МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра інформаційно-обчислювальних систем і управління

МОГИЛЬСЬКА Марія Богданівна

Модель оцінювання надійності веб-сайтів / Model for Evaluating Website Reliability

спеціальність: 122 – Комп'ютерні науки
освітньо-професійна програма – Комп'ютерні науки

Кваліфікаційна робота

Виконала студентка групи
КНм-21
М. Б. Могильська
_____

Науковий керівник:
к.е.н., доцент Г. М. Гладій
_____

Кваліфікаційну роботу
допущено до захисту:
«___» _____ 2022 р.
Завідувач кафедри
_____ М. П. Комар

ТЕРНОПІЛЬ – 2022

Факультет комп'ютерних інформаційних технологій
Кафедра інформаційно-обчислювальних систем і управління
Освітній ступінь «магістр»
Спеціальність 122 Комп'ютерні науки
Освітньо-професійна програма «Комп'ютерні науки»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____М. П. Комар
«____» _____2021 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
Могильська Марія Богданівна
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи:
Модель оцінювання надійності веб-сайтів / Model for Evaluating Website Reliability
керівник роботи: к.е.н., доцент Гладій Г. М.,
затверджені наказом по університету від 31 грудня 2021 року №606.

2. Строк подання студентом закінченої кваліфікаційної роботи: 16 листопада 2022 року.

3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.

4. Основні питання, які потрібно розробити:
- уточнити поняття надійності вебсайту в аспекті його «вузького» і «широкого» трактування;
- виявити критерії оцінювання надійності та метрики її вимірювання;
- проаналізувати методи оцінювання надійності вебсайтів;
- розробити багатокритеріальну модель оцінювання надійності вебсайтів;
- провести апробацію моделі оцінювання надійності вебсайтів;
- дати рекомендації для підвищення надійності вебсайтів.

5. Перелік графічного матеріалу у роботі:
- схема моделі на основі Fuzzi-AHP;
- діаграми результатів оцінювання надійності вебсайтів.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 3 грудня 2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів кваліфікаційної роботи	Примітка
1	Теоретичні аспекти надійності вебсайту та її оцінювання	12.2021 р. – 03.2022 р.	
2	Методи аналізу надійності вебсайту та розроблення моделі її оцінювання	03.2022 р. – 05.2022 р.	
3	Апробація моделі оцінювання надійності вебсайту	05.2022 р. – 11.2022 р.	
4	Повне завершення та представлення кваліфікаційної роботи на кафедру	16.11.2022 р.	

Студентка _____ М. Б. Могильська

Керівник роботи _____ к.е.н., доцент Г. М. Гладій

РЕЗЮМЕ

Кваліфікаційна робота за освітньо-професійною програмою «Комп’ютерні науки» спеціальності 122 «Комп’ютерні науки» написана обсягом 108 сторінок і містить 16 таблиць, 21 ілюстрацій, 2 додатки і 53 використаних джерел.

Мета роботи – розробка математичної моделі оцінювання надійності вебсайтів на засадах багатокритеріального підходу.

Методи дослідження: системний підхід, математичне моделювання, багатокритеріальне прийняття рішень, нечітка логіка, експертне оцінювання.

Основні результати дослідження: уточнено поняття надійності вебсайту в аспекті його «вузького» і «широкого» трактування; виявлені критерії оцінювання надійності та метрики її вимірювання; проаналізовано методи оцінювання надійності вебсайтів; розроблено багатокритеріальну модель оцінювання надійності вебсайтів; проведено апробацію моделі оцінювання надійності вебсайтів; дано рекомендації для підвищення надійності вебсайтів.

Ключові слова: НАДІЙНІСТЬ ВЕБСАЙТУ, КРИТЕРІЇ ЯКОСТІ, ЕКСПЕРТНЕ ОЦІНЮВАННЯ, БАГАТОКРИТЕРІАЛЬНА МОДЕЛЬ, НЕЧІТКА ЛОГІКА.

RESUME

Master’s thesis on the educational program "Project Management" in specialty 122 "Computer Science" is 108 pages long and contains 16 tables, 21 illustrations, 2 appendicle, and 53 used sources.

The purpose of the work is to develop a mathematical model for assessing the reliability of websites based on a multi-criteria approach.

Research methods: systematic approach, mathematical modeling, multi-criteria decision-making, fuzzy logic, expert evaluation.

The main results of the study: the concept of website reliability in the aspect of its "narrow" and "broad" interpretation has been clarified; identified criteria for reliability assessment and metrics for its measurement; the methods of assessing the reliability of websites were analyzed; developed a multi-criteria model for evaluating the reliability of websites; the approbation of the website reliability assessment model was carried out; recommendations are given to increase the reliability of websites.

Keywords: WEBSITE RELIABILITY, QUALITY CRITERIA, EXPERT EVALUATION, MULTI-CRITERIA MODEL, FUZZY LOGIC.

ЗМІСТ

Вступ ……... 7
1 ТЕОРЕТИЧНІ АСПЕКТИ НАДІЙНОСТІ ВЕБСАЙТУ ТА ЇЇ ОЦІНЮВАННЯ …… 10
1.1 Поняття надійності програмних систем як характеристики їх якості …….. 10
1.2 Особливості надійності вебсайтів …… 21
1.3 Метрики вимірювання надійності вебсайтів …….. 28
Висновки до розділу 1 ……. 36
2 МЕТОДИ АНАЛІЗУ НАДІЙНОСТІ ВЕБСАЙТУ ТА РОЗРОБЛЕННЯ МОДЕЛІ ЇЇ ОЦІНЮВАННЯ …… 37
2.1 Порівняння методів оцінювання надійності вебсайту ……... 37
2.2 Обґрунтування вибору критеріїв оцінювання надійності вебсайту ……. 49
2.3 Модель експертного оцінювання надійності вебсайту на основі багатокритеріального вибору ……. 62
Висновки до розділу 2 ……. 70
3 АПРОБАЦІЯ МОДЕЛІ ОЦІНЮВАННЯ НАДІЙНОСТІ ВЕБСАЙТУ ……... 71
3.1 Реалізація експерименту з моделлю оцінювання надійності вебсайту …… 71
3.2 Рекомендації з підвищення надійності вебсайтів ……... 76
Висновки до розділу 3 ……. 87
Висновки ……... 88
Список використаних джерел ……. 90
Додаток А. Взірець розробленої анкети для опитування експертів ……... 95
Додаток Б. Копія публікацій автора …….. 96

ВСТУП

Актуальність теми дослідження. Сьогодні вебсайт є невід'ємною частиною іміджу практично будь-якої компанії, а також необхідним інструментом ведення бізнесу для різноманітних інтернет-компаній. Для успішного функціонування вебсайту необхідне чітке розуміння його можливостей, щоб звести до мінімуму ймовірність відмови в роботі та обслуговуванні сайту. Тому для вебсайту як системи, розрахованої на постійну безперебійну роботу, надійність відіграє важливу роль.

Такі компанії, як Amazon, Google або Microsoft, втрачають мільярди доларів щохвилини, якщо їхні системи виходять з ладу, тому їм довелося знайти спосіб забезпечити резервування, відмовостійкість і безперебійну роботу з клієнтами. Відповідальність за це завдання покладено на інженерну надійність сайту.

Інженерія надійності сайту (SRE, Site reliability engineering) передбачає набір принципів і практик, який охоплює аспекти розроблення програмного забезпечення та застосовує їх до проблем інфраструктури й операцій. Основними цілями є створення масштабованих і високонадійних програмних систем. Саме до таких систем належать сучасні вебсайти. Це підкреслює актуальність теми кваліфікаційної роботи.

Під надійністю сайту розуміють його експлуатаційну характеристику, котра визначається ймовірністю безвідмовної роботи сайту протягом певного періоду із збереженням параметрів, встановлених у технічному завданні. Одним з основних показників надійності сайту є можливість безвідмовної роботи. І щоб зменшити ймовірність відмови в обслуговуванні сайту, варто знати кількісне значення цієї характеристики.

Крім того, актуальність дослідження полягає в тому, що останнім часом створюється досить багато сайтів і для уникнення можливих ризиків, пов'язаних з фактичним зростанням кількості користувачів, котра перевищує очікувану, вже на етапі проєктування сайту необхідно оцінювати його надійність.

Проблема надійності вебсайтів має принаймні два аспекти: забезпечення та оцінювання (вимірювання) надійності. Переважно існуюча література присвячена першому аспектові, а питання оцінювання надійності вебсайтів недостатньо опрацьоване.

На даний момент існують немало методів оцінювання «вузької» надійності сайту, таких як аналіз видів і наслідків відмов, аналіз дерев несправностей, аналіз схем функціональної цілісності тощо. Однак «широке» трактування надійності передбачає також забезпечення його безпеки та конфіденційності доступу до ресурсів.

Метою кваліфікаційної роботи є розробка математичної моделі оцінювання надійності вебсайтів на засадах багатокритеріального підходу.

Об'єктом дослідження є процес оцінювання надійності вебсайту, а **предметом дослідження** – модель оцінювання надійності вебсайту.

Для досягнення поставленої мети потрібно вирішити такі завдання:

– уточнити поняття надійності вебсайту в аспекті його «вузького» і «широкого» трактування;

– виявити критерії оцінювання надійності та метрики її вимірювання;

– проаналізувати методи оцінювання надійності вебсайтів;

– розробити багатокритеріальну модель оцінювання надійності вебсайтів;

– провести апробацію моделі оцінювання надійності вебсайтів;

– дати рекомендації для підвищення надійності вебсайтів.

Методи дослідження. Вирішення зазначених завдань проводилося на засадах системного підходу, математичного моделювання, багатокритеріального прийняття рішень, нечіткої логіки, експертного оцінювання.

Наукова новизна дослідження полягає в тому, що:

1) уточнено поняття надійності вебсайту на основі «широкого» трактування надійності;

2) запропоновано математичну модель оцінювання надійності вебсайту із врахуванням багатокритеріальності та нечіткої інформації.

Практична значимість дослідження полягає в тому, що отримані результати дадуть змогу оцінити надійність проєктованого вебсайту та ухвалити правильні рішення для його розвитку.

Апробація і публікації результатів. Результати дослідження доповідалися автором на міжнародній мультидисциплінарній науковій інтернет-конференції «Світ наукових досліджень» (Тернопіль – Пшеворськ, 25-26 жовтня 2022 р.) і міжнародній науковій інтернет-конференції «Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення», (м. Тернопіль, 18-19 жовтня 2022 р.), та опубліковані в матеріалах вказаних конференцій (див. додаток Б).

1 ТЕОРЕТИЧНІ АСПЕКТИ НАДІЙНОСТІ ВЕБСАЙТУ І КРИТЕРІЇ ЇЇ ОЦІНЮВАННЯ

1.1 Поняття надійності програмних систем як характеристики їх якості

Надійність є однією з ключових характеристик якості програмних систем (ПС), до яких належать вебсайти. Тому доречно проаналізувати вимоги та рекомендації міжнародних стандартів як основу для формування вимог щодо якості (у т.ч. і надійності) ПС, а також вимірювання вказаної якості, що зменшить ризики при розробленні, впровадженні та супроводі ПС. Актуальність цього питання підтверджується ще й тим, що ці стандарти прийняті в Україні як національні.

На сьогодні розроблена серія стандартів ISO 25000 SQuaRE (Systems and software Quality Requirements and Evaluation), яка охоплює два основні процеси: специфікація вимог та оцінювання якості ПС. Зокрема в стандарті ДСТУ ISO/IEC 25010:2016 [1] наведено модель якості ПС, яка використовується для встановлення вимог, розроблення показників і вимірювання якості.

По суті модель якості – це сукупність класів характеристик (показників), розбитих на підхарактеристики, кожній з яких властиві певні атрибути (рис.1.1).

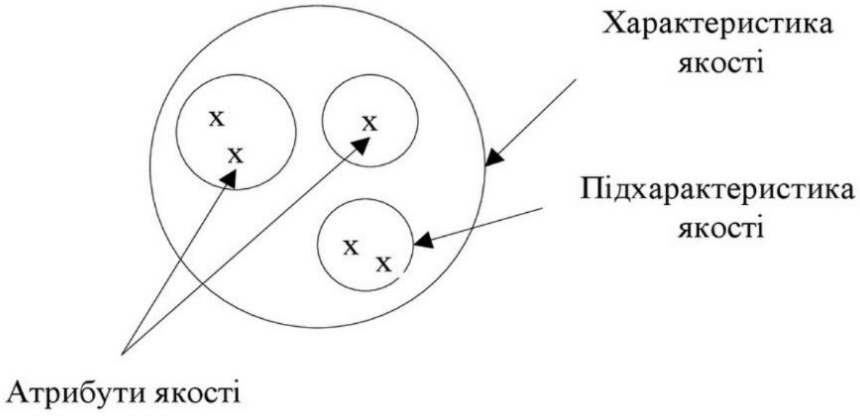


Рисунок 1.1 – Структура моделі якості

Якість у стандартах SQuaRE описується чотирма моделями:

- модель якості у використанні (ISO/IEC 25010);
- модель якості продукту (ISO/IEC 25010);
- модель якості IT-сервісів (ISO/IEC 25011);

– модель якості даних (ISO/IEC 25012).

«Загальний підхід до моделювання якості програмного забезпечення полягає у тому, щоб спочатку ідентифікувати невеликий набір атрибутів якості найвищого рівня абстракції та потім у напрямку «згори-донизу» розбити ці атрибути на набори підлеглих атрибутів. Нижній рівень ієрархії представляє собою безпосередньо атрибути програмного засобу, які підлягають точному опису та вимірюванню. Вимоги якості в свою чергу можуть бути представлені як обмеження на модель якості»[2].

Важливо, щоб характеристики якості були визначені, виміряні та оцінені з використанням перевірених чи поширених показників і методів вимірювання. Для ідентифікації відповідних характеристик якості, які можуть надалі використовуватися для визначення вимог, критеріїв їх задоволення та відповідних показників, розглянемо основні моделі якості.

Модель якості програмного продукту (рис.1.2) зводить якісні характеристики до восьми характеристик, кожна з яких, відповідно, охоплює низку підхарактеристик. Модель може застосовуватися як до програмних продуктів (характеризуються статичними властивостями), так і до комп’ютерних систем (характеризуються динамічними властивостями).

Тепер перейдемо до моделі якості у використанні. Під якістю у використанні (quality in use) розуміють «ступінь, з якою система або програмний продукт, які використовуються конкретними користувачами, задовольняє їх потреби у досягненні конкретних цілей із заданою ефективністю, продуктивністю, безпекою та задоволеністю у конкретних умовах використання»[3]. Тут передбачається, що критерії якості встановлюються не лише до програмної частини, а й до всієї комп’ютерної інформаційної системи загалом.

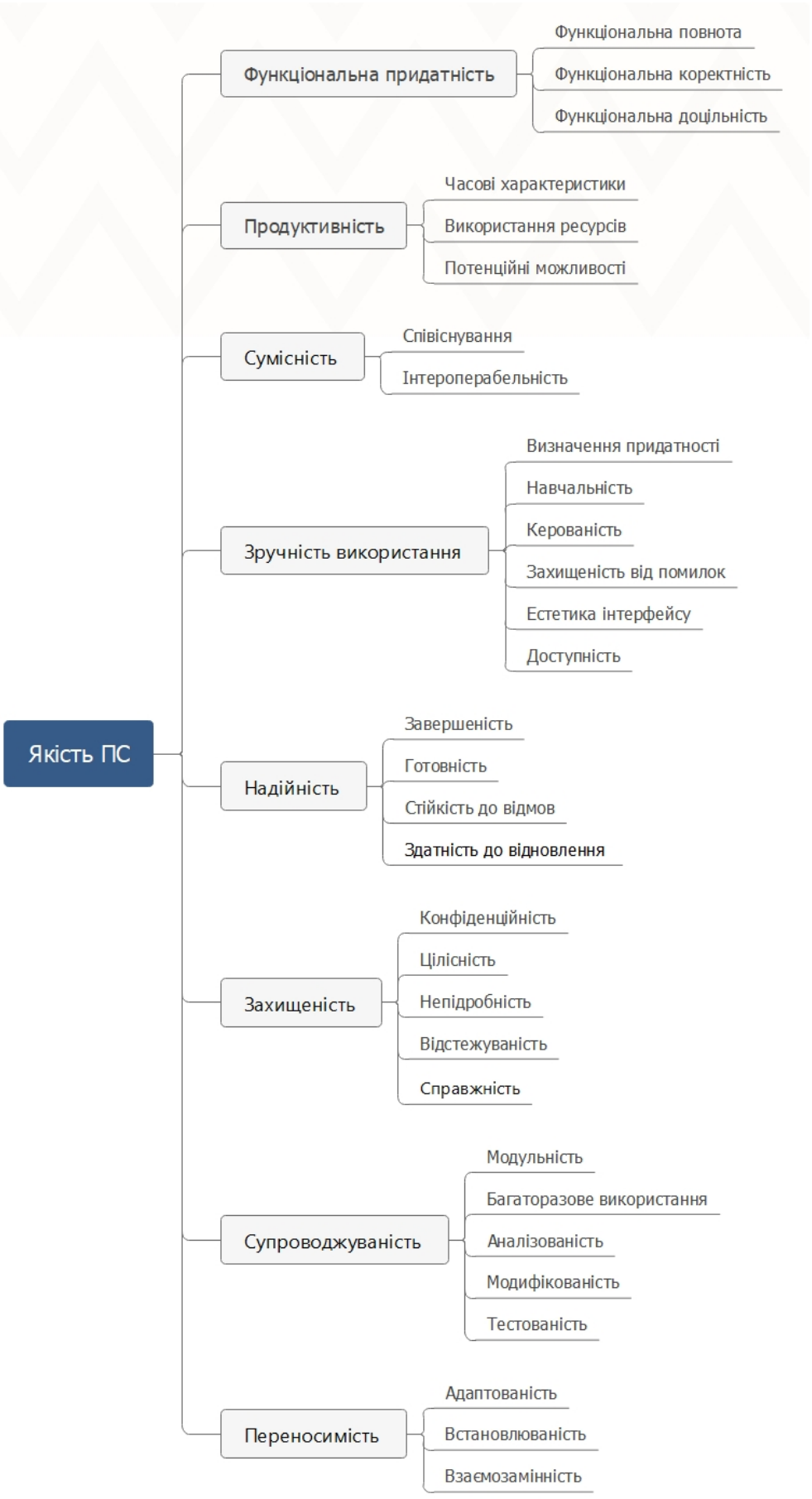


Рисунок 1.2 – Модель якості програмної системи

На рис.1.3 представлено ієрархічну модель якості у використанні, яка охоплює 5 характеристик і 9 підхарактеристик.

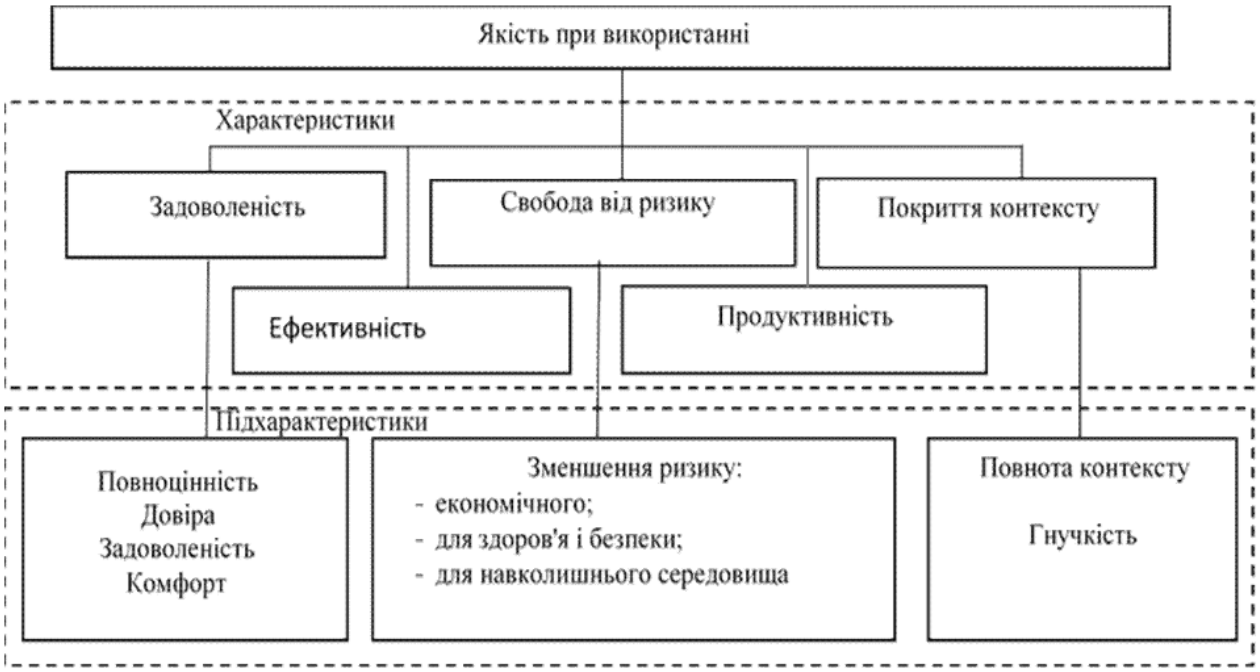


Рисунок 1.3 – Структура моделі якості у використанні

Якість при використанні залежить не лише від якості ПС, а й від конкретного контексту її використання [4]. Даний контекст залежить від впливу чинників користувача й завдання, а також фізичних і соціальних чинників довкілля. Тому порівнювати якість використання ПС доцільно лише за умови того ж самого контексту використання. Серед переліку характеристик якості у цій моделі відсутня надійність.

Третій тип моделей якості стосується IT-сервісів, які забезпечують потреби як окремих користувачів, так і підприємств. Ці послуги можуть надаватися особисто чи дистанційно людьми або IT-застосунком, який може бути локальним або віддаленим. Сюди входять два типи IT-послуг:

– повністю автоматизовані послуги, надавані IT-системою;

– послуги, надавані людиною за допомогою IT-системи.

Модель якості IT-послуг охоплює вісім характеристик, поділених на 25 підхарактеристик. Вони стосуються властивостей IT-послуги, утворених

комбінацією елементів, у т.ч. людей, процесів, технологій, обладнання та інформації.

Згідно із стандартом ISO/IEC 25011:2017 [5] надійність ІТ-сервісу (як характеристика якості) – це ступінь забезпечення ІТ-послугою відповідних і стабільних результатів. Вона характеризується такими атрибутами:

– неперервність (continuity) – ступінь надання ІТ-послуги за всіх передбачуваних обставин, у т.ч. пом'якшення ризиків внаслідок переривання, до прийнятного рівня;

– відновлюваність (recoverability) ІТ-сервісу – ступінь відновлення та доступності її функцій та даних у випадку переривання, збою чи катастрофи початкового ІТ-сервісу;

– готовність (availability) – ступінь доступності ІТ-послуги користувачам у випадку потреби.

У стандартах дано таке визначення надійності: «Ступінь виконання системою, продуктом або компонентом певних функцій за зазначених умов протягом встановленого періоду часу» [1]. При цьому зношування й старіння ПС не враховується. Проблеми з надійністю ПС виникають через недоліки у вимогах до них на етапах розроблення та реалізації або через зміни умов використання.

Поряд з цим визначенням в стандартах ISO застосовується і таке: «здатність програмного продукту підтримувати заданий рівень продуктивності за певних умов» [6].

Відповідно до ДСТУ ISO/IEC 25010:2016 надійність має свої власні підхарактеристики:

– завершеність (maturity) – ступінь відповідності системи вимогам надійності за нормальної роботи;

– готовність (availability) – ступінь працездатності та доступності системи, необхідний для її використання;

– стійкість до відмов (fault tolerance) – здатність продукту працювати як призначено, незважаючи на наявність дефектів програмного забезпечення чи апаратних засобів;

– здатність до відновлення (recoverability) – здатність системи відновити дані та необхідний стан системи у випадку переривання чи збою. Стосовно надійності в англомовній літературі переважно використовуються два терміни – «reliability» і «dependability». Якщо з перекладом першого терміну проблем немає (тобто розуміється надійність у вузькому сенсі), то з другим терміном не все так просто і досі точиться дискусія у вітчизняній науці. Найпоширеніші переклади терміну «dependability»: функціональна надійність, надійність (обладнання), гарантоздатність, загальна надійність.

Англомовні джерела дають такі трактування поняття «dependability»:

1. Достовірність (trustworthiness) комп'ютерної системи, що дає змогу виправдано покладатися на послугу (сервіс), яку вона надає [7].

2. Вимірювання ступеня працездатності елемента та його здатності виконувати необхідні функції в будь-який (випадковий) час протягом визначеного профілю місії, враховуючи доступність елемента з початку місії [6]. Причому тут вважається, що надійність (reliability), доступність (availability) і ремонтопридатність (maintainability) є аспектами надійності.

3. Здатність виконувати як і коли потрібно [8].

В. Харченко вважає, що надійність комп'ютерних інформаційних систем «повинна розглядатися у більш широкому контексті як комплексна властивість, що включає не тільки традиційні складові, перед усім, безвідмовність і готовність, але й безпечність… За міжнародною практикою така властивість має назву «dependability» (на відміну від «reliability»), якій у найбільшій мірі відповідає україномовний варіант «гарантоздатність» (надійність у широкому сенсі)»[9].

Залежно від застосувань ПС може бути зроблений різний акцент на різних аспектах надійності, тобто надійність може розглядатися згідно з різними, але взаємодоповнюючими властивостями, які дають змогу визначити атрибути надійності (dependability):

– підготовленість до використання веде до готовності (availability);

– неперервність послуг веде до надійності (reliability);

– відсутність катастрофічних наслідків для навколишнього середовища веде до безпеки (safety);

– відсутність несанкціонованого розголошення інформації призводить до конфіденційності (confidentiality);

– відсутність недозволених змін інформації призводить до цілісності (integrity);

– здатність відновлюватися і розвиватися призводить до ремонтопридатності (maintainability).

Тому під надійністю в даній роботі використовуватимемо «широке» поняття надійності (dependability), яке охоплює різні аспекти. Подібний підхід зазначено і в «Електропедії»: «Надійність (dependability) використовується як збірний термін для пов'язаних із часом характеристик якості системи» [8]. Надійність (dependability) охоплює доступність, надійність (reliability), можливість відновлення, ремонтопридатність і ефективність підтримки технічного обслуговування, а в деяких випадках й інші характеристики, такі як довговічність, безпека та захист [8]. Отже, ПС має діяти, навіть коли система зазнає атак або природних збоїв.

Згідно з [10], гарантоздатність (dependability) об'єднує такі основні атрибути (поняття): безвідмовність (reliability); живучість (survivability); готовність (availability); функціональна безпека (safety); конфіденційність (confidentiality); цілісність (integrity); обслуговуваність (maintainability); ремонтопридатність (maintainability).

Отже, на наш погляд, існує широке (dependability) і вузьке (reliability) трактування надійності ПС. Вузька надійність вважається одним із декількох вимірів широкої надійності, поряд з доступністю, безпекою, цілісністю тощо. Широка надійність вимагає вузької надійності, тоді як остання має свою частку в забезпеченні широкої надійності.

Якщо виразити коротко щодо програмних засобів, то «reliability» означає, що програма не зависає, а «dependability» означає, що програма завжди дає коректні результати.

Існує різниця між неправильним (помилковим) і некоректним результатом. Некоректність означає неточний результат, але не обов'язково неправильний. Як наприклад можна навести GPS: він дає приблизне місцезнаходження, а не точне.

Однак його покази розташування не є хибними, а лише приблизними, що робить їх некоректними.

Таким чином, можна дати таке уточнене поняття надійності вебсайту: «Надійність є збірним терміном часових характеристик якості вебсайту, який охоплює поняття вузької надійності (reliability), доступності, можливості відновлення, стійкості до відмов, а також його безпеки та конфіденційності».

Основні аспекти надійності та їхній взаємозв'язок підсумовані у формі дерева, як показано на рис.1.4 [11].

Поняття, пов'язані з надійністю, можна згрупувати в три класи:

1. Порушення надійності: a) несправності, b) помилки, c) відмови. Вони небажані, проте в принципі не є неочікуваними. Це обставини, що спричиняють або є наслідком ненадійності (визначення якої дуже просто виводиться з визначення надійності: покладатися на послугу більше неможливо).

Збій системи виникає, коли надаваний сервіс відхиляється від виконання призначених функцій системи. Помилка – це та частина стану системи, яка може спричинити подальший збій: помилка, яка впливає на службу, є ознакою того, що стався збій. Передбачуваною або гіпотетичною причиною помилки є несправність.

2. Засоби забезпечення надійності: a) попередження несправностей, b) усунення несправностей, c) відмовостійкість, d) прогнозування несправностей. Ці методи та прийоми дають змогу:

– забезпечити здатність надавати послугу, на яку можна покластися;

– досягти впевненості в цій здатності.

3. Атрибути надійності: a) готовність, b) надійність, c) безпека, d) конфіденційність, e) цілісність, f) ремонтопридатність. Вказані атрибути дають змогу:

– виразити властивості, очікувані від системи;

– оцінити якість системи внаслідок порушень і засобів, які їм протистоять.

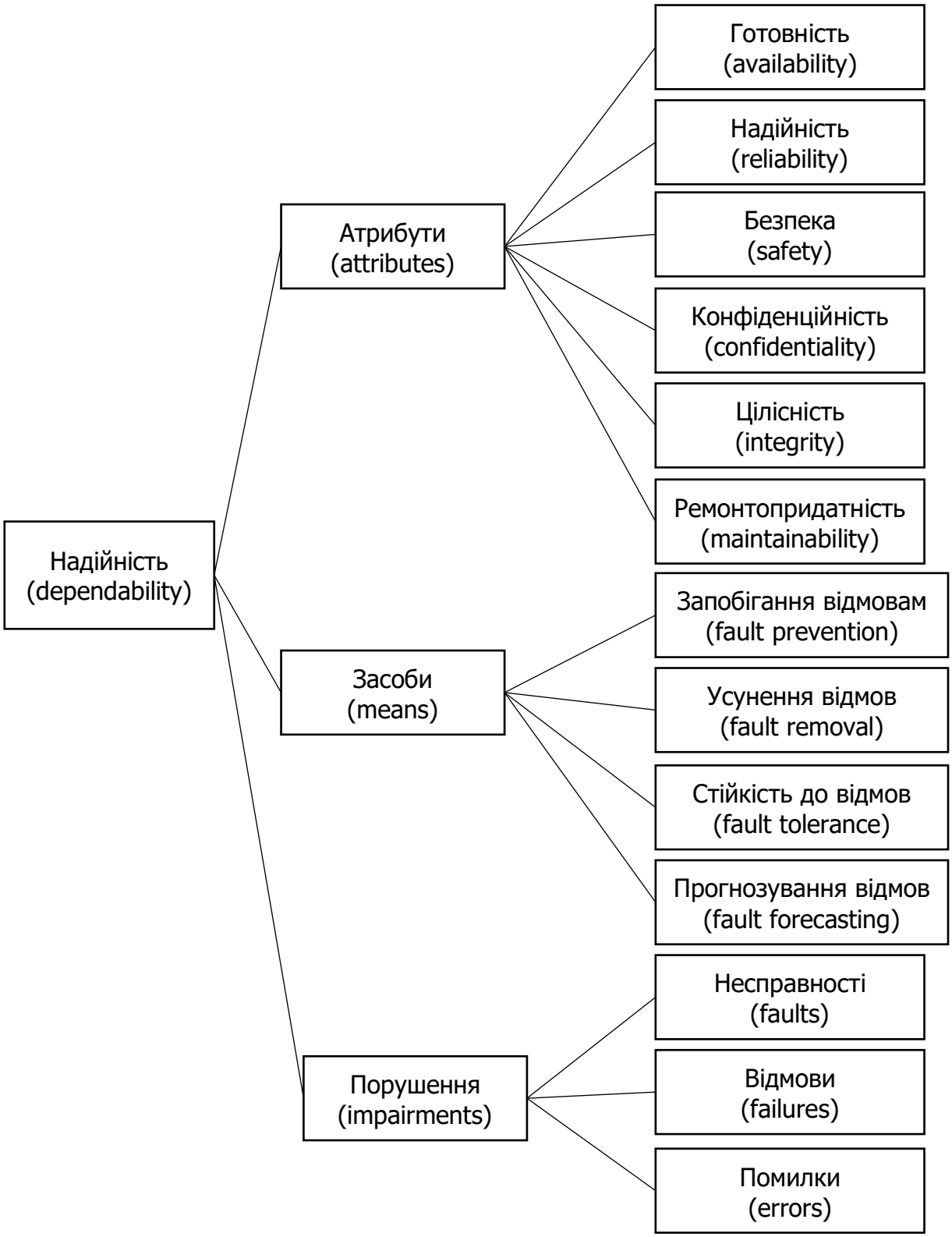


Рисунок 1.4 – Взаємозв’язок порушень, засобів і атрибутів надійності ПС

Атрибути надійності є невід'ємною властивістю або характеристикою ПС, кількісні або якісні відмінності яких можуть встановлюватися людиною або засобами автоматизації.

Розробка надійної ПС вимагає комбінованого використання набору методів і технік, які можна класифікувати на:

– запобігання несправності: як запобігти виникненню несправності;

– усунення несправностей: як зменшити наявність (кількість, серйозність) несправностей;

– відмовостійкість: як забезпечити сервіс, здатний виконувати функцію системи за наявності збоїв;

– прогнозування несправностей: як оцінити поточну кількість, майбутню частоту та наслідки несправностей.

Разом з тим, оцінювання якості може здійснюватися з точки зору різних зацікавлених сторін (стейкголдерів), які взаємодіють з ПС. У даному випадку існує багато зацікавлених сторін, до яких належать розробники, набувачі, користувачі чи клієнти компаній, які використовують ПС. Детальна специфікація та оцінювання їх якості є ключовими чинниками забезпечення корисності для стейкголдерів. Оцінювання може виконуватись на засадах визначення необхідних характеристик якості, пов'язаних із завданнями стейкголдерів і цілями системи, а також враховуючи вплив системи на зацікавлені сторони. Варто зазначити, що в кожної категорії можуть бути власні вимоги та критерії до надійності ПС.

Атрибути надійності ПС є її невід'ємними властивостями (характеристиками). Вони можуть характеризувати кількісні чи якісні відмінності, які встановлюються людиною або засобами автоматизації.

У стандартах якості термін «показник» використовується для загального позначення вимірюваних і похідних параметрів, а також атрибутів [12]. Для оцінювання якості ПС використовуються поняття внутрішній (internal) і зовнішній (external) показник якості.

Характеристики та підхарактеристики якості на будь-якому рівні мають бути виміряними, прямо чи опосередковано, через набір пов'язаних вимірюваних властивостей. Фундаментальним у підході ISO є розрізнення між внутрішніми

властивостями ПС (які сприяють внутрішній якості), її зовнішніми властивостями (які сприяють зовнішній якості) та властивостями її якості під час використання в певних контекстах. Усі ці властивості комплексно впливають одна на одну та на результуючу якість, як схематично показано на рис.1.5.

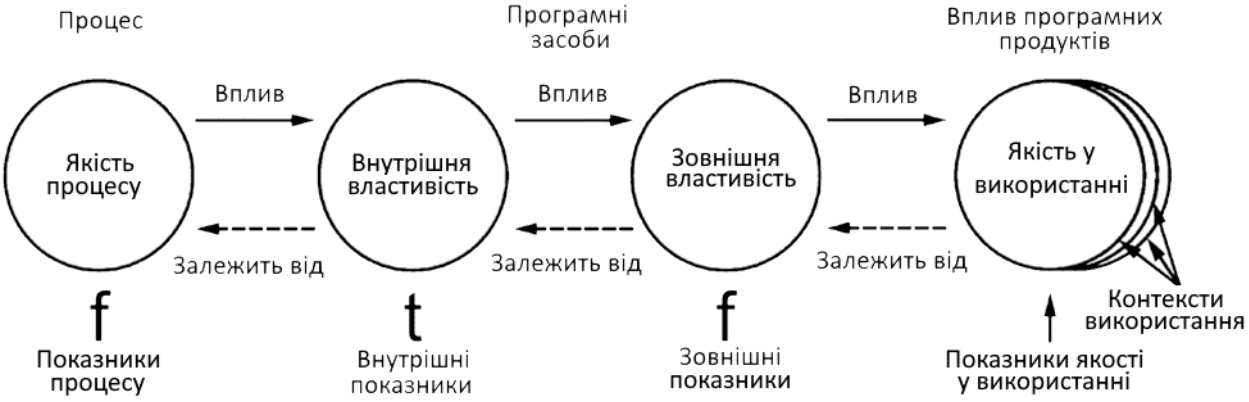


Рисунок 1.5 – Концептуальний підхід до якості згідно з ISO/IEC 25010 [1]

Внутрішній показник якості програмного продукту – це ступінь задоволення заявлених потреб набором статичних параметрів функціонування програмної продукції. Прикладами внутрішніх показників є складність, кількість, серйозність і частота відмов, виявлених упродовж тестування ПС.

Внутрішні показники надійності використовуються для прогнозування того, чи задовольнить конкретна ПС певним потребам у надійності в процесі її створення [13].

Зовнішній показник якості ПС – це ступінь задоволення заявлених надсистемою потреб параметрами функціонування ПС з урахуванням умов функціонування. Ці параметри можуть бути перевірені та/або підтверджені функціонуванням ПС упродовж тестування та експлуатації. Наприклад, кількість відмов, виявлених під час тестування, є зовнішнім мірилом якості програмної продукції, пов’язаної з кількістю несправностей у системі.

Зовнішні показники надійності використовуються для «оцінювання атрибутів, пов’язаних з поведінкою системи, частиною якої є програмна система чи продукт під час виконання тестування, для визначення ступеня надійності

програмного продукту в системі під час функціонування. Програмний продукт чи систему не відрізняють один від одного в більшості випадків» [13].

Використання моделі якості для вебсайтів має акцентуватися на практичних цілях такої моделі, яка розглядається не як проста класифікація атрибутів якості, а радше як практичний інструмент для керування процесами розроблення і оцінювання сайту. На нашу думку, про це необхідно постійно пам’ятати, визначаючи модель якості (і надійності як її складової).

1.2 Особливості надійності вебсайтів

Термін «надійність» стосовно вебсайтів має свої особливості. Надійність системи, за визначенням, охоплює всі частини системи, у т.ч. апаратне та програмне забезпечення, допоміжну інфраструктуру, операторів і процедури. Хоча традиційно розробка надійності зосереджується на критичних апаратних частинах системи, однак програмне забезпечення стає все більш важливою частиною всіх сучасних систем.

Міжнародні стандарти визначають чотири загальні категорії продукції: апаратне забезпечення, програмне забезпечення, послуги та оброблювані матеріали [14]. З них програмне забезпечення та послуги, зазвичай, є невловимими (intangible). Часто продукти містять елементи, які стосуються кількох із зазначених загальних категорій продуктів, наприклад, апаратно-програмний комплекс. Визначальним тоді буде домінуючий елемент.

Оскільки вебсайт є віртуальним товаром, то застосування до нього тих же критеріїв оцінювання надійності, що і до звичайних товарів або механізмів можливе лише з низкою застережень.

Надійність (у вузькому сенсі) вебсайту – це його якість, котра характеризується ймовірністю безвідмовної роботи сайту впродовж певного проміжку часу із збереженням параметрів, вказаних у технічному завданні.

Коли йдеться про надійність роботи вебсайту, то зазвичай мають на увазі певний період часу, протягом якого сайт знаходиться в робочому стані та без

проблем завантажується на комп’ютерах користувачів. Чим довше триває цей період, тим вища надійність сайту.

Надійність вебсайту зменшується через помилки у вимогах до його функціональних можливостей та якості, допущених і не усунених у процесі проєктування і розроблення. Аналізуючи причини появи помилок упродовж експлуатації вебсайту, їх ліквідовують, завдяки чому його надійність постійно зростає. Інтенсивна експлуатація сайту призводить до частішого виявлення помилок і швидшого їх усунення, і, відповідно, до зростання його надійності.

Розглянемо основні чинники, які впливають на надійність роботи вебсайтів [15, 16, 17]:

1. Ступінь незалежності від ПЗ, застосовуваного хостинг-провайдером. Не завжди ПЗ хостингу повністю сумісне з функціоналом вебсайту. Іноді відсутня підтримка певного функціоналу, наприклад, останньої версії PHP, JavaScript тощо. Тому не варто використовувати на сайті жодних зайвих модулів, плагінів та іншого непотрібного функціоналу, оскільки вони сильно ускладнюють та заплутують програмний код, збільшують загальну кількість файлів і обсяг вебсайту.

2. Загальна кількість файлів, з яких утворено сайт. Чим більше файлів різних форматів (HTML, PHP, JavaScript, CSS), тим вища ймовірність їхньої відмови. Можливі помилки, через які втрачаються зв’язки між окремими файлами (вони стають недоступними). Внаслідок цього вебсайт повністю чи частково втратить свою працездатність. Саме тому відносно невеликі вебпроєкти є стабільнішими та надійнішими, ніж великі.

3. Система навігації вебсайту. Зростання обсягу контенту спричиняє складність системи навігації. Характеристикою складності навігації є загальна кількість гіперпосилань. Тому, чим їх більше в системі навігації, тим ймовірніша поява непрацюючих гіперпосилань.

3. Ступінь незалежності від цілісності файлової системи та функціональних модулів. Це означає, що в ідеалі сайт має продовжувати працювати навіть у ситуації, коли з окремих директорій видалено певні файли чи перестають функціонувати окремі плагіни, тощо.

4. Ступінь незалежності від браузерів, використовуваних користувачами. Якість відображення вебсторінок на моніторі інтернет-відвідувача залежить від властивостей та характеристик браузера. Наприклад, є старі версії браузера, при використанні якого з'їжджають убік окремі блоки, зникають або сильно змінюються рамки, відступи та ін. Для підвищення надійності роботи вебсайту, приходиться встановлювати спеціальні латки для старих версій популярних браузерів. Щоби не втрачати користувачів, варто оптимізувати сайт під різні браузери.

5. Сукупність внутрішніх і зовнішніх загроз, котрі спричиняють несприятливі наслідки роботи та збитки для власника вебсайту. Через порушення системи безпеки внаслідок хакерських атак або шкідливих програм виникають спотворення та втрата даних, а також порушується функціонування самого вебсайту. Тому з позиції безпеки доцільно створити декілька дзеркал вебсайту. Якщо щось трапиться з одним дзеркалом, відвідувачі зможуть потрапити на сторінки через інші дзеркала.

6. Надійність хостинг-провайдера й хмарних сервісів. На надійність вебсайту впливатимуть інциденти на стороні провайдера, такі як простій сервера, збій програмного забезпечення, порушення безпеки, помилки обслуговуючого персоналу та ін.

7. Давність проведення редизайну вебсайту. Реконструкція (редизайн) необхідний, коли вебсайт містить багато помилок і застарілий контент, перевантажений медіаресурсами, погано стикується з базою даних, його важко знайти в пошукових системах тощо. Найкращий показник необхідності редизайну – співвідношення кількості відвідувачів сайту до кількості відвіданих сторінок упродовж певного часового інтервалу.

Коротко опишемо найважливіші із вказаних чинників надійності.

До основних характеристик сучасних вебсайтів у аспекті надійності насамперед належить стабільність його безпомилкової роботи (ймовірність безвідмовної роботи). Не всі вебсайти стабільно працюють без відмов. На це впливають різні причини – від помилок розробників і до проблем на стороні хостингу (старе обладнання, DDoS-атаки на сервері, помилки самого хостингу).

Перевірку працездатності вебсайту можна виконати з допомогою різних онлайн-сервісів, котрі повідомляють, коли і чому сайт був недоступним: Load Impact (k6) [18], BrowserMob [19], Alertra [20], site24x7 [21], You get signal [22], HOST-TRACKER [23] та ін.

Стабільно працюючий вебсайт не має допускати виникнення помилок, що впливають на його працездатність, наприклад, при зміні налаштувань в адміністративній панелі без виправлення коду. Стабільний вебсайт не має спричиняти помилок за будь-яких комбінацій налаштувань.

Під час оновлення вебсайту до нової версії можливе виникнення критичної помилки, яка спричиняє його непрацездатність. Цей аспект надійності пов’язаний із застосуванням систем керування контентом (Content Management System, CMS) і стосується оновлень, випущених розробниками.

У сучасному швидкоплинному діловому світі – особливо в торгівлі, де продукти змінюються щодня, навіть щогодини – постійно зростає потреба у швидких змінах вмісту вебсайту. Раніше за це відповідали вебмайстри та програмісти, які створювали HTML-код, модулі JavaScript і плагіни, проте в цьому була фундаментальна проблема: критично важливе завдання залежало від кількох людей. Процес довелося децентралізувати, тому був розроблений новий метод – система керування вебконтентом. CMS – це спеціалізоване програмне забезпечення, що допомагає керувати вебсайтом і наповнювати його контентом без володіння спеціальними знаннями та навичками програмування. Сьогодні вони включаються як стандартна функція послуг вебхостингу.

Серед найпопулярніших на даний момент CMS виділимо такі [24]: WordPress, Shopify, Wix, Squarespace, Joomla, Drupal, Blogger. Всі CMS періодично випускають оновлені версії. В оновлених движках присутні не лише нові функції та можливості для сайту та його розвитку, а й удосконалена система безпеки.

Попри їхню популярність і ефективність, платформи CMS також мають проблеми з безпекою. Помилки в системі безпеки застарілої CMS вебсайту приваблюють хакерів. Саме вебсайти на застарілій CMS насамперед зазнають атак і зламів. Такі злами здійснюються з метою примусового перенаправлення

відвідувача вебсайту на абсолютно сторонній ресурс або з метою поширення вірусу серед відвідувачів.

Майже всі сучасні CMS в автоматичному режимі перевіряють наявність оновлень системи та дають змогу адміністратору виконати оновлення з адміністративної панелі. Проте, на жаль, трапляються випадки, коли після оновлення сайт стає непрацездатним або відбувається порушення його важливих функцій. Тому для уникнення вказаних проблем власникам вебсайтів варто стежити за виходом нових версій ПЗ і своєчасно його оновлювати. Проблеми іноді виникають через допущені помилки при розробці, тому їх можна усунути лише на стороні розробника.

Помилки можуть також виникати в процесі оновлення встановлених легальних компонентів, плагінів, шаблонів. Виявляється, що не всі CMS мають централізовану систему оновлень компонентів і відображення оновлень, крім того не всі розробники вебсайтів підтримують свої продукти. Іноді адміністратору доводиться самому перевіряти налаштування окремих плагінів або розширень на наявність оновлень, або навіть проводити постійний моніторинг вебсайтів цих розширень на наявність оновлень, шо є досить незручним. Наприклад, у Joomla потрібно окремо перевіряти оновлення самої системи, а окремо – оновлення компонентів. При розробці вебсайтів з використанням таких систем розробнику доводиться завжди перевіряти сумісність плагінів між собою та з версією використовуваної системи.

Важливою особливістю надійності вебсайтів є його резервне копіювання, тобто створення бекапів. Під бекапом (back up) розуміють створення повної чи часткової резервної копії даних (операційних систем, сайтів або програмного забезпечення). Вся суть тут зводиться до копіювання даних, FTP-акаунтів, файлів сайту, поштових даних та інших параметрів хостингу. Іншими словами, відбувається збереження всього вебсайту та його налаштувань в окремому місці, а за потреби адміністратор сайту може повернути сайт до збереженої версії. Таке копіювання даних може здійснюватися на поточний сервер, розташований окремо від серверів провайдера, чи зовсім в іншому дата-центрі. Бекап здійснюється на той

випадок, коли щось трапиться із сервером, де розташований сам вебсайт. Існує можливість відновити виконаний бекап самостійно чи хостинг-провайдером.

Проте може виникнути й складніша (форс-мажорна) проблема, внаслідок чого працездатність сервера порушиться, а вебсайти та розміщені бекапи теж перестануть працювати. Для підвищення надійності в таких непередбачених випадках існує обслуговування подвійного резервного копіювання. Хостинг-провайдер має можливість оперативного відновлення роботи своїх сервісів і виконання відновлення резервних копій цих користувачів з іншого бекапного сервера, розташованого в іншому дата-центрі, який не зазнав впливу непередбачуваних обставини, котрі порушили роботу сервера та вебсайтів.

Тому перед придбанням хостингу варто вияснити у провайдера, чи надає він замовникам сервіс резервного копіювання даних, наскільки регулярно виконує таке резервне копіювання і впродовж якого часу зберігаються копії. Саме від цього залежить безперебійне функціонування вебсайту, розміщеного на вказаному хостингу.

Задля надійності доцільно робити резервне копіювання вебсайту щодня. Переважно сам хостинг в автоматичному режимі створює резервні копії й вони зберігаються приблизно два тижні. Також рекомендується зберігати їх на диску (чи хмарному сховищі) щонайменше 1-2 рази на місяць, що буде доброю запорукою гарантоздатності вебсайту.

На жаль, частина CMS не мають надійної системи резервного копіювання. Наприклад, WordPress дає змогу копіювати лише контент вебсайту, а не всю базу даних і файли. Для вирішення проблеми доводиться встановлювати плагіни резервного копіювання.

Також створені бекапи завжди доцільно перевіряти на працездатність, адже неперевірений бекап рівнозначний його відсутності. Оптимальним вважається здійснювати 12-25 копій щорічно.

Ще однією проблемою надійності вебсайту є складність його поновлення після помилки, котра спричинила непрацездатність. Попри постійне вдосконалення інтернету та засобів безпечної роботи в ньому, все ще продовжуються хакерські атаки, виникають збої та помилки в роботі вебсайтів. Перерви в працездатності

сайту – цілком реальне явище, котре завдає незручності та збитки для його власників, понижуючи ефект будь-якого бізнесу, невід'ємним інструментом якого є вебсайт. Після збою у роботі вебсайту без його поновлення неможливо обійтися. Якщо вебсайт функціонує довший час і багатий різноманітним контентом, то швидке відновлення його працездатності без втрати даних є важливим показником надійності.

На відновлення вебсайту може затратити багато часу, якщо займатися цим самостійно і за відсутності необхідних знань. А якщо не було збережено резервні копії останньої версії, то процес відновлення може взагалі бути неможливим.

Для відновлення вебсайту з резервної копії здійснюють декілька основних кроків:

1) створення резервної копії, якщо в процесі відновлення й далі стануться збої;

2) зміна паролів і ключів доступу до початку процесу очищення вебресурсу – задля впевненості, що у зловмисників не залишився несанкціонований доступ;

3) запуск сканери вебсайту для виявлення пошкоджених зон;

4) переустановлення движка сайту;

5) перевірка контенту, оскільки в ньому можуть міститися підозрілі елементи, що шкодять роботі вебсайту;

6) перевірка і, за необхідності, переустановлення всіх необхідних плагінів.

Отже, чим менше зусиль потребує відновлення сайту, тим вищий рівень його надійності.

Надійність вебсайту можна розглядати з різних позицій. Наприклад, з погляду бізнесу це може бути здатність вебсайту залишатися конкурентоспроможним серед аналогічних вебсайтів упродовж певного періоду часу. З точки зору відвідувача, це може бути довіра до вебсайту, наскільки останній є достовірним і безпечним.

Крім того, оцінювання надійності буде відрізнятися на різних стадіях життєвого циклу вебсайту. Так критерії оцінювання відрізнятимуться на етапі проєктування і розроблення вебсайту від критеріїв на стадії його експлуатації.

На процес оцінювання також впливає тип вебсайтів. Наприклад, статичні та динамічні вебсайти мають свої особливості. Для динамічних сайтів характерна їх постійна підтримка та оновлення даних, оскільки більшість з них містить базу даних. За таких умов застосування критеріїв надійності вебсайту буде відрізнятися. На рівень функціональної надійності вебсайтів впливають не лише відмови та збої програмно-апаратних засобів, а й надійність (стійкість) процесів обробки зберігання та передачі даних, а також захищеність і забезпечення цілісності.

Як показано в попередньому підрозділі надійність вебсайту можна розглядати у «вузькому» і «широкому» сенсі.

У «вузькому» значенні надійність нерозривно пов’язана з відсутністю відмов у роботі сайту, тобто це його властивість зберігати працездатність протягом заданого проміжку часу та здатність до відновлення. Проте поняття надійності неможливо розглядати окремо від інших сторін процесу експлуатації вебсайту. Надійність в «широкому» значенні поєднує в собі сукупність інших властивостей, до яких можна віднести безвідмовність, придатність до відновлення та збереження, готовність, конфіденційність тощо.

Зрештою, забезпечення надійності завжди є компромісом з іншими і здебільшого суперечливими вимогами, такими як безпека, захист, вартість, графік і т.д. Детальніше огляд критеріїв оцінювання надійності вебсайтів розглянуто в розділі 2.

1.3 Метрики вимірювання надійності вебсайту

Варто визнати, що абсолютно надійних програм немає, оскільки неможливо теоретично довести абсолютну ступінь їх надійності, а тому він недосяжний. Однак важливо знати, наскільки надійним є конкретний вебсайт.

Практика розробки вебпродуктів передбачає пріоритет завдання забезпечення надійності над завданням її оцінювання. Складається парадоксальна ситуація: цілком очевидно, що, перш ніж забезпечувати надійність, варто навчитися її вимірювати (оцінювати). Але для цього потрібно мати практично прийнятну одиницю вимірювання надійності та модель її розрахунку.

Як уже згадувалося а попередніх підрозділах, показники якості ПС можна розділити на внутрішні та зовнішні. Відповідно, і показники надійності вебсайту класифікуються на внутрішні та зовнішні.

Зовнішній показник (external measure) відображає ступінь задоволення затверджених і виявлених вимог до вебсайту за певних умов, тоді як внутрішній показник (internal measure) – ступінь задоволення набором статичних атрибутів вебсайту заявленим і очевидним потребам у ньому за використання у певних умовах. Під статичними розуміють атрибути, що стосуються архітектури вебсайту, його структури та компонентів. Ці атрибути можна перевірити з допомогою аналізу, моделювання або автоматизованих елементів.

Для визначення надійності та розроблення заходів щодо її забезпечення та оптимізації використовують як якісні, так і кількісні показники. Останні можуть бути розмірною чи безрозмірною величиною.

Часто показники надійності поділяють на два типи: одиничні та комплексні показники. Одиничні показники надійності описують лише одну властивість, що визначає надійність об’єкта. Комплексні показники визначають деяку сукупність властивостей, котрі характеризують надійність об’єкта.

Розглядаючи різні показники надійності важливо звернути увагу на їхні найменування та кількісні значення. Також важливими характеристиками показників є їхні математичні формулювання та визначення. Аналізуючи числові значення, варто пам’ятати, що показник може змінювати своє значення залежно від умов його створення та застосування чи від періоду його існування.

В стандарті ICO 25023 [13] описана процедура вимірювання якості ПС. Адаптуємо її для вимірювання надійності, як базової характеристики якості вебсайту. На рис.1.7 представлено схема для показника надійності «Середній час між відмовами».

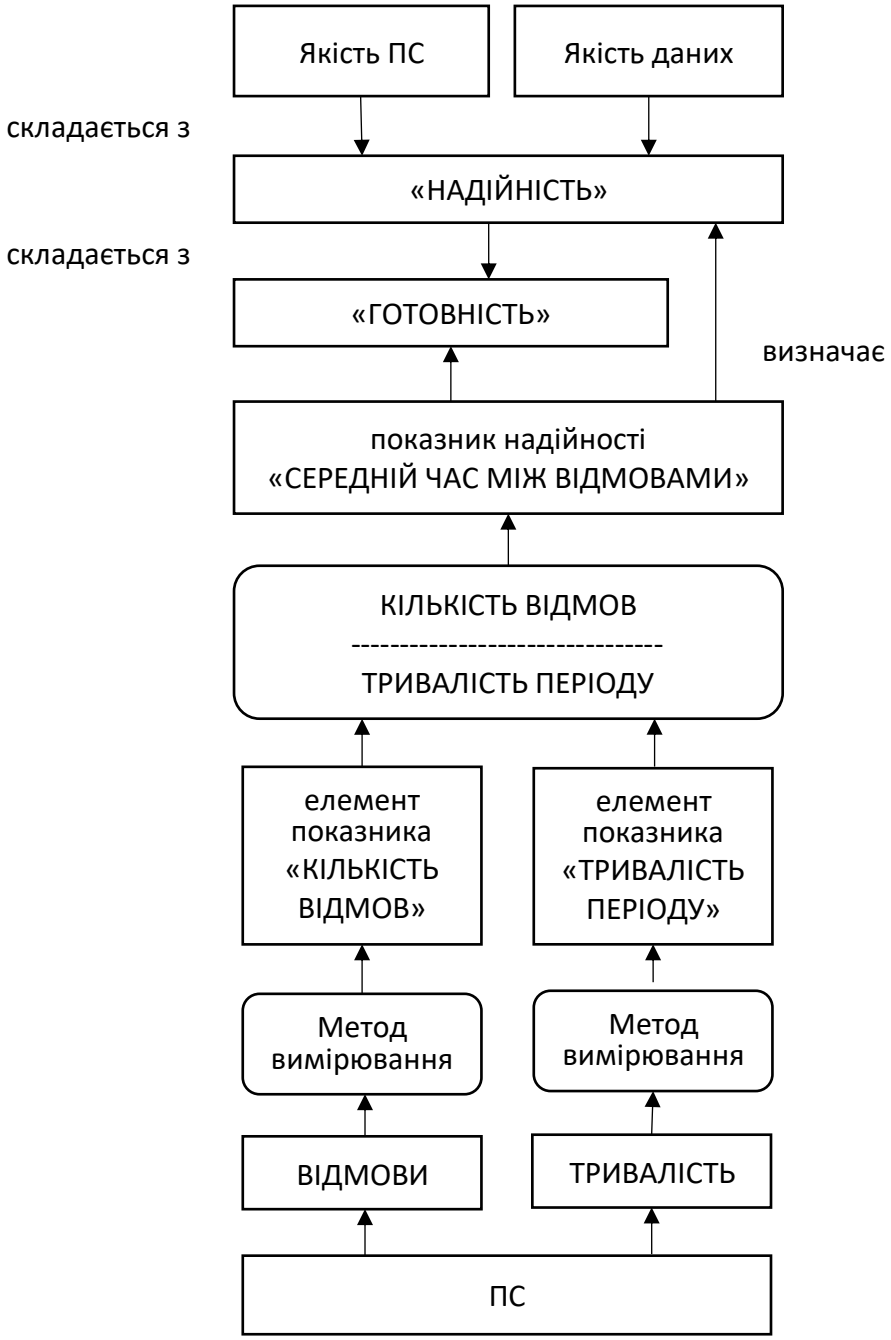


Рисунок 1.7 – Взаємозв’язок між моделлю якості,
показником надійності та її елементами (адаптовано з [13])

В системі якості спочатку мають справу з елементом вимірювання (measure element), котрий визначається кількісно, включаючи перетворення математичною функцією, з використанням певного методу вимірювання. А далі отримують показник (measure) надійності, який визначається як функція вимірювання двох або більше значень елементів вимірювання.

Вимірні властивості вебсайту, що стосуються якості, називаються властивостями для вимірювання та можуть бути пов’язані з показниками якості. Ці властивості вимірюються з допомогою методу вимірювання, тобто логічної послідовності операцій, що використовуються для кількісного оцінювання. Результат методу вимірювання згенерований елементом вимірювання. Підхарактеристики надійності можуть бути кількісно визначені шляхом застосування функції вимірювання – алгоритму для об’єднання елементів вимірювання надійності. Результат застосування вказаної функції і буде показником надійності. Для вимірювання характеристики показника якості може використовуватися більше одного показника надійності.

Показники надійності використовуються для оцінювання ступеня, в якому вебсайт виконує певні функції за заданих умов протягом встановленого періоду часу. Внутрішні показники надійності використовуються для прогнозування того, чи задовольнить даний сайт певним потребам надійності при його розробленні. Зовнішні показники надійності використовуються для оцінювання атрибутів, пов’язаних з поведінкою вебсайту для визначення ступеня його надійності під час функціонування. Вебсайт в даному випадку не відрізняють від ПС.

1. Показники стабільності.

Показники стабільності, наведені в табл.1.5, використовують для оцінювання ступеня задоволення вебсайтом потреби надійності при нормальному функціонуванні. Значення показника напрацювання на відмову може використовуватися для порівняння надійності різних вебсайтів, а значення показника частота відмов – для прогнозування надійності вебсайту.

Таблиця 1.5 – Показники стабільності

	Назва	Опис	Функція вимірювання
1.	Корекція помилок	Яку частину виявлених критичних для стабільності помилок було усунуто?	X = A/B, де A – кількість усунених критичних помилок; B – кількість виявлених критичних помилок

Продовження таблиці 1.5			
2.	Напрацювання на відмову	Яке напрацювання на відмову при експлуатації вебсайту?	X = A/B, де A – час експлуатації; B – кількість відмов, що трапилися за час експлуатації
3.	Частота відмов	Яка середня кількість відмов за певний проміжок часу?	X = A/B, де A – кількість відмов, виявлених за час спостереження; B – тривалість спостереження

2. Показники готовності до роботи.

Показники готовності до роботи, наведені у таблиці 1.6, використовуються з метою оцінювання ступеня готовності вебсайту до експлуатації. Додатково готовність до роботи може бути оцінена через сумарний проміжок часу, коли вебсайт був доступним. Готовність до роботи загалом є комбінацією стабільності (яка визначає частоту збоїв), відмовостійкості та відновлюваності (яка визначає тривалість часу недоступності після кожного зі збоїв).

Таблиця 1.6 – Показники готовності до роботи

	Назва	Опис	Функція вимірювання
1.	Доступність системи	Протягом якої частини із запланованого часу роботи вебсайт доступний?	X = A/B, де A – дійсний час роботи вебсайту; B – запланований час роботи
2.	Середній час недоступності	Як довго вебсайт залишається недоступними у випадку відмови?	X = A/B, де A – сумарний час недоступності вебсайту; B — кількість виниклих відмов

3. Показники стійкості до відмов.

Показники стійкості до відмов, наведені в таблиці 1.7, використовуються для оцінювання того, в якій мірі вебсайт працює за призначенням, незважаючи на наявність несправностей. Внутрішня або зовнішня міра може бути пов’язана з

можливостями вебсайту підтримувати заявлений рівень функціонування у випадках дефектів функціонування або порушення інтерфейсу.

Таблиця 1.7 – Показники стійкості до відмов

	Назва	Опис	Функція вимірювання
1.	Запобігання збоям	Яка частина сценаріїв, які потенційно призводять до відмов, обробляється з метою недопущення серйозних чи критичних відмов?	X = A/B, де A – кількість запобіганих відмов; B – кількість тестових випадків, що призводять до відмови
2.	Надмірність компонентів	Яка частина компонентів вебсайту має надмірність, щоб уникнути відмови системи?	X = A/B, де A – кількість надлишкових компонентів; B – загальна кількість компонентів вебсайту
3.	Середній час сповіщення про відмову	Як швидко система повідомляє про виникнення відмови?	$X = \sum_{i=1}^{n}(A_i - B_i)/n$, де A – момент часу, в який вебсайт сповістив про виникнення відмови; B – момент виявлення відмови; n – кількість виявлених відмов

4. Показники відновлюваності

Показники відновлюваності, наведені в таблиці 1.8, використовуються для оцінювання ступеня, за якого у випадку переривання чи збою вебсайт може відновити безпосередньо порушені дані та досягти необхідного стану.

Таблиця 1.8 – Показники відновлюваності

	Назва	Опис	Функція вимірювання
1.	Середній час відновлення	Який час потрібен вебсайту для відновлення після відмови?	$X = A/n = \sum_{i=1}^{n} A_i/n$, де A – сумарний час на відновлення вебсайту; n – кількість відмов

Продовження таблиці 1.8			
2.	Повнота резервної копії даних	Для якої частини даних регулярно створюються резервні копії?	X = A/B, де A – кількість структур даних, резервні копії яких створюються регулярно; B – кількість структур даних, резервне копіювання яких необхідне

Показники, пов’язані з безпекою та конфіденційністю, використовуються для оцінювання ступеня захисту інформації та даних вебсайтом, щоб особи або інші системи мали ступінь доступу до даних, що відповідає їхнім типам і рівням авторизації.

5. Показники конфіденційності.

Показники конфіденційності, наведені в таблиці 1.9, використовують для оцінювання ступеня гарантування вебсайтом доступності даних лише для зареєстрованих користувачів.

Таблиця 1.9 – Показники конфіденційності

	Назва	Опис	Функція вимірювання
1.	Контроль доступу	Яка частина конфіденційних даних захищена від несанкціонованого доступу?	X = 1-A/B, де A – кількість конфіденційних елементів даних, доступ до яких дозволено без авторизації; B – кількість конфіденційних елементів даних, доступ до яких обмежений
2.	Коректність шифрування даних	Наскільки коректно реалізовано шифрування та дешифрування елементів даних щодо вимог до вебсайту?	X = A/B, де A – кількість елементів даних, що шифруються і дешифруються коректно; B – кількість елементів даних, шифрування та дешифрування яких потрібне

Продовження таблиці 1.9			
3.	Складність криптографічних алгоритмів	Яка частина використовуваних криптографічних алгоритмів є досить складною?	X = 1-A/B, де A – кількість ненадійних криптографічних алгоритмів; B – кількість використовуваних криптографічних алгоритмів

6. Показники цілісності

Показники цілісності, наведені в таблиці 1.10, використовуються для оцінювання ступеня запобігання вебсайтом несанкціонованому доступу до програм і даних.

Таблиця 1.10 – Показники цілісності

	Назва	Опис	Функція вимірювання
1.	Цілісність даних	Якою мірою запобігається компрометація чи несанкціонована зміна даних?	X = 1-A/B, де A – кількість елементів даних, скомпрометованих при несанкціонованому доступі; B – кількість елементів даних, компрометації яких необхідно запобігти
2.	Захист від пошкодження даних	Наскільки передбачено захист даних від пошкодження?	X = A/B, де A – кількість реалізованих методів захисту даних від пошкодження; B – кількість доступних для реалізації методів

Розглянуті метрики вимірювання надійності в процесі ефективного управління проєктом під назвою «вебсайт» доцільно використовувати для:

- вчасного інформування про поточний стан і виникнення проблем;
- передбачення різноманітних моментів у процесі функціонування;
- діагностування проблем, їх локалізації та виправлення;
- розуміння того, що саме потрібно вдосконалювати;

- оптимізації структури та процесів;
- ухвалення правильних рішень.

Висновки до розділу 1

1. У розділі розглянуто існуючі підходи до визначення поняття надійності вебсайту. На наш погляд, існує широке (dependability) і вузьке (reliability) трактування надійності програмних систем, у т.ч. і вебсайтів. Вузька надійність вважається одним із декількох вимірів широкої надійності, поряд з доступністю, безпекою, цілісністю тощо.

2. У «вузькому» значенні надійність нерозривно пов’язана з відсутністю відмов у роботі сайту, тобто це його властивість зберігати працездатність протягом заданого проміжку часу та здатність до відновлення. Проте поняття надійності неможливо розглядати окремо від інших сторін процесу експлуатації вебсайту. Надійність в «широкому» значенні поєднує в собі сукупність інших властивостей, до яких можна віднести безвідмовність, придатність до відновлення та збереження, готовність, конфіденційність тощо.

3. Розробка надійного вебсайту вимагає комбінованого використання набору методів і технік, які можна класифікувати на: запобігання несправності; усунення несправностей; відмовостійкість; прогнозування несправностей.

4. Для оцінювання ступеня, в якому вебсайт виконує певні функції за заданих умов протягом встановленого періоду часу використовуються показники (метрики) надійності. Внутрішні показники надійності використовуються для прогнозування того, чи задовольнить даний сайт певним потребам надійності при його розробленні. Зовнішні показники надійності використовуються для оцінювання атрибутів, пов’язаних з поведінкою вебсайту для визначення ступеня його надійності під час функціонування.

2 МЕТОДИ АНАЛІЗУ НАДІЙНОСТІ ВЕБСАЙТУ ТА РОЗРОБЛЕННЯ МОДЕЛІ ЇЇ ОЦІНЮВАННЯ

2.1 Порівняння методів оцінювання надійності вебсайту

Надійність вебсайту приходиться оцінювати на всіх етапах його життєвого циклу, починаючи від формування вимог і закінчуючи тестуванням і внесенням змін. Не менш важливою є фаза експлуатації вебсайту, особливо тих, які підлягають динамічній модифікації та зміні інформаційної бази. Така сфера як надійність охоплює низку методик та інструментів їх практичної реалізації, а також порядок їх застосування для забезпечення високого рівня надійності та стабільності вебсайту для досягнення необхідного рівня готовності продукту, мінімізації вкладень і максимізації строку експлуатації програмної системи.

Існує достатня кількість методів аналізу надійності, які мають особливості для конкретних галузей промисловості та застосувань. Кількість моделей надійності на сьогодні перевищує сотню і продовжує зростати. Залежно від точки зору на надійність і поняття глибини дослідження визначаються різні критерії та нюанси. Тому побудова повної схеми є досить трудомісткою справою, а встановлення всіх зв’язків між моделями та критеріями ще більше ускладнює процес класифікації та вибору. Зазвичай система показників надійності має змішану мережево-ієрархічну структуру.

На рис.2.1 представлена схема класифікації моделей надійності вебсайту на стадії його розроблення, причому надійність розглядається у «вузькому» сенсі.

Наведена схема не є єдиною. Існує варіант класифікації всіх моделей надійності на аналітичні та емпіричні. Останні, відповідно, поділяють на моделі складності та моделі, що визначають час, необхідний на «доведення» вебсайту. Так і аналітичні моделі надійності поділяють на динамічні (дискретні та неперервні) та статичні (за помилкам, за даними).

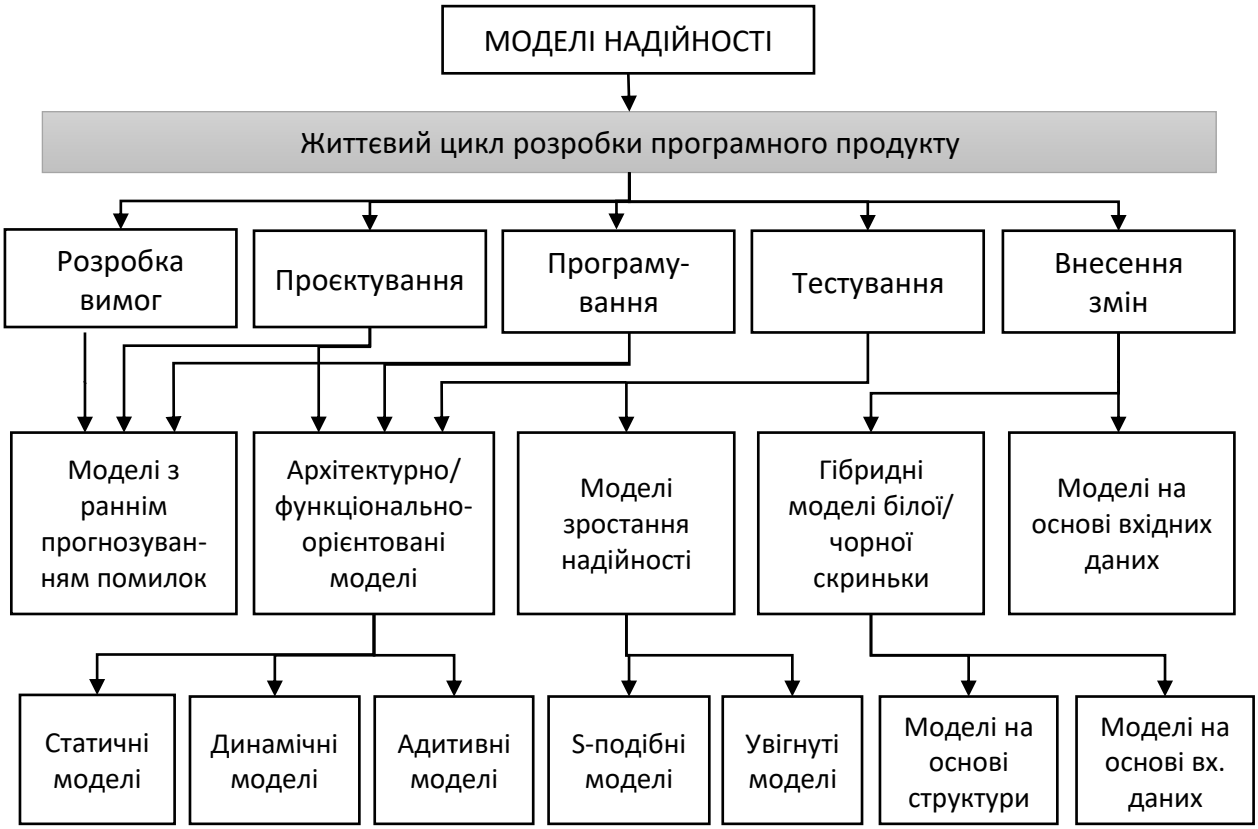


Рисунок 2.1 – Класифікації моделей надійності на стадії проєктування

До найзагальніших методик надійності можна віднести такі:

– аналіз видів і наслідків відмов;
– імітаційне моделювання надійності;
– аналіз схем функціональної цілісності;
– дослідження небезпеки та зручності використання;
– аналіз блок-схем надійності;
– аналіз дерев несправностей;
– аналіз дерева подій;
– аналіз діагностики відмов;
– аналіз надійності людського чинника;
– статистичні методи надійності;
– аналіз рівнів захисту;
– марковський аналіз.

Для виявлення ідеального балансу між різними обмеженнями й вимогами та надійністю використовуються різноманітні дослідження. Під час проведення аналізу істотну допомогу можуть надати програмні комплекси для розрахунку надійності. За способом використання методи оцінювання надійності прийнято ділити на висхідні та низхідні (досліджують наслідки комбінацій несправностей).

Далі наведемо аналіз деяких із наведених вище методів аналізу надійності.

1. Аналіз видів і наслідків відмов (Failure Mode and Effect Analysis, FMEA).

Аналіз видів і наслідків відмов – метод, який використовується для ідентифікації способів відмови компонентів, систем або процесів, які можуть призвести до невиконання призначеної функції [25]. Це процедура, за допомогою якої проводиться аналіз усіх можливих помилок системи та визначення результатів або ефектів на систему з метою класифікації всіх помилок щодо їх критичності для роботи системи.

Метод FMEA допомагає ідентифікувати [26]:

– всі види відмов різних частин і компонентів системи;

– наслідки відмов для системи;

– механізми відмови;

– способи досягнення безвідмовної роботи та/або пом’якшення наслідків для системи.

Розширеною версією методу FMEA є FMECA (Failure mode effects and criticality analysis), що дає змогу оцінити критичність та значущість кожного ідентифікованого виду відмови. Аналіз критичності зазвичай є якісним або змішаним, але може бути кількісним з використанням показника фактичного відсотка відмов.

Сенс цього методу полягає в оцінюванні надійності вебсайту за допомогою розрахунку критичності відмов кожної окремої його частини, а потім порівняння критичності відмови цієї частини з пороговим значенням, яке було встановлене до оцінювання.

Критичністю відмови є сукупність частоти появи та тяжкості наслідків або інших властивостей відмови як показник необхідності ідентифікації причин,

джерел та скорочення кількості чи частоти появи цієї відмови та мінімізація тяжкості його наслідків.

Критичність (C_i) обчислюється за допомогою формули:

$$C_i = B_{1i} + B_{2i} + B_{3i} ,$$

де B_{1i} – бальна оцінка ймовірності виникнення i-ої відмови за час експлуатації;

B_{2i} – бальна оцінка тяжкості наслідків i-ої відмови;

B_{3i} – бальна оцінка ймовірності виявлення i-ої відмови до запуску вебсайту.

Процес оцінювання методом FMEA тягне за собою необхідність обробки та формування великого обсягу даних, які є обов’язковими для виконання наступних етапів: виявлення причин та опис відмов, розрахунок ймовірності виникнення відмов, визначення наслідків цих відмов та їх критичності.

Алгоритм проведення вказаного аналізу можна здійснити на основі таких етапів нижче [26]:

1) побудова й аналіз функціональної та ієрархічної схем вебсайту;

2) аналіз взаємодії елементів вебсайту;

3) виділення найвідповідальніших елементів;

4) складання переліку відмов вебсайту та його причин;

5) оцінювання ступеня серйозності та частоти відмов з використанням експертного методу;

6) розрахунок показників критичності відмов;

7) розподіл відмов за рівнями критичності;

8) встановлення коригуючих дій та рекомендацій.

Перші п’ять етапів представляють якісний аналіз, етапи 6 і 7 – кількісне оцінювання критичності відмов. Початкові аналізу передує формування експертної групи.

Розглянемо докладніше шостий етап, пов’язаний з розрахунками на критичність відмов. Головна ідея для розрахунку критичності відмови включає три чинники:

– ймовірність (частота) відмов;

– можливість виявити дефект до експлуатації;

– наслідки відмови.

Ці три чинники разом і становлять критичність відмови [27]. Зрозуміло, що чим вище значення хоча б одного з трьох чинників, тим вище значення критичності відмови. Коефіцієнти B_{1i}, B_{2i} та B_{3i} визначають експерти за шкалою від одного до десяти.

У випадку достатнього обсягу статистичної інформації про відмови елементів вебсайту чи аналітичного визначення ймовірності їх виникнення кожній відмові присвоюються бали відповідно до інтервалу значень, в якому знаходиться значення ймовірності виявлення чи виникнення відмови. Якщо зазначені дані відсутні, то коефіцієнти визначаються експертами.

Далі значення критичності, розраховані для кожної відмови C_i, порівнюються з пороговим значенням $C_{кр}$, прийнятим ще до проведення аналізу надійності. У випадку, коли $C_i > C_{кр}$, необхідно ухвалити рішення про необхідність введення коригування, оскільки ця відмова визнається значущою.

Виконання заходів щодо оцінювання надійності вебсайтів на сьогодні має низьку результативність. Це пов’язано з недосконалістю методик, з відсутністю повноцінних рекомендацій. При використанні методу FMEA для аналізу надійності, застосовується інформація про вже виявлені відмови. Безумовно, для вже працюючого вебсайту за допомогою цього методу можливо виявити рівень надійності, але на стадії його проєктування таке оцінювання буде досить складним процесом, оскільки він ґрунтується на експертній думці.

2. Аналіз дерев несправностей (Fault tree analysis, FTA).

Аналіз дерева відмов (несправностей) або в англійській термінології – метод аналізу відмов складних систем, в якому відмови системи або небажані стани піддаються аналізу з використанням методів булевої алгебри, поєднуючи послідовність відмов нижчого рівня (нижчих подій), що призводять до відмови всієї системи [28].

Аналіз дерева відмов інтенсивно використовується у різних сферах, щоби зрозуміти, як система може вийти з ладу, визначити метод мінімізації ризиків або визначення частоти системної відмови.

Умови відмови класифікуються за тяжкістю наслідків. Найважчі умови вимагають найбільшого аналізу дерева відмов. Ці «умови відмови системи» та їх класифікація часто попередньо визначаються у функціональному аналізі небезпек і ризиків виникнення відмов.

Метод FTA ефективно використовується для:

- розуміння логіки спричинення небажаного стану (відмови) системи;
- визначення відповідності вимогам щодо надійності (безпеки);
- ранжування учасників, що ведуть до вершини (небажаного стану);
- моніторингу та контролю показників стану складних систем;
- мінімізації та оптимізації ресурсів;
- допомоги у проєктуванні системи як засобу для формування вимог;
- виявлення та виправлення причин результуючої події.

Аналіз дерева відмов складається з логічних схем, які дають змогу визначити стан, у якому перебуває система. FTA будують із застосуванням методів графічного проєктування. Інколи в дерево вводять людський чинник, тобто відсоток механічної чи логічної помилки людини, до якого належить, наприклад, неправильне введення інформації людиною. Однак, цей чинник не є основною частиною FTA.

Аналіз дерева відмов є цінним інструментом, що застосовується до визначення ймовірності потенційних відмов Нерідко цей аналіз застосовують як інструмент діагностики, який з деякими припущеннями передбачає можливість помилок системи, якщо виникне збій.

Порівнюючи з деревом успіху, варто зазначити, що проведення FTA за допомогою аналізу дерева відмов менш трудомісткий процес визначення ймовірності відмови. Однак, незважаючи на це, ця методика є трудомісткою і дорогою, якщо намагатися застосувати її до всієї системи. Тому найчастіше обмежуються використанням аналізу дерева відмов у межах підсистем, а не системи загалом.

Побудуємо дерево несправностей для деякого досліджуваного сайту, зображене рис.2.2. Нехай встановлено список з N критеріїв надійності. Порушення кожного критерію позначатимемо цифрою, що означає його порядковий номер у

списку. Наприклад, причинами порушення критерію 1 можуть бути помилки коду вебсайту (критерій 1.1) або недостатня потужність обладнання (критерій 1.2). Це свідчить про те, що сайт недостатньо протестований (критерій 1.3). Порушення критерію 2 можливе через помилки щодо призначення прав адміністраторам вебсайту (критерій 2.1) або помилки адміністративної панелі (критерій 2.2). Це вказує на порушення роботи адміністративної панелі вебсайту (критерій 2.3).

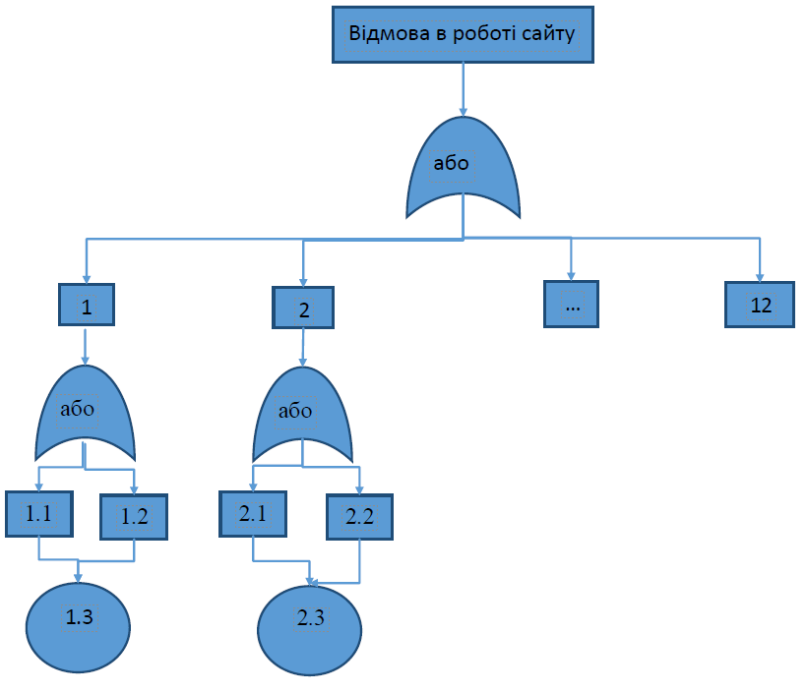


Рисунок 2.2 – Дерево несправностей для веб-сайту

Після побудови дерева відмов для вебсайту очевидно, що цей метод дає змогу оцінити його надійність лише на якісному рівні. Його можна використати для аналізу причин вже виявлених несправностей на діючому сайті, однак на етапі проєктування він не може кількісно обчислити можливість безвідмовної роботи вебсайту.

3. Аналіз дерева подій (Event Tree Analysis, ETA).

Аналіз дерева подій є висхідним (індуктивним) методом визначення можливих наслідків і, якщо це необхідно за умовами аналізу, ймовірностей (частот) реалізації деякої початкової події. Метод переважно спрямований на дослідження наслідків поодиноких небажаних подій для складних систем.

Варто зазначити, що для проведення детального аналізу надійності рекомендують спільно застосовувати методи аналізу дерева відмов й аналізу дерева подій.

4. Дослідження HAZOP (HAZard and Operability).

HAZOP (Небезпека й Працездатність) є процесом, виконуваним групою фахівців для ідентифікації та деталізації проблем небезпеки й працездатності системи. Дане дослідження спрямоване на ідентифікацію потенційних відхилень від цілей, виявлення їхніх можливих причин та оцінювання наслідків. HAZOP, як і метод FMEA, є міжнародним стандартом [29] для ідентифікації небезпек шляхом виявлення слабких місць. Цей аналіз ґрунтується на створенні «штучних» відхилень від запланованих параметрів. В результаті цього оцінюється критичність відхилень.

HAZOP охоплює три основні кроки:

1) ідентифікація компонентів системи та визначення параметрів;
2) розгляд варіації робочих параметрів;
3) визначення точок відмови та опис загроз.

5. Аналіз схем функціональної цілісності (СФЦ)

СФЦ є графічним засобом для структурного представлення обраних досліджуваних якостей системних об’єктів. Використання так званого апарату функціональної цілісності дає змогу реалізувати математичну логіку в повному обсязі в межах логіки «АБО», «І» та «НЕ». Таке застосування дає змогу правильно описувати різноманітні варіанти структурних схем, починаючи від базових або традиційних (дерева відмов, блок-схеми тощо) і закінчуючи некогерентними моделями структур різних якостей аналізованих систем.

Функціональна схема цілісності містить у своєму складі певні графічні позначення: вершини (функціональні та фіктивні); різноспрямовані дуги (диз’юнктивні та кон’юнктивні); виходи дуг з вершин (інверсний і прямий).

Для прикладу наведемо перелік подій, що є вершинами функцій у схемах функціональної цілісності:

– у період експлуатації вебсайту не отримують відмови у його роботі;
– у період визначеного періоду часу відбувається відмова вебсайту;

– на певному етапі роботи чи управління сайтом приймають або не приймають певне рішення;

– на певному етапі управління сайтом відбувається коректне чи некоректне виконання операції адміністратором.

Схему функціональної цілісності дерева несправностей вебсайту, можна представити таким способом (рис.2.3). Тут використано такі цифрові позначення:

– 1 – відмова через порушення стабільності роботи вебсайту при великій кількості відвідувачів;

– 2 – відмова через порушення в роботі адміністративної панелі вебсайту, і т.д.

Кожна подія відмови визначається відповідною цифрою його критерію.

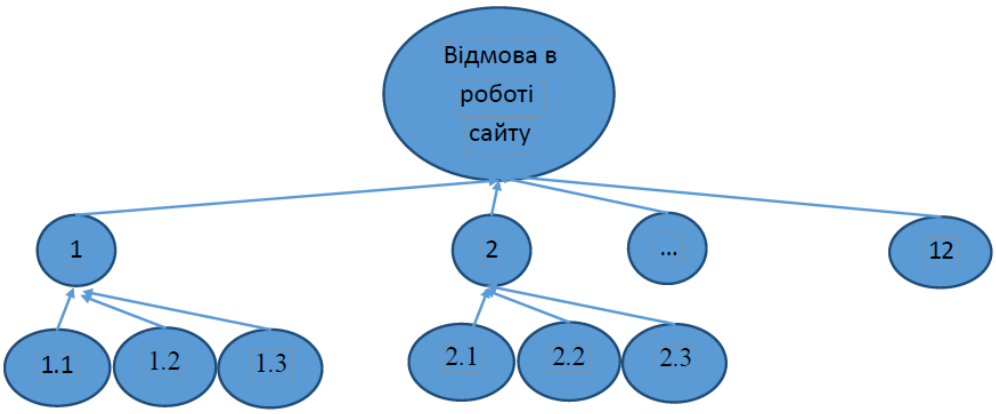


Рисунок 2.3 – СФЦ для дерева несправностей

Метод аналізу схем функціональної цілісності досить повно показує схему виникнення відмови й зв’язків між елементами, від яких залежить виникнення відмови. Застосування методу буде корисним на стадії проєктуванні вебсайту. Однак за допомогою нього неможливо кількісно визначити ймовірність цієї відмови.

6. Аналіз рівнів захисту (Layers of Protection Analysis, LOPA).

LOPA – це новітня методологія оцінювання небезпеки та ризику, заснована на виборі пар причин і наслідків та ідентифікації рівнів захисту, які можуть запобігти причині, що призводить до небажаного наслідку.

Управління безпекою означає розуміння багатьох чинників, які сприяють ризику, і вироблення відповідних заходів для його зменшення. LOPA відповідає на ключові запитання: «наскільки безпека достатня?»; «скільки незалежних шарів захисту необхідно?»; «наскільки понизити ризик має забезпечити кожен рівень?».

LOPA можна візуалізувати як серію скибочок сиру (рис.2.4), кожна з яких є шаром захисту з різною кількістю та розміром отворів, котрі представляють недоліки. Сценарій з великими наслідками виникає, лише коли принаймні одна з дірок у кожному зрізі «вишикується в ряд», що сприяє розповсюдженню відмов. Для управління системою безпеки важливо знати чи оцінювати ймовірність відмови компонентів системи.

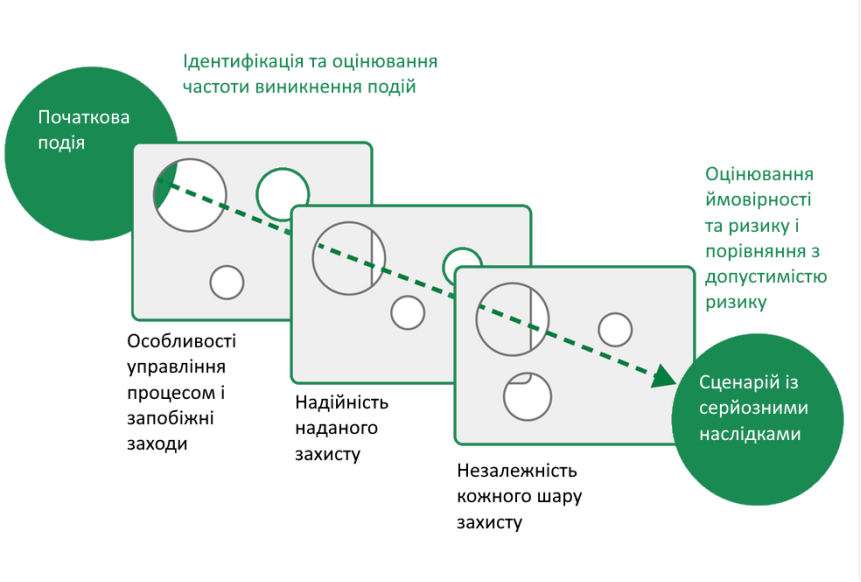


Рисунок 2.4 – Сценарії аналізу рівнів захисту

Дехто проводить LOPA як частину HAZOP, використовуючи тих самих членів команди. Цей підхід може бути ефективним, оскільки команда знайома зі сценарієм, а рішення можна записати як частину рекомендацій HAZOP.

7. Марковський аналіз.

Основними особливостями відновлюваних систем є велика кількість станів, наявність післядії відмов елементів, залежність показників надійності від великої кількості чинників. Марковський аналіз застосовують, коли майбутній стан системи залежить лише від її поточного стану. Даний аналіз для складних систем базується на так званих ланцюгах Маркова.

Методика аналізу надійності, заснована на теорії марківських процесів, охоплює такі етапи:

1. Формулювання поняття «відмова» та визначення вихідних даних.

2. Побудова розміченого графа станів системи, причому розглядаються всі можливі стани системи та можливі переходи з одного стану до іншого та їхня послідовність.

3. Упорядкування за графом станів диференціальних рівнянь Колмогорова.

4. Вирішення системи рівнянь та визначення ймовірностей станів системи.

Досліджувана система в довільний момент часу може перебувати в одному з двох станів: працездатному S_0 з ймовірністю $P_0(t)$ і непрацездатному S_1 з ймовірністю $P_1(t)$. Зі стану S_0 в стан S_1 система переходить в результаті відмов з інтенсивністю λ, а зі стану S_1 в стан S_0 переходить в результаті відновлення з інтенсивністю μ.

Процес функціонування системи відображено графом станів (рис.2.5).

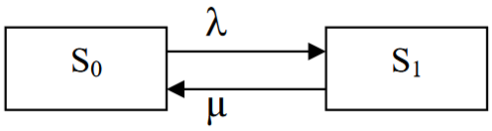


Рисунок 2.5 – Граф станів системи

Хоча ймовірність станів системи характеризується системою диференціальних рівнянь Колмогорова, показники надійності можна розрахувати безпосередньо з розміченого графа станів топологічним методом, не вдаючись до складання та вирішення системи диференціальних рівнянь. Особливостями топологічного методу є:

– простота обчислювальних алгоритмів;

– висока наочність процедур визначення кількісних характеристик надійності;

– можливість наближених оцінок показників надійності;

– відсутність обмежень на вигляд структурної схеми.

Цей метод може бути дискретним (перехід між станами ґрунтується на ймовірності) чи неперервним (на основі швидкості зміни станів).

8. Імітаційне моделювання.

Завдяки інтенсивному розвитку комп'ютерних технологій стало набагато простіше вирішувати складні завдання, що потребують великих часових та фінансових витрат. Спростити їх можна з використанням моделювання. Одним з найпоширеніших та зручних способів моделювання складних систем є імітаційне комп'ютерне моделювання об'єктів та процесів реального світу.

Імітаційна модель – це комп'ютерна програма, яка визначає структуру та відтворює поведінку реальної системи у часі. Вона дає змогу отримувати докладну статистику щодо різних аспектів функціонування системи залежно від вхідних даних.

Імітаційне моделювання – розробка комп'ютерних моделей та постановка експериментів на них. Програмні засоби імітаційного моделювання дають змогу будувати моделі (динамічні, дискретно-подійні, агентні), що імітують практично будь-який реальний процес, а також конструювати та виконувати аналіз моделей на комп'ютері без проведення реальних експериментів і самостійних складних обчислень. Використання імітаційного моделювання є перспективним напрямком у процесі оцінювання надійності веб-сайтів, однак вимагає певних навиків побудови моделей і проведення на їх основі експериментів.

Усі ці методи аналізу застосовні переважно для оцінювання кількісних характеристик поведінки системи в експлуатації. Достовірність результату оцінювання характеристик надійності залежить від точності та правильності даних. Однак жоден метод аналізу надійності не може бути вичерпним і універсальним для усестороннього аналізу реально існуючих вебсайтів. Для проведення оцінювання надійності складних або багатофункціональних систем, зазвичай, необхідно застосувати кілька методів.

Оцінювання надійності вебсайту (як однієї з найважливіших характеристик його якості) охоплює багато критеріїв і оцінюються за допомогою різних моделей [30, 31]. Серед цих методів і моделей останнім часом набуває популярності та привертають увагу дослідників багатокритеріальні методи прийняття рішень

(Multiple Criteria Decision Making – MCDM). Вони передбачають оцінювання ситуації в реальному світі за допомогою якісних або кількісних критеріїв у певних і невизначених ризикованих середовищах з метою пошуку відповідного курсу дій, вибору, стратегії чи політики серед кількох варіантів. Їх широко застосовують у різних сферах, і на даний час вони також широко застосовні для оцінювання веб-сайтів з точки зору їхньої якості. Тому нами обрано цей багатокритеріальний підхід для експертного оцінювання надійності вебсайту. Детально метод описаний в п.2.3.

2.2 Обґрунтування вибору критеріїв оцінювання надійності вебсайту

Визначення (проєктування) функціональних і нефункціональних вимог є ключовим кроком у процесі веброзробки, який стосується не лише розробки ПЗ, а й вебсайту. Від початку важливо знати для чого насправді призначений вебсайт і як він має функціонувати. І з цієї точки зору функціональні та нефункціональні вимоги можуть гарантувати очікування клієнтів, вони настільки ж важливі у створенні вебсайту, гарантуючи, що його сторінки взаємодіють, функціонують (поведінка, час завантаження тощо) одна з одною та користувачем згідно з очікуванням клієнтів.

Функціональні вимоги описують, що має робити вебсайт (його функції). На відміну від них, нефункціональні вимоги стосуються не функцій вебсайту, а натомість розглядають критерії, яким вебсайт має відповідати, тобто яким він має бути. Для прикладу нефункціональні вимоги можуть охоплювати час відгуку, час розробки, зручність використання та надійність. Вони також можуть бути тісно пов’язані зі задоволеністю користувачів.

Отже, нефункціональною є вимога, яка визначає критерії, за якими можна оцінити роботу вебсайту, а не конкретну поведінку. Кожна така вимога не пов’язана з операцією чи тим, що має робити програма. Натомість основним акцентом у цьому випадку є простота використання та продуктивність. Через це нефункціональні вимоги важко виміряти та визначити, коли їх успішно виконано.

Якщо реалізація функціональних вимог деталізується в проєкті вебсайту, то нефункціональних вимог – в його архітектурі, бо вони переважно є архітектурно

значущими вимогами [32]. Деякі дослідники виокремлюють архітектурні вимоги в окрему групу [33].

Різні джерела використовують різну термінологію. Наприклад, стандарти серії ISO/IEC 25000 [3] визначають нефункціональні вимоги як вимоги до якості системи та якості програмного забезпечення. BABOK, одне з основних джерел знань для бізнес-аналітиків [34], пропонує термін нефункціональні вимоги (non-functional requirements, NFR), який наразі є найпоширенішим визначенням. Тим не менш, ці настанови розглядають один і той же підхід – вимоги, які описують експлуатаційні властивості, а не поведінку продукту. Їхній перелік також змінюється залежно від джерела, і для різних продуктів він може відрізнятися. Наприклад, якщо ви маєте намір збирати будь-які дані користувачів і ваш вебсайт працює в ЄС, ви повинні підпорядковуватися правилам GDPR [35].

Оскільки нефункціональні вимоги важче виразити вимірним способом, це ускладнює їхній аналіз. Переважно вони є властивостями системи в цілому, а тому не можуть бути перевірені для окремих компонентів.

Деякими дослідниками [36] пропонується перейти до формалізації узагальненого критерію рівня якості (гарантоспроможності, надійності) ПС. Така модель передбачає для кожного атрибута комплексну метрику, яка може визначатися розрахунковими, експериментальними чи експертними методами. Далі оцінки окремих атрибутів згортаються в узагальнену оцінку якості як комплексної властивості ПС. Наприклад, це може бути лінійний функціонал, який поєднує кількісні метрики атрибутів з їхніми ваговими коефіцієнтами.

Зазвичай, метрики значною мірою є суб’єктивними та залежать від знань експертів, які проводять кількісне оцінювання атрибутів вебсайту, використаних моделей та шкали оцінок, мети та контексту оцінювання тощо.

На наш погляд, критерії для оцінювання «широкої» надійності вебсайтів мають охоплювати критерії «вузької» надійності та безпекові критерії.

Надійний вебсайт характеризується мінімальним часом простою, хорошою цілісністю даних і відсутністю помилок, які безпосередньо впливають на користувачів. Для оцінювання надійності вебсайту насамперед необхідно сформулювати критерії такого оцінювання. Аналізуючи моделі якості, набір

метрик і показників для оцінювання безпеки і надійності програмних продуктів, нами відібрано 5 ключових критеріїв, які надалі будуть використані для побудови моделі оцінювання надійності вебсайту.

Таблиця 2.1 – Критерії оцінювання надійності вебсайту

№	Критерій	Опис
1.	Готовність (availability)	Ступінь працездатності та доступності вебсайту
2.	Стійкість до відмов (fault tolerance)	Здатність вебсайту працювати як призначено, незважаючи на наявність дефектів програмно-апаратних засобів
3.	Здатність до відновлення (recoverability)	Здатність вебсайту відновити дані та необхідний стан у випадку збою чи несанкціонованого впливу
4.	Цілісність (integrity)	Ступінь запобігання несанкціонованому доступу чи модифікації комп’ютерних програм або даних
5.	Конфіденційність (confidentiality)	Забезпечення обмеження доступу до даних недозволеним особам

Готовність (availability).

У сучасному цифровому світі люди очікують, що вебресурси безперебійно працюватимуть у реальному часі та постійно. Однак базова технологія, яка підтримує цифрові послуги, неймовірно складна для управління, тому збої неодмінно трапляються. Тим часом вартість простою вебсайту зростає в геометричній прогресії, і деякі торговці через це втрачають сотні тисяч доларів за хвилину. Тому IT-організації підтримують угоди про рівень обслуговування (Service Level Agreement, SLA) щодо надійності вебсайтів і часу безвідмовної роботи, визначаючи стандарти, необхідні для безперебійної роботи бізнесу, незважаючи на неминучі збої в IT.

Готовність вебсайту (або час його безвідмовної роботи) означає здатність користувачів отримати доступ до вебсайту чи вебресурсу та використовувати їх. Говорячи про готовність, часто мають на увазі співвідношення доступного часу до загального часу. Доступність вебсайту зазвичай показують у відсотках за певний

проміжок часу (наприклад доступність 99,9%). 100% безвідмовна робота – це недосяжна, якщо не нездійсненна мета в довгостроковій перспективі.

Готовність, як міру безвідмовної роботи, можна розрахувати у такий спосіб:

Відсоток доступності = (*загальний період часу – сумарний час простоїв*) / *загальний період часу*

Часто постачальники послуг укладають угоду про рівень доступності (SLA) на основі таблиці відсотка доступності, зобов'язуючись гарантувати, що функціональні можливості працюють згідно з очікуваннями власників сайту і користувачів. За умови відсутності запланованих простоїв у табл.2.2 вказано, скільки часу простою дозволено для досягнення певного рівня готовності. Залежно від необхідного рівня точності, можна використовувати години, хвилини, секунди чи мілісекунди. Так вебсайт з однією годиною простою протягом усього року матиме 99,99% безвідмовної роботи.

Таблиця 2.2 – Готовність вебсайтів [37]

Рівень доступності	Дозволене вікно недоступності					
	За рік	За квартал	За місяць	За тиждень	За день	За годину
90%	36,5 дн.	9 дн.	3 дн.	16,8 год.	2,4 год.	6 хв.
95%	12,85 дн.	4,5 дн.	1,5 дн.	8,4 год.	1,2 год.	3 хв.
99%	3,65 дн.	21,6 год.	7,2 год.	1,68 год.	14,4 хв.	36 сек.
99,5%	1,83 дн.	10,8 год.	3,6 год.	50,4 хв.	7,20 хв.	18 сек.
99,9%	8,76 год.	2,16 год.	43,2 хв.	10,1 хв.	1,44 хв.	3,6 сек.
99,95%	4,38 год.	1,08 год.	21,6 хв.	5,04 хв.	43,2 сек.	1,8 сек.
99,99%	52,6 хв.	12,96 хв.	4,32 хв.	60,5 сек.	8,64 сек.	0,36 сек.
99,999%	5,26 хв.	1,30 хв.	25,9 сек.	6,05 сек.	0,87 сек.	0,04 сек.

Чи готовність означає лише доступність вебсайту? Однак для багатьох брендів, які обіцяють високу доступність, готовність стосується лише часу, протягом якого користувач може ввести URL-адресу та не отримати помилку вебсторінки, наприклад: 404, 500, 503, 504.

Можна зіткнутися з багатьма іншими помилками в результаті збою. Це означає, що користувач не може отримати доступ до сайту чи служби з якоїсь причини, яка не залежить від нього. Тому готовність охоплює не лише можливість

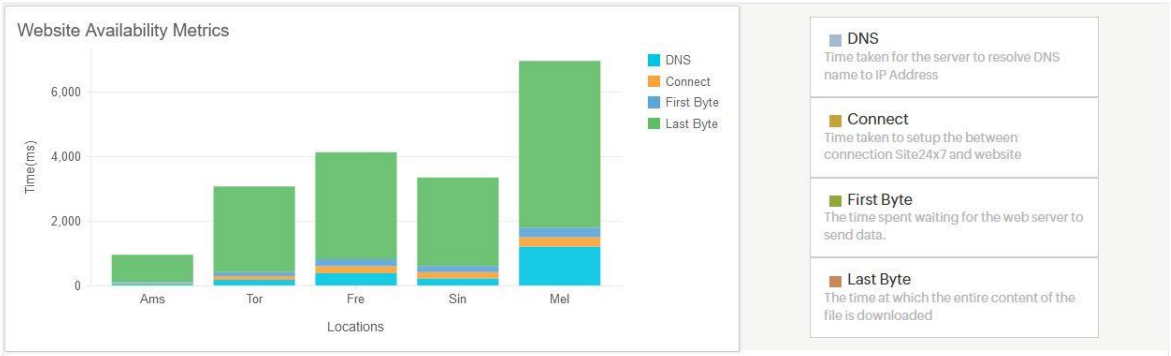
отримати доступ до вебсторінки, а й здатність користувача виконати завдання. Коли власне вебсайт несправний, то з точки зору провайдера хостингу сайт доступний, а з позиції користувача – неготовий. Отже, якщо користувач не може отримати потрібну інформацію чи виконати завдання, вебсайт потрібно вважати неактивним. Для виявлення цього типу збою можна скористатися моніторингом транзакцій [38].

На готовність вебсайту також впливає його продуктивність, оскільки низька продуктивність заважає користувачеві виконати завдання. Тому надійна продуктивність також є чинником готовності. Крім того, повільне завантаження, особливо на мобільних пристроях, також призводить до відтоку споживачів.

Періоди планового технічного обслуговування вебсайту не вважаються простоєм. У цей період розробники переважно перенаправляють користувача на сторінку з вибаченням та поясненням, що сайт перебуває на технічному обслуговуванні, а не повертає код помилки. Техобслуговування в хмарних сервісах проходить легше, оскільки вміст розподіляється між кількома серверами, і у випадку обслуговування одного сервера запити просто перенаправляються на інші доступні сервери, уникаючи простоїв.

Комплексна стратегія моніторингу – найкращий вибір для підтримки високої готовності вебсайту. Для відстеження доступності власникам доводиться перевіряти, чи користувачі без помилок можуть підключатися до їхнього вебсайту впродовж регулярних частих тестових інтервалів. Автоматизоване тестування може перевіряти час безвідмовної роботи так часто, що навіть короткі збої, які впливають на їхніх користувачів, фіксуються у звітах про безвідмовну роботу. У процесі моніторингу перевіряється відповідь вебсайту з допомогою зовнішніх серверів. Використовуючи зовнішні сервери, можна виявити проблеми безвідмовної роботи та затримки на основі розташування користувачів. Приклад тестування готовності вебсайту наведено на рис.2.6.

Website Availability Results: 22 Sep 2022 02:01:54 PM Test results : - http://wunu.edu.ua



Location	Status	IP	(ms)	(ms)	(ms)	(ms)	Size	Response Time (ms)
Fremont-CA - US	OK	193.104.213.106	384	215	214	3,306	65 KB	4,119
Toronto - CA	OK	193.104.213.106	176	119	120	2,643	65 KB	3,058
Amsterdam - NL	OK	193.104.213.106	53	30	29	843	65 KB	955
Melbourne - AUS	OK	193.104.213.106	1,204	291	292	5,147	65 KB	6,934
Singapore - SG	OK	193.104.213.106	225	194	189	2,731	65 KB	3,339

Рисунок 2.6 – Результати зовнішнього оцінювання доступності вебсайту

Стійкість до відмов (fault tolerance).

Під відмовою розуміють втрату здатності вебсайту виконувати потрібну функцію або нездатність виконувати її за визначених умов [39]. Стійкість до відмов – це здатність вебсайту залишатися доступним користувачеві при виникненні технічних проблем та перевантажень. Щоб зробити його максимально стійким до відмов, необхідно заздалегідь оцінити потенційне навантаження і забезпечити продуктивність вебсервера. Повністю убезпечити вебсайт від збоїв неможливо. Однак звести кількість помилок до мінімуму і забезпечити безперебійний доступ до нього цілком реально.

Відмовостійкість безпосередньо пов’язана з навантаженням на вебсайт і здатністю сервера впоратися з обсягом завдань.

У процесі взаємодії користувачів з вебсайтом виконується велика сукупність завдань, різних за характером та обсягом. Навантаження на сайт відповідно призводить до навантаження на сервер. Якщо останній не може впоратися з кількістю запитів, це спричиняє помилки та обмеження доступу до вебсторінок. Помилкам, спричиненим проблемами на стороні сервера, виділено номери в діапазоні 500-599, які користувачі можуть побачити на екрані. Хоча періодичні збої в роботі вебсайту зазвичай є нормою, проте систематичне накопичення згаданих

помилок (5xx) часто спричиняє зниження авторитетності вебресурсу в пошуковій системі та є свідченням низької надійності вебсайту.

Для забезпечення високої стійкості до відмов варто подбати про достатню кількість ресурсів сервера, тобто обсяг навантаження на вебсайт необхідно контролювати. Висока відмовостійкість пов’язана з сервером, програмним забезпеченням, створенням копій даних на декількох серверах – за відмови одного сервера, вебсайт продовжить роботу на іншому.

До основних причин зниження відмовостійкості вебсайту належать:

– зростання трафіку;
– DDoS-атаки;
– активне сканування сайту роботом;
– некоректна робота скриптів.

Працюючи з показником стійкості до відмов необхідно оцінити продуктивність сервера – який час займає опрацювання запитів і наскільки він відповідає встановленим критеріям.

Тестування навантаження та балансування ресурсів сервера зробить відмовостійкість вищою. Навантажувальне тестування полягає в створенні штучного навантаження на вебсайт і відстеженні наскільки система справляється з цим обсягом. Зараз широко використовуються он-лайн послуги з навантажувального тестування (Site24x7.com, Alertra.com, Builtwith.com, Gtmetrix.com, Webpagetest.org), а також спеціальні додатки для визначення очікуваного навантаження на вебсайт (Apache JMeter, WebLOAD RadViews, Gatling).

Стійкість до відмов допомагає зрозуміти, як і коли вебсайт функціонуватиме за реальних сценаріїв, знаючи частоту та вплив збоїв. Найзагальніші показники для вимірювання відмовостійкості:

Середній час напрацювання на відмову (*Mean time between failures, MTBF*) = *загальний час роботи* / *кількість відмов*.

Частота відмов (*frequency of failures*) = *кількість відмов* / *загальний час роботи*.

Іншими класичними показниками для вимірювання стійкості до відмов є:

– MTTF: Mean time to failure (середній час до відмови);

– PFD: Probability of failure on demand (ймовірність відмови при запиті);

– DC: Diagnostic coverage (діагностичне покриття) – відношення кількості виявлених відмов до загальної кількості відмов.

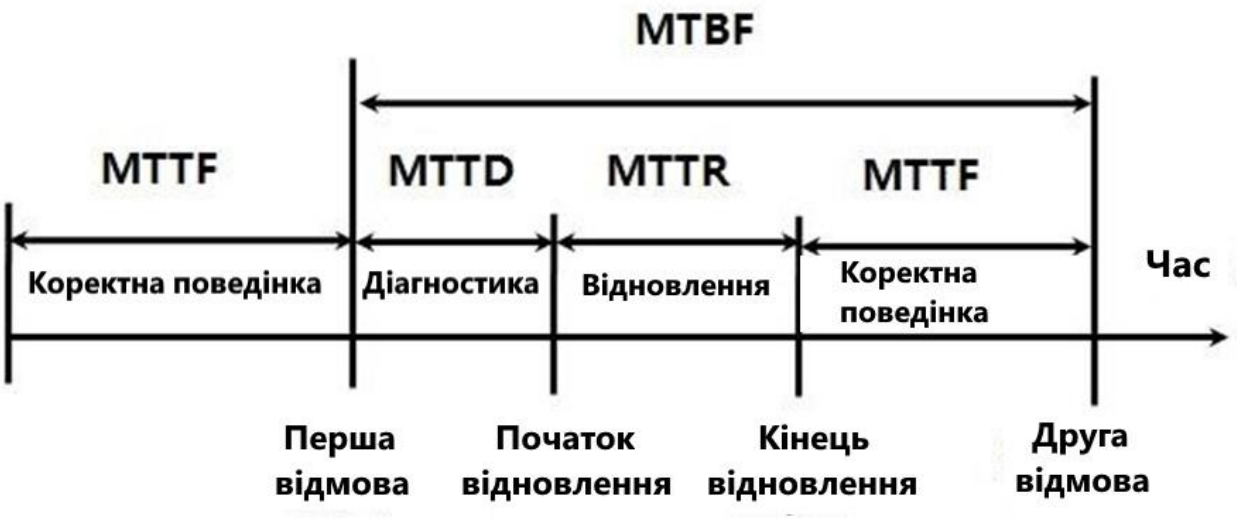


Рисунок 2.7 – Взаємозв’язок показників MTTF, MTTR, і MTBF

Здатність до відновлення (recoverability).

Стратегія стійкості вебсайту також має містити цілі аварійного відновлення (Disaster Recovery, DR), базовані на відновленні працездатного стану у випадку відмов. Таке відновлення необхідне у відповідь на стихійні лиха, масштабні технічні збої чи людські загрози, такі як атака чи помилка.

З цим критерієм пов’язані два поняття, котрі визначаються власником вебсайту (рис.2.8):

– цільовий час відновлення (Recovery Time Objective, RTO) – максимально прийнятна затримка між перериванням обслуговування та його відновленням, тобто прийнятне часове вікно, коли вебсайт недоступний;

– цільова точка відновлення (Recovery Point Objective, RPO) – максимально прийнятний проміжок часу з останньої точки відновлення даних. Вона показує точку часу, на яку можна відновити дані.

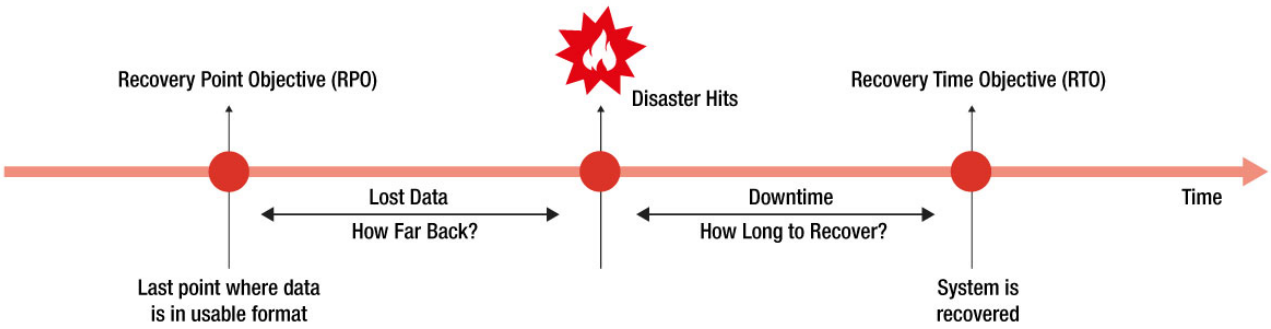


Рисунок 2.8 – Цільовий час відновлення і цільова точка відновлення

По суті, RPO – це вік файлів, відновлених із резервного сховища, які необхідні для відновлення нормальної роботи вебсайту. Наприклад, якщо RPO рівний одній годині, резервне копіювання здійснюється принаймні один раз на годину. Це означає, що у аварійному випадку потенційно втрачається до однієї години даних. Формуючи план неперервності бізнесу, важливо визначитися з обсягом даних, від яких готові відмовитися, якщо резервне копіювання знадобиться для роботи.

RTO – це максимальний час, протягом якого вебсайт може бути недоступним. Він визначає, скільки часу вебсайт може бути непрацездатним, перш ніж втрати – як у доходах, так і в даних – і витрати на відновлення роботи систем стануть нездоланними. Інколи рентабельним залишається втратити сервер на тиждень, тоді як в інших випадках кожна хвилина простою може означати втрату критичних даних, клієнта або доходу.

В ідеальній ситуації обидва ці показники мають бути максимально близькими до нуля. Однак у реальному житті витрати на досягнення нульових RPO та RTO будуть надто високі та, ймовірно, не окупляться. Значення цих показників можуть різнитися в різних компаніях, проте завжди вони мають бути компромісом між вимогами бізнесу до доступності даних та необхідними інвестиціями в IT. Їхні значення переважно визначать в ході діалогу між бізнес-підрозділами та IT-спеціалістами компанії. Для полегшення обчислень цих показників можна скористатися он-лайн калькуляторами часу відновлення, наприклад [41]. Для

оцінювання відновлюваності вебсайту можна використати також показник MTTR (Mean time to recovery) – середній час до відновлення працездатності.

Резервне копіювання (бекап) захистить дані та дасть змогу швидко повернути працюючу версію вебсайту. Без щоденного резервного копіювання є ризик втратити вебсайт зі всіма його напрацюваннями, даними та відвідувачами.

Переважно всі дані вебсайту (БД, файли налаштувань та ін.) зберігаються на сервері хостинг-провайдера. Завдяки бекапу вони копіюються в інше місце (на запасний сервер, яким може бути власний комп'ютер або віддалений сервер іншого провайдера, а також файлообмінник або хмарне сховище).

При оцінюванні критерію відновлюваності конкретного вебсайту варто враховувати такі аспекти резервного копіювання:

– регулярність (чим частіше проводиться бекап, тим більше актуальних даних вдається відновити);

– комп'ютеризованість (дає змогу забезпечити постійне копіювання);

– ізольованість (копії не варто зберігатися на тому ж сервері, що й вихідні дані; бажано мати кілька резервних копій);

– цілісність (після створення бекапу варто перевіряти його на можливість відновлення).

Таким чином, надійність вебсайту значною мірою залежить від частоти і засобів резервування.

Цілісність (integrity).

Цілісність означає ступінь запобігання несанкціонованому доступу або модифікації комп'ютерних програм чи даних. Вона безпосередньо пов'язана з його захищеністю. Ця категорія вимог до якості вебсайту описує, що потрібно для блокування несанкціонованого доступу до певних функцій, як запобігти втраті інформації, як забезпечити захист системи від вірусної інфекції та як захистити конфіденційність і безпеку даних, що вводяться в систему.

У сучасну епоху великих даних, коли обробляється та зберігається все більше обсягів інформації, справність даних стала актуальною проблемою, а впровадження заходів, які зберігають цілісність зібраних даних, стає дедалі

важливішим. Розуміння основ цілісності даних і принципів їх роботи є першим кроком у захисті даних.

Варто зазначити, що для вебсайтів характеристика цілісності даних відрізняється від якості даних і безпеки даних, хоча часто відбувається підміна понять.

Безпека даних – це сукупність заходів, вжитих для запобігання пошкодженню даних, яка передбачає використання систем, процесів і процедур, що обмежують неавторизований доступ і зберігають дані недоступними для інших, які можуть використовувати їх у шкідливий або ненавмисний спосіб. Тоді як цілісність даних пов’язана зі збереженням інформації в недоторканості та точності впродовж усього її існування. Тому безпека даних є лише одним із багатьох аспектів цілісності даних і недостатньо широка, щоб охопити багато процесів, необхідних для збереження даних незмінними протягом тривалого часу.

Аналогічно якість даних є лише частиною цілісності даних. Якість даних пов’язана з відповідністю даних у базі даних стандартам, визначеним компанією, та підтримується низкою процесів, які вимірюють вік, актуальність, точність, повноту та надійність даних. Тоді як цілісність даних охоплює всі аспекти якості даних і йде далі, реалізуючи ряд правил і процесів, які керують тим, як дані вводяться, зберігаються, передаються тощо.

На цілісність інформації з вебсайту може впливати низка чинників, таких як:

– людські помилки – коли інформація вводиться неправильно, дублюються або видаляють дані, не дотримуються відповідних протоколів або допускають помилки під час виконання процедур, спрямованих на захист інформації;

– помилки передавання – коли дані невдало передані з одного місця в базі даних до іншого;

– помилки (bugs) та віруси – шпигунське чи зловмисне програмне забезпечення та віруси, які можуть вторгнутися у вебсайт і змінити, видалити або викрасти дані;

– пошкоджене апаратне забезпечення – раптові збої комп’ютера чи сервера та проблеми з функціонуванням пристроїв є прикладами серйозних збоїв і

можуть свідчити про те, що ваше обладнання зламано. Внаслідок цього пошкоджене апаратне забезпечення може відтворювати дані неправильно чи неповно, обмежувати або забороняти доступ до даних, ускладнювати використання інформації.

Ризики через порушення цілісності можна мінімізувати або усунути, виконавши такі контрзаходи:

– контроль доступу та сувора автентифікація, які допомагають запобігти внесенню авторизованими користувачами несанкціонованих змін;

– використання цифрових підписів, які дають змогу переконатися про автентичність транзакцій;

– проведення регулярних внутрішніх аудитів шляхом перевірки хешу і моніторингу журналів вебсайту, щоб вияснити, чи файли не змінено або пошкоджено;

– резервне копіювання, яке дає можливість відновити пошкоджені дані та вебресурси;

– використання спеціалізованих ПЗ для виявлення помилок;

– засоби адміністративного контролю, такі як розподіл обов’язків і навчання персоналу, що підвищує відповідальність персоналу.

Цілісність даних охоплює:

– фізичну цілісність – дані зберігаються на безпечній, надійній фізичній платформі;

– логічну цілісність – дані є точними, правильними та незмінними, навіть якщо вони використовуються в різних контекстах у реляційній базі даних;

– відповідність – дані відповідають і підтримують необхідні стандарти відповідності.

Звідси до основних характеристик цілісності даних належать:

– повнота – чи всі записи бази даних заповнені;

– точність – чи дані мають правильну форму та надають відповідну інформацію в контексті;

– узгодженість – чи всі дані відформатовані однаково;

– своєчасність – дані, зібрані в режимі реального часу мають найвищу цінність;

– відповідність – чи відповідають дані всім застосовним стандартам, наприклад нормативним актам щодо конфіденційності.

Метриками атрибуту цілісності вебсайту можна розглядати [41]:

1) рівень цілісності обчислювальних ресурсів – можливість виключати непередбачені структурні зміни та послуги;

2) рівень цілісності програмних ресурсів – можливість виключати непередбачені зміни програмних ресурсів;

3) рівень цілісності інформації – здатність системи забезпечувати незмінність інформації в умовах випадкового та (або) навмисного спотворення (руйнування).

Конфіденційність (confidentiality).

Конфіденційність означає, що дані та ресурси вебсайту захищені від несанкціонованого перегляду та іншого доступу. Захист конфіденційності може починатися з визначення та контролю рівнів доступу до інформації всередині та ззовні. Коли доступність даних обмежена, значно знижується ймовірність випадкового чи навмисного витоку інформації.

Зазвичай вебсайти містять інформацію з певним ступенем конфіденційності. Це може бути конфіденційна бізнес-інформація, яку конкуренти можуть використати у своїх інтересах, або особиста інформація про працівників або клієнтів. Конфіденційна інформація має певну цінність, тому вебсайти часто піддаються атакам, оскільки зловмисники шукають уразливості, щоб використати їх. Діапазон загроз – від прямих атак, таких як викрадення паролів і захоплення мережевого трафіку, і до багатошарових атак (соціальна інженерія та фішинг).

Зрештою, не всі порушення конфіденційності є навмисними. Причиною також може бути людська помилка чи недостатній контроль безпеки. Наприклад, хтось може не захистити свій пароль для робочої станції або для входу в зону обмеженого доступу. Користувачі можуть поділитися своїми обліковими даними з кимось іншим або дозволити комусь бачити свій логін під час введення. В інших ситуаціях користувач може неправильно зашифрувати зв’язок, даючи змогу

зловмиснику перехопити його інформацію. Часто такі порушення є наслідком халатності (безвідповідальності) персоналу.

Для боротьби з порушеннями конфіденційності можна класифікувати та маркувати обмежені дані, увімкнути політики контролю доступу, шифрувати дані та використовувати системи багатофакторної автентифікації (MFA).

Конфіденційність є важливим атрибутом для вебсайтів як відкритих і розподілених систем, в основу яких закладена мережева ідеологія. Для оцінювання конфіденційності рекомендують скористатися такими метриками як ймовірність загроз і рівень секретності [41].

Отже, якщо цілісність можна трактувати як критерій зовнішньої безпеки вебсайту, як його властивість бути незмінним при функціонуванні за умов випадкових або навмисних спотворень чи руйнівних впливів ззовні (зовнішнім агентом), то конфіденційність можна вважати критерієм його внутрішньої безпеки, тобто властивістю забезпечувати захист від несанкціонованого використання інформації, її заміни чи пошкодження зсередини (внутрішнім агентом).

2.3 Модель експертного оцінювання надійності вебсайту на основі багатокритеріального вибору

У літературі існують різні погляди на те, як варто вимірювати якість вебсайту, і його надійності зокрема [42, 43]. Оскільки вимірювання надійності вебсайту охоплює як матеріальні, так і нематеріальні заходи, воно розглядається як багатокритеріальна проблема прийняття рішень (multi-criteria decision making, MCDM). У літературі описано багато доступних методів вирішення проблем MCDM [44]. Але метод аналітичної ієрархії (AHP), розроблений Т. Сааті [45], є одним із найпрактичніших методів експертного оцінювання, який широко використовується і виявився успішним у багатьох галузях.

Метод дає змогу включати судження як щодо матеріальних даних, так і нематеріальних даних. AHP базується на створенні матриць попарного порівняння за допомогою відповідної шкали для оцінювання критеріїв й альтернатив і дає

змогу особам, які приймають рішення, структурувати ієрархію, щоб вибрати найкращу з різних альтернатив (рис.2.6).

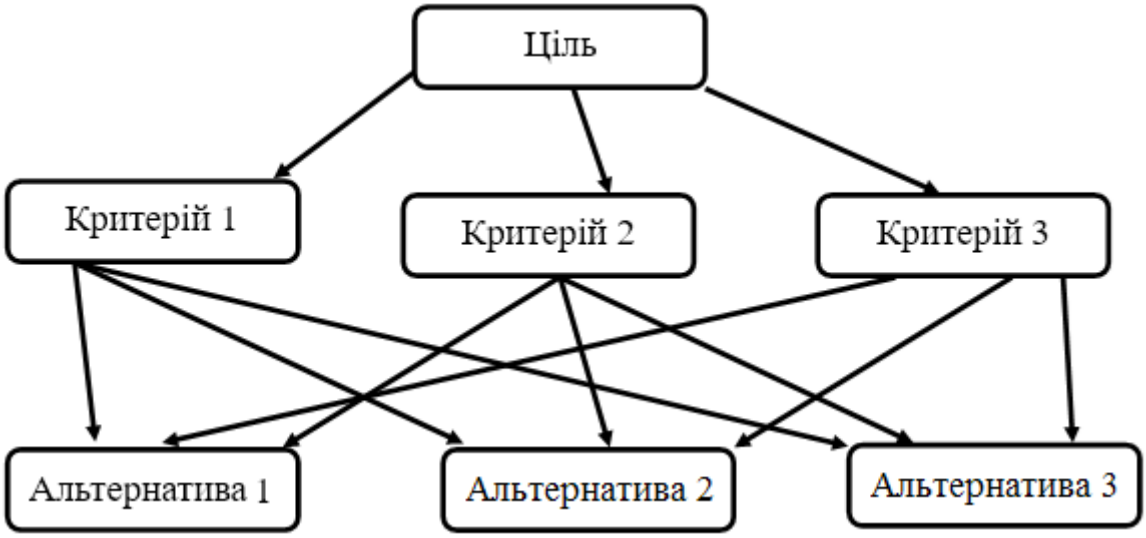


Рисунок 2.6 – Ієрархічна структура проблеми багатокритеріального вибору

Метод аналітичної ієрархії (AHP) є корисним методом для вирішення складних проблем прийняття рішень, пов'язаних із суб'єктивним судженням [45]. У ньому вимірювання ваги обчислюється через попарне порівняння відносної важливості двох чинників. Якщо припустити, що існує N елементів прийняття рішень, позначених як (E_1, ... , E_i, . . . , E_n), його матриця оцінок буде $A = [a_{ij}]$, де a_{ij} представляє відносну важливість E_i та E_j. Потім, використовуючи нормалізацію середнього вектора-рядка, запропоновану Сааті [45], вага E_i обчислюється як

$$w_i = \frac{\left(\prod_{j=1}^{n} a_{ij}\right)^{1/n}}{\sum_{i=1}^{n}\left(\prod_{j=1}^{n} a_{ij}\right)^{1/n}}, \quad i, j = 1, 2, \ldots, n, \tag{2.1}$$

де w_i – вага i-го елемента рішення,

w – вектор ваги: $w = (w_i)$, $i = 1,..., n$.

Оскільки вебтехнології та середовища їх застосування містять невизначеність і нематеріальність (intangible), оцінювання надійності вебсайту стає непростою справою як для користувачів, так і розробників. Більшість ОПР схильні оцінювати цю характеристику вебсайту на основі власних суб'єктивних і неточних

суджень. У результаті необхідне глибше розуміння відносної важливості надійності вебсайту для різних груп зацікавлених осіб. З цих причин у цьому дослідженні застосовано нечіткий підхід AHP для створення нечіткої моделі оцінювання, яка визначає відносну важливість чинників надійності вебсайту. Це розширить здатність ОПР аналізувати рішення.

Хоча AHP розроблений для отримання знань особами, які приймають рішення, звичайний AHP не повністю відображає стиль людського мислення. Загальновизнано, що людина оперує лінгвістичними та неточними моделями при вирішенні складної проблеми. Такі лінгвістичні та неточні описи неможливо було застосувати в методі AHP до появи можливостей нечіткого прийняття рішень. Теорія нечітких множин нагадує людські міркування з використанням приблизної інформації та невизначеності у процесі прийняття рішень. Основним внеском цієї теорії є її здатність представляти нечіткість, тоді як AHP було розроблено для вирішення проблеми прийняття рішень за кількома атрибутами. Завдяки поєднанню теорії нечітких множин з AHP, Fuzzy-AHP дає змогу точніше описувати процес прийняття рішень за багатьма атрибутами. Найпершою роботою з Fuzzy-AHP була [46], де порівнювали нечіткі співвідношення, описані за допомогою трикутних функцій належності. Після появилося багато досліджень з використанням Fuzzy-AHP для розрахунку важливості (ваги) елементів оцінювання [44]. Тому в даному дослідженні надано перевагу нечіткому підходу AHP, оскільки він є адекватним для явного фіксування оцінок важливості за неточних суджень людини.

Для вирішення проблеми з неоднозначністю людського мислення Л. Заде вперше представив теорію нечітких множин, яка може ефективно описати неточні знання чи людське суб'єктивне судження за допомогою лінгвістичних термінів, які мають нечіткий характер. Оскільки лінгвістичні терміни лише наближені до суб'єктивного судження тих, хто приймає рішення, для представлення нечіткості цих лінгвістичних термінів використовується широко поширена техніка нечітких трикутних чисел [47, 48]. Під трикутним нечітким числом розуміють спеціальну нечітку множину $\tilde{F}$, що характеризується функцією приналежності $\mu_{\tilde{F}}(x)$, яка пов'язує дійсне число з інтервалу [0, 1] з кожним елементом *x* в *X*, щоб представити

ступінь приналежності x до $\tilde{F}$. Трикутне нечітке число можна визначити як $\tilde{T} = (l, m, u)$, а його функція належності дорівнює:

$$\mu_{\tilde{F}}(x) = \begin{cases} \dfrac{x-l}{m-l},\ l \le x \le m \\ \dfrac{u-x}{u-m},\ m \le x \le u \\ 0, \text{ в інших випадках} \end{cases} \tag{2.2}$$

де l та u – нижнє та верхнє значення з кортежу $\tilde{T}$ відповідно;

m – середнє значення $\tilde{T}$.

Якщо дано будь-які два трикутних нечітких числа, $\tilde{T}_1 = (l_1, m_1, u_1)$ і $\tilde{T}_2 = (l_2, m_2, u_2)$, та додатне дійсне число r, то деякі основні операції трикутних нечітких чисел $\tilde{T}_1$ і $\tilde{T}_1$ можуть бути виражені таким чином:

$$\tilde{T}_1 \oplus \tilde{T}_2 = (l_1 + l_2, m_1 + m_2, u_1 + u_2) \tag{2.3}$$

$$\tilde{T}_1 \otimes \tilde{T}_2 \cong (l_1 \times l_2, m_1 \times m_2, u_1 \times u_2) \tag{2.4}$$

$$r \otimes \tilde{T}_1 \cong (rl_1, rm_1, ru_1) \tag{2.5}$$

$$\tilde{T}_1^{-1} \cong (1/l_1, 1/m_1, 1/u_1) \tag{2.6}$$

Процедура обчислення в Fuzzu-AHP розпочинається зі шкалування відносної важливості критеріїв. Конструкція анкети передбачає попарне порівняння елементів рішення в ієрархічній структурі. Кожного оцінювача просять виразити відносну важливість двох критеріїв на одному рівні за 9-бальною шкалою. Бали попарного порівняння формують матрицю попарного порівняння для кожного з K експертів.

Далі оцінки попарного порівняння перетворюються на лінгвістичні змінні, представлені трикутними нечіткими числами (див. табл.2.6).

Таблиця 2.6 – Трикутні нечіткі числа

Лінгвістичні змінні	Трикутні нечіткі числа
Рівна важливість	(1, 1, 1)
Проміжне значення	(1, 2, 3)
Слабка важливість	(2, 3, 4)
Проміжне значення	(3, 4, 5)
Сильна важливість	(4, 5, 6)
Проміжне значення	(5, 6, 7)
Дуже сильна важливість	(6, 7, 8)
Проміжне значення	(7, 8, 9)
Абсолютна важливість	(9, 9, 9)

Матрицю нечітких оцінок можна визначити як:

$$\tilde{R}^k = \left[\tilde{r}_{ij} \right]^k, \tag{2.7}$$

де $\tilde{R}^k$ – матриця нечітких суджень *k*-го експерта;

$\tilde{r}_{ij}^k$ – нечіткі оцінки між критерієм *i* та критерієм *j* *k*-го експерта:

$$\tilde{r}_{ij}^k = (l_{ij}^k, m_{ij}^k, u_{ij}^k);$$

n – кількість відповідних критеріїв на цьому рівні;

$\tilde{r}_{ij}^k = (1,1,1), \ \forall i = j;$

$\tilde{r}_{ij}^k = 1/\tilde{r}_{ji}^k, \ \forall i, j = 1,2,...,n$

Наступним кроком є тест на узгодженість. Нехай $\tilde{R} = \left[\tilde{r}_{ij} \right]$ є матрицею нечітких суджень із трикутними нечіткими числами $\tilde{r}_{ij} = (\alpha_{ij}, \beta_{ij}, \gamma_{ij})$ і формою $R = \left[\beta_{ij} \right]$. Якщо *R* узгоджено, то й $\tilde{R}$ узгоджено. Сааті [45] запровадив індекс узгодженості для вимірювання будь-якої невідповідності в оцінках кожної матриці попарного порівняння, а також для всієї ієрархії. Індекс узгодженості (*CI*) формулюють наступним чином:

$$CI = \frac{\lambda_{\max} - n}{n-1}, \tag{2.8}$$

де λ_{max} – максимальне власне значення,

n – розмірність матриці.

Відповідно, коефіцієнт узгодженості (*CR*) можна розрахувати за допомогою наступного рівняння:

$$CR = \frac{CI}{RI}, \tag{2.9}$$

де *RI* – випадковий індекс узгодженості, взятий з таблиці.

Якщо розраховане значення *CR* матриці попарного порівняння менше 0,1, послідовність попарного судження можна вважати прийнятною. Однак, якщо узгодженість не пройдена, вихідні значення в матриці парного порівняння мають бути переглянуті експертами.

Далі переходять до проведення дефазифікації. Існують різні методи дефазифікації, і метод, використаний у цьому дослідженні, був отриманий з методу дефазифікації перетворення нечітких даних у чіткі оцінки, запропонованим в [49] для виконання нечіткого агрегування. Цей підхід може чітко виражати нечітке сприйняття, базоване на процедурі визначення нижнього та верхнього балів за нечітким *min* і нечітким *max*, а загальний бал визначається як середньозважене відповідно до функцій належності.

Нехай $\tilde{r}_{ij}^{k} = (l_{ij}^{k}, m_{ij}^{k}, u_{ij}^{k})$ вказують на нечіткі оцінки між критерієм *i* та критерієм *j k*-го експерта. Тоді процедури дефазифікації можна описати наступним чином:

1) нормалізація:

$$xl_{ij}^{k} = (l_{ij}^{k} - \min l_{ij}^{k}) / \Delta_{\min}^{\max}, \tag{2.10}$$

$$xm_{ij}^{k} = (m_{ij}^{k} - \min l_{ij}^{k}) / \Delta_{\min}^{\max}, \tag{2.11}$$

$$xu_{ij}^{k} = (u_{ij}^{k} - \min l_{ij}^{k}) / \Delta_{\min}^{\max}, \tag{2.12}$$

де $\Delta_{\min}^{\max} = \max u_{ij}^{k} - \min l_{ij}^{k}$;

2) обчислення нижнього (*ls*) і верхнього (*us*) нормалізованих значень:

$$xls_{ij}^{k} = xm_{ij}^{k} / (1 + xm_{ij}^{k} - xl_{ij}^{k}), \tag{2.13}$$

$$xus_{ij}^{k} = xu_{ij}^{k} / (1 + xu_{ij}^{k} - xm_{ij}^{k}); \tag{2.14}$$

3) обчислення загального нормалізованого чіткого значення:

$$x_{ij}^{k} = \left[xls_{ij}^{k}(1 - xls_{ij}^{k}) \right] / \left[1 - xls_{ij}^{k} + xus_{ij}^{k} \right]; \quad (2.15)$$

4) обчислення чіткого значення:

$$r_{ij}^{*k} = \min l_{ij}^{k} - x_{ij}^{k} \Delta_{\min}^{\max}, \quad (2.16)$$

де r_{ij}^{*k} – чіткі оцінки між критерієм *i* та критерієм *j* *k*-го експерта, $\forall i, j$ =1, 2, ..., *n*;

5) інтеграція чітких значень:

Геометричне середнє використовується для інтеграції чітких значень *K* експертів,

$$r_{ij}^{*} = \sqrt[K]{(r_{ij}^{*1} \times ... \times r_{ij}^{*K})}, \quad (2.17)$$

де r_{ij}^{*} – сукупність чітких оцінок критерію *i* та критерію *j* *K* експертів, $\forall i, j$ =1, 2, …, *n*,

K – кількість експертів.

Після застосування методу дефазифікації для виконання процедури нечіткої агрегації встановлюється агрегатна матриця чітких суджень. Цю матрицю можна створити як:

$$R^{*} = \left[r_{ij}^{*} \right], \quad (2.18)$$

де R^{*} – сукупна чітка матриця суджень *K* експертів;

r_{ij}^{*} – сукупність чітких оцінок критерію *i* та критерію *j* *K* експертів, $\forall i, j$ =1, 2, ..., *n*.

Завершує побудову моделі розрахунок ваг критеріїв і отримання остаточного рейтингу.

Відповідно до процедури розрахунку ваги, запропонованої в AHP, використовуючи рівняння (2.1), розраховують вершину ваг $W^{*} = (w_i^{*})$, i =1, ..., *n* для агрегованої матриці чітких оцінок *R**. Порядок ранжування критеріїв визначається ваговою вершиною *W**.

Загальна схема процесу, розробленого для моделювання оцінок надійності вебсайту показана на рис.2.7.

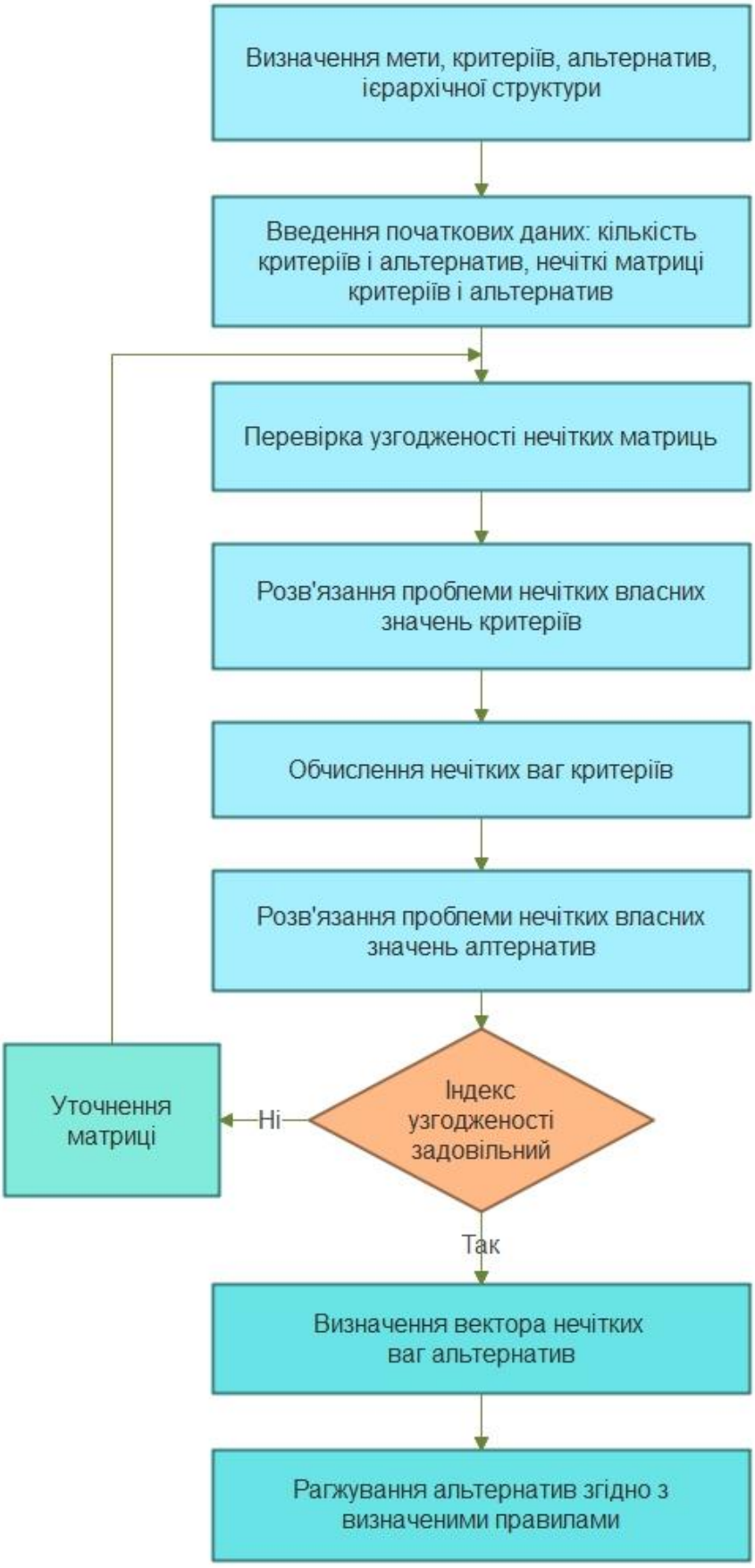


Рисунок 2.7 – Схема моделі на основі Fuzzi-AHP

Отже, через те, що процес оцінювання надійності вебсайту характеризується когнітивною невизначеністю, породженою суб’єктивними судженнями користувачів, для побудови моделі використано теорію нечітких множин. Це розширить можливості осіб, які приймають рішення, краще аналізувати рішення. Використання нечітких чисел у поєднанні з AHP для моделі нечіткого оцінювання, дає змогу точніше визначати пріоритетність відносної ваги чинників, котрі впливають на надійність вебсайтів.

Висновки до розділу 2

1. Здійснено обґрунтування вибору критеріїв оцінювання надійності вебсайту, до яких відібрано:

2. Оскільки вимірювання надійності вебсайту охоплює як матеріальні, так і нематеріальні заходи, воно розглядається як багатокритеріальна проблема прийняття рішень (multi-criteria decision making, MCDM). Тому для вказаного оцінювання доцільно використати один із методів MCDM.

3. Критерії оцінювання надійності вебсайту мають як об’єктивний, так і суб’єктивний характер, через що в даному дослідженні надано перевагу нечіткому підходу AHP (Fuzzy-AHP), оскільки він є адекватним для явного фіксування оцінок важливості за неточних суджень людини.

4. У розділі дано детальний опис моделі, в основу якої покладено нечіткий метод аналітичної ієрархії.

3 АПРОБАЦІЯ МОДЕЛІ ОЦІНЮВАННЯ НАДІЙНОСТІ ВЕБСАЙТУ

3.1 Реалізація експерименту з моделлю надійності вебсайту

Згідно з методологією дослідження розроблено ієрархічну структуру (рис.3.1), на вершині якої перебуває мета – оцінювання надійності вебсайту. Для процедури оцінювання необхідно визначити набір критеріїв, які утворюють наступний рівень ієрархії. Завершує структуру множина альтернатив – вебсайтів, котрих потрібно оцінити, тобто сформувати їх рейтинг для подальшого вибору найкращого з точки зору надійності. Обґрунтування вибору критеріїв було проведено в попередньому розділі.

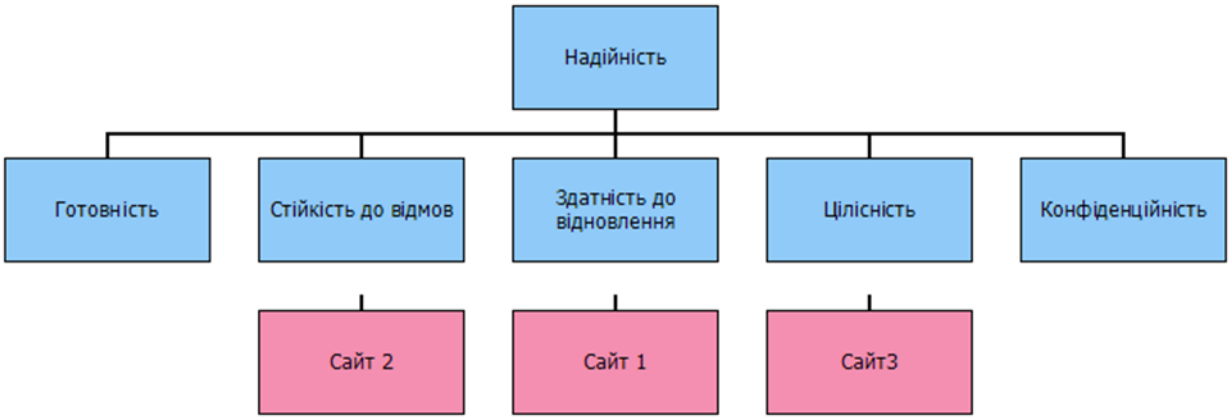


Рисунок 3.1 – Ієрархічна структура оцінювання надійності вебсайту

Для дослідження надійності вебсайтів і проведення оцінювання нами використано метод експертних оцінок. Експертне оцінювання – це оцінювання параметрів процесів або предметів, які неможливо безпосередньо виміряти, тому оцінювання проводиться на підставі професійного досвіду спеціаліста чи групи експертів. Вказаний підхід використано через те, що для деяких критеріїв оцінювання «широкої» надійності неможливо виміряти параметри вебсайтів або вони мають конфіденційний характер.

Метод аналітичної ієрархії передбачає формування двох рейтингів – рейтинг критеріїв і рейтинг альтернатив. Вхідними даними для їхнього обчислення є експертні оцінки, для чого нами було використано анкетування. Анкети

забезпечують відносно швидкий, дешевий та ефективний спосіб отримання значної кількості інформації від великої вибірки людей. Ці дані можна відносно швидко зібрати, оскільки досліднику не завжди потрібно бути присутнім під час заповнення анкет. Таке опитування корисне для великих груп населення, коли інтерв'ю було б недоцільним. Для цього нами розроблено два види анкет для опитування експертів.

Перша анкета розроблена у формі попарного порівняння критеріїв на основі описаної вище ієрархічної структури (рис.3.1). Формат опитувальника (дев'ятибальна шкала оцінок) вказує на відносну важливість кожного критерію в ієрархії (рис.3.2).

Scale table

code	Linguistic variables	L	M	U
1	Рівна важливість	1	1	1
2	Проміжна важливість	1	2	3
3	Слабка важливість	2	3	4
4	Проміжна важливість	3	4	5
5	Сильна важливість	4	5	6
6	Проміжна важливість	5	6	7
7	Дуже сильна важливість	6	7	8
8	Проміжна важливість	7	8	9
9	Абсолютна важливість	9	9	9

Рисунок 3.2 – Шкала оцінювання

Оцінювання здійснювалося 15 експертами, які мають від 1 до 10 років досвіду розробки вебсайтів. Кожен з експертів заповнював індивідуальну анкету (матрицю) (рис.3.3), на основі яких сформована узагальнена матриця нечітких оцінок (рис.3.4). Знайдене середнє всіх думок експертів використовується надалі для формування матриці прямих зв'язків.

Pairwise comparison tables (Expert 1)

Please enter scale codes in the table, for Reciprocal scale enter negative codes.

Table 1: Pairwise comparison with respect to Надійність
Inconsistency ratio: CRm: 0.038,CRg: 0.09 (Consistent matrix)

	Готовність	Відмовостійкість	Відновлюваність	Цілісність	Конфіденційність
Готовність		-9	-8	-5	-8
Відмовостійкість			1	4	-2
Відновлюваність				4	1
Цілісність					-4
Конфіденційність					

Рисунок 3.4 – Приклад матриці оцінок окремого експерта

Mean

mean method

Table 1: Pairwise comparison with respect to Надійність
Inconsistency ratio: CRm:0.023 , CRg:0.057 (Consistent matrix)

	Готовність	Відмовостійкість	Відновлюваність	Цілісність	Конфіденційність
Готовність		(0.111,0.118,0.143)	(0.111,0.145,0.200)	(0.111,0.149,0.250)	(0.111,0.118,0.143)
Відмовостійкість			(1.000,1.732,4.000)	(1.000,2.000,5.000)	(0.333,0.500,1.000)
Відновлюваність				(0.200,1.000,5.000)	(0.250,0.577,1.000)
Цілісність					(0.200,0.354,1.000)
Конфіденційність					

Рисунок 3.4 – Усереднена матриця попарних порівнянь критеріїв

Метою опитування було зібрати думки експертів, щоби виміряти відносну вагу критеріїв надійності вебсайту. Експертні оцінки перевірялися на узгодженість. Якщо величина коефіцієнта узгодженості (CR) перевищувала 0.1, оцінки підлягали коригуванню.

На основі узагальнених нечітких оцінок критеріїв розраховувались ваги цих критеріїв. Результати обчислень наведено на рис.3.5.

Найвищий рейтинг отримав критерій «Конфіденційність» (0,296), а далі слідують критерії «Відмовостійкість», «Відновлюваність», «Цілісність» і «Готовність». Несподіваний результат у експертів отримав критерій «Готовність»

(0). Очевидно, що це є синтезуючий показник, який залежить від інших чотирьох, тобто готовність вебсайту залежить від стійкості до відмов, здатності до відновлення, цілісності та конфіденційності.

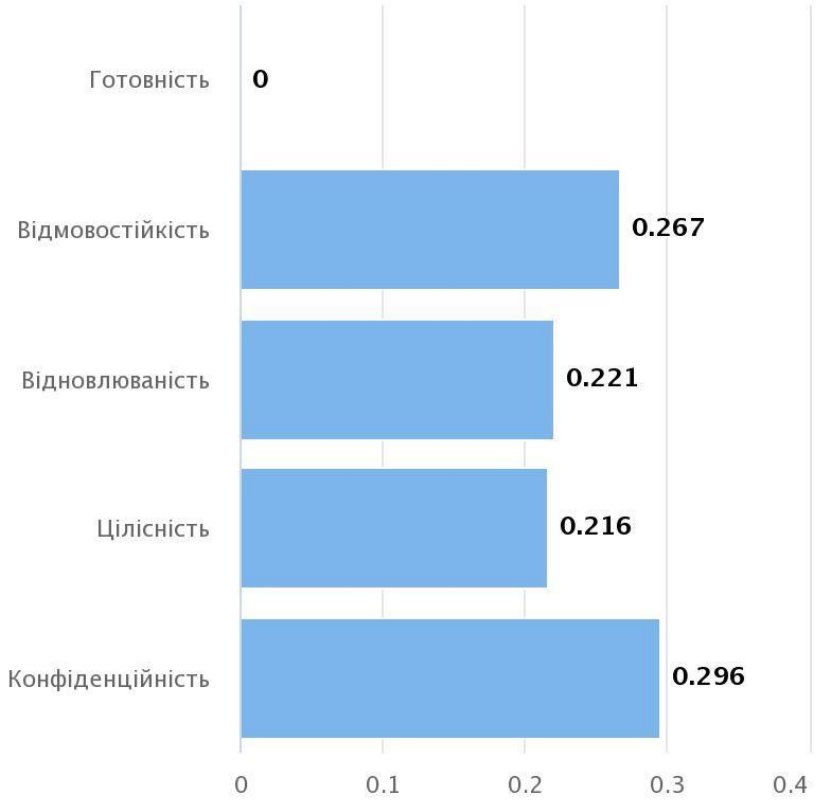


Рисунок 3.5 – Ваги критеріїв оцінювання надійності

Другий тип анкети спрямований на визначення рейтингу вебсайтів. Для апробації моделі було вибрано три вебсайти, які оцінювалися за вказаними вище критеріями. Оцінювання альтернатив (вебсайтів) проводилося за тією ж шкалою, що й критеріїв (рис.3.2).

Розраховані узагальнені матриці нечітких оцінок експертів для кожного критерію показані на рис.3.6. Коректність цих оцінок підтверджується коефіцієнтом узгодженості, значення якого знаходиться в межах допустимого (0,1).

Підсумок порівняння вебсайтів у розрізі кожного критерію зведено в табл.3.1.

Table 6: Alternative pairwise comparisons with respect to Конфіденційність
Inconsistency ratio: CRm:0.001 , CRg:0.021 (Consistent matrix)

	Вебсайт 1	Вебсайт 2	Вебсайт 3
Вебсайт 1		(4.000,5.916,8.000)	(3.000,4.472,6.000)
Вебсайт 2			(0.333,0.707,1.000)
Вебсайт 3			

Table 3: Alternative pairwise comparisons with respect to Відмовостійкість
Inconsistency ratio: CRm:0.017 , CRg:0.006 (Consistent matrix)

	Вебсайт 1	Вебсайт 2	Вебсайт 3
Вебсайт 1		(4.000,5.000,6.000)	(2.000,3.000,4.000)
Вебсайт 2			(0.250,0.408,1.000)
Вебсайт 3			

Table 4: Alternative pairwise comparisons with respect to Відновлюваність
Inconsistency ratio: CRm:0.006 , CRg:0.009 (Consistent matrix)

	Вебсайт 1	Вебсайт 2	Вебсайт 3
Вебсайт 1		(4.000,5.476,7.000)	(1.000,2.828,5.000)
Вебсайт 2			(0.250,0.408,1.000)
Вебсайт 3			

Table 5: Alternative pairwise comparisons with respect to Цілісність
Inconsistency ratio: CRm:0.001 , CRg:0.037 (Consistent matrix)

	Вебсайт 1	Вебсайт 2	Вебсайт 3
Вебсайт 1		(2.000,3.000,4.000)	(2.000,3.873,6.000)
Вебсайт 2			(1.000,1.414,3.000)
Вебсайт 3			

Table 2: Alternative pairwise comparisons with respect to Готовність
Inconsistency ratio: CRm:0.002 , CRg:0.051 (Consistent matrix)

	Вебсайт 1	Вебсайт 2	Вебсайт 3
Вебсайт 1		(1.000,2.449,4.000)	(1.000,2.000,3.000)
Вебсайт 2			(0.333,0.707,1.000)
Вебсайт 3			

Рисунок 3.6 – Усереднені матриці нечітких оцінок для кожного критерію

Таблиця 3.1 – Рейтинг і порівняльні ваги вебсайтів за критеріями

Критерії	Ваги			Рейтинг		
	Вебсайт1	Вебсайт2	Вебсайт3	Вебсайт1	Вебсайт2	Вебсайт3
Готовність	0,471	0,205	0,324	1	3	2
Відмовостійкість	0,780	0	0,220	1	3	2
Відновлюваність	0,676	0	0,324	1	3	2
Цілісність	0,723	0,265	0,012	1	2	3
Конфіденційність	0,996	0	0,004	1	3	2

Розрахунки ваг критеріїв і їхній рейтинг, а також рейтинг вебсайтів здійснювалися з допомогою програмного забезпечення Online Output Software [50]. Кінцевий рейтинг оцінюваних вебсайтів представлено на рис.3.7.

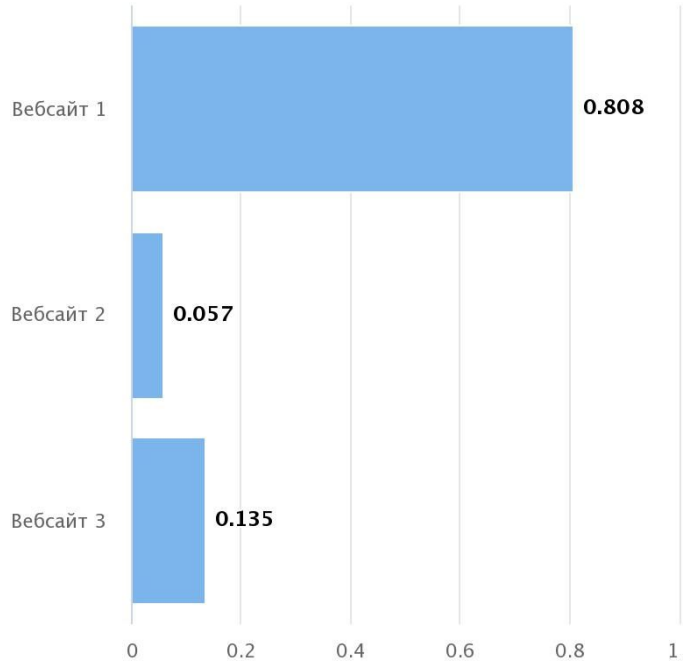


Рисунок 3.7 – Підсумковий рейтинг вебсайтів

Як бачимо, в підсумку Вебсайт 1 суттєво випереджує інші вебсайти за надійністю загалом, а також за кожним критерієм зокрема.

Отже, тестування багатокритеріальної моделі оцінювання надійності вебсайту продемонструвало її ефективність, практичну спроможність та можливість застосування на різних етапах життєвого циклу вебсайту.

3.2 Рекомендації з підвищення надійності вебсайтів

Аналіз особливостей надійності вебсайтів, критеріїв оцінювання надійності та метрик її вимірювання в даному дослідженні дав змогу сформувати низку рекомендацій щодо підвищення рівня надійності вебсайтів. Деякі з них передбачають одноразові процедури, налаштувань та рідкісних перевірок

працездатності, а інші вимагають на постійних перевірок, оновлень та пильної уваги.

1. Виберіть кращий сервер для хостингу.

Основне завдання забезпечення доступності до вебсайту як одної з найважливішої його характеристики лежить на хостингу. Оскільки надійність роботи вебсайту прямо залежить від хостинг-провайдера, тому його вибір є відповідальною справою. Багато з них пропонують клієнтам послуги регулярного резервного копіювання, моніторингу мережі, підтримки PHP і вебскриптів, а також вбудовані панелі управління сервером, захист від вірусів й інших атак.

Кожен вебхостинг має різні функції, тому звертають увагу на такі ключові елементи, як власні технології кешування, твердотільні накопичувачі чи контроль над критичними областями. Спільний хостинг часто має менше ресурсів, і тоді може знадобитися VPS або хмарний хостинг. На надійність вебсайту впливатимуть інциденти на стороні провайдера, наприклад, простій сервера, збій програмного забезпечення, порушення безпеки, помилки обслуговуючого персоналу та ін. Важливим елементом є оперативна та доступна технічна підтримка у випадку виникнення будь-яких проблем.

Усі плани вебхостингу згідно з угодою про рівень послуг (SLA) мають заздалегідь визначену кількість ресурсів для використання. Якщо вебсайт постійно використовує чи перевищує обсяг виділених йому ресурсів, можуть виникнути проблеми. Недостатні ресурси можуть призвести до сповільнення або навіть призупинення облікового запису. Варто пам’ятати, що переважно ви ділитеся ресурсами з багатьма іншими користувачами. Якщо хтось постійно максимізує використання ресурсів, уся система може страждати від низької продуктивності.

Тому при виборі (чи переході до) кращого вебхостингу доцільно витратити деякий час на дослідження для переконання, що обраний хостинг-провайдер відповідає сучасним технічним вимогам і зможе вчасно відреагувати на непередбачені проблеми.

Однак не завжди доступність вебсайту залежить від хостингу. Якщо останній працює нормально, а в коді вебсайту з’явилася помилка, то він не відкриватиметься

і буде недоступним для користувачів. Тому на доступність вебсайту впливає його технічна справність.

2. Регулярно контролюйте обслуговування облікового запису на стороні хостингу.

Вебсайт і обліковий запис хостингу потребують тривалого обслуговування. Наприклад, у процесі експлуатації вебсайту кількість таблиць на боці провайдера мають тенденцію збільшуватися, тому, можливо, доведеться їх скоротити. Так само в обліковому записі хостингу може вичерпатися місце на диску, оскільки вебсайт і бази даних зростають. Важливо мати провайдера, котрий завчасно перевірить і вирішить такі проблеми задля безперебійної роботи вебсайту. Доцільно також контролювати строки угоди з хостинг-провайдером і своєчасність оплати послуг, щоби вебсайт не відключили у несподіваний момент.

3. Розробляйте вебсайт незалежним (від програмного забезпечення провайдера, браузера чи девайса користувача).

Програмне забезпечення хостингу не завжди повністю сумісне з функціоналом вебсайту. Іноді відсутня підтримка певного функціоналу, наприклад, останньої версії PHP, JavaScript тощо. Тому варто вияснити це у хостинг-провайдера відразу та бути готовим до цього в майбутньому.

Якість відображення вебсторінок на моніторі інтернет-відвідувача залежить від властивостей та характеристик браузера. Наприклад, в старих версіях браузера можуть з’їжджати окремі блоки, зникати чи значно змінюватися рамки, відступи тощо. Для підвищення надійності роботи вебсайту доводиться враховувати можливість роботи в старих версіях популярних браузерів. Щоби не втрачати користувачів, варто оптимізувати сайт під різні браузери.

Незалежність також має проявлятися від цілісності файлової системи та функціональних модулів. Тобто в ідеалі сайт має продовжувати працювати навіть у ситуації, коли з окремих каталогів видалено певні файли чи перестають функціонувати окремі плагіни, тощо.

4. Дотримуйтесь принципу KISS

KISS є абревіатурою від «Keep It Simple, Stupid». Термін придумано в 1960-х роках, і він наголошує на ефективності простих систем. Цей принцип стосується і

створення вебсайтів. Архітектура й загальна кількість файлів, які формують вебсайт, суттєво можуть впливати на його надійність. Чим більше файлів різних форматів (HTML, PHP, JavaScript, CSS), тим вища ймовірність їхньої відмови. Можливі помилки, через які втрачаються зв'язки між окремими файлами (вони стають недоступними). Внаслідок цього вебсайт повністю чи частково втратить свою працездатність. Кожна додаткова частина коду програми є потенційним шлюзом для зловмисника. Тому не варто використовувати на сайті жодних зайвих модулів, плагінів та іншого непотрібного функціоналу, оскільки вони сильно ускладнюють та заплутують програмний код, збільшують загальну кількість файлів і обсяг вебсайту. Саме тому відносно невеликі вебпроєкти є стабільнішими та надійнішими, ніж великі. Уникаючи надто складних реалізацій і дизайнів, вебсайт стає швидшим і, що важливіше, простішим в управлінні та обслуговуванні.

Старайтесь не ускладнювати систему навігації вебсайту. Зростання обсягу контенту спричиняє складність системи навігації. Характеристикою складності навігації є загальна кількість гіперпосилань. Тому, чим їх більше в системі навігації, тим ймовірніша поява непрацюючих гіперпосилань.

5. Підтримуйте вебсайт в актуальному стані.

На етапі розгортання вебсайту найкращим способом уникнути помилок є дотримання найкращих практик щодо впровадження оновлень і змін на вебсайті. Передові методи охоплюють тестування всіх змін у середовищі розробки до того, як надсилати їх у робоче середовище. Під час цього процесу завжди потрібно проходити ретельний процес тестування прийнятності користувачами (User Acceptance Testing) для переконання, що зміни, застосовані до сайту, не порушили його нормальне функціонування.

Усі оновлення коду на вебсайті варто ретельно перевіряти, перш ніж надсилати на активний вебсайт. Крім того, варто застосовувати стандарти кодування та найкращі практики. Це допоможе гарантувати чистоту коду, який завантажуватиметься швидко та ефективно, і, таким чином, допоможе підвищити рейтинг у пошукових системах і уникнути простоїв і помилок замість безперебійної роботи.

Усе програмне забезпечення, необхідне для роботи вебсайту, має бути оновлено до останньої версії. Існує багато різних вразливостей вебсайтів, тому важливо оновити компоненти сторонніх розробників, таких як плагіни, теми та розширення. Також це стосується антивірусних програм і баз. Підтримуючи все в актуальному стані, зменшуємо ймовірність відмов і загроз для вебсайту.

6. Не забувайте про редизайн вебсайту.

Якщо вебсайт містить багато помилок і застарілий контент, перевантажений медіаресурсами, погано стикується з базою даних, його важко знайти в пошукових системах, тоді варто провести реконструкція (редизайн). Найкращим індикатором необхідності проведення редизайну є співвідношення кількості відвідувачів до кількості відвіданих вебсторінок упродовж певного часового інтервалу. Завдяки редизайну усуваються помилки в його структурі, що, відповідно, підвищує надійність його роботи і стійкість до відмов, зокрема.

Разом з тим, існує інша крайність. Усі вебсайти дуже динамічні, їхня еволюція є постійною та суттєвою, тому важливо постійно контролювати їхню якість (і надійність у т.ч.), щоб уникнути поступового руйнування здорового проєкту через часті зміни. Це особливо важливо для сучасних вебсайтів, еволюція яких визначається не лише керівництвом сайту, а й спільнотою користувачів.

7. Заздалегідь вирішуйте проблему масштабованості.

Необхідно, щоби вебсайт витримав раптові стрибки трафіку, тобто він має функціонувати безперебійно, а середовище хостингу готове обробляти його трафік. Тому варто провести тест завантаження вебсайту для переконання, що сайт і хостинг готові до пікового одночасного трафіку. Особливо це актуально для сфери електронної комерції. Якщо потрібна додаткова потужність хостингу для майбутнього трафіку, деякі хости можуть за потреби запустити додаткові «підсилювальні» сервери. За умови непередбачуваних стрибків трафіку (наприклад, раптовий вірусний трафік із соціальних мереж), варто скористатися засобами автоматичного масштабування, щоби завжди бути готовими до несподіванок.

Одним з інструментів тестування вебсайту є інженерія хаосу – практика навантаження на сайт шляхом створення руйнівних подій, таких як раптове

збільшення споживання ЦП або пам’яті, спостереження за реакцією системи та впровадження вдосконалень. Сучасні вебсайти настільки ускладнилися, що потрібні автоматизовані засоби (наприклад, AWS Fault Injection Simulator [51]) для виявлення невідомих проблем.

8. Періодично виконуйте аудит плагінів.

Сьогодні багато вебсайтів використовують систему керування вмістом (CMS), зокрема WordPress, яку використовують понад 30% усіх вебсайтів в інтернеті. Вона проста у застосуванні, використовує модульний підхід, що дає змогу користувачеві замінити кодування так званими плагінами. Однак WordPress є відкритим вихідним кодом, куди кожен (від професіоналів до аматорів) може зробити свій внесок у пул плагінів. У результаті якість плагінів у цьому пулі значно відрізняється.

Навіть вебсайти, які не працюють на WordPress, можуть стати жертвами «синдрому плагінів», оскільки використовують сторонні додатки для покращення своїх сайтів. Застосування надмірної кількості плагінів може значно сповільнити вебсайт, а також створити більшу загрозу його безпеці.

Перед переходом до оптимізації вебсайту, варто оцінити використовувані теми та плагіни. Потрібно задатися питаннями, чи всі використовувані плагіни потрібні, чи всі вони створені професійними розробниками з хорошими відгуками та документацією. Адже чимало плагінів розроблено з думкою про дохід, тобто пропонують зручні функції, проте не враховують продуктивність та безпеку. Більшість вебдизайнерів займаються тим, що виглядає добре, а не тим, що швидко і надійно працює.

9. Забезпечте вебсайтові відповідний рівень стійкості до відмов.

Серйозні проєкти мають працювати без перебоїв навіть у випадку відмови окремих підсистем. А причин для збоїв у роботі вебсайту чимало – вихід із ладу серверної апаратури, збої програмного забезпечення, аварії на рівні дата-центрів. Проте всіх цих ризиків можна уникнути чи мінімізувати їхні наслідки.

Варто врахувати, що побудова і супровід системи з відмовостійкістю складніші та дорожчі, ніж розробка й підтримка звичайної системи. Тому підходити до проєктування кожного конкретного рішення варто з погляду

економічної доцільності. Для цього часто доводиться приймати компромісні рішення, а тому критерії прийняття рішення мають бути об’єктивними.

Щоби забезпечити нормальний рівень доступності вебсайту не потрібно будувати відмовостійку систему: досить якісно написаного коду програми, адекватних процесів супроводу, а також скористатися послугами професійних хостингових компаній, які резервують канали зв’язку, живлення та охолодження обладнання, використовують надійні виділені сервери.

Досягнення високого рівня доступності вже ґрунтується на механізмі побудови відмовостійких систем, зокрема дублювання всіх критичних підсистем, що дає змогу вебсайту функціонувати навіть за умови виходу з ладу одного з його компонентів.

Чим стійкіший до відмов вебсайт, тим дорожча інфраструктура і тим складніші інженерні завдання, пов’язані зі забезпеченням її роботи. Економічна доцільність підходів до відмовостійкості визначається індивідуально в кожному конкретному випадку.

10. Не нехтуйте безпекою вашого вебсайту.

Більшість власників вебсайтів помилково вважають, що їх сайт не представляє жодної цінності для хакерів, а тому немає сенсу його зламувати. Хоча найпривабливішими цілями для зловмисників залишаються інтернет-банкінги та онлайн-магазини, кількість зламів різноманітних вебсайтів невпинно зростає. Навіть якщо порушення роботи вебсайту чи його дані не дають безпосередньої вигоди зловмисникам, вони можуть використовувати зламаний сайт для подальшого нападу на інші об’єкти, для розсилання спаму чи файлів незаконного характеру. За це власники вебсайту можуть нести відповідальність. Саме тому критично важливо заздалегідь підготувати захист усіх своїх вебресурсів.

Також можна передати безпеку вебсайту на аутсорсинг професіоналам, завдяки чому будуть заощаджені час і кошти.

11. Забезпечте ведення журналу вебсайту та моніторинг подій безпеки.

Рекомендація, що стосується відслідковування в журналі всіх подій та моніторингу подій безпеки, пов’язана з виявленням атак і їх протидією, а також розслідуванням інцидентів безпеки, котрі вже відбулися. Тому, крім стандартних

журнальних засобів, надаваних вебсервером, необхідно переконатися в реєстрації часу події та ідентифікатора користувача, а також потенційно небезпечної активності, характерної для вебсайту. У випадку виявлення шкідливої активності необхідно заблокувати сесію користувача чи заблокувати за IP-адресою, загалом вжити заходів і повідомити про це адміністратору.

З багатьох категорій захисних рішень лише WAF (Web Application Firewall) здатен забезпечити комплексний захист вебзастосунків від відомих і невідомих загроз, а також забезпечити відповідність вимогам безпеки.

Іноді виникають проблеми, які виходять за межі планового технічного обслуговування. Це можуть бути проблеми з безпекою та завантаженням, які надзвичайно важливо своєчасно вирішити. Тому повинна бути моніторингова команда (це може бути вебхостинг), яка стежить за простоєм вебсайту та іншими критичними проблемами, щоб своєчасно повідомити й допомогти пом’якшити проблему.

12. Придбайте для вебсайту сертифікат TLS.

TLS (Transport Layer Security), а також його попередник SSL (Secure Sockets Layer), є криптографічним протоколом, котрий забезпечує безпечне передавання даних в інтернеті. Вказаний сертифікат необхідний кожному вебсайтові. У деяких браузерах вже передбачено режими, де сайти без сертифікату не відображаються взагалі. Сертифікат TLS забезпечує конфіденційність інформації та підтверджує автентичність вебсайту, що особливо важливо при використання відкритих бездротових мереж. Банківські карти, логіни, паролі та інші особисті дані, захищені сертифікатом, приховані від чужих очей. Крім цього, сертифікат важливий для SEO (пошукової оптимізації). Наприклад, пошукувач Google надає перевагу вебсайтам з наявністю сертифікату. Варто також оновлювати версії сімейства протоколів TLS, щоби залишатися захищеними, адже протоколи з часом старіють і стають небезпечними.

13. Регулярно виконуйте резервне копіювання.

Важливо мати налагоджені процеси створення резервних копій (бекапів) із певною періодичністю. Таким чином можна застрахуватися від втрати даних у випадках:

– зараження вірусами;
– зламу вебсайту;
– несправності сервера;
– механічного пошкодження носія;
– випадкового видалення файлів сайту;
– аварії хостера.

Бекапи – справді універсальний захід безпеки. Єдина проблема безпеки, від якої не захищає резервне копіювання – це витік інформації. Зазвичай бекапи вебсайтів здійснюються автоматично за допомогою спеціальних плагінів, модулів або скриптів. Періодичність і вид бекапів зазвичай задаються в CMS, але можливий варіант резервного копіювання вручну.

При резервуванні важливими є місце та вид зберігання даних. Ефективним підходом є шифрування сховищ критичних даних і резервних копій, а також зберігання файлів резервних копій не разом з файловою системою, а в іншому місці, безпека якого не викликає сумнівів і яке завжди буде під рукою для швидкого розгортання.

З позиції безпеки доцільно створити декілька дзеркал вебсайту. Якщо щось трапиться з одним дзеркалом, відвідувачі зможуть потрапити на вебсторінки через інші дзеркала.

14. Обов’язково перевіряйте завантажувані на вебсайт файли.

Можливість користувачів завантажувати файли на вебсайт є величезним ризиком. Варто з обережністю ставитися до всіх файлів, навіть непримітних, бо вони можуть містити шкідливі скрипти, які через сервер відкриють зловмисникам доступ до вебсайту. Необхідно перевіряти файли на віруси перед завантаженням і відкриттям. Виконувані файли, завантажені з підозрілих джерел, повинні відкриватися в ізольованому середовищі, наприклад під віртуальною машиною. Доцільно використовувати системи перевірки цілісності файлів на сервері та щодня переглядати їхні звіти.

Ніколи не довіряйте користувачеві та завжди чітко фільтруйте те, що надсилається на вебсайт. Випадкове пошкодження може бути таким же шкідливим, як і навмисне.

Загальним заходом захисту для запобігання ін’єкції SQL-коду та міжсайтового виконання сценаріїв (XSS-атаки), є перевірка всіх вхідних даних на відповідність синтаксичної та семантичної норми. Під синтаксичною нормою розуміють повну відповідність вхідних даних очікуваній формі представлення, а семантична норма підтверджує, що вхідні дані не виходять межі конкретного функціонала.

15. Забезпечте надійну парольну політику.

Важливо забезпечити використання користувачами та адміністраторами вебсайту складних унікальних паролів. Це один із найкращих і найпростіших способів захистити облікові записи від зламу, а закриту інформацію – від крадіжок. Для керування паролями використовуйте відповідні інструменти, що забезпечить надійність та унікальність паролів. З боку вебсайту також важливо не зберігати паролі у відкритому вигляді в базі даних, а використовувати відомі бібліотеки та функції для хешування паролів. Також установіть термін дії паролів, завдяки чому вони будуть надійними та своєчасно оновленими.

Окрім пароля, варто скористатися двофакторною автентифікацією (2FA) або двокроковою верифікацією (2SV) як додатковим бар’єром захисту у випадках витоку паролів. У цьому випадку для входу в обліковий запис користувачеві необхідно буде ввести підтвердження, наприклад, у вигляді одноразового коду з мобільного додатку. Ця функція значно підвищить рівень безпеки, ускладнивши процес крадіжки облікового запису.

16. Перевіряйте вебсайт на наявність вразливостей.

Ефективним методом оцінювання безпеки веб-сайту є тестування, яке можна реалізувати кількома способами:

– сканування –для пошуку різних вразливостей та проблем безпеки, а також для перевірки безпеки інфраструктури вебсайту;

– перевірка – для виявлення рівня захищеності вебресурсу від загроз і переконання у відсутності шкідливих програм, які хакери часто впроваджують у контент, розміщений на вебсайті третіми особами;

– тестування на проникнення – для знаходження вразливостей фахівцями з безпеки з метою оцінювання рівня захисту вебсайту та ймовірності витоку інформації, збоїв сервісу чи несанкціонованого доступу.

Існує широкий спектр проактивних і реактивних засобів для захисту від хакерських атак через використання вразливостей на вебсайті. Потрібно переконатися, що на вебсайті встановлено найновіші патчі безпеки. Для середовища хостинг-сервера знадобляться останні версії програмного забезпечення, наприклад PHP. Необхідно розгорнути та налаштувати профілактичні рішення, такі як брандмауер вебзастосунків (Web Application Firewall). Потрібно регулярно запускати сканери шкідливих програм і виявлення вторгнень, щоби стежити за підозрілою активністю. Також перевірте журнал на наявність відхилень, щоби виявити всю важливу інформацію, таку як некоректна конфігурація програм, випадки збоїв, спроби нападу тощо.

Для переконання, що безпека вебсайту перебуває на належному рівні, варто провести ретельніший аудит безпеки.

17. Організуйте детальний розподіл прав доступу.

Задля безпеки варто обмежити можливості кожного члена команди з управління вебсайту. Наприклад, надання прав адміністратора широкому колові є одним із ризиків безпеки, який можна обмежити за допомогою правильних дозволів. Дизайнеру, який розробляє вебсайт, не потрібні права адміністратора. Це також відносно простий спосіб посилити захищеність.

Деякі області вебсайту потребують обмежувальних рівнів доступу, тому варто скористатися багатофакторною автентифікацією для зміцнення конфіденційності.

Дозволяйте публічний доступ лише до загальнодоступних областей вашого вебсайту, за умовчанням забороніть весь інший трафік. Розмежування доступу можна організувати за допомогою правил конфігурації сервера, встановлення дозволів на файли та папки та використання брандмауера.

Дозволяйте адміністраторам лише безпечний доступ, заборонивши прямий доступ до вебсайту із загальнодоступних точок. Це можна дозволити лише через

захищений канал, тому переконайтеся, що адміністратори мають доступ лише із захищених пристроїв.

18. Захистіть доступ до адміністративної панелі вебсайту.

Заключною рекомендацією є захист адміністративної панелі – одного із слабких місць вебсайту завдяки великому функціоналові, пов’язаному з додаванням (редагуванням) постів і сторінок, роботою з файлами та ін. Тому важливо забезпечити належний контроль доступу, а також максимальну прихованість від зловмисників місцезнаходження адміністративної панелі, що можна реалізувати шляхом простого перенесення адреси на нестандартний пристрій та максимальною захищеністю цієї точки входу від перебору, фільтрацією за IP-адресами та ін. Створення системи контролю доступу варто базувати на таких принципах: відправлення всіх запитів через систему контролю доступу; заборона доступу за замовчуванням (тобто відхиляти запит, якщо він не був дозволений спеціально); встановлення мінімальних привілеїв усім користувачам, програмам чи процесам; реєстрація всіх подій, пов’язаних із контролем доступу.

Висновки до розділу 3

1. На основі ієрархічної структури, до котрої входить п’ять відібраних критеріїв, реалізовано експеримент з моделлю надійності на прикладі трьох вебсайтів. Для цього розроблено два типи анкет і проведено експертне опитування. Експертні оцінки перевірялися на узгодженість. Якщо величина коефіцієнта узгодженості перевищувала 0.1, оцінки підлягали коригуванню.

2. На основі узагальнених нечітких оцінок критеріїв розраховувались ваги критеріїв. Найвищий рейтинг отримав критерій «Конфіденційність» (0,296), а далі слідують критерії «Відмовостійкість», «Відновлюваність», «Цілісність» і «Готовність». Аналогічним чином розраховувався рейтинг тестованих вебсайтів.

3. Проведене тестування розробленої моделі продемонстрували її ефективність та можливість застосування у практичній діяльності.

4. За результатами дослідження сформовано набір рекомендацій для підвищення надійності вебсайтів.

ВИСНОВКИ

1. У роботі розглянуто існуючі підходи до визначення поняття надійності вебсайту. На наш погляд, існує широке (dependability) і вузьке (reliability) трактування надійності програмних систем, у т.ч. і вебсайтів. Вузька надійність вважається одним із декількох вимірів широкої надійності, поряд з доступністю, безпекою, цілісністю тощо.

2. Зроблено уточнення поняття «широкого» трактування надійності вебсайту: «Надійність є збірним терміном часових характеристик якості вебсайту, який охоплює поняття вузької надійності (reliability), доступності, можливості відновлення, стійкості до відмов, а також його безпеки та конфіденційності».

3. Виявлено особливості надійності вебсайтів. До основних чинників, які впливають на надійність їх роботи належать: ступінь незалежності від програмного забезпечення, застосовуваного хостинг-провайдером; загальна кількість файлів, з яких утворено сайт; система навігації вебсайту; ступінь незалежності від цілісності файлової системи та функціональних модулів; ступінь незалежності від браузерів, використовуваних користувачами; надійність хостинг-провайдера й хмарних сервісів; давність проведення редизайну вебсайту; сукупність внутрішніх і зовнішніх загроз, котрі спричиняють несприятливі наслідки роботи та збитки для власника вебсайту; використовувана система безпеки та конфіденційність доступу до ресурсів.

4. На основі аналізу моделей якості, набору метрик і показників для оцінювання безпеки і надійності програмних продуктів сформовано п’ять ключових критеріїв оцінювання надійності вебсайту: готовність, стійкість до відмов, здатність до відновлення, цілісність і конфіденційність. Вказані критерії були використані для побудови моделі оцінювання надійності вебсайту.

5. Оцінювання надійності вебсайту (як однієї з найважливіших характеристик його якості) охоплює багато критеріїв і оцінюються з допомогою різних методів і моделей. У роботі проаналізовано методи оцінювання надійності програмних систем і обґрунтовано вибір багатокритеріальних методів прийняття рішень

(Multiple Criteria Decision Making) для експертного оцінювання надійності вебсайту.

6. Розроблено багатокритеріальну модель оцінювання надійності вебсайтів на основі нечіткого методу аналітичної ієрархії. Використання нечіткої логіки обумовлено суб’єктивним характером експертних оцінок надійності вебсайту.

7. Проведено тестування розроблення багатокритеріальної моделі оцінювання надійності вебсайту, яке продемонструвало її ефективність, практичну спроможність та можливість застосування на різних етапах життєвого циклу вебсайту. Виявлено, що чинник готовності вебсайту є синтезуючим показником надійності, який залежить від інших чотирьох: стійкості до відмов, здатності до відновлення, цілісності та конфіденційності.

8. За результатами дослідження дано набір рекомендацій для підвищення надійності вебсайтів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ДСТУ ISO/IEC 25010:2016. Інженерія систем і програмних засобів. Вимоги до якості систем і програмних засобів та її оцінювання (SQuaRE). Моделі якості системи та програмних засобів (ISO/IEC 25010:2011, IDT). [Чинний від 2018-01-01]. Київ: УкрНДНЦ, 2018. 32 с.

2. Говорущенко Т. О. Дослідження відомих моделей оцінювання характеристик програмного забезпечення. *Вісник Хмельницького національного університету*. 2013. №1. С.117-121.

3. ДСТУ ISO/IEC 25000:2015. Інженерія програмних засобів і систем. Вимоги щодо якості та оцінювання систем і програмного продукту (SQuaRE). Настанова щодо SQuaRE. [Чинний від 2016-01-01]. Київ: УкрНДНЦ, 2016.

4. ISO/IEC 25063:2014. Systems and software engineering – Systems and software product Quality Requirements and Evaluation (SQuaRE) – Common Industry Format (CIF) for usability: Context of use description. 2014. 33 p.

5. ISO/IEC TS 25011:2017. Information technology – Systems and software Quality Requirements and Evaluation (SQuaRE) – Service quality models. 2017. 21 p.

6. ДСТУ ISO/IEC/IEEE 24765:2018. Інженерія систем і програмних засобів. Словник термінів (ISO/IEC/IEEE 24765:2017, IDT). [Чинний від 2018-08-15]. Київ: УкрНДНЦ, 2018.

7. IEEE Std 982.1-2005 IEEE Standard Dictionary of Measures of the Software Aspects of Dependability. 2006.

8. Electropedia: The World's Online Electrotechnical Vocabulary. Area: 192: Dependability. URL: https://www.electropedia.org/iev/iev.nsf/display?openform&ievref=192-01-22 (дата відвідання: 14.10.2022).

9. Харченко В. С. Гарантоздатність комп’ютерних систем: проблеми і результати. Авиационно-космическая техника и технология. 2005. №7 (23). С.352-376.

10. Звіт про науково-дослідну роботу «Розробка теоретичних засад створення та дослідження високоефективних гарантоздатних комп’ютерних систем». – шифр

«Гарантоздатність» / Б. Г. Мудла, В. Г. Сербін, А. І. Сухомлин [та ін.]. Держреєстраційний №0105U000532. Київ: ІПММС НАНУ, 2009. 366 с.

11. Laprie J-C. Dependable Computing and Fault Tolerance: Concepts and terminology. Proc. 15th IEEE Int. Symp. on Fault-Tolerant Computing, 1985.

12. ISO/IEC 15939:2017. Systems and software engineering – Measurement process. 2017. 39 p.

13. ДСТУ ISO/IEC 25023:2019 (ISO/IEC 25023:2016, IDT) Інженерія систем і програмних засобів. Вимоги до якості систем програмних засобів та їхнього оцінювання (SQuaRE). Вимірювання якості систем та програмних продуктів. [Чинний від 2019-11-01]. Київ: УкрНДНЦ, 2019.

14. ДСТУ ISO 9000:2007 Системи управління якістю. Основні положення і словник строків. (ISO 9000:2005, IDT). Київ: УкрНДНЦ, 2008.

15. Надежность работы сайта и основные факторы, влияющие на нее. URL: https://www.avahost.ru/nadezhnost-raboty-sajta-i-osnovnye-faktory-vliyayushhie-na-nee/ (дата відвідання: 14.10.2022).

16. Long D. Caroll J. Park C. A Study of the Reliability of Internet Sites. *Proceedings of the Tenth Symposium on Reliable Distributed Systems*. October 1991.

17. Василевський О. М., Ігнатенко О. Г. Нормування показників надійності технічних засобів: навч. посібник. Вінниця: ВНТУ, 2013. 160 с.

18. k6. Grafana Labs. URL: https://k6.io/ (дата відвідання: 30.11.2021)

19. BrowserMob Proxy. URL: http://bmp.lightbody.net/ (дата відвідання: 30.11.2021)

20. Alertra. URL: https://www.alertra.com/ (дата відвідання: 30.11.2021)

21. All-in-One Monitoring Solution. URL: https://www.site24x7.com/ (дата відвідання: 30.11.2021)

22. You get signal. URL: https://www.yougetsignal.com/ (дата відвідання: 30.11.2021)

23. Сервисы, похожие на Host-Tracker. URL: https://startpack.ru/application/host-tracker/alternatives (дата відвідання: 30.11.2021)

24. Usage statistics of content management systems. URL: https://w3techs.com/technologies/overview/content_management (дата відвідання: 30.11.2021)

25. FMEA. URL: http://sewiki.ru/FMEA (дата відвідання: 30.11.2021).

26. Stamatis D. H. Failure Mode and Effect Analysis: FMEA From Theory to Execution, Second Edition. ASQ Quality Press, 2003. 300 p.

27. Векслер Е. М. Менеджмент якості: ентропійний і статистичний підходи. Навчально-методичний посібник. Київ: Наша справа, 2004. 265 с.

28. ДСТУ IEC/ISO 31010:2013 Керування ризиком. Методи загального оцінювання ризику. Київ: УкрНДНЦ, 2013.

29. IEC 61882:2016 Hazard and operability studies (HAZOP studies) – Application guide. International Standard. 2016.

30. Rekik R., Kallel I., Casillas J., Alimi A. Using Multiple Criteria Decision-Making Approaches to Assess the Quality of Web Sites. *International Journal of Computer Science and Information Security*. 2016. Vol.14, No.7. P.747-761.

31. Aydin S., Kahraman C. Evaluation of E-commerce website quality using fuzzy multi-criteria decision-making approach. *IAENG International Journal of Computer Science*. 2012. Vol.39, No.1. P.64–70.

32. Chen L., Ali Babar M., Nuseibeh B. Characterizing Architecturally Significant Requirements. *IEEE Software*. 2013. 30 (2): 38-45.

33. Oshana R. System Requirements. *Developing and Managing Embedded Systems and Products*. 2015. P.159-188.

34. A Guide to the Business Analysis Body of Knowledge (BABOK Guide). Version 3.0, IIBA. 2015. 512 p.

35. General Data Protection Regulation. URL: https://gdpr-info.eu/ (дата відвідання: 30.11.2021).

36. Муха А. А. Количественная оценка уровня гарантоспособности компьютерных систем. *Математичні машини і системи*. 2019. № 4. С.146-153.

37. Google SRE Availability Table. URL: https://sre.google/sre-book/availability-table (дата відвідання: 30.11.2021).

38. What is website availability? URL: https://www.uptrends.com/what-is/website-availability (дата відвідання: 30.11.2021).

39. ДСТУ ISO/IEC 25021:2016 (ISO/IEC 25021:2012, IDT) Інженерія систем і програмних засобів. Вимоги до якості систем і програмних засобів та її оцінювання (SQuaRE). Елементи показника якості. [Чинний від 2016-11-01]. Київ: УкрНДНЦ, 2016.

40. Recovery Time Calculator. URL: https://www.iuvotech.com/recovery-time-calculator (дата відвідання: 14.10.2022).

41. Федухин А. В., Сеспедес Гарсия Н. В. Атрибуты и метрики гарантоспособных компьютерных систем. *Математичні машини і системи*. 2013. № 2. С.195-201.

42. Goi C. L. A Review of Web Evaluation Criteria for E-Commerce Web Sites. *Journal of Internet Banking and Commerce*. December 2012. Vol. 17, No.3.

43. Zahran D. I., Al-Nuaim H. A., Rutter M. J., Benyon D. A Comparative Approach to Web Evaluation and Website Evaluation Methods. *International Journal of Public Information Systems.* 2014. Vol.10. P.21-39.

44. Tzeng G. H., Huang J. J. Multiple Attribute Decision Making: Methods and applications. CRC Press, 2011.

45. Saaty, T. L.: The Analytic Hierarchy Process. McGraw-Hill, New York, 1980.

46. van Laarhoven, P. J. M., & Pedrycz, W. (1983). A fuzzy extension of Saaty's priority theory. Fuzzy Sets and Systems, 11(3), 229–241.

47. Желдак Т. А., Коряшкіна Л. С., Ус С. А. Нечіткі множини в системах управління та прийняття рішень: навч. посіб. Дніпро: НТУ «ДП», 2020. 387 с.

48. Кирик В. В. Математичний апарат штучного інтелекту в електроенергетичних системах: підручник. Київ: Політехніка, 2019. 224 с.

49. Opricovic S., Tzeng G. H. (2003). Defuzzification within a multicriteria decision model. *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems*, 11(5), 635–652.

50. Online Output Software. URL: https://onlineoutput.com/ (дата відвідання: 14.10.2022).

51. Leblanc B. Increase your e-commerce website reliability using chaos engineering and AWS Fault Injection Simulator. URL: https://aws.amazon.com/blogs/devops/increase-e-commerce-reliability-using-chaos-engineering-with-aws-fault-injection-simulator/ (дата відвідання: 14.10.2022).

52. Гладій Г. М., Могильська М. Б. Метрики вимірювання надійності вебсайтів. *Збірник наукових публікацій Мультидисциплінарної наукової інтернет-конференції «Світ наукових досліджень»*. (25-26 жовтня 2022 р.). Випуск 13. Тернопіль, 2022. С.63-65.

53. Могильська М. Б. Критерії оцінювання надійності вебсайту. *Міжнародна наукова інтернет-конференція «Світ наукових досліджень»* (м. Тернопіль – м. Пшеворськ, 18-19 жовтня 2022 р.). Випуск 71. С.32-35.

Додаток А

Взірець розробленої анкети для опитування експертів

Ми проводимо академічне дослідження «Оцінювання надійності вебсайту», мета якого – дослідити рівень впливу між критеріями надійності. Для нас надзвичайно важливо отримати Вашу компетентну думку про дану проблему. Завдяки їй результативність і надійність цього дослідження надзвичайно підвищаться. Уся надана інформація буде анонімно використана лише для академічного статистичного аналізу і окремо не передаватиметься третім особам або для іншого застосування.

Ваша підтримка буде дуже цінною для успішного завершення нашого дослідження. Ми щиро сподіваємося, що Ви приділите деякий час для висловлення Вашого погляду на цю проблему. Заздалегідь дякуємо і бажаємо Вам усього найкращого.

Це опитування складається з двох частин: інструкція до заповнення та заповнення бланку для порівняння впливів 5 критеріїв.

1. **Інструкція для заповнення анкети**

   Рівень впливу чинників визначається за шкалою:

   1 – Рівний вплив
   3 – Слабкий вплив
   5 – Сильний вплив
   7 – Дуже сильний вплив
   9 – Абсолютний плив
   2, 4, 6, 8 – проміжні значення.

Наприклад: ступінь впливу критерію А на критерій В є екстремальним, тоді у рядку А проставляємо 9 у стовпчику В. Якщо навпаки, ступінь впливу критерію В на критерій В є екстремальним, то проставляємо –9.

Критерій	**A**	**B**
A		9
B		

Заповнювати табличку бланку потрібно лише над головною діагоналлю.

2. **Бланк для експертних оцінок**

Критерії	Готовність	Стійкість до відмов	Здатність до відновлення	Цілісність	Конфіденційність
Готовність					
Стійкість до відмов					
Здатність до відновлення					
Цілісність					
Конфіденційність					

Які критерії, на Ваш погляд, не враховано в дослідженні?

_____

Додаток Б

Копія публікацій автора