Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет Комп'ютерних наук
(повна назва)

Кафедра Інформаційних управляючих систем
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Дослідження методів оцінки ризиків під час планування IT-проєкту інформаційної системи мережі спортивно-оздоровчих центрів
(тема)

Виконав:
здобувач 2 року навчання,
групи УПГІТм-23-1
Вячеслав СУСЛА
(власне ім'я, прізвище)

Спеціальність 122 Комп'ютерні науки
(код і повна назва спеціальності)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма Управління проектами в галузі IT
(повна назва освітньої програми)

Керівник: доц. каф. ІУС Тетяна БІЛОВА
(посада, власне ім'я, прізвище)

Допускається до захисту

Зав. кафедри ІУС _____ Костянтин ПЕТРОВ
(підпис) (власне ім'я, прізвище)

2025 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерних наук

Кафедра Інформаційних управляючих систем

Рівень вищої освіти другий (магістерський)

Спеціальність 122 Комп'ютерні науки
(код і повна назва)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма Управління проектами в галузі інформаційних технологій
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)

" 21 " квітня 20 25 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Сусла Вячеславу Олександровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження методів оцінки ризиків під час планування ІТ-проєкту Інформаційної системи мережі спортивно-оздоровчих центрів

затверджена наказом по університету від " 28 " березня 2025 р. № 235Ст

2. Термін подання здобувачем роботи до екзаменаційної комісії " 5 " червня 2025 р.

3. Вихідні дані до роботи Науково-технічні публікації; джерела інтернету; науково-технічна література, що стосується теми кваліфікаційної роботи, матеріали переддипломної практики

4. Перелік питань, що потрібно опрацювати у роботі Аналіз існуючих підходів та методів оцінки ризиків у процесі планування ІТ-проєктів. Виділити особливості оцінки ризиків для ІТ-проєктів спортивно-оздоровчих центрів. Розробити метод оцінки ризиків під час планування ІТ-проекту ІС системи, враховуючі всі особливості. Практично реалізувати застосування розробленого методу для оцінки ризиків під час планування ІТ-проекту ІС мережі спортивно-оздоровчих центрів.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Аналіз предметної області, особливостей розробки ІТ проєктів для ІС систем спортивно-оздоровчих центрів	21.04.2025 - 25.04.2025	Виконано
2	Постановка мети і завдання	25.04.2025 - 27.04.2025	Виконано
3	Аналіз існуючих методів оцінки ризиків для ІТ проєктів	27.04.2025 - 06.05.2025	Виконано
4	Розробка комбінованого методу для оцінки ризиків ІТ проєкту ІС для спортивно-оздоровчих центрів	06.05.2025 - 10.05.2025	Виконано
5	Практична апробація розробленого методу	10.05.2025 - 15.05.2025	Виконано
6	Оформлення пояснювальної записки	15.05.2025 – 17.05.2025	Виконано
7	Оформлення графічної частини та презентаційних матеріалів	17.05.2025 - 18.05.2025	Виконано
8	Представлення на рецензування	25.05.2025 – 29.05.2025	Виконано
9	Представлення атестаційної роботи до ЕК	5.05.2025	Виконано

Дата видачі завдання 21 квітня 2025 р.

Здобувач _____
(підпис)

Керівник роботи _____ доц. каф. ІУС Тетяна БІЛОВА
(підпис) (посада, власне ім’я, прізвище)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 92 с., 21 рис., 3 табл., 32 джерела.

ВІРТУАЛЬНА ІНФРАСТРУКТУРА, ІНФОРМАЦІЙНА СИСТЕМА, НЕВІРТУАЛЬНА ІНФРАСТРУКТУРА, ОЦІНКА РИЗИКІВ, РИЗИК-МЕНЕДЖМЕНТ.

Об’єктом дослідження є процес оцінки ризиків під час планування IT-проєкту інформаційної системи мережі спортивно-оздоровчих центрів, що включає як віртуальну, так і невіртуальну інфраструктуру.

Метою дослідження є аналіз та розробка підходів до оцінки ризиків у процесі впровадження інформаційної системи, що дозволяють виявити, оцінити та мінімізувати потенційні загрози для функціонування.

У ході дослідження застосовано методи якісного та кількісного аналізу ризиків, зокрема FMEA, FTA, SWOT-аналіз, матрицю ризиків та методи оцінки вразливостей для визначення рівня загроз у різних компонентах проєкту. Окремо було розглянуто підходи до оцінки ризиків у віртуальній та невіртуальній інфраструктурі, після чого виконано їх інтеграцію в межах концепції ERM для отримання комплексної оцінки ризикованості проєкту.

У результаті дослідження було сформовано метод для аналізу ризиків у ході планування проєкту інформаційної системи мережі спортивно-оздоровчих центрів, в основу якого лягла комбінація та модифікація декількох існуючих методів оцінки ризиків.

ABSTRACT

Master’s thesis: 92 pages, 21 figure, 3 tables, 32 sources.

INFORMATION SYSTEM, NON-VIRTUAL INFRASTRUCTURE, RISK ASSESSMENT, RISK MANAGEMENT, VIRTUAL INFRASTRUCTURE.

The object of the study is the risk assessment process during the planning of an IT project for the information system of a network of sports and wellness centers, which includes both virtual and non-virtual infrastructure.

The purpose of the study is to analyze and develop approaches to risk assessment in the implementation of the information system, allowing for the identification, evaluation, and minimization of potential threats to its functionality.

The study employs qualitative and quantitative risk analysis methods, including FMEA, FTA, SWOT analysis, risk matrix, and vulnerability assessment methods to determine the level of threats in various project components. Separate approaches to risk assessment for virtual and non-virtual infrastructure were examined, followed by their integration within the ERM concept to obtain a comprehensive risk assessment of the project.

As a result of the study, a method was developed for risk analysis during the planning of an information system project for a network of sports and wellness centers, based on the combination and modification of several existing risk assessment methods.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

ПЗ – програмне забезпечення

ERM – Enterprise Risk Management (управління ризиками підприємства)

FMEA – Failure Mode and Effects Analysis (аналіз видів і наслідків відмов)

FTA – Fault Tree Analysis (аналіз дерева відмов)

HAZOP – Hazard and Operability Study

IT – Information Technology (інформаційні технології)

SWOT – Strengths, Weaknesses, Opportunities, Threats (аналіз сильних та слабких сторін, можливостей і загроз)

ВСТУП

Процес відкриття нового бізнесу та успішність бізнесу у майбутньому значною мірою закладається на етапі планування проєкту підприємства, а також оцінки ризиків майбутнього підприємства. Правильно оцінені ризики та обрані запобіжні заходи – це ключ до успіху підприємства у майбутньому.

Процес оцінки ризиків під час планування ІТ-проєкту мережі спортивно-оздоровчих центрів включає в себе не тільки аналіз розроблюваної інформаційної мережі для мережі спортивно-оздоровчих центрів, а також включає в себе аналіз фізичної інфраструктури спортивно-оздоровчих центрів.

До віртуальної інфраструктури підприємства мережі спортивно-оздоровчих центрів відноситься усе, що стосується технологій розробки, засобів зберігання даних, засобів забезпечення безпеки даних, безпосередньо веб-сайт та мобільний додаток мережі спортивно-оздоровчих центрів, витрати на роботу невіртуальної інфраструктури, а також команда, яка розроблює та підтримує програмне забезпечення мережі спортивно-оздоровчих центрів та цільові користувачі мережі.

До невіртуальної інфраструктури підприємства мережі спортивно-оздоровчих центрів відноситься усе, що стосується будівель та приміщень, де розташовані спортивно-оздоровчі центри мережі, спортивне, медичне та комп'ютерне обладнання центрів, касове обладнання, а також працівники спортивно-оздоровчих центрів та відвідувачі.

Відповідно до того, що характеризує діяльність віртуальної та невіртуальної інфраструктури спортивно-оздоровчих центрів, можна зробити висновки стосовно оцінки ризиків для кожної із інфраструктур окремо.

Актуальність даного дослідження визначається зростаючими вимогами до надійності інформаційних систем у спортивно-оздоровчій сфері, а також необхідністю впровадження методик управління ризиками для забезпечення безперебійної роботи проєкту.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ, ОСОБЛИВОСТЕЙ ТА НАЯВНИХ РІШЕНЬ ОЦІНКИ РИЗИКІВ ПІД ЧАС ПЛАНУВАННЯ ПРОЄКТУ ІС

1.1 Аналіз предметної області та особливостей оцінки ризиків під час планування ІТ-проєкту мережі спортивно-оздоровчих центрів

Темою даного дослідження є оцінка різноманітних факторів ризику при створенні ІТ-проєкту інформаційної системи та фізичної мережі спортивно-оздоровчих центрів. Створення централізованої системи спортивно-оздоровчих центрів є актуальним наразі питанням, оскільки питання охорони здоров'я та забезпечення середовища для комфортного заняття спортом із кваліфікованими тренерами та зручним записом на тренування є однією із важливих потреб людини. Створення інформаційної системи для мережі спортивно-оздоровчих центрів дозволить автоматизувати збір та надання інформації за роботою центрів мережі, а насамперед надасть користувачам мережі можливість оформлення бронювань абонементів на тренування, створювати записи на заняття із тренером або у групах, не виходячи із дому [1].

Спортивно-оздоровчий центр – це спеціальний заклад, що надає послуги, спрямовані на відновлення та покращення здоров’я, заняття спортом, підвищення фізичної активності людей та покращення загального самопочуття [2]. Такі центри можуть включати різні тренажерні зали, інші приміщення для тренувань, басейни, спортивні майданчики, зони для групових занять (таких, як фітнес, йога та інші), масажні кабінети, тощо. Основною метою спортивно-оздоровчих центрів є створення умов для фізичної активності, реабілітації, покращенню здоров’я та запобіганню захворювань.

Актуальність спортивно-оздоровчих центрів зростає разом із тим, як поступово люди починають вести все менш рухливий спосіб життя [3]. Особливо це стало актуально за часів карантину та повномасштабної війни,

коли багато хто почали працювати віддалено. В даному випадку спортивно-оздоровчі центри відіграють роль тих місць, де люди можуть підвищити свою фізичну активність, покращити свою форму та завдяки ним вести більш активний спосіб життя.

Спортивно-оздоровчими центрами можуть користуватись люди різних соціальних та вікових груп. Я було описано вище, то різноманітні офісні працівники, бізнесмени, інші люди з малорухливим способом життя можуть відвідувати такі центри для підвищення своєї фізичної активності та підтримання свого тіла у формі. Діти та підлітки можуть відвідувати різноманітні секції: такі як плавання, бойові мистецтва, танці, гімнастика, що дозволить сформувати їм здорові звички займатись спортом із самого дитинства. Також, зараз є актуальною темою реабілітація, зокрема і військових після різноманітних травм, хвороб, тощо. Для швидшого відновлення є можливість скористатися програмами фізіотерапії, лікувальної фізкультури, різноманітні відновлювальні курси масажів, тощо. Спортивно-оздоровчі центри також можуть використовуватись як професійними спортсменами для підтримання форми, тренувань, підготовки до змагань, так і спортсменами-аматорами, починаючими свій шлях у спорті або просто людьми, які хочуть покращити свою фізичну форму: схуднути, накачати м’язи, тощо.

Таким чином спортивно-оздоровчі центрі є актуальними та затребуваними закладами, якими можуть користуватися дуже багато людей всіх статей, вікових та соціальних груп.

Для того, щоб мати змогу оцінити ризики для підприємства, зокрема розглянутого підприємства мережі спортивно-оздоровчих центрів, яке включає віртуальну та невіртуальну інфраструктури, а саме інформаційну систему та фізичні спортивно-оздоровчі центри, необхідно сформулювати перелік вимог зі сторони пропозицій ринку послуг обраної сфери.

Оскільки планується дослідження підприємства мережі спортивно-оздоровчих центрів у різних містах на території України, тож необхідно дослідити, якими мережами спортивно-оздоровчих центрів представлений

ринок послуг області, а також, які послуги пропонуються в наразі реалізованих мережах спортивно-оздоровчих центрів завдяки інформації, представленій на відповідних інформаційних ресурсах центрів [4].

З метою виділення мереж спортивно-оздоровчих центрів для проведення аналізу, було зроблено пошук за мережами спортивно-оздоровчих центрів України, серед яких було виділено дві найбільші мережі, а саме мережі спортивних центрів Sport Life [5] та мережу жіночих фітнес-клубів FitCurves [6].

Першою розглянемо мережу спортивних центрів Sport Life [5]. Головну сторінку мережі спортивних центрів Sport Life для геолокації Харків наведено на рис 1.1.

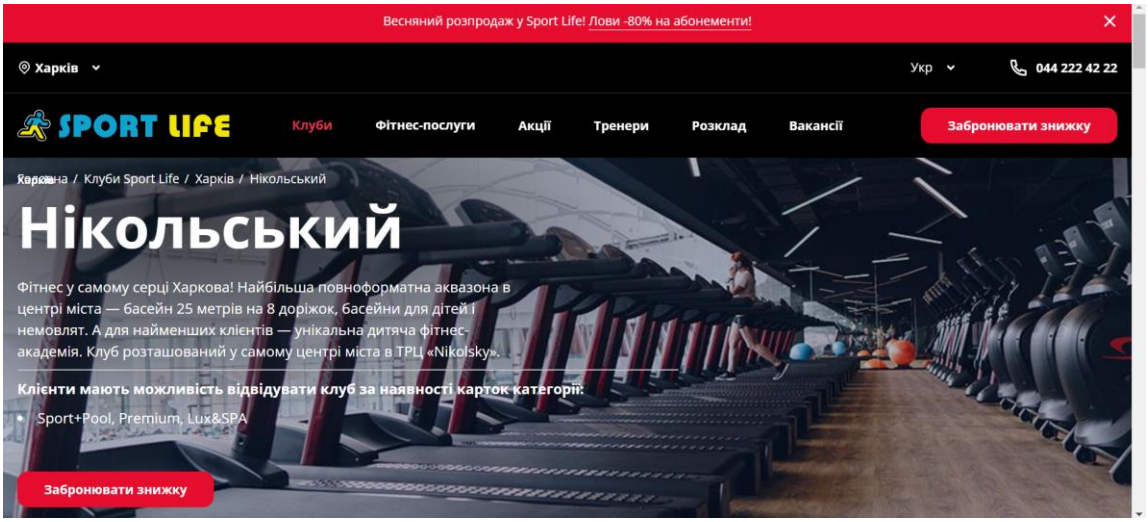

Рисунок 1.1 – Головна сторінка мережі спортивних центрів Sport Life для геолокації Харків

Відповідно до інформації, представленої на офіційному сайті мережі спортивних центрів Sport Life, дана мережа має спортивні центри у всіх великих містах на території України, зокрема, сама мережа налічує 48 спортивних центрів, більша частина яких розташована у місті Київ.

Стосовно спектру надаваних послуг, як це представлено на офіційному сайті мережі спортивних центрів Sport Life, центри даної мережі надають

фітнес-послуги, серед яких басейни для різних вікових категорій, тренажерний зал, кросфіт, бокс, йога, аеробіка та багато інших видів фізичної активності. Більш детальний перелік списку доступних послуг наведено на рис. 1.2.

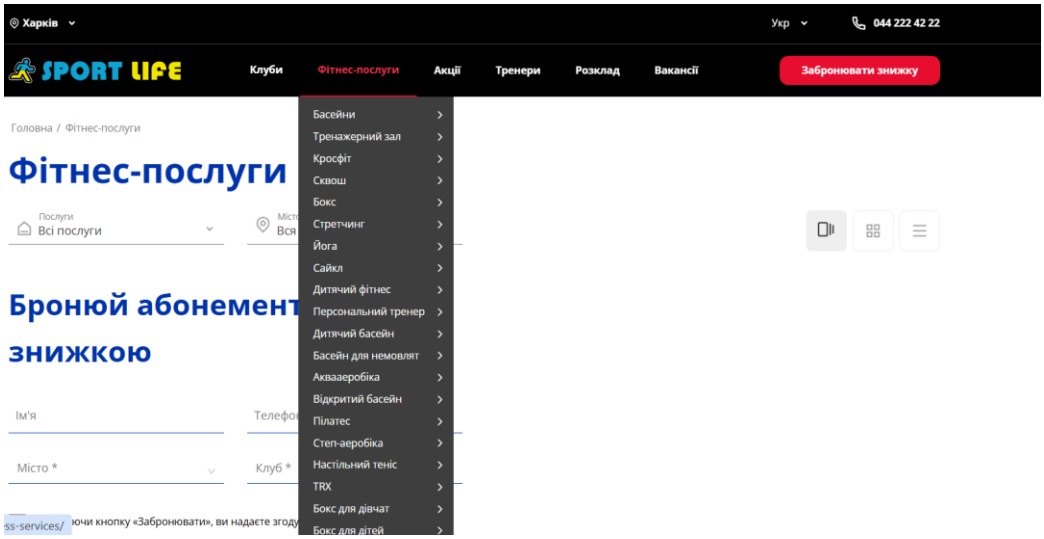

Рисунок 1.2 – Перелік доступних послуг мережі спортивних центрів Sport Life

Також доступні заняття із тренерами, які доступні для занять у тренажерному залі, для заняття спортом із дітьми, для аквафітнесу, для групових спортивних занять, для занять бойовими мистецтвами та сквошем. Відповідну інформацію із сайту мережі спортивно-оздоровчих центрів Sport Life наведено на рис. 1.3.

Веб-сайт мережі спортивних центрів Sport Life також містить функціонал для перегляду поточних акцій, а також для бронювання абонементу у спортзал онлайн. Для цього існує проста та інтуїтивна форма бронювання, яку наведено на рис. 1.4. Для того, щоб ознайомитись із можливим розкладом тренувань, можна відкрити відповідне меню на сайті.

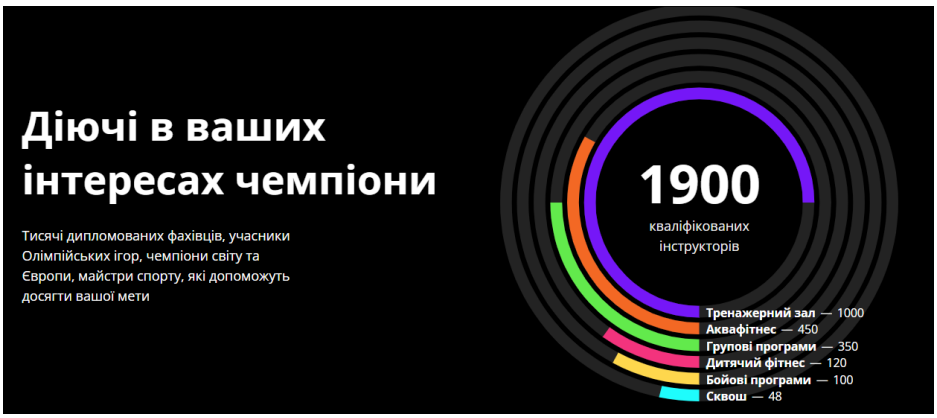

Рисунок 1.3 – Інформація про заняття із кваліфікованими тренерами на сайті мережі спортивних центрів Sport Life

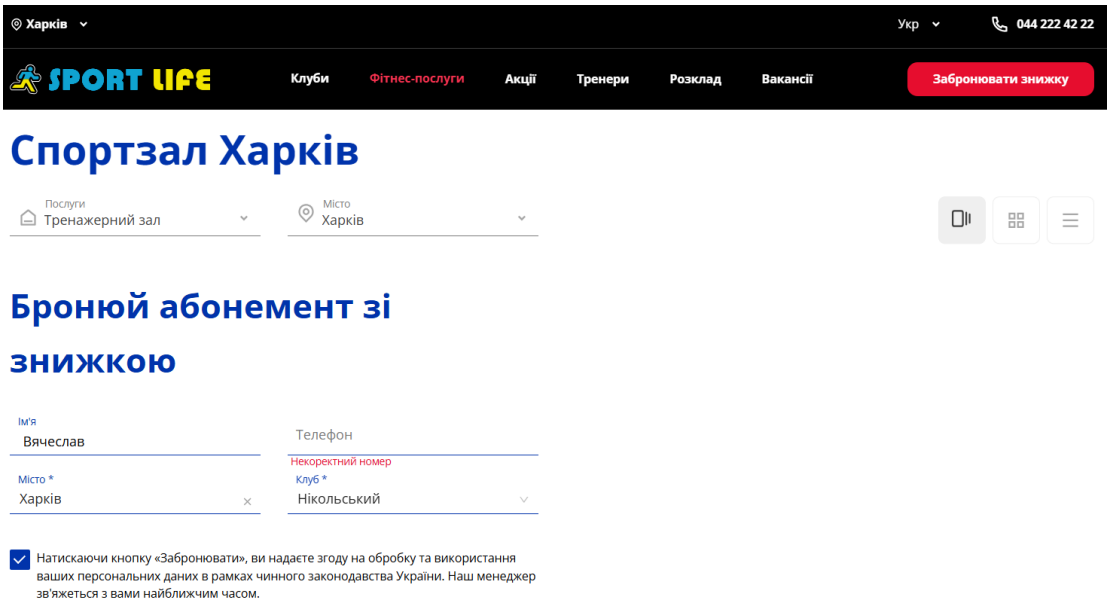

Рисунок 1.4 – Форма бронювання абонементу до тренажерного залу у місті Харків

Перейдемо до аналізу доступного функціоналу інформаційної системи мережі жіночих фітнес-центрів FitCurves [6]. Відповідно до інформації, представленої на даному веб-сайті, фітнес-центри FitCurves є вийнятково жіночими та спрямованими на підтримання здоров’я та позбавлення від зайвої ваги. Головну сторінку веб-сайту мережі жіночих фітнес-центрів FitCurves наведено на рис. 1.5.

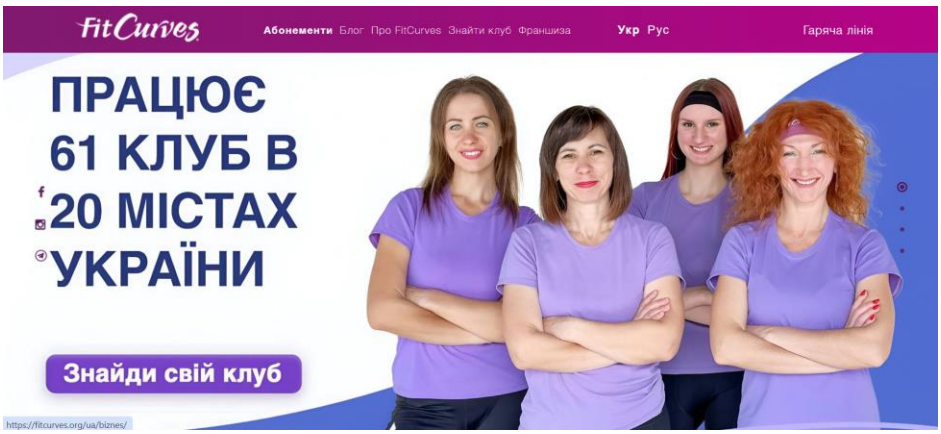

Рисунок 1.5 – Головна сторінку веб-сайту мережі жіночих фітнес-центрів FitCurves

Відповідно до інформації, представленої на офіційному сайті мережі FitCurves, дана мережа має філіали у 86 країнах світу, а в Україні представлена 61 фітнес-центром у 20 містах.

Перейдемо до аналізу послуг, які надають жіночі фітнес-центри мережі FitCurves.

Відповідно до представленої інформації, представленої на сайті FitCurves, у фітнес-центрах мережі проводять комплексні заняття, які включають силові, танцювальні, кардіотренування, а також можливості формування спеціальної дієти за індивідуальними потребами. Даний перелік послуг доступний за онлайн абонементом, тож слідкувати за здоров'ям можливо не виходячи із дому. Перелік послуг, які входять до онлайн абонементів фітнес-клубів мережі FitCurves наведено на рис. 1.6.

Також доступні абонементи до фізичних фітнес-центрів FitCurves із гнучкими правилами. Згідно інформації на сайті, абонементи можна призупиняти, тимчасово або постійно, переводити до іншого міста, країни. Для відвідування тренування у центрі не потрібно мати попереднього запису на фіксований час, а також усі заняття проходять із тренером без додаткової доплати. Перелік абонементів до фізичних фітнес-центрів FitCurves наведено на рис. 1.7.

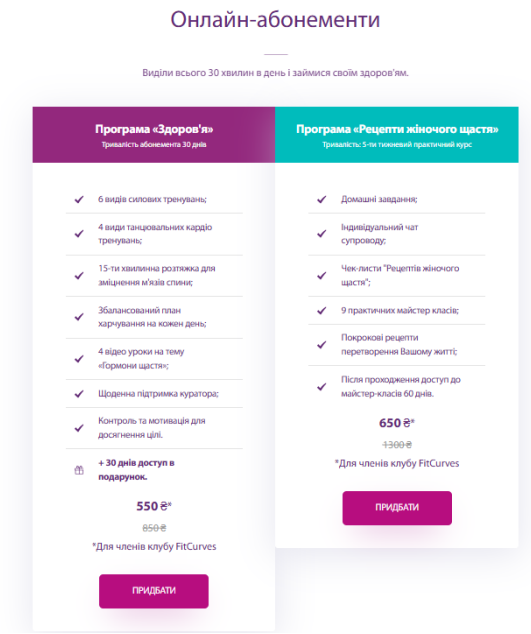

Рисунок 1.6 – Перелік послуг, які входять до онлайн абонементів фітнес-клубів мережі FitCurves

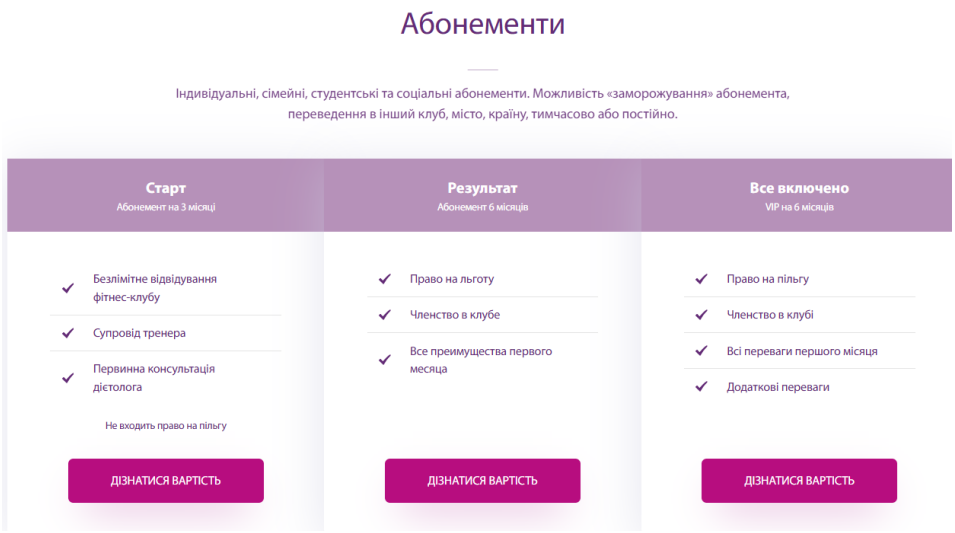

Рисунок 1.7 – Перелік абонементів до фізичних фітнес-центрів FitCurves

Також, веб-сайт мережі фітнес-центрів FitCurves має можливості до придбання абонементів онлайн.

Відповідно до проведеного аналізу реалізованих інформаційних систем мереж спортивно-оздоровчих центрів на території України можемо

сформулювати, який функціонал буде необхідним для віртуальної та невіртуальної мережі спортивно-оздоровчих центрів.

Таким чином, для віртуальної інфраструктури мережі спортивно-оздоровчих центрів є необхідним наступний функціонал:

- онлайн-запис та управління розкладом;
- система управління клієнтами (CRM);
- онлайн-оплата;
- моніторинг завантаженості центрів;
- система керування персоналом;
- аналітика та звітність;
- мобільний додаток, інтеграція з різними фітнес-браслетами, годинниками, трекерами;
- система управління доступом до центру (електронні перепустки, картки, тощо);
- віртуальні консультації та тренування;
- персоналізовані рекомендації;
- кібербезпека, захист даних;
- служба підтримки клієнтів.

Таким чином, для невіртуальної інфраструктури мережі спортивно-оздоровчих центрів є необхідним наступний функціонал:

- тренажерні зони;
- сучасне обладнання;
- зали для групових занять;
- басейни;
- реабілітаційні кабінети;
- зони відпочинку;
- ресепшн, зони очікування;
- системи безпеки та контролю доступу, охорона для запобігання несанкціонованим проникненням;
- роздягальні та душові кімнати;

- спортивні майданчики;
- зони паркування;
- складські приміщення;
- адміністративні приміщення.

З метою остаточного виокремлення розподілу інфраструктури мережі спортивно-оздоровчих центрів на віртуальну та невіртуальну, ключові відмінності за виділеними категоріями порівняння наведено у таблиці 1.1. Дані, представлені у таблиці 1.1 можна також розглядати як перелік потенційно вразливих активів підприємства та враховувати під час формування та оцінки ризиків підприємства мережі спортивно-оздоровчих центрів.

Таблиця 1.1 – Порівняльна характеристика віртуальної та невіртуальної інфраструктур мережі спортивно-оздоровчих центрів

№	Категорія порівняння	Складові віртуальної інфраструктури	Складові невіртуальної інфраструктури
1	2	3	4
1	Користувачі підприємства	Клієнти, персонал спортивно-оздоровчих центрів, ІТ-персонал	Клієнти, тренери, менеджери спортивно-оздоровчих центрів, технічний персонал центрів
2	Обладнання підприємства	Мережеве обладнання ІТ-системи, сервери, сховища даних	Будівлі та приміщення спортивно-оздоровчих центрів, медичне обладнання, обладнання для тренувань, охоронне та касове обладнання

Продовження таблиці 1.1

1	2	3	4
3	Засоби програмного забезпечення підприємства	База даних, CRM-система, білінгова система, інформаційна система мережі спортивно-оздоровчих центрів	Системи автоматизації доступу, касові системи, інформаційна система мережі спортивно-оздоровчих центрів
4	Засоби забезпечення безпеки підприємства	Налаштування параметрів шифрування даних та розмежування доступу до даних підприємства, встановлення антивірусного ПЗ, налаштування брендмауерів	Охорона спортивно-оздоровчих центрів мережі, налаштування відеоспостереження, охоронна та пожежна сигналізація
5	Дані підприємства	Дані працівників та клієнтів мережі центрів, платіжні дані, медичні дані, дані розкладу роботи	Дані відвідувань клієнтами, дані стану та використання обладнання, дані про використання будівель або приміщень

Кінець таблиці 1.1

1	2	3	4
6	Фінансові витрати підприємства	Витрати ІТ-працівникам за розробку та підтримку, витрати на ПЗ, витрати на оплату хостингу для веб-сайту	Витрати на оренду приміщень або будівель, витрати на оновлення та ремонт обладнання, витрати на заробітню плату персоналу
7	Регламент роботи підприємства	Внутрішні регламенти підприємства для роботи із даними, внутрішні та загальноприйняті політики безпеки, ISO 27001	Державні вимоги до сертифікації обладнання, санітарні вимоги, стандарти безпеки праці

1.2 Особливості розробки ІТ-проєктів для ІС спортивно-оздоровчих центрів

Виходячи з аналізу предметної області, можна сказати, що ІТ-проєкти для мереж спортивно-оздоровчих центрів повинні мати широкий та багатий функціонал, що задовольнить весь широкий спектр вимог. Так як подібні заклади мають багато послуг, таких як: спортивні тренування, реабілітаційні та оздоровчі послуги, різноманітні групові тренування і т.д., то ІС повинна мати різноманітні модулі, такі як: реєстрація, авторизація, управління розкладом занять, облік клієнтів та їх даних, планування програм тренувань.

Також необхідно враховувати, що кожний клієнт очікує індивідуального підходу до нього. Тому система повинна зберігати, та підтримувати в

актуальному стані дані про фізичні параметри клієнта, рівень його підготовки, здоров’я, особливості, історію тренувань, дані по проходженню тренування та прогрес. Враховуючи широкий спектр послуг, що надаються спортивно-оздоровчими комплексами, ІС має забезпечувати гнучкість в роботі з різними послугами та клієнтськими запитами.

Так, як ІС зберігатиме чутливу інформацію про клієнтів, то велике має значення захист персональних даних клієнтів та кібербезпека. В таких ІС зазвичай обробляються чутливі дані щодо здоров’я, фізичного стану та підготовки осіб, тому система має відповідати вимогам безпеки інформації, включаючи шифрування даних, аутентифікацію користувачів, обмеження доступу до функціоналу за ролями, тощо.

Ще однією особливістю може бути інтеграція з фізичними пристроями та обладнанням. Наприклад, це може бути система контролю доступу до центру за спеціальними пропускними електронними картками. Також це може бути опція інтеграції з фітнес-браслетами. Наприклад, отримання даних з фітнес-браслету під час тренування, зберігання отриманих даних в системі. Це може бути реалізовано через підключення такого браслета до застосунку на мобільному пристрої клієнта, або безпосередньо встановлення такого застосунку на сам браслет, якщо він це підтримує. Це вимагатиме інтеграції з різними брендами браслетів, їх розпізнавання, та використовування відповідного API. Аналогічною може бути опція інтеграції системи з тренажерами із вбудованими сенсорами та/або можливістю передачі даних про використання (навантаження, швидкість, тощо). Зокрема необхідна також робота із терміналами для оплати, в тому числі і засобами безконтактної/онлайн оплати.

Крім того, велику роль відіграють мобільність та онлайн доступ до системи. Необхідно надавати користувачам дистанційно записуватись на тренування, бачити заповненість залу (може бути реалізовано через інтеграцію із системою доступу), бачити передбачувану заповненість на обраний час (враховуватиметься кількість записів на тренування). Також необхідно надати

можливість відстежувати та вносити результати тренувань, відстежувати прогрес за різними параметрами, отримувати рекомендації та плани подальших тренувань від тренерів. Це може бути реалізовано за допомогою розробки мобільних додатків та веб-сайту.

Не менш важливим є також модуль управління лояльністю клієнтів. ІС має враховувати можливість впровадження бонусних програм, індивідуальних знижок окремим користувачам, акцій, сповіщень про нові можливості та пропозиції. Це дозволить підвищити утримання старих клієнтів та збільшити приток нових.

Для подібного роду систем також дуже важливими є аналітика та звітність. Для ефективного керування такими центрами необхідно отримувати найрізноманітніші аналітичні дані від відвідуваності та потоків клієнтів до результатів тренувань та прогресу клієнтів.

Таким чином, розробка ІТ-проєктів для спортивно-оздоровчих центрів вимагає комплексного підходу та врахування багатьох факторів. Це доволі складний процес, що потребує врахування багатьох особливостей в різноманітних галузях з великою кількістю інтеграцій з різними системами.

1.3 Аналіз наявних рішень для оцінки ризиків під час планування ІТ-проєкту мережі спортивно-оздоровчих центрів

Як вже було зазначено, дане дослідження включає аналіз ризиків ІТ-проєкту створення інформаційної системи мережі спортивно-оздоровчих центрів, так і мережі фізичних спортивно-оздоровчих центрів із обладнанням, тренерами та іншим персоналом, що відповідає віртуальній та невіртуальній інфраструктурі підприємства мережі спортивно-оздоровчих центрів.

Таким чином, до віртуальної інфраструктури підприємства мережі спортивно-оздоровчих центрів відноситься усе, що стосується технологій

розробки, засобів зберігання даних, засобів забезпечення безпеки даних, безпосередньо веб-сайт та мобільний додаток мережі спортивно-оздоровчих центрів, витрати на роботу невіртуальної інфраструктури, а також команда, яка розроблює та підтримує програмне забезпечення мережі спортивно-оздоровчих центрів та цільові користувачі мережі.

До невіртуальної інфраструктури підприємства мережі спортивно-оздоровчих центрів відноситься усе, що стосується будівель та приміщень, де розташовані спортивно-оздоровчі центри мережі, спортивне, медичне касове та комп'ютерне обладнання центрів, касове обладнання, а також працівники спортивно-оздоровчих центрів та відвідувачі.

Відповідно до того, що характеризує діяльність віртуальної та невіртуальної інфраструктури спортивно-оздоровчих центрів, можна зробити висновки стосовно оцінки ризиків для кожної із інфраструктур окремо. Так, оскільки віртуальна та невіртуальна інфраструктури мережі спортивно-оздоровчих центрів мають різні активи, а тому, ризики та наслідки настання ризиків є різними, необхідно проводити аналіз ризиків окремо.

Вимоги до методів оцінки ризиків відповідно до того, якою є природа інфраструктури, віртуальною, або невіртуальною, є різною. Детальніше про основні відмінності у вимогах до методів оцінки ризиків для віртуальної та невіртуальної інфраструктури підприємства мережі спортивно-оздоровчих центрів наведено у таблиці 1.2.

Ризики для віртуальної інфраструктури мережі спортивно-оздоровчих центрів можна охарактеризувати, як такі, що потребують кількісного аналізу. Кількісний аналіз може бути забезпечено завдяки використанню оцінок ймовірностей настання збоїв в системі, кібератак, можливих вразливостей системи та настання ефекту вразливостей [7].

Таблиця 1.2 – Основні відмінності у вимогах до методів оцінки ризиків для віртуальної та невіртуальної інфраструктури підприємства мережі спортивно-оздоровчих центрів

№	Категорія порівняння	Складові віртуальної інфраструктури	Складові невіртуальної інфраструктури
1	2	3	4
1	Походження джерела ризиків	Загрози кібератак, вразливості програмного забезпечення (ПЗ), збої у роботі системи, часткова або повна втрата даних підприємства	Загрози безпеці клієнтів, фізичні загрози, фінансові та операційні ризики
2	Вплив від настання ризиків	Пошкодження, часткова або повна втрата даних, фінансові втрати, часткова або повна відмова роботи системи, компрометація безпеки системи	Травмування клієнтів під час відвідування спортивно-оздоровчого центру, вихід зі строю обладнання, втрати репутації, невідповідність нормам, простої обладнання

Кінець таблиці 1.2

1	2	3	4
3	Основний метод оцінки ризиків	Проведення кількісної оцінки ризиків шляхом розрахунку ймовірності настання ризику та моделювання ситуацій настання ризику	Проведення якісної оцінки ризиків шляхом застосування експертного аналізу та оцінки за методом сценарного аналізу ризиків
4	Можливі методи зниження або нівелювання ризиків	Впровадження технологій захисту даних, підвищення рівня кібербезпеки, тестування функціоналу системи та створення резервної копії даних	Впровадження заходів страхування, регулярного технічного огляду обладнання, проведення спеціальної підготовки персоналу та докладного кадрового відбору

У рамках віртуальної інфраструктури мережі спортивно-оздоровчих центрів, а саме її ІТ-системи, до ризиків можна віднести ряд ризиків, які стосуються забезпечення безпеки даних, неперервність роботи серверів, можливість отримання доступу до системи та її даних. Іншою групою ризиків є також ризики, безпосередньо пов’язані із відповідністю роботи ІТ-системи мережі спортивно-оздоровчих центрів актуальним законодавчим вимогам та нормам, наприклад у питанні відповідності впроваджених рішень із безпечності фінансових операцій та захисту персональних даних клієнтів та працівників центрів.

Для проведення аналізу ризиків віртуальної інфраструктури мережі спортивно-оздоровчих центрів можна використати один, або сукупність із наступних методів: FMEA (Failure Modes and Effects Analysis), FTA (Fault Tree Analysis) та Vulnerability Assessment.

Метод FMEA, або метод аналізу видів та наслідків відмов, полягає у тому, що дає можливим виявити гіпотетичні вразливості IT-системи підприємства мережі спортивно-оздоровчих центрів, які можуть спричинити суттєві збої в роботі IT-системи [8]. Також, даний метод дозволяє визначити ступінь впливу виявлених вузьких місць системи, що, у свою чергу, дозволяє визначити перелік запобіжних заходів від настання виявленого гіпотетичного ризику [9]. Зокрема, даний метод може бути корисним для забезпечення кібербезпеки інформаційної системи мережі спортивно-оздоровчих центрів [4].

Метод FTA, або метод аналізу дерева відмов, є схожим за принципом із описаним вище методом, але ставить у фокус характер отриманої відмови системи та, завдяки детальному аналізу факторів впливу та дерева відмов для отриманої відмови IT-системи, формулює перелік запобіжних заходів для мінімізації ризику настання збою, або відмови, IT-системи [10]. Для IT-інфраструктури інформаційної системи мережі спортивно-оздоровчих центрів даний метод також може бути використано у якості перевірки інформаційної безпеки системи та підвищення її рівню завдяки візуалізації за допомогою методу слабких місць IT-системи [11].

Метод Vulnerability Assessment, або метод аналізу вразливостей системи, дозволяє виділити вразливості та потенційні загрози інформаційній безпеці IT-системи, зокрема IT-інфраструктури мережі спортивно-оздоровчих центрів [12]. Даний метод демонструє найбільшу ефективність для виявлення потенційних вузьких місць витоку даних та можливих вразливих ділянок для хакерських атак на систему [13].

У рамках невіртуальної інфраструктури мережі спортивно-оздоровчих центрів, а саме фізичних спортивно-оздоровчих центрів, до ризиків можна віднести ряд ризиків, які стосуються фізичної експлуатації обладнання спортивно-оздоровчих центрів, експлуатацією приміщень і будівель, де розташовані спортивно-оздоровчі центри, проблеми організаційного та фінансового характеру, проблеми кваліфікації персоналу, особливо,

персоналу, який призначає та проводить тренування, а також ряд ризиків, спричинених безпекою клієнтів під час занять у спортивно-оздоровчому центрі та використання клієнтами обладнання центру [14].

Для проведення аналізу ризиків невіртуальної інфраструктури мережі спортивно-оздоровчих центрів можна використати засоби, які надаються за методом SWOT-аналізу. Алгоритм, за яким проводиться SWOT-аналіз інфраструктури підприємства наведено на рис. 1.8 [15]. За даними критеріями пропонується провести SWOT-аналіз невіртуальної інфраструктури підприємства мережі спортивно-оздоровчих центрів.

Рисунок 1.8 – Алгоритм SWOT-аналізу інфраструктури підприємства

Даний метод дозволяє надати проєкту або підприємству різносторонню характеристику, а саме визначити сильні сторони, або внутрішні переваги, порівняно із визначеними конкурентами підприємства; слабкі сторони, або внутрішні недоліки підприємства, які можуть перешкоджати швидкого досягнення ним успіху; можливості підприємства, побудовані на основі

зовнішніх факторів, які позитивно впливають на розвиток підприємства; загрози підприємству, які представляють зовнішні фактори ризику успіху або існуванню проєкту [14]. Даний метод дозволить створити комплексний погляд та висновок за невіртуальною частиною підприємства мережі спортивно-оздоровчих центрів.

Для виконання більш детального аналізу, результати, отримані за SWOT-аналізом, можна об’єднати із підходом створення матриці ризиків. Матриця ризиків, у свою чергу, являє собою такий метод оцінки ризиків, який використовується для візуалізації існуючих ризиків та поєднує перелік ризиків та ймовірностей їх настання [11].

Отримані у ході виконання SWOT-аналізу ризику та слабкої сторони необхідно визначити ймовірність виникнення за відносною шкалою, (наприклад, «немає ризику», «сильний ризик»), а також ступінь впливу на проєкт, також за відносною шкалою, (наприклад, «низький», «помірний»). Згідно отриманих результатів можна визначити слабкі сторони та ризики невіртуальної інфраструктури мережі спортивно-оздоровчих центрів. Також, такий підхід дозволить виставити пріоритети у боротьбі із ризиками для управляючих осіб мережі спортивно-оздоровчих центрів. Іншою стороною боротьби із ризиками можна також вважати зміцнення сильних сторін підприємства.

Останнім кроком, коли було виконано окремо аналіз віртуальної та невіртуальної інфраструктур підприємства мережі спортивно-оздоровчих центрів, переходимо до останнього етапу – підсумування отриманих результатів. Виконання етапу підсумування результатів дослідження методів оцінки ризиків для визначеного підприємства є можливим завдяки використанню методу Enterprise Risk Management (ERM), або корпоративного управління ризиками [16]. Даний метод використовується для оцінки ризиків віртуальної та невіртуальної інфраструктур підприємства з метою створення системного та стратегічного підходу до управління його ризиками [4]. Даний підхід дозволяє оцінити усі типи ризиків, які є властивими для віртуальної та

невіртуальної інфраструктури підприємства мережі спортивно-оздоровчих центрів.

Розроблений алгоритм управління ризиками підприємства може бути вдалим рішенням для співставлення отриманих результатів та формування повного рішення та стратегії управління ризиками підприємства мережі спортивно-оздоровчих центрів, оскільки воно дозволяє кількісно та якісно оцінити діяльність та організацію підприємства з різних сторін для формування виваженого рішення.

1.4 Постановка задачі дослідження методів оцінки ризиків під час планування ІТ-проєкту мережі спортивно-оздоровчих центрів

З огляду на поточні вимоги часу, коли будь-яке підприємство, яке надає послуги, очікується, що буде мати інформаційну систему, або веб-сайт, який буде представляти перелік товарів або послуг, які пропонує підприємство із детальною інформацією про них та можливості до придбання, наявність такої системи стає просто необхідною. Дана хвиля сучасних тенденцій також стосується й мереж спортивно-оздоровчих центрів на теренах України, як це було продемонстровано раніше.

Однак, наявність як віртуальної, так і невіртуальної інфраструктури підприємства, зокрема мережі спортивно-оздоровчих центрів, пов’язана із різносторонніми ризиками, які мають як різний ступінь появи, так і різний ступінь впливу на роботу підприємства. Тому ризики необхідно оцінювати як під час створення ІТ-проєкту мережі спортивно-оздоровчих центрів, так і постійно їх контролювати у ході функціонування підприємства.

Приймаючи до уваги той факт, що підприємство складається із віртуальної та невіртуальної інфраструктурний складових, оцінити ризики для такого підприємства стає дедалі складніше. Виходячи із описаної ситуації

чітко постає необхідність формування комплексного підходу до оцінки ризиків для віртуальної та невіртуальної інфраструктури підприємства мережі спортивно-оздоровчих центрів. Оскільки наразі більша частина підприємств наразі складається із віртуальної та фізичної інфраструктури, розроблений підхід можна розширити й на інші предметні області, що формує актуальність та масштабованість дослідження ризиків під час планування ІТ-проєкту інформаційної системи для мережі спортивно-оздоровчих центрів, оскільки розроблений підхід дозволить дослідити взаємний зв’язок інфраструктур.

Відповідно до сформульованої актуальності, метою дослідження ризиків під час планування ІТ-проєкту інформаційної системи для мережі спортивно-оздоровчих центрів є дослідження та розробка методу оцінки ризиків, який дозволить оцінити загрози та ризики для віртуальної та невіртуальної інфраструктури розглянутого підприємства. Розроблений метод оцінки ризиків буде являти собою послідовність використання методів для різносторонньої оцінки ризиків діяльності підприємства.

Об’єктом дослідження є процес оцінки ризиків під час планування ІТ-проєкту інформаційної системи для мережі спортивно-оздоровчих центрів.

Предметом дослідження є методи оцінки ризиків під час планування ІТ-проєкту інформаційної системи для мережі спортивно-оздоровчих центрів, що передбачає виконання оцінки ризиків для віртуальної та невіртуальної інфраструктури підприємства.

Ключовою проблемою даного дослідження виступає потреба у розробці комплексного рішення, яке б дозволило проводити оцінку ризиків для підприємств із віртуальною та невіртуальною складовими комплексно, оцінюючи підприємство як єдине ціле. Складність та протиріччя даного питання полягають у тому, що природа ризиків для віртуальної та невіртуальної інфраструктури є різною, а тому, відповідно, підходи до оцінки ризиків також будуть різними.

Розглянуті традиційні методи для оцінки ризиків у ІТ-проєктах є ефективними в окремо взятому аспекті застосування та не є пристосованими

для використання на сукупності аспектів, які являє собою оцінка ризиків для підприємства із віртуальною та невіртуальною інфраструктурою.

Відповідно до наведеного вище, у рамках даного дослідження необхідно розробити комбінований підхід до оцінки ризиків для підприємств із віртуальною та невіртуальною інфраструктурою, зокрема для мережі спортивно-оздоровчих центрів. Розроблений метод повинен являти собою комбінацію послідовного застосування традиційних методів оцінки ризиків, який також повинен функціонувати в рамках єдиної системи для управління ризиками підприємства. Розробка такого методу дозволить всебічно оцінити загрози для підприємств, які мають як фізичну, так і віртуальну інфраструктуру.

Таким чином, для виконання мети дослідження ризиків під час планування проєкту мережі спортивно-оздоровчих центрів із віртуальною та невіртуальною інфраструктурою, необхідно виконати ряд наступних завдань, серед яких:

− виконати докладний аналіз актуальних практик визначення ризиків під час планування IT-проєкту мережі спортивно-оздоровчих центрів із віртуальною та невіртуальною інфраструктурою;

− виділити перелік методів, які можуть бути використані для визначення ризиків під час планування IT-проєкту мережі спортивно-оздоровчих центрів із віртуальною та невіртуальною інфраструктурою;

− розробити метод оцінки та аналізу ризиківів, що буде враховувати такі особливості як: комплексність системи, тісну взаємодію віртуальної і фізичної інфраструктур, посилені вимоги до кібербезпеки, інтеграція із фізичними пристроями та сенсорами, тощо;

− провести аналіз ризиків за допомогою розробленого методу оцінки ризиків під час планування IT-проєкту мережі спортивно-оздоровчих центрів із віртуальною та невіртуальною інфраструктурою із використанням необхідних таблиць та розрахунків, які передбачають виділені методи;

− сформувати перелік висновків відповідно ризиків під час планування

ІТ-проєкту мережі спортивно-оздоровчих центрів із віртуальною та невіртуальною інфраструктурою, сформулювавши також перелік рекомендацій для нівелювання або зменшення ризику настання виділених ризиків підприємству.

2 АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ОЦІНКИ РИЗИКІВ ІТ-ПРОЄКТІВ

2.1 Методи оцінки рівня ризику

2.1.1 Метод Failure Modes and Effects Analysis

Метод FMEA використовується для виявлення, оцінки та попередження можливих відмов системи. Його мета полягає в тому, щоб проаналізувати та виявити можливі відмови або збої, їх причини, наслідки, вірогідність настання, серйозність наслідків та можливість виявити проблему до її настання [17].

Даний метод виник у 1940-х роках у військово-промисловій сфері США, зокрема в авіаційній та космічній галузях, де потрібна була висока надійність обладнання. Пізніше цей метод набув популярності в автомобільній промисловості, електроніці, охороні здоров’я та інформаційних технологіях, оскільки дозволяє системно запобігати проблемам ще на стадії проектування.

Суть FMEA полягає в тому, щоб для кожного компонента системи або функції визначити потенційні відмови, причини їх виникнення та можливі наслідки. Для кожного ризику визначаються три параметри: ймовірність настання події, серйозність наслідків, здатність виявити настання події до того, як вона відбудеться. Ці показники оцінюються за шкалою від 1 до 10, де 1 це найменший ризик, а 10 – найбільший [18].

Далі обчислюється RPN (Risk Priority Number) – пріоритетного числа ризику за формулою (2.1.),

$$RPN = O * S * D, \tag{2.1}$$

де O – ймовірність настання ризику;

S – серйозність наслідків;

D – здатність до виявлення ризику до його настання.

Більше значення RPN означає вищий пріоритет для усунення або хоча б пом’якшення даного ризику.

До переваг методу можна віднести можливість кількісної оцінки ризиків, гнучкість використання та наочність отриманих результатів. Метод допомагає покращити розуміння системи, підвищити надійність системи ще до її запуску шляхом реагування на більш пріоритетні ризики.

Недоліком даного методу можна назвати значні витрати часу на складання таблиць, залежність від експертних оцінок, що може призвести до суб’єктивності [19].

2.1.2 Метод Risk Matrix (Матриця ризиків)

Матриця ризиків дозволяє провести не тільки якісний аналіз, але ще й кількісний у різних сферах, включаючи управління проектами. Його історія бере початок у середині XX століття, коли зросла потреба у простих, але ефективних підходах для оцінки ризиків без застосування складних математичних моделей. Концепція матриці ризиків швидко набула популярності, оскільки дозволяла менеджерам приймати зважені рішення навіть за відсутності повних статистичних даних.

Суть методу полягає в побудові матриці, де одна вісь відображає ймовірність настання ризику, а інша – ступінь його впливу чи наслідків. Комбінація цих двох параметрів дозволяє визначити рівень ризику, наприклад, низький, середній або високий, що допомагає у встановленні пріоритетів для управління ризиками. Відповідно, якщо ризик знаходиться ближче до правого верхнього кута, то це високий рівень ризику, він є найбільш пріоритетним та вимагає найбільшої уваги. Чим ризик ближче до нижнього лівого кута матриці, тим він є менш пріоритетним, а іноді їм можна і взагалі знехтувати [24]. Для заповнення матриці залучають експертів, які на основі доступної інформації та власного досвіду оцінюють ймовірність і вплив кожної потенційної події.

Переваги методу Risk Matrix полягають у його простоті, наочності та гнучкості, а також у можливості застосовувати його на ранніх етапах проєкту без потреби у великих обсягах даних.

До недоліків даного методу можна віднести суб’єктивність оцінок та обмежену точність.

2.2 Методи ідентифікації та структурного аналізу ризиків

2.2.1 Метод Fault Tree Analysis

Метод FTA використовується для ідентифікації причин потенційних відмов, прогнозування їх впливу на роботу системи. Він був розроблений наприкінці 1960-х років у США, зокрема для потреб військової та аерокосмічної галузі, а згодом його застосування поширилося на промисловість, енергетику, IT, медицину та інші сфери.

Результатом методу є графічне представлення дерева відмов, де відображаються логічні зв’язки між небажаною подією та її причинами. Першим кроком є визначення небажаної події (відмови), що розміщатиметься на верхівці дерева. Наступним кроком визначаються всі можливі причини події. Причини події можуть бути базовими або проміжними, що комбінацією базових причин. Комбінації причин відображаються через логічні операції (найчастіше це AND або OR) [20].

До переваг методу можна віднести наочність представлення результатів, можливість аналізу складних систем, виявлення критичних комбінацій помилок та розуміння їх впливу на систему.

Недоліком даного методу є висока трудомісткість при застосуванні до великих або слабо формалізованих систем. Також даний метод є малоефективним для аналізу систем із численними взаємозв’язками, зворотними зв’язками, динамічними структурами, там де зв’язки системи

постійно змінюються. Застосування методу FTA до такого роду систем є складним через те, що стає складно відображати взаємозв’язки між причинами можливої небажаної події.

2.2.2 Метод Vulnerability Assessment

Метод Vulnerability Assessment, або оцінка вразливостей спрямований на виявлення, аналіз і оцінку слабких місць у системах, які можуть бути використані для здійснення атак або порушення безпеки. Цей підхід сформувався на основі потреб у кібербезпеці, військовій сфері та промисловості ще в середині XX століття, але найбільшого розвитку набув з розвитком комп’ютерних мереж, інтернету та складних інформаційних систем у 1990–2000-х роках. Сьогодні його застосовують не лише в IT, а й у фізичній безпеці, енергетиці, транспорті, охороні здоров’я, а також в управлінні критичною інфраструктурою.

Суть методу полягає в пошуку та ідентифікації слабких місць системи, що можуть призвести до порушення конфіденційності або працездатності системи. Оцінка вразливостей включає етапи збору інформації про об’єкт дослідження, аналізу конфігурацій, сканування мереж та систем, аналізу вихідного коду, перевірки політик безпеки та стандартів, а також моделювання потенційних сценаріїв атак. За підсумками формується перелік знайдених вразливостей із описом їхньої суті, потенційних наслідків, рівня ризику та рекомендацій щодо усунення [21].

Основною перевагою методу є те, що він дозволяє запобігти атакам до того, як вони стануться. Даний метод дозволяє підвищити рівень безпеки, сформувати стратегії реагування на інцеденти.

До недоліків можна віднести високу трудомісткість методу, потреба у залученні багатьох експертів у різних галузях, залежність від якості та повноти

вхідних даних, ризик отримання неповної картини стану та реалізації системи.

Даний метод підходить коли вже є реалізована система або частина функціоналу, де можна виявити якісь вразливості. Так як даний метод вимагає вже якогось реалізованого функціоналу, то він не підходить до етапу планування.

2.2.3 Метод SWOT-аналізу

SWOT-аналіз - це метод, що дозволяє оцінити зовнішні та внутрішні фактори, що впливають на проєкт. Ці фактори поділяються на сильні сторони, слабкі сторони, можливості та загрози: Strengths, Weaknesses, Opportunities, Threats відповідно, звідки і походить назва цього методу.

Метод SWOT-аналізу сформувався у 1960–1970-х роках у США завдяки дослідницькій роботі групи під керівництвом Альберта Гамфрі в Стенфордському дослідницькому інституті, коли вивчали причини успіху та провалів великих компаній. Згодом метод набув поширення як простий інструмент для аналізу ситуації перед прийняттям стратегічних рішень.

Суть даного методу полягає в тому, щоб визначити ключові сільні та слабкі сторони, зовнішні можливості та загрози, що можуть вплинути на успішність проєкту в майбутньому. Слабкі та сильні сторони характеризують внутрішнє середовище, а можливості і загрози, відповідно, характеризують зовнішнє середовище [22]. Процес аналізу складається зі збору інформації, обговорення в командах, аналізу ринку та документів. Далі все це систематизують у вигляді матриці, на якій відображено кожні з перелічених чотирьох критеріїв. Отримана матриця допомагає побачити загальну картину та визначитись із подальшими стратегіями розвитку, реагування на загрози та методами запобіганню загроз.

Основними перевагами даного методу є простота його застосування,

наочність отриманих результатів, гнучкість та можливість залучення різних учасників із різних сфер, що підвищує якість аналізу та прийняття рішень.

До недоліків можна віднести ризик отримання неповної інформації про проєкт, залежність від від суб’єктивної думки учасників та їх власного досвіду. SWOT-аналіз не надає конкретних механізмів впровадження рішень. Даний метод допомагає створити основу для стратегічного мислення та подальшого планування дій.

2.2.4 Метод Hazard and Operability Study

Метод HAZOP є підходом до ідентифікації небезпек та проблем, що впливають на працездатність системи. Цей метод був розроблений у 1960-х роках у Великій Британії компанією Imperial Chemical Industries (ICI) для аналізу ризиків на хімічних виробництвах, оскільки такі об’єкти характеризуються високим ступенем складності та небезпеки. Основною метою HAZOP є виявлення потенційних відхилень від нормальної роботи системи, які можуть призвести до аварій, загрози здоров’ю людей або порушення виробничого процесу [23].

Суть даного методу полягає в тому, щоб проаналізувати кожен елемент системи, виявити можливі відхилення, їх можливі наслідки, засоби запобігання або зменшення ризику.

До переваг методу HAZOP можна віднести його системність, та здатність виявляти як очевидні, так і приховані ризики. Він дозволяє підвищити безпеку процесів у системі, запобігти помилкам на етапі експлуатації.

До недоліків даного методу можна віднести значні витрати часу та ресурсів, а також залежність від досвіду та кваліфікації експертів. Для складних систем HAZOP може потребувати кількох раундів аналізу, що

збільшує витрати, однак це компенсується високою якістю отриманих результатів.

2.2.5 Метод Bow-Tie Analysis

Метод Bow-Tie Analysis – це метод, в якому поєднуються якісна та кількісна оцінка ризиків. Даний метод дозволяє візуалізувати причинно-наслідкові зв’язки між джерелами загроз, подіями – і та наслідками. Назва методу походить від форми діаграми, що нагадує метелик. Цей метод розвивався у промисловості у 1970–1980-х роках, а перше офіційне застосування в документах відбулося у нафтовій галузі в 1990-х, коли компанії BP та Shell почали використовувати його для аналізу безпеки та управління ризиками на виробництві. З часом метод поширився на такі сфери, як авіація, енергетика, хімічна промисловість, медицина, IT-сфера та управління проєктами.

Суть даного методу полягає в тому, щоб виявити основну загрозу, відобразити її в центрі діаграми. Далі визначаються можливі причини даної події і зображуються ліворуч від події, що аналізується [25]. Після цього аналізуються можливі наслідки настання подій і відображаються у правій частині діаграми. Для кількісної оцінки використовується формула (2.2.),

$$R = P * I, \tag{2.2}$$

де R – величина ризику (Risk);

P – ймовірність настання ризику (Probabilty);

I – серйозність ризику, величина його впливу (Impact).

Перевагами даного методу є зрозуміла візуалізація, гнучкість у застосуванні, а також можливість інтеграції з іншими методами аналізу

ризиків.

До недоліків можна віднести високі вимоги до якісного збору даних та експертних оцінок, а також ризик спрощення складних ризикових ситуацій.

2.3 Інтегровані методи управління ризиками та методи оцінки ймовірностей

2.3.1 Методологія Enterprise Risk Management

ERM - це методологія управління ризиками, що дозволяє визначати ризики, оцінювати, контролювати і моніторити їх задля підвищення і забезпечення стабільності роботи системи. Історія ERM розпочалася в середині XX століття, але в сучасному вигляді він став популярним на початку 2000-х років, коли великі організації почали розуміти важливість управління ризиками для забезпечення стійкості і досягнення своїх довгострокових цілей. Спочатку ERM застосовувався в основному в банківському секторі та фінансових компаніях, а з часом метод поширився на інші галузі, включаючи IT, виробництво, енергетику, охорону здоров'я та інші.

Суть ERM полягає в тому, щоб ідентифікувати всі потенційні ризики для організації (як позитивні, так і негативні), оцінити ймовірність їх виникнення та можливі наслідки, розробити стратегії для їх мінімізації або використання в разі позитивних ризиків і забезпечити їх моніторинг протягом часу [26]. У рамках цього методу використовуються різноманітні інструменти та моделі для оцінки ризиків, такі як SWOT-аналіз, FMEA, FTA, монте-карло, а також методи оцінки вразливостей та інші.

За допомогою цього методу можна об’єднати оцінки ймовірності та впливу ризиків, розробити стратегії мінімізації ризиків, визначити пріоритети для кожного з ризиків на основі їх ймовірності та впливу.

Головною перевагою ERM є його всеосяжний характер, що дозволяє

організації мати повний огляд усіх ризиків і відповідно більш ефективно ними керувати.

До недоліків можна віднести потребу в значних ресурсах для впровадження та підтримки ERM, а також складність в оцінці деяких типів ризиків, особливо тих, для яких недостатньо історичних даних або чітких моделей.

2.3.2 Методи визначення ймовірності настання несприятливої події

Вірогідність настання події може бути визначена декількома способами:

- використання історичних статистичних даних;
- експертна оцінка;
- аналітичні моделі;
- опитування, анкетування.

Історичні дані можуть бути отримані шляхом використання даних з попередніх проєктів компаніх, пошуку у публічних джерелах, за можливістю звернення до інших компаній, у яких є аналогічні проєкти, тощо.

У випадку відсутності історичних даних, або неможливості їх отримання можна прибігти до методів експертних оцінок, опитувань та анкетувань. Можна опитати менеджерів, розробників, тестувальників, адміністраторів, які мають великий досвід у своїй сфері, та які знайомі з багатьма можливими несприятливими подіями, частотою їх виникнення та серйозністю наслідків.

Якщо ж всі попередні методі ускладнені або неможливі з якихось причин, то можна прибігти до аналітичних моделей, наприклад, методу Монте-Карло.

Суть методу полягає у проведенні великої кількості випадкових симуляцій моделі або системи з використанням різних комбінацій вхідних параметрів, після чого результати статистично аналізуються для отримання

оцінки шуканої величини[27]. Даний метод широко використовується в аналізі фінансових ризиків, управлінні проєктами, інженерних розрахунках, розробці програмного забезпечення, біологічному моделюванні, аналізі безпеки та в багатьох інших сферах. Він дозволяє враховувати невизначеність і варіативність вхідних даних, що робить його особливо корисним там, де неможливо дати точну детерміновану відповідь.

Ймовірність настання несприятливої події розраховується за формулою (2.3.),

$$P = \frac{1}{N}\sum_{i=1}^{N} f(x_i), \tag{2.3}$$

де P – вірогідність настання несприятливої події;

N – кількість симуляцій;

x_i – випадково згенеровані вхідні значення;

$f(x_i)$ – результат моделі для кожного і-го набору.

Чим більше число експериментів (N), тим більше точність оцінки завдяки закону великих чисел. Тому на реалізацію цього методу може піти не мало часу, щоб оцінити ймовірності настання всіх подій з великою точністю.

Основними перевагами методу є універсальність, здатність працювати зі складними імовірнісними моделями та відносна простота реалізації за допомогою комп’ютерних симуляцій.

Серед недоліків можна виокремити значні обчислювальні витрати, особливо для високоточних оцінок, в також необхідність мати коректні розподіли величин вхідних даних.

3 РОЗРОБКА МЕТОДУ АНАЛІЗУ РИЗИКІВ ДЛЯ ІТ ПРОЄКТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ МЕРЕЖІ СПОРТИВНО-ОЗДОРОВЧИХ ЦЕНТРІВ

3.1 Аналіз вимог до розроблюваного методу оцінки ризиків

ІТ-проєкти для спортивно-оздоровчих центрів мають специфічні особливості, зумовлені необхідністю забезпечення безперервності обслуговування клієнтів, надійності системи бронювання, розкладів тренувань, обліку відвідуваності та управління персоналом, а також високого рівня безпеки даних. Крім того, така система має підтримувати інтеграцію із сенсорними мережами (наприклад, для контролю доступу або обліку використання обладнання), що обумовлює складну взаємодію між фізичною (невіртуальною) та цифровою (віртуальною) інфраструктурою. Це створює додаткові вимоги до методу оцінки ризиків, зокрема необхідність врахування не лише типових ІТ-ризиків, але й ризиків, що пов’язані з фізичними процесами та середовищем.

Метод повинен бути адаптивним до неоднорідності вхідних даних і забезпечувати можливість комплексної оцінки ризиків як для окремих підсистем, так і для всієї інфраструктури в цілому. З огляду на це розроблюваний метод повинен включати механізми аналізу різних типів ризиків (технічних, організаційних, фізичних, інформаційних) і дозволяти поєднувати результати з різних джерел для формування цілісного уявлення про ризики проєкту.

Оцінюючи переваги та недоліки залучених методів, таких як FMEA, SWOT-аналіз, Risk Matrix, Bow-Tie та ERM, стає очевидним, що кожен із них має власну нішу застосування. Метод FMEA забезпечує детальний розбір кожної можливої відмови системи, дозволяючи ідентифікувати критичні компоненти на ранньому етапі, однак потребує значного обсягу даних і експертних оцінок, що може бути обмеженням для нових проєктів. SWOT-

аналіз дозволяє структурувати зовнішні та внутрішні фактори, проте має переважно якісний характер і потребує подальшої кількісної деталізації. Матриця ризиків ефективна для візуалізації рівнів ризику та ухвалення оперативних рішень, однак не дає глибокого розуміння причин ризикових ситуацій. Bow-Tie дозволяє зв'язати причини і наслідки подій, формуючи наочну модель керування ризиками, однак вимагає ретельного моделювання логічних зв'язків. Метод ERM забезпечує інтеграцію результатів і стратегічний підхід до керування ризиками, що є ключовим для систем із високим ступенем комплексності, проте для його успішної реалізації необхідно забезпечити повноту вихідних даних і міжсистемну взаємодію.

Враховуючи ці характеристики, вимоги до розроблюваного методу повинні включати врахування модульності структури, що дозволить поетапно оцінювати ризики в окремих доменах (віртуальна і невіртуальна інфраструктури) і інтегрувати результати на завершальному етапі. Метод має забезпечувати гнучкість щодо використання різних джерел даних, зокрема можливість роботи як із історичними даними, так і з даними, що отримуються шляхом моделювання або експертних опитувань.

Метод також має враховувати сценарії взаємозалежності між ризиками фізичної інфраструктури (наприклад, відмова електропостачання або пошкодження обладнання) та ризиками віртуальної частини (наприклад, збої в роботі програмного забезпечення або кібератак). Таким чином, одним із ключових вимог є інтеграція результатів на рівні концепції ERM для формування цілісної системи управління ризиками.

3.2 Алгоритм комбінованого методу оцінки ризиків під час планування IT-проєкту

Алгоритм оцінки ризиків розбито на три основні частини: аналіз ризиків

для віртуальної інфраструктури, фізичної інфраструктури та їх інтеграція. Для оцінки ризиків віртуальної інфраструктури передбачено за допомогою методу FMEA (Failure Modes and Effects Analysis). Цей метод спрямований на систематичне виявлення потенційних відмов компонентів IT-системи, аналіз причин їх виникнення, наслідків для роботи всієї системи та визначення пріоритетів управління ризиками.

Для визначення вірогідності настання відмови передбачено використання історичних даних та наявної статистика. У випадках, коли історичних даних недостатньо або вони недоступні, застосовується метод Монте-Карло, який ґрунтується на числових експериментах і моделюванні великої кількості випадкових сценаріїв, що дозволяє отримати оцінку ймовірності відмов.

Для оцінки серйозності наслідків відмови та здатності її виявлення проводиться опитування експертів – фахівців з інформаційних технологій, адміністраторів мереж та аналітиків. На схемі, що показана на рисунку 3.1 зображена послідовність дій для оцінки ризиків віртуальної інфраструктури.

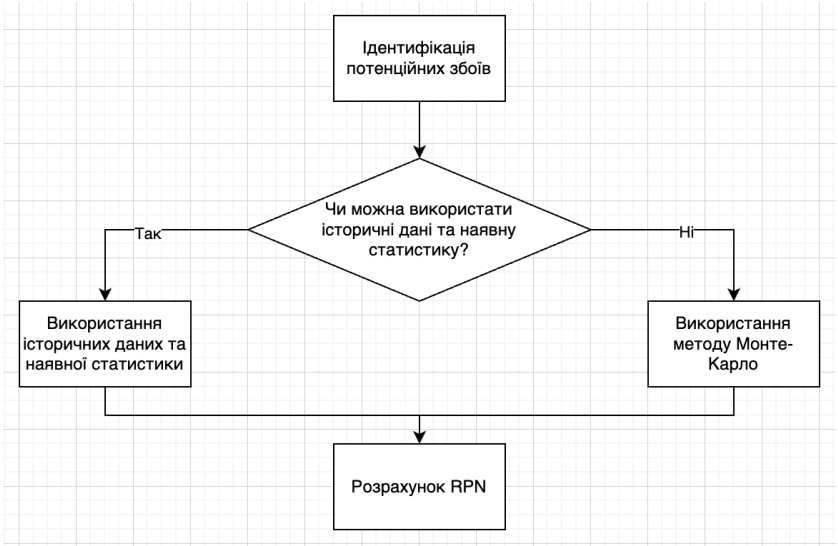

Рисунок 3.1 – Схема алгоритму оцінки ризиків для віртуальної інфраструктури

Ідентифікація потенційних збоїв та їх кількісний аналіз складається з декількох кроків. Перший крок полягає в ідентифікації всіх основних компонентів віртуальної інфраструктури. На цьому етапі формуються структуровані списки серверів, мережевого обладнання, віртуальних машин, баз даних, додатків та допоміжного ПЗ. Вхідними даними є архітектурні схеми, технічна документація, інвентаризаційні звіти та дані з систем моніторингу. Другий крок передбачає визначення потенційних видів відмов для кожного компонента. Наприклад, для сервера це може бути збій живлення, для бази даних – пошкодження файлів, для мережевого вузла – втрата зв’язку. Ця робота проводиться за участю ІТ-експертів, адміністраторів систем та технічних консультантів. Третій крок фокусується на аналізі причин кожної потенційної відмови. Причини можуть включати як технічні фактори (наприклад, зношення обладнання), так і організаційні (наприклад, помилки персоналу чи неправильні налаштування). Для цього використовуються дані журналів подій, історичні дані про інциденти, а також експертні інтерв’ю. Четвертий крок присвячений оцінці наслідків кожної відмови для роботи всієї системи. Наприклад, збій сервера баз даних може призвести до повної недоступності сервісу, а втрата мережевого з’єднання – до обмеження доступу лише для певної групи користувачів. На цьому етапі описуються як технічні, так і бізнесові наслідки, такі як фінансові втрати, зниження якості послуг або репутаційні ризики. П’ятий крок – це кількісна оцінка ризиків. Тут застосовуються три ключові показники: ймовірність виникнення відмови (Occurrence, O), серйозність наслідків (Severity, S) та здатність до виявлення проблеми (Detection, D). Ймовірність визначається на основі історичних даних або методом Монте-Карло, коли таких даних немає. Серйозність та здатність до виявлення оцінюються експертами, що враховують складність системи, час відгуку служб підтримки та можливості моніторингових інструментів. Шостий крок полягає в обчисленні індексу Risk Priority Number (RPN) Це дозволяє ранжувати ризики від найбільш до найменш критичних, що дає змогу зосередити увагу на найважливіших загрозах. Сьомий крок включає розробку

коригувальних дій. На основі розрахованих RPN формуються рекомендації щодо покращення надійності, наприклад, впровадження резервування, оновлення обладнання, підвищення кваліфікації персоналу або вдосконалення процесів моніторингу.

Друга частина присвячена оцінці ризиків фізичної інфраструктури спортивно-оздоровчих центрів. Схему алгоритму для оцінки ризиків фізичної інфраструктури зображено на рисунку 3.2.

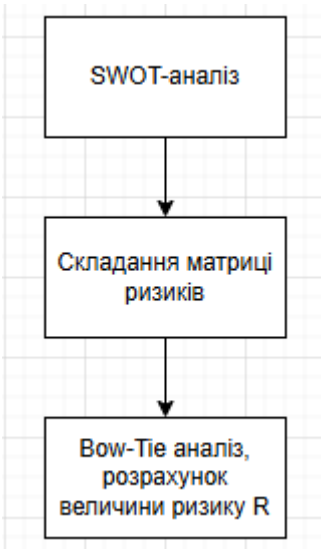

Рисунок 3.2 – Схема алгоритму для оцінки ризиків фізичної інфраструктури

Етап розпочинається з проведення SWOT-аналізу, що дозволяє систематично ідентифікувати сильні сторони (наприклад, наявність сучасного обладнання), слабкі сторони (наприклад, застарілі комунікації), можливості (наприклад, розширення послуг) та загрози (наприклад, природні катастрофи, відключення електропостачання). Даний передбачає побудову матриці SWOT. У цій матриці структуровано записуються всі виявлені сильні та слабкі сторони, можливості й загрози. Важливо, що ці фактори формулюються у вигляді коротких чітких тез, що описують конкретні характеристики або події. На цьому етапі формується єдина картина поточного стану фізичної інфраструктури з позицій внутрішнього та зовнішнього середовища. Далі

проводиться аналіз взаємозв’язків між елементами матриці. Вивчається як сильні сторони можуть допомогти використати можливості або мінімізувати загрози, а слабкі сторони – посилити ризики чи зменшити шанс реалізації можливостей. Це дає змогу побачити основні точки концентрації ризиків та сформувати основу для подальшої роботи. Фінальним кроком SWOT-аналізу є формування списку основних ризиків. На цьому етапі визначаються конкретні події або сценарії, що мають ризиковий характер. Ці ризики формують основу для побудови матриці ризиків на наступному етапі аналізу.

На основі результатів SWOT-аналізу формується матриця ризиків, яка дозволяє оцінити ризики за двома вимірами: ймовірністю настання події та ступенем впливу наслідків. Для побудови матриці ризиків використовуються результати попереднього етапу, зокрема визначені загрози та слабкі сторони, а також експертні оцінки, що дозволяють кількісно оцінити ймовірність та вплив. Спочатку розроблюється шкала оцінки ймовірності настання кожного ризику. Джерелами даних є історична статистика (якщо вона доступна), дані технічних аудитів, експертні оцінки, результати моделювання. Наприклад, ймовірність можна поділити на п’ять рівнів: дуже низька, низька, середня, висока та дуже висока, кожному з яких відповідає числовий коефіцієнт. Далі розробляється шкала оцінки впливу ризику. Тут оцінюється, наскільки серйозними будуть наслідки реалізації кожної ризикової події. Для цього використовуються техніко-економічні показники, нормативна документація, експертні опитування, а також результати аналізу критичних точок інфраструктури. Вплив також можна поділити на п’ять рівнів: незначний, малий, середній, серйозний, катастрофічний, з присвоєнням числових значень. Наступний крок присвячений побудові самої матриці ризиків. Вісь абсцис (горизонталь) представляє ймовірність, вісь ординат (вертикаль) – вплив. На перетині кожного рівня ймовірності та впливу формується комірка, що відображає рівень ризику.

Далі застосовується метод Bow-Tie Analysis, метою якого є деталізація аналізу шляхом розмежування причин виникнення ризику, самої ризикової

події та наслідків, що можуть настати. Спочатку обирається центральна ризикова подія, яка вже була визначена під час аналізу за допомогою матриці ризиків. Далі передбачається визначення всіх можливих причин, що можуть призвести до цієї події. Це потребує глибокого аналізу, який включає вивчення технічної документації, аналіз історичних даних, проведення експертних опитувань та оцінки технічного стану обладнання. Причини записуються у лівій частині схеми й з'єднуються стрілками з центральною подією. На цьому етапі можуть використовуватися як дані з попередніх кроків, так і нові, зібрані під час консультацій з технічним персоналом. Останній крок полягає у виявленні наслідків, що настануть у разі реалізації події. Ці наслідки розташовуються у правій частині схеми. Джерелами даних можуть бути техніко-економічні розрахунки, нормативні документи, результати моделювання, а також висновки експертів.

Фінальним етапом є застосування методології ERM (Enterprise Risk Management), яка дозволяє інтегрувати результати аналізу ризиків для обох типів інфраструктури у єдину систему управління. ERM забезпечує розробку цілісної стратегії управління ризиками, яка включає заходи запобігання, плани реагування на випадок реалізації ризикових подій, а також системи моніторингу для відстеження змін у рівні ризику. ERM допомагає розподілити ресурси між різними сферами, визначити відповідальних осіб, окреслити строки впровадження заходів, а також інтегрувати ризик-менеджмент у загальну стратегію розвитку спортивно-оздоровчих центрів.

Верхньорівнево розроблений комбінований метод можна зобразити як показано на рисунку 3.3.

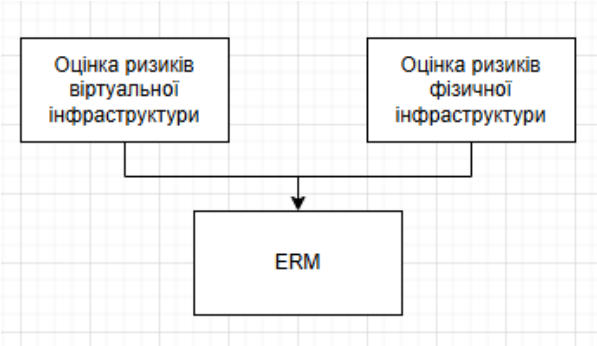

Рисунок 3.3 – Верхньорівнева схема комбінованого методу

Таким чином, розроблений метод забезпечує глибокий, багатоаспектний аналіз ризиків, що базується як на кількісних, так і на якісних підходах. Такий підхід підвищує точність оцінок, дозволяє врахувати особливості кожного типу інфраструктури, формує єдину інтегровану стратегію управління.

4 ПРАКТИЧНА АПРОБАЦІЯ КОМБІНОВАНОГО МЕТОДУ

4.1 Практичне застосування розробленого методу для оцінки ризиків віртуальної на фізичної інфраструктури під час планування ІТ проєкту ІС мережі спортивно-оздоровчих центрів

Першим етапом була виконана оцінка ризиків віртуальної інфраструктури модифікованим методом FMEA. У ході застосування даного методу було виявлено основні можливі відмови, вірогідності їх настання, серйозність наслідків, можливість до виявлення відмові ще до її появи та заплановано дії для реагування. На рисунку 4.1 зображено розрахункову таблицю із порахованим RPN для кожної відмови, що дозволяє визначити до якої проблеми треба приділити більше уваги.

Компонент системи	Потенційна відмова	Потенційний ефект	Причини	Вірогідність настання	Серйозність	Здатність до виявлення	RPN	Заплановані заходи реагування
База даних користувачів	Втрата або спотворення фізіологічних параметрів клієнтів	Невірна персоналізація послуг, зниження якості обслуговування, втрата довіри	Програмна помилка, синхронізація, людський фактор	3	8	5	120	Аудит змін, розширене логування, автоматичне виявлення аномалій
Модуль авторизації та безпеки	Несанкціонований доступ до персональних або медичних даних	Юридичні наслідки, ризик репутації	Слабка автентифікація, вразливості, відсутність 2FA	1	9	9	81	Впровадження 2FA, пенетрейшн-тести, автоматичне блокування при спробах злому
Інтеграція з фізичними пристроями	Некоректне зчитування або передача даних	Помилки в оцінці стану клієнта, неточна аналітика, збої в послугах	Несумісність, проблеми енергоживлення	5	4	3	60	Підтримка декількох SDK
Мобільний додаток	Відсутність доступу клієнта до персональних даних і планів	Зниження зручності, зростання незадоволеності клієнтів, потенційний відтік	Відсутність інтернету, помилки сумісності, збої в додатку	4	6	3	72	Підтримка офлайн режиму роботи, налаштування синхронізації мобільного додатку із сервером
Модуль аналітики та звітності	Некоректні або несвоєчасні звіти	Хибні рішення керівництва, неправильне коригування тренувань	Помилки агрегації, затримки обробки, логічні помилки	2	6	7	84	Валідація звітів, CI/CD для аналітики
Модуль управління лояльністю	Некоректне нарахування знижок/бонусів	Невдоволення клієнтів, фінансові втрати, негативні відгуки	Конфлікт умов акцій, неактуальні налаштування	2	5	6	60	Тестування правил, ручна перевірка
Серверна частина	Перевантаження, відмова або повільна обробка запитів	Затримки або збої в обробці запитів, недоступність системи, відтік користувачів	Недостатня продуктивність, відсутність масштабування, витік пам`яті	1	10	9	90	Моніторинг навантаження, алерти про відмови, автоматичне масштабування (autoscaling)

Рисунок 4.1 – Результати FMEA аналізу і розрахунку RPN

Втрата або спотворення фізіологічних параметрів клієнтів стосується бази даних користувачів, що зберігає ключову інформацію про фізичні характеристики клієнтів, як-от вага, зріст, медичні показники та інші біометричні параметри. Причинами можуть бути як програмні помилки при

обробці даних, так і помилки синхронізації між клієнтським додатком і сервером, або втручання персоналу. Наслідком є недостовірність даних, що призводить до помилкових рекомендацій тренерам, неправильних навантажень, зниження якості обслуговування та втрати довіри клієнтів. Заплановані заходи включають поглиблений аудит змін, введення системи розширеного логування всіх маніпуляцій з даними та впровадження механізмів автоматичного виявлення аномалій у записах.

Несанкціонований доступ до персональних або медичних даних можуть призвести до витоку конфіденційної інформації, що є особливо критичним з огляду на зберігання чутливих медичних відомостей. Основні причини полягають у відсутності двофакторної автентифікації, недоліках у політиках доступу або використанні застарілих бібліотек безпеки. Наслідки охоплюють порушення норм законодавства щодо захисту персональних даних, репутаційні втрати та потенційні фінансові санкції. Заплановані заходи передбачають реалізацію двофакторної автентифікації, регулярне проведення пенетрейшн-тестування та автоматичне блокування облікових записів при аномальній активності.

Некоректне зчитування або передача даних з фізичних пристроїв може виникати в результаті програмної несумісності між програмним забезпеченням та підключеним обладнанням (наприклад, фітнес-браслетами, смарт-вагами тощо). Це призводить до отримання спотвореної або неповної інформації про активність клієнта, що унеможливлює якісний аналіз фізичного стану. Заплановано підтримку декількох стандартів SDK для сумісності з різними пристроями та ручний ввод даних в мобільному додатку.

Відсутність доступу клієнта до функціоналу мобільного додатку критично впливає на досвід користувача. Причинами можуть бути відсутність або нестабільність інтернет-з’єднання, помилки в оновленнях, несумісність з деякими пристроями або версіями ОС. Це викликає фрустрацію, знижує рівень залучення клієнта та може призвести до відтоку. Заплановані рішення включають кешування ключових даних, офлайн-режим роботи з обмеженою

функціональністю, синхронізація даних, змінених в офлайн режимі, одразу за наявності стабільного інтернет з’єднання

Модуль аналітики формує дані для прийняття управлінських рішень та індивідуального планування тренувань. Якщо внаслідок помилок агрегації, некоректної логіки обчислень чи затримок в обробці формуються неточні звіти, це може призвести до прийняття неправильних рішень, невірного навантаження або помилок у формуванні стратегій розвитку. Заплановано запровадити повноцінний CI/CD-процес для аналітичних скриптів та валідацію звітів.

Щодо некоректного нарахування знижок або бонусів у системі лояльності, то цей тип відмови виникає через логічні конфлікти в умовах акцій, помилки у зберіганні промокодів або невірне оновлення налаштувань бонусної програми. Це прямо впливає на фінансові показники та може викликати невдоволення з боку клієнтів. Заплановані заходи передбачають ручну перевірку при внесенні змін до умов акцій, а також тестування сценаріїв перед запуском промокампаній.

Відмова серверної частини виникає у випадках, коли вона перестає обробляти запити через перевантаження, витік ресурсів або помилки в логіці обробки даних. Найбільш поширені причини – це надмірна кількість одночасних підключень клієнтів під час пікових навантажень, неконтрольоване споживання пам’яті окремими мікросервісами, неефективне кешування або погано оптимізовані SQL-запити. Також суттєвим ризиком є внесення змін до конфігурації без належного тестування. Наслідки включають повне припинення доступу до функціоналу системи: користувачі не можуть переглядати свої дані, бронювати послуги, отримувати рекомендації або проводити платежі. Заплановано автоматичне горизонтальне масштабування інстансів серверів, постійний моніторинг навантаження та у рази наближення навантаження до пікового, або у разі збоїв, то передбачені алерти про такого роду відмови.

Для визначення рівнів впливу та можливості завчасно передбачити

настання події було зібрано експертну групу, яка складалася з фахівців із різних областей. Для визначення вірогідності настання відмови для всіх відмов окрім серверної частини було також використано метод експертної оцінки, опираючись на історичні та статистичні дані.

Роботу сервера для визначення вірогідності його відмови було просимульовано із використанням методу Монте-Карло.

Для симуляції було обрано ряд параметрів, а саме кількість симуляцій, максимальну кількість запитів, яку може обробити сервер у хвилину, поріг відмови сервера у відсотках його навантаження від загальної потужності сервера, кількість користувачів, які одночасно роблять запити до сервера, та максимальну та мінімальну кількість запитів, які робить користувач під час використання інформаційної системи мережі спортивно-оздоровчих центрів.

Кількість симуляцій методу Монте-Карло було встановлено рівною 50000, оскільки дана кількість є оптимальною за балансом точності та потужності обчислювальних ресурсів [27].

Параметр максимальної кількості запитів, які може обробити сервер у хвилину було обрано рівним 250000 запитів, що відповідає потужності веб-сервера для систем із середнім рівнем навантаження [28].

Значення параметру відмови сервера було встановлено рівним 95% відсотків навантаження від загальної потужності сервера оскільки саме при досягненні або перевищенні даного порогу навантаження найчастіше трапляються перебої у роботі сервера [29].

Параметр кількості користувачів, які одночасно роблять запити за хвилину було встановлено такими, що перевищують очікування від даної системи, відповідно статистичних показників [30]. Було взято значення 5000, 10000, 20000 та 25000.

Значення мінімального та максимального порогу кількості запитів до системи, які може надіслати користувач протягом хвилини було встановлено 3 та 20 відповідно та призначено випадковим чином для обраної кількості поточних активних протягом хвилини користувачів. Встановлений розмах

показників пояснюється тим, що користувачі переглядають веб-сторінки та сторінки мобільного додатку із різною швидкістю та метою: ознайомлення зазвичай провокує меншу активність за хвилину, а придбання абонементу – більшу [31].

Симуляцію було проведено у середовищі Jupyter Notebook із використанням мови програмування Python. Навантаження на сервер було розраховано як частку суми кількості запитів від усіх користувачів та максимальної кількості запитів, яку може обробити сервер за хвилину, помножену на 100. Для кожної кількості користувачів було виведено середнє навантаження на сервер у відсотках та ймовірність відмови сервера відповідно до згенерованих системою значень.

На рис. 4.2 представлено результати експерименту симуляції роботи сервера із використанням методу Монте-Карло для кількості користувачів за хвилину рівною 5000. Із представлених результатів можемо зробити висновок про те, ще така кількість користувачів не являє собою суттєвого навантаження на систему та дає середнє навантаження лише 23% від загальної потужності сервера.

Рисунок 4.2 – Результати роботи методу Монте-Карло для кількості користувачів рівною 5000

На рис. 4.3 представлено результати експерименту симуляції роботи сервера із використанням методу Монте-Карло для кількості користувачів за хвилину рівною 10000. Із представлених результатів можемо зробити висновок про те, ще така кількість користувачів дає середнє навантаження рівним 46% від загальної потужності сервера та не є знову суттєвою для заданих потужностей.

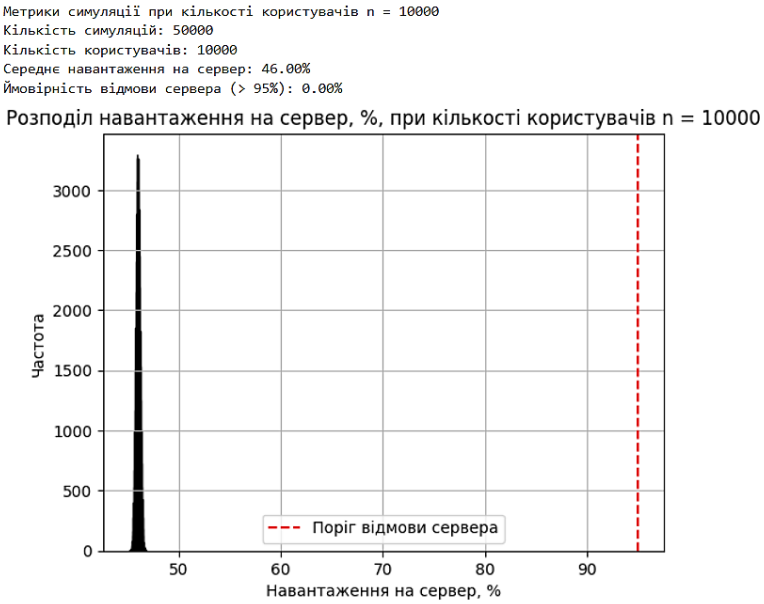

Рисунок 4.3 – Результати роботи методу Монте-Карло для кількості користувачів рівною 10000

На рис. 4.4 представлено результати експерименту симуляції роботи сервера із використанням методу Монте-Карло для кількості користувачів за хвилину рівною 20000. Із представлених результатів можемо зробити висновок про те, ще така кількість користувачів є майже максимальною та дає середнє навантаження у розмірі 92% від загальної потужності сервера. При значенні показника ймовірності відмови 0% дане значення можна вважати максимальним значенням кількості користувачів, які можуть одночасно використовувати веб-сайт інформаційної системи мережі спортивно-

оздоровчих центрів без можливості відмов сервера через його перевантаження.

Рисунок 4.4 – Результати роботи методу Монте-Карло для кількості користувачів рівною 20000

Для того, щоб перевірити, яким чином змінюється значення ймовірності відмови сервера протягом симуляцій методу було прийнято рішення розрахувати показник сходимості методу Монте-Карло кожні 5000 розрахованих симуляцій [32]. Заради даного експерименту було взято кількість користувачів рівною 25000. Результати даного експерименту наведено на рис. 4.5.

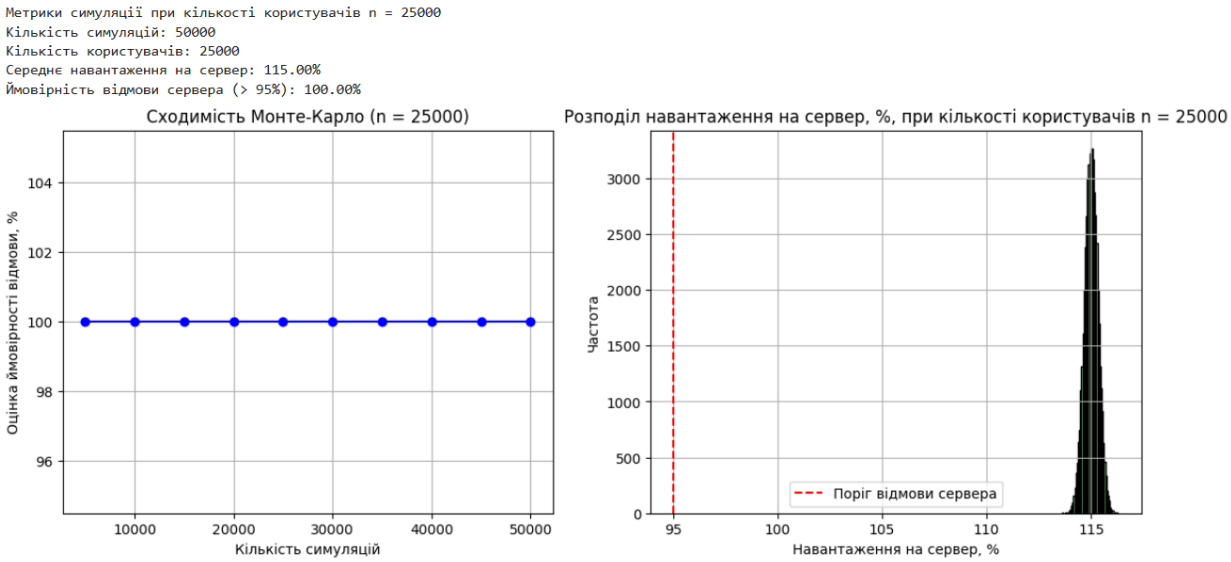

Рисунок 4.5 – Результати роботи методу Монте-Карло для кількості користувачів рівною 25000

Відповідно до даних експерименту, представлених на рис. 4.5, можна зробити висновок, що показник ймовірності відмови сервера протягом усіх симуляцій було розраховано однаково, тож, кількість симуляцій є достатньою, а показник методу сходимості у даному експерименті є сталим. Також, відповідно до значення середнього навантаження на сервер, 115% та 100% ймовірності відмови, можна зробити висновок, що система не витримає навантаження у 25000 одночасно активних користувачів за хвилину.

У якості узагальнення отриманих результатів дослідження методу Монте-Карло для симуляції процесу навантаження на сервер у ході його використання протягом роботи інформаційної системи спортивно-оздоровчих центрів було створено таблицю 4.1. У даній таблиці наведено кількість користувачів , які одночасно використовують інформаційну систему, а, отже, посилають запити до сервера, а також розраховані значення середнього навантаження на сервер та ймовірність отримання відмови сервера у відсотках.

Таблиця 4.1 – Результати застосування методу Монте-Карло для симуляції навантаження на сервер в залежності від кількості користувачів

Кількість користувачів	Середнє навантаження на сервер, %	Ймовірність отримання відмови сервера (при навантаженні на сервер більше 95%), %
5000	23%	0%
10000	46%	0%
20000	92%	0%
25000	115%	100%

Відповідно до даних, представлених у таблиці 4.1, можна зробити висновок стосовно того, яким є порогове значення кількості одночасно активних користувачів для того, щоб сервер працював без збоїв.

У представлених результатах чітко прослідковується закономірність прямо порційного збільшення навантаження на сервер зі збільшенням кількості користувачів, що дозволяє розрахувати середню кількість користувачів за хвилину, які спричиняють 1% навантаження на сервер. Так, 217 користувачів за хвилину у середньому спричиняють 1% навантаження сервера. Приймаючи до уваги той факт, що порогове значення відмови та збоїв у роботі сервера становить 95% навантаження від загальної потужності, тож, за умови його навантаження на 93-94% кількість користувачів в середньому може бути близько 20300 активних користувачів за хвилину.

Таким чином, за умови, що користувачі будуть проявляти таку активність, яку було закладено під час розрахунків, максимально допустима межа роботи без збоїв для сервера становить 20000 користувачів, що проходить прямо по межі можливого навантаження на сервер.

Далі було проведено SWOT-аналіз, в ході якого було проаналізовано та виявлено сильні сторони, слабкі сторони, можливості та загрози проєкту.

Фізична інфраструктура, яка охоплює тренажери, сенсори, термінали

доступу, системи контролю клімату й енергоживлення, формує надійну основу для збору та моніторингу фізіологічних параметрів клієнтів є сильною стороною проєкту. Її інтеграція з IT-системою дозволяє реалізувати персоналізовані тренувальні програми, відстеження прогресу й корекцію навантаження в реальному часі. Наявність сучасного обладнання з API-інтерфейсами забезпечує сумісність із хмарними або локальними сервісами обробки даних, що полегшує масштабування рішень.

В той же час фізична інфраструктура схильна до зносу, фізичних пошкоджень, деградації сенсорів і нестабільності живлення, що ускладнює її надійне функціонування без регулярного технічного обслуговування. Висока вартість оновлення обладнання та обмежена гнучкість у налаштуванні функціоналу можуть сповільнювати адаптацію до нових вимог IT-системи. Крім того, складність у стандартизації пристроїв від різних виробників ускладнює інтеграцію та потребує розробки специфічних програмних адаптерів. Проблемою є також залежність від локального мережевого середовища, що може впливати на стабільність зв’язку з віртуальним середовищем. Це все є слабкими сторонами.

Можливістю є подальший розвиток IoT-технологій, що дає нові горизонти для моніторингу стану обладнання, прогнозування відмов і зниження витрат на обслуговування. Завдяки розвитку стандартів передачі даних можлива побудова єдиної платформи обміну між фізичними та віртуальними компонентами системи. Використання фізичної інфраструктури як джерела даних для аналітики, трендів та візуалізацій створює передумови для стратегічного керування клієнтським досвідом і підтримки прийняття рішень на основі даних.

Основними загрозами є високий ризик простоїв через технічні несправності обладнання, які напряму впливають на функціонування IT-системи та задоволення клієнтів. Кіберфізичні ризики, пов’язані з несанкціонованим доступом до фізичних пристроїв, можуть викликати витоки або підробку критичних даних. Вразливість до порушень у мережевій

інфраструктурі, особливо при централізованій обробці даних, може паралізувати роботу всієї системи. Крім того, постачальницька залежність від конкретних виробників створює ризики пов’язані з відсутністю запасних частин або припиненням підтримки.

За результатом було сформовано матрицю SWOT-аналізу, що зображено на рисунку 4.6.

Рисунок 4.6 – Матриця SWOT-аналізу

За результатами SWOT-аналізу було побудовано матрицю ризиків, що зображено на рисунку 4.7. Кожному ризику в цій матриці було визначено ймовірність виникнення та ступінь впливу завдяки експертним оцінкам. Далі, кожен ризик було поміщено в комірку відповідно до рівня ймовірності виникнення та впливу.

Чим ризик знаходиться вище та ближче до правого боку матриці, тим він є критичнішим і на такі ризики слід звернути увагу в першу чергу при виборі заходів запобігання виникнення ризиків та усунення їх наслідків.

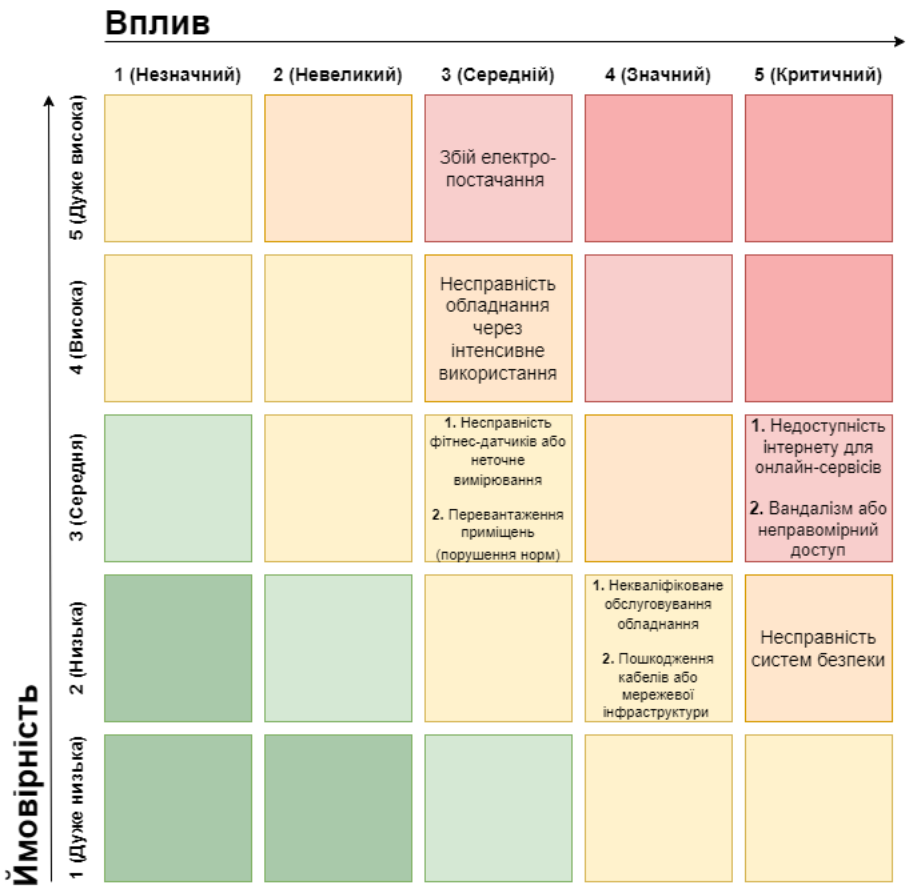

Рисунок 4.7 – Матриця ризиків

Ризик несправності обладнання через інтенсивне використання виникає через постійне і нерівномірне навантаження на спортивне та діагностичне обладнання, особливо у пікові години. При відсутності своєчасного обслуговування або заміни зношених компонентів можливий вихід техніки з ладу. Такі відмови можуть призвести до зниження якості обслуговування, скорочення доступності послуг, зростання невдоволення клієнтів, а також – у критичних випадках – до небезпеки травмування. Наявність цифрового моніторингу зносу обладнання значно знижує ризик, проте не усуває його повністю.

Перебої з електропостачанням можуть бути спричинені як зовнішніми чинниками (аварії на електромережі), так і внутрішніми (перевантаження, коротке замикання, несправність стабілізаторів). Вони унеможливлюють використання електрозалежного обладнання, ведуть до збоїв у роботі серверів,

терміналів, освітлення, що створює небезпеку для персоналу та відвідувачів. Впровадження резервного живлення мінімізує ці наслідки.

Ризик пошкодження сенсорних пристроїв, що застосовуються для моніторингу фізіологічних параметрів клієнтів або неточне їх вимірювання, є критичним через високу залежність індивідуальних тренувальних планів від точних даних. Основні причини включають механічне пошкодження внаслідок неправильного поводження, вплив води, поту або пилу, а також можливі дефекти виробництва або програмного забезпечення. Наслідками є неточні показники стану клієнта, що може вплинути як на ефективність занять, так і на безпеку, особливо у випадку клієнтів із медичними обмеженнями.

Ризик перевантаження приміщень спортивно-оздоровчих центрів є критичним через обмеженість фізичного простору та необхідність забезпечення безпеки, комфорту і ефективності надання послуг клієнтам. Основними причинами такого ризику є недосконале планування графіків занять, неузгодженість у системах бронювання, технічні збої в системі обліку відвідувачів або помилки персоналу при ручному контролі кількості присутніх. Наслідками можуть стати перевищення допустимої місткості, що призводить до порушення санітарно-епідеміологічних норм, зниження якості тренувального процесу, підвищеного травматизму через нестачу простору або обладнання, а також до формування негативного досвіду клієнтів і зниження рівня лояльності.

Ризик недоступності інтернету для онлайн сервісів у спортивно-оздоровчих центрах є суттєвим, оскільки більшість функцій сучасної IT-інфраструктури базується на постійному підключенні до мережі. Причинами цього ризику можуть бути технічні збої на стороні провайдера, пошкодження мережевого обладнання, проблеми з електропостачанням, програмні помилки в маршрутизаторах або неналежна конфігурація системи. Наслідками стає втрата доступу до облікових записів клієнтів, неможливість проведення онлайн-реєстрації та бронювання, переривання в роботі тренерів і персоналу, відсутність синхронізації з фітнес-трекерами, а також неможливість надання

дистанційних послуг. Усе це призводить до зниження ефективності функціонування центру, втрати довіри клієнтів і потенційних фінансових втрат.

Фізичний доступ сторонніх осіб до обладнання є серйозним ризиком, який неможна недооцінювати. Неналежна організація контролю доступу до фізичної інфраструктури (наприклад, відкриті тренажерні зони поза розкладом, неавторизований персонал) може спричинити випадки пошкодження обладнання, крадіжки або навіть травмування. Цей ризик часто недооцінюється, але його наслідки включають як прямі фінансові втрати, так і репутаційні збитки. Використання засобів електронного контролю доступу камер відеонагляду та зонування є важливими мірами профілактики. Сюди можна також додати пошкодження обладнання (екрани, інфо-термінали). Цифрові інформаційні панелі, термінали самообслуговування, інтерактивні екрани є важливою частиною сучасної фізичної інфраструктури. Їхнє пошкодження – як навмисне, так і випадкове – призводить до втрати каналу комунікації з клієнтами, порушення навігації по залу, та в окремих випадках – до зупинки процесів реєстрації або оплати. Причинами можуть бути удар, перегрів, або вандалізм. Захист у вигляді міцних матеріалів корпусу та антивандального монтажу знижує ризик. Для зопобігання даним ризикам, або для полегшення усунення їх наслідків є важливою стабільність роботи систем безпеки.

Ризик некваліфікованого обслуговування обладнання у спортивно-оздоровчих центрах становить серйозну загрозу для безперервності надання послуг і безпеки клієнтів. Основними причинами цього ризику є залучення технічного персоналу без належного рівня підготовки або сертифікації, відсутність регламентованих процедур технічного обслуговування, нехтування рекомендаціями виробників або використання неякісних запчастин. Наслідками можуть стати передчасні збої в роботі тренажерів, несправності систем кондиціонування чи вентиляції, а також пошкодження елементів інфраструктури, що створює потенційно небезпечне середовище

для клієнтів і знижує рівень довіри до закладу. У довгостроковій перспективі це може призвести до зростання витрат на ремонт, зупинки в роботі і втрати лояльності відвідувачів.

Ризик пошкодження кабелів або елементів мережевої інфраструктури у спортивно-оздоровчих центрах є критичним через залежність цифрових сервісів, систем доступу, відеоспостереження та онлайн-обліку клієнтів від безперебійного з’єднання. До основних причин належить випадкове механічне пошкодження під час ремонтних або прибирань приміщень, недостатній захист кабелів у зонах активного користування, зношення ізоляції, вплив вологи або температурних коливань, а також некоректне прокладання мереж на етапі будівництва чи модернізації. Наслідками є часткова або повна втрата зв’язку між елементами інфраструктури, недоступність онлайн-сервісів, порушення процесу ідентифікації клієнтів та фіксації тренувань, що створює перешкоди для нормальної роботи закладу та знижує якість обслуговування. Це також підвищує ризик зниження безпеки, особливо при паралізації систем відеонагляду або тривожної сигналізації.

Завдяки побудові матриці ризиків було відібрано три найбільш критичні ризики і проведено Bow-Tie аналіз. Це дало більш глибоке розуміння природи даних ризиків, їх причин, наслідків, а також засобів запобігання та реагування.

На рисунку 4.8 зображена Bow-Tie діаграма для ризику несправності обладнання через інтенсивне використання.

Причини виникнення цього ризику полягають у надмірному навантаженні на обладнання через тривале або інтенсивне використання без належного перерв на відпочинок і технічне обслуговування. Відсутність регулярних технічних оглядів та запізніла заміна зношених компонентів може призвести до раптових поломок. Крім того, використання обладнання поза межами його технічних характеристик або без урахування специфікацій для конкретних типів тренувань також підвищує ймовірність відмови. Деякі проблеми можуть виникати через необережне поводження з обладнанням під час налаштування чи експлуатації.

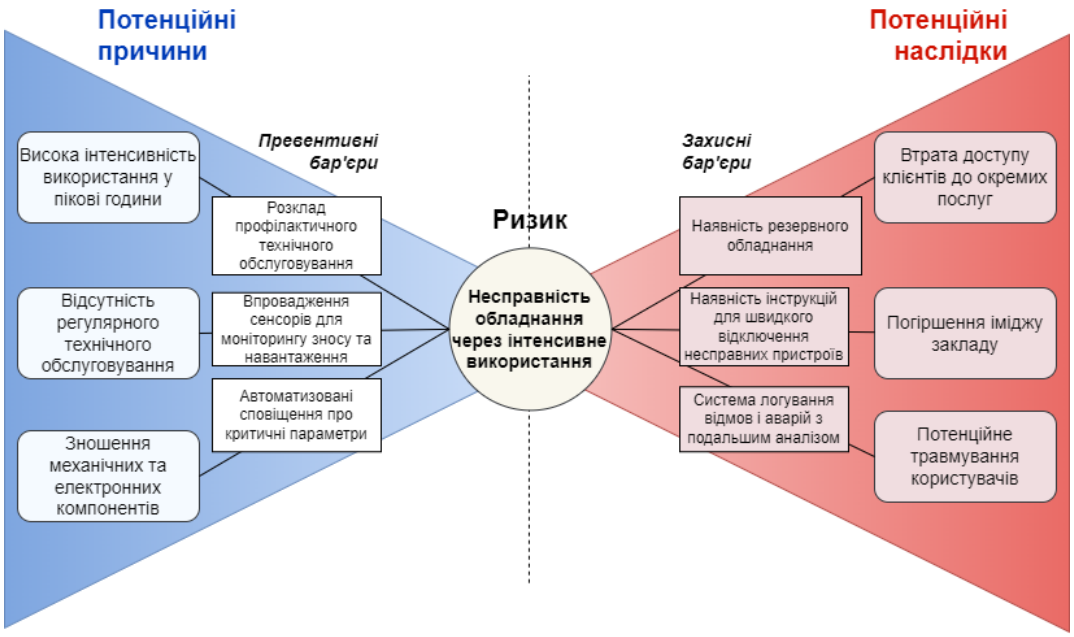

Рисунок 4.8 – Bow-Tie діаграма для ризику несправності обладнання через інтенсивне використання

Наслідки цієї відмови можуть бути різноманітними. Найперше, це може призвести до зниження ефективності роботи обладнання, що впливає на точність результатів, які використовують клієнти. Втрата працездатності обладнання також може порушити виконання тренувальних програм, що знижує рівень обслуговування і призводить до незадоволення клієнтів. Крім того, якщо несправність стається під час роботи з клієнтами, це може призвести до травм або інших небажаних наслідків, що негативно позначиться на безпеці. Репутаційні втрати та додаткові витрати на ремонт і заміну обладнання – також серйозні наслідки.

Бар'єри, які можна вжити для попередження або мінімізації цього ризику, включають регулярні перевірки стану обладнання та технічне обслуговування. Забезпечення належного навчання персоналу з правильного використання та налаштування обладнання знижує ризик помилок у роботі. Для більшості типів обладнання доцільно ввести систему моніторингу технічного стану в режимі реального часу. Крім того, важливо встановити

чіткі стандарти для використання обладнання відповідно до його технічних характеристик.

На рисунку 4.9 зображена Bow-Tie діаграма для ризику недоступності інтернету для онлайн-сервісів.

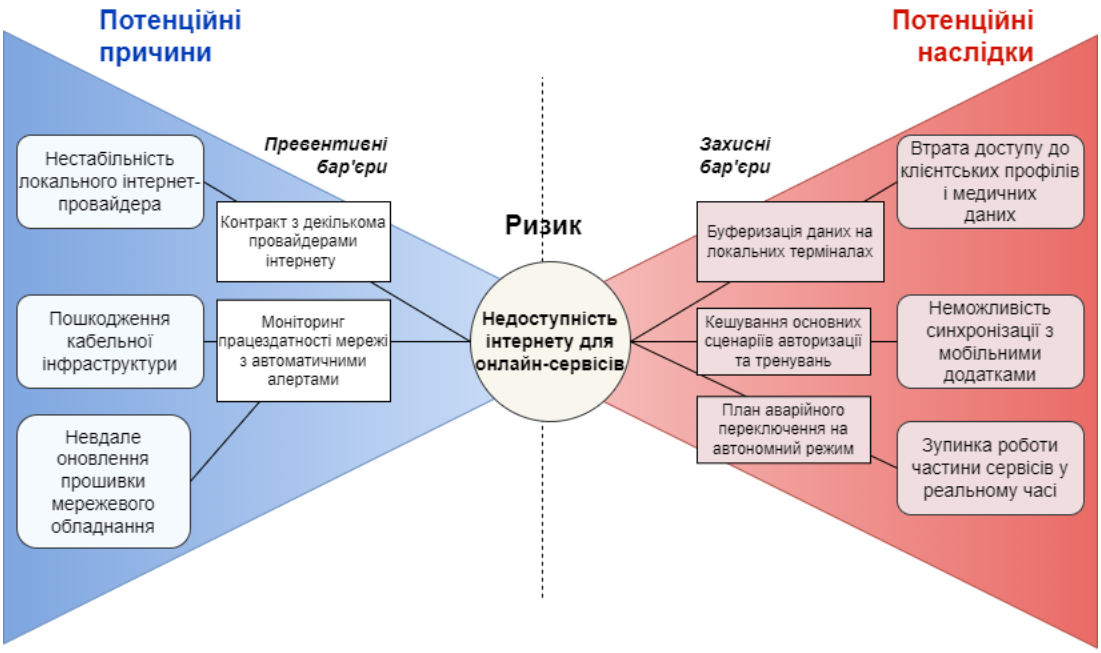

Рисунок 4.9 – Bow-Tie діаграма для ризику недоступності інтернету для онлайн-сервісів

Причини виникнення ризику відмови мережевого з’єднання з платформою охоплюють як внутрішні технічні обставини, так і зовнішні фактори інфраструктурного характеру. Частою причиною є пошкодження кабелів або мережевого обладнання, спричинене механічним втручанням або природними умовами, такими як волога, коливання температур або стрибки напруги. До факторів ризику також належить перевантаження локальної мережі через недостатню пропускну здатність або погано спроєктовану архітектуру. Неправильне конфігурування мережевого обладнання, несумісність протоколів або помилки в оновленнях програмного забезпечення також можуть спричинити втрату з’єднання. У разі використання зовнішнього постачальника інтернету, додаткову загрозу становлять відмови з боку

провайдера або аварії на транспортних магістралях зв’язку.

Наслідками цього ризику є тимчасова або тривала недоступність цифрової платформи як для персоналу, так і для клієнтів. Втрата доступу означає неможливість проведення онлайн-реєстрацій, доступу до особистих кабінетів, моніторингу тренувальних сесій та збору фізіологічних даних, а також блокування адміністрування тренувальних планів. Це створює фрагментацію сервісу, дезорганізує роботу персоналу та викликає роздратування у користувачів. У разі хронічних збоїв формується негативне враження про надійність системи, що підриває довіру та призводить до втрати клієнтів. При пов’язаності мережі з системами безпеки або системами контролю доступу, наслідки можуть стати критичними для фізичної безпеки об’єкта.

Бар’єри для зниження імовірності цього ризику включають створення резервної схеми підключення, що передбачає використання незалежного каналу доступу до Інтернету з автоматичним перемиканням при виявленні збоїв основного. Доцільним є розгортання внутрішньої локальної мережі з фокусом на фізичну безпеку кабельної інфраструктури та використання захищених каналів з’єднання. Встановлення якісного обладнання з можливістю моніторингу статусу інтерфейсів у реальному часі, автоматичне виявлення порушень конфігурації та логування інцидентів дозволяє швидко виявляти й локалізовувати проблему. Крім того, слід передбачити локальну автономність критично важливих функцій платформи на випадок короткотривалих відключень. Надання персоналу чітких протоколів дій при втраті зв’язку зменшує рівень організаційного хаосу та пришвидшує відновлення працездатності системи.

На рисунку 4.10 зображена Bow-Tie діаграма для ризику пошкодження сенсорів або трекерів.

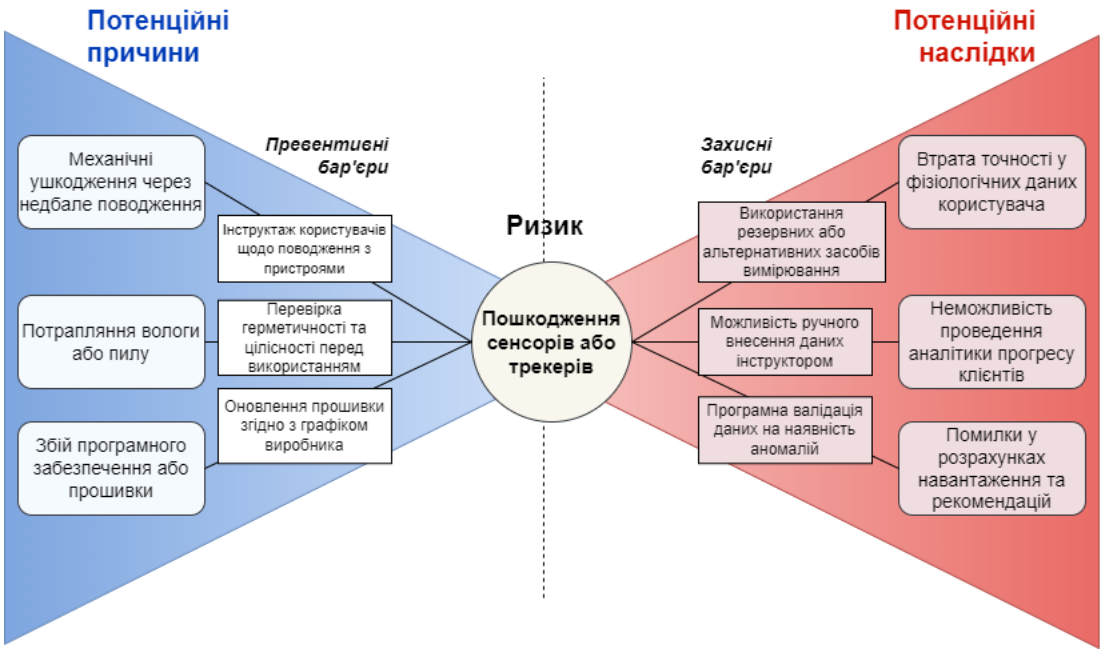

Рисунок 4.10 – Bow-Tie діаграма для ризику пошкодження сенсорів або трекерів

Причинами таких пошкоджень можуть бути як експлуатаційні фактори, так і технічні дефекти. Найбільш поширеними є механічні ушкодження через недбале поводження користувачів, падіння під час інтенсивних тренувань, проникнення вологи або пилу в корпус пристрою, що порушує герметичність. Також можливе зношення матеріалів через інтенсивне використання або невідповідність умов експлуатації до специфікацій виробника. У деяких випадках причиною є некоректне оновлення прошивки або збої в синхронізації з мобільним додатком чи сервером.

Наслідками є втрата достовірності або повна відсутність фізіологічних показників, що знижує ефективність персоналізованих тренувальних програм і в деяких випадках створює ризик для здоров’я клієнтів, які мають медичні обмеження. Некоректні дані можуть викликати хибні висновки щодо фізичного стану користувача, що впливає як на прийняття рішень тренерами, так і на автоматизовану аналітику. Погіршується користувацький досвід, оскільки клієнти не бачать результатів або бачать спотворені показники, що знижує мотивацію і рівень довіри до системи. При системному характері таких

відмов страждає репутація платформи.

Запобігання цьому ризику включає впровадження протоколів технічного обслуговування та регулярну перевірку стану сенсорних пристроїв з боку персоналу. Рекомендується застосування лише сертифікованих моделей сенсорів, що мають захист від вологи та пилу, а також тестування пристроїв перед введенням в експлуатацію. Клієнтів слід інформувати про правила користування пристроями та передбачити механізм оперативної заміни несправних екземплярів. У майбутньому доцільно реалізувати функцію автоматичного виявлення аномальних показників, що можуть свідчити про відмову сенсора, з відповідними сповіщеннями для персоналу. Крім того, резервування ключових фізіологічних показників через альтернативні канали збору даних (наприклад, мануального вводу даних) або дублювання сенсорів підвищує надійність загальної системи моніторингу.

Фінальними кроками згідно ERM стали пріорітизація ризиків та розробка стратегій управління ними. Було розроблено стратегії управління ризиками як для віртуальної інфраструктури, так і для фізичної інфраструктури.

Стратегії управління ризиками для віртуальної інфраструктури спрямовані на зниження ймовірності настання негативних подій і мінімізацію їхнього впливу на операційну діяльність спортивно-оздоровчих центрів. Оскільки віртуальна інфраструктура є важливою складовою IT-проєкту, ці стратегії повинні враховувати високі вимоги до безпеки, доступності та ефективності.

Одним із найважливіших ризиків є втрати або порушення захисту персональних даних клієнтів. Оскільки ці дані є дуже чутливими, порушення їх захисту може призвести до серйозних юридичних, фінансових та репутаційних втрат. Стратегією управління для цього ризику є покращення безпеки даних. Перше, що необхідно зробити, це зміцнити політики безпеки. Крім того, необхідно запровадити шифрування для всіх особистих і фінансових даних клієнтів на всіх етапах їх обробки. Іншим важливим кроком

є впровадження багаторівневої аутентифікації для доступу до системи. Це дозволить значно підвищити рівень безпеки акаунтів. Варто також проводити регулярні аудити безпеки, залучаючи зовнішніх фахівців, щоб виявити потенційні слабкі місця в системах захисту. Моніторинг у реальному часі дозволить швидко виявляти аномалії та загрози, зменшуючи можливість несанкціонованого доступу. Крім того, регулярні тренінги для співробітників щодо методів захисту даних та профілактики фішинг-атак є невід'ємною частиною стратегії захисту персональних даних.

Ще одним значущим ризиком є перевантаження серверів, особливо під час пікових навантажень. У цьому випадку стратегією управління є масштабування інфраструктури та оптимізація навантаження. Важливо використовувати хмарні технології для автоматичного масштабування потужностей, щоб система могла адаптуватися до змін навантаження. Масштабування не повинно обмежуватись лише вертикальним масштабуванням, тому варто впроваджувати мікросервісну архітектуру, що дозволяє розширювати окремі компоненти системи без потреби масштабувати всю інфраструктуру. Крім того, балансувальники навантаження повинні рівномірно розподіляти запити між серверами, що зменшує ймовірність перевантаження. Застосування CDN (Content Delivery Networks) допоможе кешувати статичні дані, що дозволить знизити навантаження на основні сервери та покращити швидкість доставки контенту. Також важливо забезпечити резервування ресурсів для обробки можливих надлишкових запитів під час пікових навантажень.

Ще один ризик, що потребує управління – це помилки в інтеграції з фізичними пристроями та обладнанням. Стратегією для цього ризику є стандартизація процесів і впровадження інтеграційних тестів. Створення єдиних стандартів для обміну даними між фізичними пристроями та програмним забезпеченням допоможе знизити ймовірність помилок. Важливо впровадити інтеграційне тестування, яке дозволить виявити будь-які несумісності між системами до їх впровадження в продуктивне середовище.

Крім того, необхідно використовувати моніторинг у реальному часі для виявлення помилок в інтеграції та оперативного реагування на збої. Оскільки інтеграція з фізичними пристроями є важливою складовою роботи системи, регулярні оновлення документації та підтримка її актуальності також повинні стати частиною стратегії управління цим ризиком.

Ще один значущий ризик стосується відмов програмного забезпечення через баги або некоректне оновлення. Стратегією управління в цьому випадку є забезпечення безпечного оновлення програмного забезпечення та запобігання критичних помилок. Для цього слід запровадити систему контролю версій, яка дозволяє відслідковувати всі зміни в коді і проводить код-рев'ю перед кожним оновленням. Автоматизовані тести на кожному етапі розробки забезпечать виявлення помилок до їх впровадження в продуктивне середовище. Важливо створити механізм автоматичного відкату оновлень у разі виявлення помилок, що дозволить швидко відновити працездатність системи після неуспішних оновлень. Стратегія безперервної інтеграції та доставки (CI/CD) дозволяє автоматизувати тестування, побудову та доставку нових версій програмного забезпечення, знижуючи ризик помилок при розгортанні оновлень.

Стратегії управління ризиками фізичної інфраструктури спортивно-оздоровчих центрів мають бути спрямовані на забезпечення безперервності роботи обладнання, збереження цілісності даних і підтримку високої якості обслуговування клієнтів. Одним із критичних ризиків є несправність обладнання через інтенсивне використання. Цей ризик вимагає активної експлуатаційної стратегії, яка базується на впровадженні регулярного профілактичного обслуговування. Для кожного типу обладнання повинні бути визначені допустимі цикли навантаження, межі зношування, контрольні точки для діагностики, а також автоматизоване ведення обліку використання. Впровадження сенсорів зношення або лічильників активності дозволяє виявляти ознаки деградації до моменту критичної відмови. Також важливо укладати контракти з постачальниками на сервісне обслуговування з

гарантованими термінами реагування. В якості запобіжного заходу слід мати резервне критично важливе обладнання на випадок виходу з ладу основного, що дозволяє уникнути повної зупинки роботи.

Інший вагомий ризик – недоступність інтернету, що забезпечує роботу онлайн-сервісів, мобільного застосунку, синхронізацію клієнтських профілів та зберігання даних у хмарі. Щоб мінімізувати його вплив, необхідно реалізувати стратегію підвищення стійкості мережевої інфраструктури. Це включає організацію багатоканального підключення до інтернету з автоматичним перемиканням у разі збою основного каналу (failover), використання резервного мобільного LTE-з'єднання, а також впровадження локального кешування критично важливих сервісів. Особливу увагу варто приділяти якості провайдерських послуг – важливо укладати договори з постачальниками. Частина онлайн-функціоналу повинна мати офлайн-режим з можливістю відкладеної синхронізації, що забезпечує мінімально допустимий рівень функціонування систем навіть за відсутності зв’язку. Також доцільно застосовувати системи моніторингу з попередженнями щодо падіння доступності каналів або зниження пропускної здатності.

Ще одним суттєвим ризиком є пошкодження сенсорів або трекерів, що використовуються для збору даних про фізичну активність клієнтів. Управління цим ризиком має базуватися на трьох напрямках: вибір якісних пристроїв з високим ступенем захисту від впливу вологи, пилу, ударів (відповідно до стандартів IP), розробка політик їхнього використання і навчання персоналу та клієнтів, а також впровадження процедур діагностики. У кожному закладі має бути відповідальний за контроль стану обладнання з періодичними перевірками працездатності сенсорів. У разі виявлення несправностей необхідна негайна заміна або сервісне обслуговування пристроїв. Стратегія також передбачає введення в експлуатацію засобів автоматичного виявлення аномалій у даних, що можуть свідчити про пошкодження пристрою, наприклад, раптові скачки, зникнення сигналу чи статичні показники протягом тривалого часу. Крім того, важливо мати запас

сумісних сенсорів, які можна оперативно видати клієнтам на заміну. У перспективі – впровадження резервного дублювання важливих даних або використання альтернативних каналів збору інформації, що дозволить зберігати безперервність моніторингу навіть при втраті окремих пристроїв.

ВИСНОВКИ

У ході виконання кваліфікаційної роботи бакалавра було проведено аналіз предметної області, виявлено особливості розробки ІТ-проєктів для спортивно-оздоровчих центрів. Приділено увагу специфіці таких систем, зокрема потребі в актуалізації персональних фізіологічних даних клієнтів, забезпеченні кібербезпеки та захисту персональних даних, інтеграції з фізичним обладнанням (фітнес-датчиками, трекерами, сенсорами), вимогам до мобільності та онлайн-доступу, а також підтримці інструментів управління лояльністю та аналітичного модулю. Враховано взаємодію віртуальної та фізичної інфраструктур, критичність безперебійної роботи серверної частини, мережевої інфраструктури, інтернет-з’єднання, джерел живлення та фізичного середовища, в якому функціонує система.

У межах роботи було проведено порівняльний аналіз існуючих методів оцінки ризиків, які потенційно придатні для використання в ІТ-проєктах зі складною багатокомпонентною інфраструктурою. Розглянуто такі підходи як FMEA (Failure Modes and Effects Analysis), SWOT-аналіз, метод матриці ризиків (Risk Matrix), Bow-Tie аналіз, а також Enterprise Risk Management (ERM). Для кожного з них було визначено ключові характеристики, прикладну доцільність, переваги та обмеження.

На основі всебічного аналізу та оцінки обраних методів було розроблено комбінований метод для оцінки ризиків, що поєднує переваги кожного з розглянутих методів та нівелює їх недоліки. Основою розробленого методу стали FMEA, SWOT-аналіз, матриця ризиків, Bow-Tie аналіз, ERM.

Розроблений метод було застосовано до проєкту з розробки ІС для мережі спортивно-оздоровчих центрів, що дозволило виявити низку критичних ризиків, зокрема: відмову серверної частини, перевантаження обладнання, пошкодження сенсорних пристроїв, недоступність інтернет-з'єднання, збої в електроживленні, некваліфіковане технічне обслуговування

та інші. Для кожного ризику були сформульовані причини виникнення, потенційні наслідки та заплановані заходи з реагування. Отримані дані стали основою для розробки стратегій реагуванні і управління ризиками обох інфраструктур. Таким чином, запропонований метод довів свою ефективність у практичному середовищі, забезпечуючи системний, деталізований та гнучкий підхід до виявлення, оцінки і нейтралізації ризиків в умовах складної гібридної IT-інфраструктури.

Наукова новизна роботи полягає в тому, що тема оцінки ризиків великих і комплексних проєктів наразі дуже мало вивчена, зокрема для такого роду інформаційних систем, де існують дві великі і тісно пов’язані між собою інфраструктури: фізична і віртуальна. Для вирішення даної задачі було розроблено комбінований метод оцінки ризиків, що дозволяє розглянути всі аспекти ІС з різних боків, розроблено стратегії реагування і управління ними. Даний метод може бути корисним для оцінки ризиків інших ІС, де віртуальна та фізична інфраструктури тісно взаємодіють між собою, наприклад: системи розумних будинків, системи автоматизації промислових підприємств, системи віддаленого моніторингу стану пацієнтів, системи інтелектуального транспорту (ITS) та інш.

Результати кваліфікаційної роботи було опробовано на VIII міжнародній науково-практичної конференції «Scientific achievements of contemporary society» [1].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Білова Т.Г., Сусла В.О. Дослідження методів оцінки ризиків під час планування ІТ-проєкту інформаційної системи мережі спортивно-оздоровчих центрів. Scientific achievements of contemporary society: тези доповідей VIII міжнародної науково-практичної конференції (Лондон, 6-8 березня 2025р.). Лондон, 2025. С. 170-175.

2. American Society for Healthcare Risk Management (ASHRM), R. Carroll Risk Management Handbook for Health Care Organizations: USA: Jossey-Bass, 2009, 672 p.;

3. F. Kavaler, R. S. Alexander Risk Management in Health Care Institutions: Limiting Liability and Enhancing Care, 3rd Edition: USA: Jones & Bartlett Learning, 2012, 534 p.

4. P. Fontaine Enterprise Risk Management: Concepts, Methods, Common Risk Areas (First Edition): Canada: Noranda Publishing, 2021, 724 p.;

5. Головна сторінка мережі Sport Life для локації Харків. URL: https://sportlife.ua/uk/clubs/kharkov/nikolskiy/ (дата звернення 28.02.2025).

6. Головна сторінка мережі жіночих фітнес-клубів FitCurves. URL: https://fitcurves.org/ua (дата звернення 28.02.2025).

7. Risk Assessment in Project Management. URL: https://www.simplilearn.com/risk-assessment-project-management-article (дата звернення 10.02.2025).

8. FMEA. URL: https://asq.org/quality-resources/fmea (дата звернення 14.02.2025).

9. A. Josephs, B. Rubenstein Risk Up Front: Managing Projects in a Complex World: USA: Lioncrest Publishing, 2018, 378 p.;

10. Fault tree analysis (FTA). URL: https://fiixsoftware.com/glossary/fault-tree-analysis/ (дата звернення 16.02.2025).

11. Project risk assessment: an example with a risk matrix template. URL:

https://bigpicture.one/blog/project-risk-assessment-examples/ (дата звернення 10.02.2025).

12. What Is Vulnerability Assessment? Benefits, Tools, and Process. URL: https://www.hackerone.com/knowledge-center/what-vulnerability-assessment-benefits-tools-and-process (дата звернення 17.02.2025).

13. The Essentials of Effective Project Risk Assessments. URL: https://www.smartsheet.com/content/project-risk-assessment (дата звернення 11.02.2025).

14. Introduction to Risk Assessment in Project Management. URL: https://projectmanagementacademy.net/resources/blog/risk-assessment-in-project-management/ (дата звернення 12.02.2025).

15. SWOT analysis: Examples and templates. URL: https://asana.com/resources/swot-analysis (дата звернення 19.02.2025).

16. Enterprise Risk Management (ERM). URL: https://corporatefinanceinstitute.com/resources/management/enterprise-risk-management-erm/ (дата звернення 20.02.2025).

17. AIAG & VDA FMEA Handbook: USA: Automotive Industry Action Group, 2019, 327 p.

18. Carl S. Carlson Effective FMEAs: Achieving Safe, Reliable, and Economical Products and Processes using Failure Mode and Effects Analysis 1st Edition: USA: Wiley, 2012, 464 p.

19. D H Stamatis PH.D. Failure Mode and Effect Analysis: FMEA From Theory to Execution: USA: ASQ Quality Press, 2003, 666 p.

20. Mohammad Modarres, Katrina Groth Reliability and Risk Analysis (What Every Engineer Should Know) 2nd Edition: USA: CRC Press, 2023, 657 p.

21. Chris Hughes, Nikki Robinson, Ron Gula Effective Vulnerability Management: Managing Risk in the Vulnerable Digital Ecosystem 1st Edition: USA: Wiley, 2024, 288 p.

22. Gerardus Blokdyk SWOT Analysis A Complete Guide - 2019 Edition: USA: 5STARCooks, 2019, 241 p.

23. Frank Crawley HAZOP: Guide to Best Practice: USA: Elsevier, 2015, 168 p.

24. Chunbing Bao, Jianping Li, Dengsheng Wu Risk Matrix: Rating Scheme Design and Risk Aggregation (Innovation in Risk Analysis): USA: Springer, 2022, 287 p.

25. Luca Fiorentini Bow-Tie Industrial Risk Management Across Sectors: A Barrier-Based Approach: USA: Wiley, 2021, 469 p.

26. John R. S. Fraser, Rob Quail, Betty Simkins Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives (Robert W. Kolb): USA: Wiley, 2021, 944 p.

27. L. G. Birta, G. Arbez Modelling and Simulation: Exploring Dynamic System Behaviour (Simulation Foundations, Methods and Applications): USA: Springer, 2020, 868 p.

28. V. Reed, J. Moore Internet Traffic & Leads: The Past, Present And Future Of Internet Marketing For Entrepreneurs Who Want To Win: USA: CreateSpace Independent Publishing Platform, 2016, 198 p.

29. B. Crawley Threat Modeling Gameplay with EoP: A reference manual for spotting threats in software architecture: UK: Packt Publishing, 2024, 256 p.

30. T. Humphrey Seniors Guide to Building Ecommerce Websites With Wordpress and Elementor: Easy Steps to Build and Launch Ecommerce Websites for Dropshipping and Online Businesses: USA: Independently published, 2020, 144 p.

31. R. Brunson Traffic Secrets: The Underground Playbook for Filling Your Websites and Funnels with Your Dream Customers: USA: Hay House Business, 2023, 352 p.

32. A. M. Law Simulation Modeling and Analysis, Sixth Edition 6th Edition: USA: McGraw Hill, 2024, 688 p.