвиток, який мінімізує екстерналії, зовнішні ефекти між поколіннями;

– розвиток, який забезпечує постійне просте і/або розширене відтворення виробничого потенціалу на перспективу;

– розвиток, при якому людству необхідно жити тільки на проценти з природного капіталу, не торкаючись його самого.

Приведене вище визначення сталого розвитку можна розглядати і крізь призму економічних відносин поколінь: всередині сучасного покоління (зокрема, соціальний аспект, проблема бідності) і між поколіннями (еколого-економічний аспект).

Теорія сталого розвитку є не тільки найбільш популярною новою теорією останнього десятиріччя (сотні конференцій, тисячі монографій, підручників і т. д.), але і цілком "практичною" теорією: всі розвинені держави світу виразили прагнення слідувати у напрямі до стійкого розвитку.

Практично всі концептуальні і "поважаючі себе" офіційні державні і міжнародні документи за останні роки в якості базової ідеології використовують поняття сталого розвитку.

Центральне місце в понятті сталого розвитку займає проблема врахування довгострокових екологічних наслідків. Необхідна мінімізація негативних екологічних наслідків, майбутніх екстерналій для наступних поколінь. Неможна жити за рахунок своїх дітей і внуків, неможна витрачати природну скарбницю тільки для себе.

Таким чином, проблема екологічних обмежень, компромісу між поточним і майбутнім споживанням повинна бути основною при визначенні темпів соціально-екологічного розвитку для будь-якої країни.

Як показує історія людства, радикальні економічні зміни останніх років, проекти і заходи, здійснювані відповідно до природних закономірностей, на тривалому тимчасовому інтервалі виявляються економічно ефективними.

І навпаки, економічні проекти, що приносять швидкі і значні вигоди, але здійснені без урахування довгострокових екологічних наслідків, екстерналий, в перспективі часто виявляються збитковими. Отже, для тривалого інтервалу часу дуже часто вірний простий принцип "що екологічне, те економічне".

Можна виділити чотири критерії стійкого розвитку на тривалу перспективу. Даний підхід базується на класифікації природних ресурсів і динаміці їх відтворення:

1. Кількість відновлюваних природних ресурсів (земля, ліс і т. д.) повинна принаймні не меншати протягом часу, тобто повинен бути забезпечений принаймні режим простого відтворення. (Наприклад, для земельних ресурсів це означає збереження площі найбільш цінних сільськогосподарських угідь або у разі зменшення їх площі збереження/збільшення рівня виробництва продукції землеробства, кормового потенціалу земель для сільськогосподарських тварин і т. д.).

2. Максимально можливе сповільнення темпів вичерпання запасів невідновлюваних природних ресурсів (наприклад, корисних копалин) з перспективою в майбутньому їх заміни на інші нелімітовані види ресурсів. (Наприклад, часткова заміна нафти, газу, вугілля на альтернативні джерела енергії-сонячну, вітрову і пр.).

3. Можливість мінімізації відходів на основі впровадження маловідходних, ресурсозберігаючих технологій.

4. Забруднення навколишнього середовища (як сумарне, так і по видах) в перспективі не повинне перевищувати його сучасний рівень. Можливість мінімізації забруднення до соціальне і економічно прийнятного рівня ("нульового" забруднення чекати нереально).

Ці чотири критерії (їх може бути і більше) повинні бути враховані в процесі розробки концепції стійкого розвитку. Їх врахування дозволить зберегти навколишнє середовище для наступних поколінь і не погіршить екологічні умови проживання.

Серед економічних показників ефективними критеріями сталого розвитку є зменшення природоємкості економіки.

Потрібно відмітити важливість зміни споживацької поведінки людей. Перехід до сталого розвитку передбачає обмеження потреб в товарах і послугах, на відміну від техногенного розвитку з його максимізацією споживання, подальшим розквітом суспільства.

Із суто споживацького погляду, чим більше продукції на душу населення виробляється в державі, тим краще. Але збільшення продукції виробництва збільшує техногенне навантаження на природу (більш детально це поняття розглянуто в III розділі) і потребує значних додаткових витрат на екологічні заходи.

Це останнє зумовлює необхідність визначення оптимального співвідношення між виробництвом продукції на душу населення країни і кількістю шкідливих відходів на одиницю поверхні її території. Девізи "Більше споживайте", "Кожному члену сім'ї по автомашині" і т. д. явно вступають в суперечність з можливостями біосфери. Для зміни поведінки важливі екологічне виховання і освіта.

Для більш детального аналізу стійкого розвитку використовуються поняття слабої стійкості і сильної стійкості.

Прихильники сильної стійкості займають жорстку, часто "анти-економічну" позицію з багатьох питань економічного розвитку: стабілізація або зменшення масштабів економіки, пріоритет прямого регулювання, жорстке обмеження споживання і т. д.

Прихильники слабкої стійкості віддають перевагу модифікованому економічному зростанню з урахуванням екологічного вимірювання економічних показників, широкому використанню еколого-економічних інструментів (плата за забруднення і т. д.), зміна споживацької поведінки і т. д.

При всіх відмінностях позицій обидві вони протистоять техногенній концепції розвитку, яка базується па необмеженому розвитку вільного ринку, орієнтації на чисто економічне зростання, експлуатацію природних ресурсів, вірі в нескінченні можливості науково-технічного прогресу, максимізації споживання і т. д. (Звичайно, самі прихильники техногенного підходу на словах виступають за охорону природи, однак їх підходи і дії часто носять антиекологічний характер).

Істотна відмінність перерахованих трьох підходів полягає у відношенні до можливої заміни природного капіталу на штучний (антропогенний). У якій мірі можлива заміна природних ресурсів, благ на засоби виробництва, що створюються людиною? Техногенний підхід говорить про нескінченні можливості заміни природного капіталу внаслідок розвитку вільного ринку і технічного прогресу.

Прихильники слабкої стійкості виступають за самі широкі можливості такої заміни, однак при збереженні загального агрегованого запасу капіталу. У концепції сильної стійкості передбачаються лише мінімальні можливості заміни природного капіталу на штучний.

На думку багатьох вчених, що займаються розробкою концепції розвитку, головним пріоритетом повинний стати розгляд цілісного еколого-економічного підходу до економічного зростання, зміни техногенного типу розвитку на сталий. Необхідні зміна існуючої економічної парадигми, нові концепції збалансованого і стійкого розвитку для запобігання глобальному і локальних екологічних криз.

7.2 Джерела теплового забруднення атмосфери і методи його зменшення

Останнім часом дедалі актуальнішою постає проблема теплового забруд-нення довкілля, яке пов'язане з нагріванням атмосфери, гідросфери, і що призво-дить до змін флори і фауни в окремих регіонах і суттєво впливає на глобальне по-тепління на Землі в цілому. Теплове (термальне) забруднення довкілля нерозрив-но пов'язане з явищем парникового ефекту.

Антропогенний вплив (домінуючим серед якого є промисловий) на довкіл-ля призводить до «підігрівання» атмосфери внаслідок спалювання великої кіль-кості вугілля, нафти, газу шляхом прямого викидання тепла у довкілля і при охо-лодженні технологічних нагрітих вод, а також нагрівання природних водоймищ

внаслідок скидання підігрітих вод з промислових підприємств і теплових елект-ростанцій в ріки й озера.

Серед найбільших техногенних джерел теплового забруднення довкілля слід відзначити об'єкти теплоелектроенергетики та теплопостачання,

металургій-ні підприємства, транспорт, підприємства, де використовується нагріта вода чи водяна пара, випаровувальні або охолоджувальні башти (градирні) тощо.

Так, викиди підприємств чорної металургії мають температуру 300–400°С, а іноді й близько 800°С. У деяких промислових районах концентрація теплової енергії за рахунок промисловості значно зросла, над промисловими центрами, де теплові аномалії вже на кілька градусів перевищують норму, з'явились теплові ореоли. Їх добре помітно на космічних знімках земної поверхні.

Найбільші проблеми термального забруднення пов'язані з теплоелектроенергетикою. Незважаючи на низку недоліків, притаманних електростанціям, де для вироблення електроенергії використовується водяна пара, зокрема низька ефективність використання потенційної енергії вугілля (37–39%) і ядерної енергії (31%), вони продовжують існувати.

Викиди теплоти є одним з основних чинників взаємодії теплоенергетичних об'єктів з навколишнім середовищем, частково з атмосферою і гідросферою. Ви-ділення тепла відбувається на всіх стадіях перетворення хімічної енергії органіч-ної речовини чи ядерного палива для вироблення теплової енергії. Велика части-на теплоти, яку отримує охолоджувальна вода в конденсаторах парових турбін, передається у охолоджувальні споруди, водойми, водостоки, а звідти в атмосферу (температура в місці скидання нагрітої води підвищується, що призводить до під-вищення середньої температури поверхні водойми, і відповідно температура ат-мосферного повітря над теплоенергетичною установкою підвищується завдяки енергії, виділеній цією установкою в атмосферу).

Так, для електростанції потужністю 1000 МВт потрібно озеро площею 810 га, глибиною близько 8,7 м.

Електростанції можуть підвищувати температуру води в порівнянні з на-вколишньою на 5–15°С. Якщо температура води у водоймі становить 16 °С, то температура відпрацьованої на станції води буде від 22 до 28°С. У літній період вона може досягати 30–36°С.

Підвищення температури води здатне порушити структуру рослинного сві-ту водойм. Характерні для холодної води водорості заміняються більш теплолю-бними і, зрештою, за високих температур цілком ними витісняються.

Усі перелічені вище наслідки теплового забруднення водойм та атмосфери наносять величезну шкоду природним екосистемам і призводять до згубних змін середовища існування людини.

Збитки, що утворилися в результаті теплового забруднення, можна ро-зділити на:

– економічні (втрати внаслідок зниження продуктивності водойм, витрати на ліквідацію наслідків від забруднення тощо);

– соціальні (естетичні втрати від деградації ландшафтів, шкода рекреацій-ним ресурсам тощо);

– екологічні (необоротні руйнування унікальних екосистем, зникнення ви-дів, генетичний збиток тощо).

На сучасному етапі проблема взаємодії промислових об'єктів – джерел теплових викидів у довкілля, і навколишнього середовища набула нових ознак, поширюючи свій вплив на значні території, велику кількість річок і озер, величезні об'єми атмосфери і гідросфери.

Вирішенню цієї проблеми повинен сприяти науково-технічний прогрес за умови його екологізації, що сприятиме розробці нових технологій охолодження або більш економічних методів та обладнання з усунення теплового забруднення.

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.

ДОДАТКИ

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.