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

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(освітній рівень)

на тему: "Модель оцінювання ризиків кібербезпеки медичної інформаційної системи із використанням методу Монте-Карло"

Виконала: студентка VI курсу, групи СБмз-61

Спеціальності:
125 «Кібербезпека та захист інформації»
(шифр і назва напряму підготовки, спеціальності)
Косарик Дарія Андріївна
підпис (прізвище та ініціали)

Керівник Козак Р. О.
підпис (прізвище та ініціали)

Нормоконтроль Стадник М. А.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2025

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2025 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека та захист інформації
(шифр і назва спеціальності)

Студенту Косарик Дарії Андріївні
(прізвище, ім'я, по батькові)

1. Тема роботи Модель оцінювання ризиків кібербезпеки медичної інформаційної системи із використанням методу Монте-Карло

Керівник роботи Козак Руслан Орестович, кандидат технічних наук, доцент кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «24» 11 2025 року № 4/7-1025

2. Термін подання студентом завершеної роботи 12.12.2025

3. Вихідні дані до роботи Наукові публікації управління ризиками в медичних системах

4. Зміст роботи (перелік питань, які потрібно розробити): Вступ, Методологічні основи оцінки ризиків і моделювання загроз у кіберпросторі, 1.1 Важливість ризик-менеджменту в медичних інформаційних системах, 1.2 Підходи до управління ризиками, 1.2.1 Підхід, заснований до досягненні рівня зрілості, 1.2.2 Ризик-орієнтований підхід, 1.2.3 Порівняння підходів до управління ризиками, 1.3 Сучасні підходи та стратегії кібербезпеки у медичних інформаційних системах, 1.4 Наслідки кіберзагроз для безпеки пацієнтів, 1.5 Висновки до першого розділу, 2 Модель оцінювання ризиків кібербезпеки медичної системи, 2.1 Опис системи, 2.2 Ідентифікація загроз і засобів контролю, 2.2.1 Виявлення загроз у системі, 2.2.2 Визначення заходів контролю та їх відповідність загрозам, 2.2 Ймовірнісне моделювання, 2.2.1 Невизначеність у моделюванні ризиків, 2.2.2 Вибір ймовірнісних розподілів для вхідних параметрів системи, 2.2.3 Джерела даних та експертні оцінки, 2.3 Математична модель оптимізації, 2.4 Висновки до другого розділу, 3 Симуляційні експерименти та аналіз результатів, 3.1 Програмна реалізація моделі оцінювання ризиків, 3.2 Проведення симуляційного моделювання, 3.2.1 Моделювання для низького рівня прийнятного ризику, 3.2.2 Моделювання для підвищеного рівня прийнятного ризику, 3.3 Аналіз отриманих результатів, 3.4 Висновки до третього розділу, 4 Охорона праці та безпека в надзвичайних ситуаціях, 4.1 Охорона праці, 4.2 Фактори ризику та можливі порушення здоров'я користувачів комп'ютерної мережі, Висновки, Перелік використаних джерел.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів):
1 Тема, 2 Актуальність, об'єкт та предмет дослідженя, 3 Мета та завдання дослідження, 4 Кібербезпека в медичних інформаційних системах, 5 Медична інформаційна система для моделювання, 6 Результати симуляційного моделювання, 7 Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., к.т.н., доцент		
Безпека в надзвичайних ситуаціях	Теслюк В.М., проректор з адміністративно-господарської роботи та будівництва		

7. Дата видачі завдання 19.09.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	19.09 – 22.09	Виконано
2.	Підбір наукових джерел про стан кібербезпеки медичних інформаційних систем	22.09 – 30.09	Виконано
3.	Опрацювання наукових джерел в галузі дослідження	02.10 – 15.10	Виконано
4.	Виконання дослідження щодо оцінювання кіберризиків у медичних інформаційних системах	15.10 – 22.10	Виконано
5.	Оформлення розділу «Методологічні основи оцінки ризиків і моделювання загроз у кіберпросторі»	26.10 – 02.11	Виконано
6.	Оформлення розділу «Модель оцінювання ризиків кібербезпеки медичної системи»	03.11 – 15.11	Виконано
7.	Оформлення розділу «Симуляційні експерименти та аналіз результатів»	16.11 – 26.11	Виконано
8.	Виконання завдання до підрозділу «Охорона праці та безпека в надзвичайних ситуаціях»	28.11 – 01.12	Виконано
9.	Оформлення кваліфікаційної роботи	02.12 – 07.12	Виконано
10.	Нормоконтроль	08.12 – 12.12	Виконано
11.	Перевірка на плагіат	16.12 – 17.12	Виконано
12.	Попередній захист кваліфікаційної роботи	18.12 – 19.12	Виконано
13.	Захист кваліфікаційної роботи	24.12.2025	

Студент _____ Косарик Д. А.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Козак Р. О.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Модель оцінювання ризиків кібербезпеки медичної інформаційної системи із використанням методу Монте-Карло // ОР «Магістр» // Косарик Дарія Андріївна // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБмз-61 // Тернопіль, 2025 // С. 93, рис. – 13, табл. – 5, додат. – 5.

Ключові слова: Оцінка ризиків, Медична інформаційна система, Симуляція, Заходи захисту, Безпека пацієнта, Ймовірнісне моделювання.

У кваліфікаційній роботі розроблено модель оцінювання ризиків для медичної інформаційної системи на основі підходу Монте-Карло, що дозволяє обрати комбінацію заходів захисту для їх імплементації в реальній системі з урахуванням значення ризику та вартості впровадження. Проаналізовано сучасні підходи до управління ризиками та виявлено відсутність методів, що поєднують шкоду для пацієнта з фінансовими аспектами. Запропонована модель враховує потенційну шкоду для пацієнтів, а також оцінює цю шкоду, ефективність контролів та витрати ймовірнісно, що забезпечує більш наближене до реальності відображення впливу загроз.

На основі описаної медичної інформаційної системи здійснено симуляції з різними параметрами, проаналізовано результати, визначено оптимальний набір заходів з урахуванням балансу між рівнем прийнятного ризику та ресурсами організації.

ABSTRACT

Cybersecurity Risk Assessment Model for Medical Information Systems Using the Monte Carlo Method // Thesis of educational level "Master"// Dariia Kosaryk // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБмз-61 // Ternopil, 2025 // p. 93, figs. 13, tbls. 5, apps. 5.

Keywords: Risk assessment, Medical information system, Simulation, Controls, Patient safety, Probabilistic modeling.

In this qualification paper, a risk assessment model for a medical information system was developed based on the Monte Carlo approach, allowing the selection of a combination of protection measures for implementation in a real system, taking into account both the level of risk and the cost of implementation. Modern approaches to risk management were analyzed, revealing a lack of methods that integrate patient harm with financial considerations. The proposed model accounts for potential harm to patients and also probabilistically evaluates this harm, the effectiveness of controls, and associated costs, providing a more realistic representation of the impact of threats.

Based on the described medical information system, simulations were performed with different parameters, the results were analyzed, and the optimal set of measures was determined, considering the balance between the level of acceptable risk and the organization’s resources.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

BLE — Bluetooth Low Energy

CVE — Common Vulnerabilities and Exposures

CFR — Cybersecurity Framework

DDoS — Distributed Denial of Service

DFD — Data Flow Diagram

EMRAM — Electronic Medical Record Adoption Model

FAIR — Factor Analysis of Information Risk

FDA — Food and Drug Administration

GDPR — General Data Protection Regulation

HIMSS — Healthcare Information and Management Systems Society

HIPAA — Health Insurance Portability and Accountability Act

HTTPS — Hypertext Transfer Protocol Secure

IoT — Internet of Things

ISO — International Organization for Standardization

NCSC — National Cyber Security Centre

NIST — National Institute of Standards and Technology

ВСТУП

За останні десятиліття кібербезпека стала однією із найактуальніших проблем для організацій у різних галузях. Зростаюча складність інформаційних технологій у поєднанні із вдосконаленням атак призвела до різкого зростання як частоти, так і вартості інцидентів безпеки. Кібератаки вже не є рідкісними чи ізольованими поодинокими інцидентами, а це наразі високотехнологічні, організовані та тривалі кампанії, які здатні порушити роботу критично важливих сервісів, скомпрометувати дані, а також завдати катастрофічної фінансової чи репутаційної шкоди [1].

Кіберзлочинність стає не лише проблемою сфери інформаційних технологій, а й перетворюється на глобальну економічну кризу. Із зростанням кількості атак із використанням шкідливого програмного забезпечення, кібервійн з боку держав та шахрайства, загальні світові втрати від кіберзлочинності, за прогнозами, досягнуть 1,2 трильйона доларів на рік до кінця 2025 року [2].

Середня вартість витоку даних для організацій у 2024 році різко зросла до 4,88 мільйони доларів США, що майже на 10% більше, ніж у попередньому році. Серед галузей із найбільшими ризиками найгірша ситуація у сфері охорони здоров’я. Середня вартість одного інциденту перевищує 10 мільйонів доларів США, що є найвищим показником серед усіх галузей.

Особливо небезпечними є кібератаки на медичні інформаційні системи, адже вони впливають не лише на конфіденційність даних, а й безпосередньо на безпеку пацієнтів. Медичні пристрої можуть бути використані зловмисно для заподіяння фізичної шкоди пацієнтам через зміну терапевтичних показників, введення замалої чи завеликої дози ліків, або навіть через використання потужного іонізуючого випромінювання, сильних магнітів, гамма-випромінювання тощо. До прикладу, інцидент з Therac-25, що був медичним пристроєм для променевої терапії раку, розробленим компанією AECL. Цей апарат пов’язують із низкою інцидентів передозування радіацією. Програмне

забезпечення пристрою містило критичні вразливості, пов’язані з помилковою реалізацією механізмів безпеки, які були виконані не на апаратному, а на програмному рівні. Через ці вразливості в певних умовах виникала ситуація гонки процесів, унаслідок чого пацієнти отримували надмірну дозу опромінення, що іноді сягало у сто разів більшу за норму. Внаслідок інцидентів постраждали щонайменше шість пацієнтів, які зазнали тяжких опіків від радіації, паралічу різних частин тіла (зокрема рук, ніг і голосових зв’язок), а також нейрогенних уражень кишечника й сечового міхура, дезорієнтації, коми та навіть смерті [3].

Існує проблема, що багато керівників інформаційної безпеки (CISO) у медичних організаціях і досі зосереджують свої зусилля на захисті інформації про пацієнтів, застосовуючи традиційні методи оцінювання ризиків. Проте такі підходи не враховують один із найважливіших аспектів, а саме вплив кібератак на безпеку самих пацієнтів.

Водночас, навіть усвідомлюючи зростаючу загрозу, більшість організацій стикаються з проблемою високої вартості впровадження комплексних заходів безпеки. Забезпечення повного спектра контролів часто є економічно невиправданим і потребує значних ресурсів, особливо для медичних установ, де фінансування обмежене, а критичність систем надзвичайно висока. Отже, виникає потреба у методах, які дозволяють визначити оптимальний баланс між рівнем безпеки, прийнятним ризиком і витратами на реалізацію заходів контролю.

Існують методи моделювання загроз та оцінки ризиків, які допомагають організаціям ідентифікувати та класифікувати загрози для цифрових активів. Такий підхід зосереджений на виявленні загроз та створенні відповідних заходів захисту. Проте не кожну загрозу можна усунути, і варто розглядати питання оптимізації та доповнювати такі традиційні методи кількісним підходом, що дозволяє досягти балансу між прийнятним рівнем ризику (так званим ризик-апетитом) та витратами організації на впровадження заходів безпеки.

Актуальність теми. Зростання кількості кібератак у сфері охорони здоров’я привертає все більшу увагу до проблеми кібербезпеки медичних

інформаційних систем, оскільки такі інциденти можуть призводити не лише до витоку конфіденційних даних, але й безпосередньо загрожувати життю та здоров'ю пацієнтів. Водночас впровадження повного спектра сучасних заходів кіберзахисту в медичних установах часто є надзвичайно дорогим і потребує значних ресурсів. Тому актуальною проблемою є досягнення прийнятного рівня ризику кібербезпеки у медичних інформаційних системах за умов оптимізації витрат на реалізацію заходів захисту, що дозволить забезпечити баланс між безпекою та економічною доцільністю.

Мета і задачі дослідження. Метою роботи є розробка моделі оцінювання ризиків кібербезпеки медичної інформаційної системи на основі симуляції Монте-Карло, що дає змогу проаналізувати різні комбінації заходів захисту з урахуванням їх вартості впровадження та ефективності, а також визначити оптимальний варіант множини заходів безпеки для організації.

Завданнями дослідження є:

1. Аналіз сучасного стану кібербезпеки медичних інформаційних систем.
2. Дослідження існуючих методів управління ризиками.
3. Визначення та опис медичної інформаційної системи як об'єкту для моделювання, опис її загроз та можливих заходів захисту.
4. Розробка симуляційної моделі оцінювання ризиків кібербезпеки на основі методу Монте-Карло з урахуванням специфіки медичної інформаційної системи.
5. Реалізація запропонованої моделі, проведення симуляційних експериментів та аналіз отриманих результатів.
6. Визначення оптимального набору контролів кібербезпеки, що забезпечує баланс між рівнем ризиків та витратами на реалізацію заходів захисту.

Об'єкт дослідження. Процес оцінювання ризиків кібербезпеки медичної інформаційної системи

Предмет дослідження. Симуляційна модель оцінювання ризиків кібербезпеки медичної інформаційної системи, побудована на основі методу Монте-Карло.

Наукова новизна одержаних результатів кваліфікаційної роботи. У роботі запропоновано комплексний підхід до оцінювання ризиків кібербезпеки медичної інформаційної системи, який поєднує моделювання загроз із використанням методики STRIDE та оцінку потенційної шкоди пацієнтам у разі реалізації загроз. Для кількісної оцінки ризиків застосовано симуляційну модель на основі методу Монте-Карло, що дозволяє аналізувати різні комбінації заходів захисту та оптимізувати співвідношення «ризик-витрати».

Практичне значення одержаних результатів. Запропонована методика використовує симуляцію на основі методу Монте-Карло для оцінки різних комбінацій заходів захисту з урахуванням їх вартості та рівня ризику, в тому числі і на здоров’я пацієнта. Це дозволяє медичним організаціям обирати оптимальний набір контролів, який забезпечує баланс між ефективністю безпеки та витратами на впровадження, враховуючи можливі наслідки для пацієнтів.

Апробація результатів роботи: Основні результати проведених досліджень обговорювались на: XIII науково-технічній конференції «Інформаційні моделі, системи та технології».

Публікації: Основні результати кваліфікаційної роботи опубліковано у працях конференції (див. Додаток А).

РОЗДІЛ 1 МЕТОДОЛОГІЧНІ ОСНОВИ ОЦІНКИ РИЗИКІВ І МОДЕЛЮВАННЯ ЗАГРОЗ У КІБЕРПРОСТОРІ

Забезпечення кібербезпеки та стійкості функціонування стає дедалі актуальнішим у контексті постійного вдосконалення методів кібератак і зростаючого використання цифрових технологій на всіх етапах бізнес-процесів організацій. Кіберзагрози постійно еволюціонують, що дає змогу зловмисникам отримувати доступ до конфіденційних даних, порушувати критичні сервіси, обмежувати доступ до них, а також завдавати значної фінансової та репутаційної шкоди. У зв’язку з цим організаціям варто не лише реагувати на інциденти, але й проактивно здійснювати аналіз ризиків, що є необхідною умовою своєчасного виявлення, пріоритезації та визначення оптимальних заходів контролю. Тому аналіз ризиків та управління ними виступає одним із ключових елементів сучасної стратегії захисту інформаційних активів, що дозволяє організаціям підвищувати свою стійкість у цифровому середовищі.

Управління ризиками - це застосування системи або діяльності для аналізу та оцінки ризиків, що можуть виникати протягом усього життєвого циклу виробу, з метою зниження їх до прийнятного рівня. Такий підхід є необхідним для запобігання або мінімізації можливих пошкоджень і небезпек.

1.1 Важливість ризик-менеджменту в медичних інформаційних системах

З огляду на постійний технологічний прогрес у різних сферах, значення управління ризиками зростає. Хоча управління ризиками є важливим у багатьох галузях, у медицині воно має особливе значення, адже йдеться про безпеку пацієнтів, що є найвищим пріоритетом. Медичні пристрої безпосередньо впливають на здоров’я й життя людей, тому забезпечення їхньої безпечної експлуатації є критично важливим.

У сучасних умовах медичні інформаційні системи належать до найуразливіших кіберфізичних систем, оскільки поєднують критичні дані пацієнтів і підключені пристрої, що часто розробляються без належного врахування вимог інформаційної безпеки. Недооцінка ризиків на етапі проєктування посилює загрозу порушення конфіденційності та безпеки медичних сервісів [4].

Із розвитком технології Інтернету речей (IoT), стає неминучим повсюдне з'єднання різноманітних пристроїв, об'єктів і систем для підвищення ефективності керування та зручності в експлуатації. Особливо активно цей прогрес проявляється в таких галузях, як медицина. Охорона здоров'я поступово переходить від традиційної клініко-центричної моделі до безперервної моделі надання медичної допомоги з акцентом на профілактику та раннє втручання. Такі медичні пристрої раннього втручання зазнали значних вдосконалень і нині інтегруються з інформаційними та комунікаційними технологіями.

Проте, у зв'язку з поєднанням різних технологій, постійно зростає як внутрішня, так і зовнішня загроза безпеці для таких девайсів, що може призвести до фізичного пошкодження, вплив на приватність пацієнтів чи фінансових втрат. До прикладу, дослідження показують, що починаючи із 2013 року спостерігається значне збільшення кількості вразливостей у декілька разів (див. рисунок 1.1).

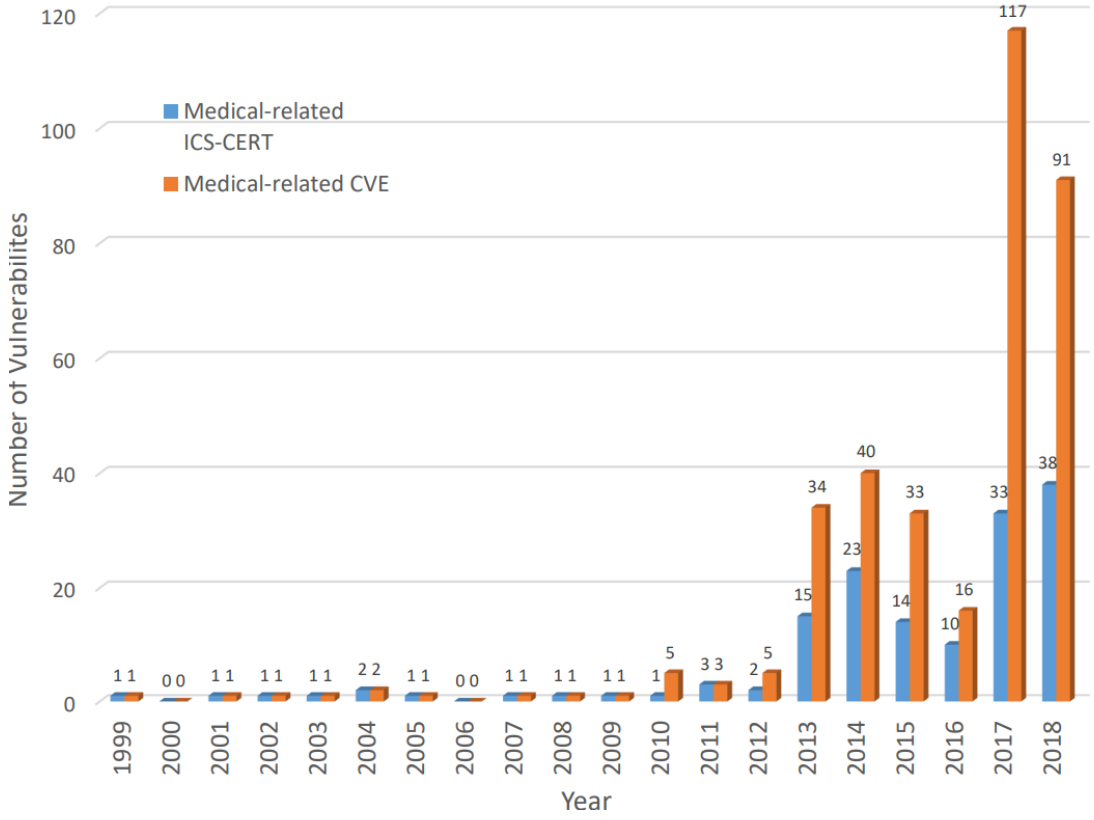

Рисунок 1.1 – Загальна кількість вразливостей для медичних девайсів (1999-2018) [5]

Було визначено близько 119 унікальних типів вразливостей, знайдених у базі CVE (Common Vulnerabilities and Exposures), наведених у таблиці 1.1.

Таблиця 1.1 – Найбільш поширені вразливості у медичних девайсах (1999-2018) [5].

Тип вразливості	Частота	Відносна частота
Неправильне керування обліковими даними та автентифікацією	36	22%
Неправильний контроль доступу, управління привілеями та авторизація	30	19%
Переповнення стеку та буфера	29	18%
Перехід по шляху (Path traversal)	14	9%
Неправильна перевірка введених даних	13	8%

Продовження таблиці 1.1

Витік інформації	12	7%
CSRF (підробка міжсайтових запитів)	9	6%
XSS (міжсайтовий скриптинг)	8	6%
Неконтрольоване споживання ресурсів	5	5%
Відсутність шифрування конфіденційних даних	5	5%

Для даних вразливостей було ідентифіковано 18 (12,8%) вразливостей, що містять публічно відомий експлойт, потенційно дозволяючи зловмисникам спрямовувати атаки на безпеку та приватність пацієнтів. Ці експлойти існують для різних груп медичних девайсів, таких як системи візуалізації, технології комунікації у лікарнях чи клініках, інсулінові помпи, програмне забезпечення для обробки чи керування медичними даними, комунікаційні пристрої [5].

Сучасні кіберфізичні медичні суттєво відрізняються від традиційних IT-рішень тим, що мають безпосередній фізичний інтерфейс, а тому кіберінциденти можуть призводити до реальних небезпечних наслідків для пацієнтів. Дослідження підкреслюють, що стандартні механізми захисту мають доповнюватися підходами, які враховують специфіку фізичного середовища та можливість унікальних атак на датчики й контролери [6].

Розглядаючи загрози, що існують у медичних системах, варто класифікувати їх за типом їхнього джерела, а саме: комунікації, програмне забепечення, платформа чи фізичний продукт, а також користувачі (див. рисунок 1.2). Поділ також відбувається на загрози конфіденційності, цілісності та доступності.

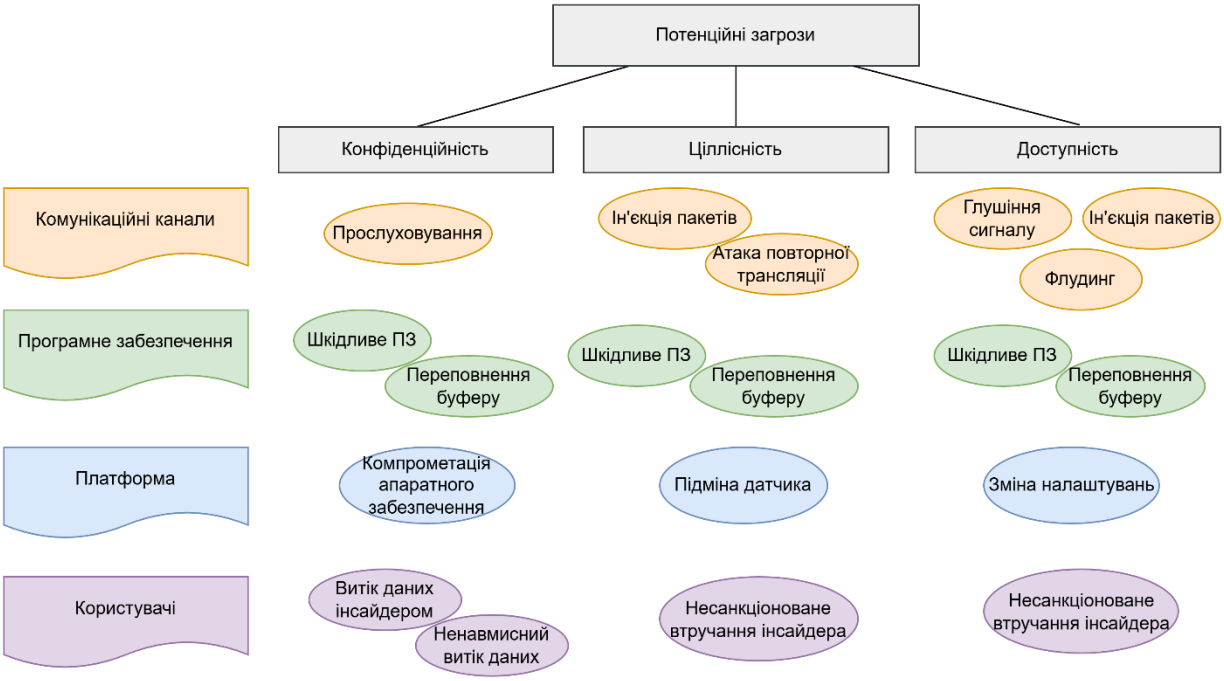

Рисунок 1.2 – Потенційні загрози в кіберфізичних медичних системах

Зазвичай у медичних системах використовується бездротова передача даних короткого діапазону. Конфіденційність може бути скомпрометована шляхом прослуховування та перехоплення даних, що не мають належного шифрування. Зловмисник може використати вразливість у програмному забезпеченні, наприклад вразливість переповнення буферу, щоб викрасти конфіденційну інформацію. Також зловмисник може отримати фізичний доступ до медичних девайсів, що дозволить йому отримати дані. І зрештою, витік даних може статися через ненавмисні дії користувачів.

Цілісність медичних систем порушується шляхом зміни існуючої або фабрикації нової інформації. Атаки, спрямовані на порушення цілісності, можуть включати використання фальшивих пакетів чи команд, а також повторну передачу застарілих даних. Також поширеним методом є експлойти програмного забезпечення, такі як переписування значень чи критично важливих змінних управління шляхом атак з пошкодженням пам’яті. Іншим вразливим місцем вважається підробка фізичного девайсу.

Атаки на відмову в обслуговуванні (DDoS/DoS) є основними загрозами щодо доступності. Сюди можна додати перенавантаження трафіку, що може

спричинити порушення комунікацій шляхом створення перешкод або колізій при передачі даних, а також переповнення буферної пам’яті мережевих карт чи розсилання підроблених мережевих пакетів.

Наслідки реалізації таких загроз можуть бути критичними. Для зменшення цих ризиків заклади охорони здоров’я повинні тісно співпрацювати з виробниками пристроїв, забезпечуючи вбудовані заходи кібербезпеки на етапі проектування та експлуатації. Важливими є постійний моніторинг, своєчасне оновлення програмного забезпечення та чітка сегментація мереж медичних пристроїв від критичних систем. При цьому слід пам’ятати, що не лише зовнішні загрози становлять ризик. Внутрішні фактори, такі як помилки або необережність співробітників, а також навмисні дії незадоволених працівників, також можуть призвести до витоків даних, збоїв у роботі системи та порушення безпеки пацієнтів.

1.2 Підходи до управління ризиками

Різні організації обирають різні підходи до організації процесу управління ризиками, залежно від ресурсів, цілей та специфіки діяльності. Підхід до управління ризиками, якого дотримуються багато організацій, еволюціонує від моделі, заснованої на зрілості можливостей, до підходу, орієнтованого на ризики.

1.2.1 Підхід, заснований до досягненні рівня зрілості

Навіть сьогодні підходи до управління ризиками, засновані на досягненні певного рівня зрілості, досі використовується та залишаються загальноприйнятою практикою. Такі підходи націлені на досягнення певного рівня зрілості шляхом розбудови функціональних можливостей. Наприклад, для досягнення бажаного рівня організація може створити центр операцій з кібербезпеки, щоб підвищити рівень зрілості в оцінюванні, моніторингу та

реагуванні на потенційні загрози для інформаційних систем чи додатків. Або ж впровадити багатофакторну автентифікацію у всій IT-інфраструктурі, щоб зміцнити контроль доступу.

Однією з найвідоміших моделей такого типу є Cybersecurity Framework (CSF), розроблена Національним інститутом стандартів і технологій США (NIST). Вона базується на п’яти основних функціях: ідентифікування, захист, виявлення загроз, реагування та відновлення. Фреймворк включає рівні реалізації від «часткової» до «адаптивної» зрілості, які охоплюють аспекти управління, ризиків і технічної реалізації.

Аналогічно, стандарти ISO/IEC 27001 та ISO/IEC 27002 є основою для побудови систем управління інформаційною безпекою. ISO/IEC 27001 описує, як систематично керувати конфіденційною інформацією, а ISO/IEC 27002 пропонує набір контрольних заходів згідно з найкращими галузевими практиками. Обидва стандарти акцентують увагу на постійному вдосконаленні, документації та відповідальності в управлінні кібербезпекою.

У сфері охорони здоров’я підхід зрілості розвивається через моделі HIMSS (Healthcare Information and Management Systems Society), зокрема EMRAM (Electronic Medical Record Adoption Model). Хоча ці моделі зосереджуються переважно на рівні цифрової готовності лікарень і IT-інфраструктури, вони опосередковано враховують і кібербезпеку, оцінюючи, наскільки безпечно інтегровані медичні IT-системи.

Такі підходи можуть бути корисними на початковому етапі розробки системи інформаційної безпеки, проте використання виключно підходу на основі зрілості є недостатнім для організацій, що вже мають розроблені засоби захисту на певному рівні. Ще одним недоліком є те, що з розвитком таких програм управління ризику в організаціях відбувається неконтрольоване зростання кількості засобів контролю. Наприклад, у сфері моніторингу подібна програма часто переростає у прагнення моніторити та контролювати «все». Зрештою, кількість застосунків, які підлягають моніторингу в межах підприємства, перевищує реальні аналітичні спроможності команди. Встановлення засобів

моніторингу починає гальмувати роботу команд, що займаються розробкою програмного забезпечення. Насправді ж деякі застосунки становлять значно більший ризик з точки зору вразливостей, аніж інші. Щоб справді зосередитися на зниженні ризиків, організації мають навчитися переходити від загального моніторингу «всього» до цільового моніторингу саме тих застосунків, які мають найвищий потенціал для створення критичних загроз.

Іншою проблемою, пов'язаною із цим підходом, є неефективне використання фінансових ресурсів. Кількість засобів контролю організації зростає з кожним роком, оскільки планування кібербезпеки постійно потребує нових витрат на впровадження додаткових механізмів. Модель, заснована на зрілості, не вимагає від організації збору достатньо інформації для того, щоб дійти висновку про необхідність переорієнтування фінансування для певних програм. В результаті очікується витрачання коштів на всі напрямки, навіть якщо одні з них матимуть значно більший вплив на зниження ризиків, ніж інші.

Якщо метою є зниження ризиків для підприємства, то найбільше ресурсів мають спрямовуватись на ті заходи, які демонструють найкращу ефективність у досягненні цього результату. Усі функції певною мірою сприяють зниженню ризику, однак більшість компаній не здатні точно визначити, наскільки саме, і яким чином конкретний засіб захисту працює.

Ще один недолік підходу, що ґрунтується на досягненні рівнів зрілості, полягає в тому, що він часто створює справжній «застій» у впровадженні заходів безпеки. Обмежене коло фахівців, які дійсно можуть реалізувати технічні рішення, швидко виявляється перевантаженим завданнями. Їхню увагу постійно розпорошують між десятками ініціатив, у результаті чого жоден проєкт не доводиться до кінця.

У сучасному світі, де всі системи тісно пов'язані між собою, такого підходу вже недостатньо. Щоб реально зменшувати ризики, потрібен більш стратегічний і гнучкий підхід, тобто такий, що базується не просто на виконанні плану, а на розумінні, які саме ризики є найважливішими, і що дійсно варто робити в першу чергу.

1.2.2 Ризик-орієнтований підхід

Наступним логічним кроком після усвідомлення обмежень зрілісного підходу є перехід до ризик-орієнтованої моделі, яку можна розглядати як наступний етап еволюції в кібербезпековій стратегії організації. Цю еволюцію умовно можна розділити на кілька ключових етапів, що зображені на рис. 1.3.

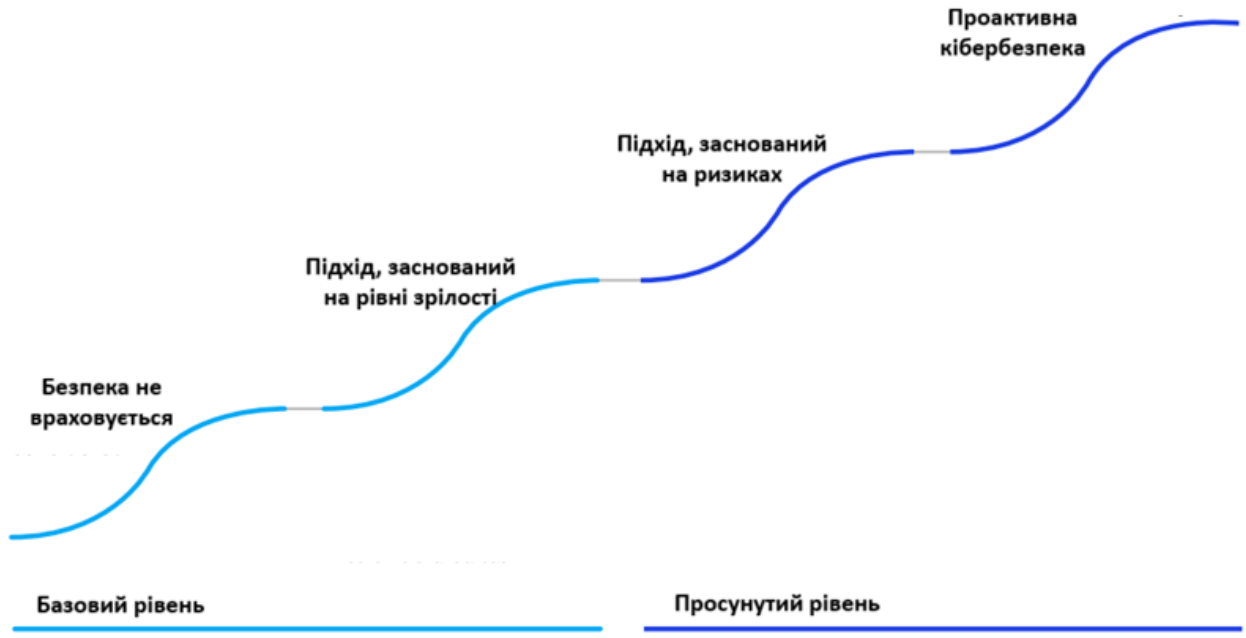

Рисунок 1.3 – Етапи розвитку кібербезпеки організації [7]

Ці етапи включають в себе:

1. Кібербпезпека відсутня, або розглядається як другорядне питання.
2. Підхід, заснований на зрілості, вибудовує базову інфраструктуру безпеки.
3. Ризик-орієнтований підхід, спрямовний на зменшення ризиків підприємства.
4. Проактивна кібербезпека та комплексна стійкість.

Перший етап означає, що немає відповідальних осіб, ані базових засобів захисту даних чи управління доступом. Керівництво часто не усвідомлює потенційних загроз і не бачить у цьому пріоритету. Відсутні навіть базові

механізми контролю, не проводиться оцінка поточних загроз або рівня захищеності. Типові дії на цьому етапі включають поверхневу оцінку зрілості (наприклад, у сфері захисту даних чи управління доступом) або оцінку загального рівня кіберобізнаності в межах організації.

Головна мета другого етапу полягає у «закритті» очевидних прогалин та підвищенні рівня підготовленості. Це може включати створення центру операцій з безпеки, розробку планів реагування на інциденти, впровадження багатофакторної автентифікації, а також призначення відповідальних осіб за безпеку. Хоча ці дії покращують загальну захищеність, вони часто реалізуються без урахування того, наскільки кожна ініціатива реально впливає на зниження ризиків.

На третьому етапі організація починає ідентифікувати, пріоритезувати й оцінювати ризики, а також впроваджувати лише ті засоби контролю, які дійсно впливають на їх зниження. Визначаються конкретні порогові значення для основних індикаторів ризику та ключових показників ефективності. Участь у формуванні кіберстратегії на цьому етапі беруть не лише спеціалізовані відділи, а вся організація загалом. Типові дії включають кількісне оцінювання ризиків, звітування про їх реальне зменшення, а не просто про впроваджені функції.

Останній етап трансформує свої процеси, впроваджуючи новітні технології для передбачення, виявлення та автоматизованого реагування на кіберінциденти. Безпека на цьому рівні інтегрується в усі бізнес-процеси, тобто від розробки продукту до його експлуатації, реалізується принцип «безпека, вбудована у дизайн». Компанія активно взаємодіє з клієнтами, партнерами, регуляторами, включає кібер-ризики у загальну стратегію управління стійкістю підприємства. До типових практик, що здійснюються цим підходом можна назвати впровадження аналітики, штучного інтелекту й машинного навчання для проактивного виявлення загроз, а також створення багаторівневих систем швидкого реагування.

Таким чином, підхід, оснований на зрілості можливостей, відіграє важливу роль як перехідний етап у формуванні системи кібербезпеки, однак на певному

рівні розвитку організація неминуче стикається з його обмеженнями. Подальше зростання ефективності вимагає не так розширення контрольних механізмів, як переосмислення самої логіки управління, тобто з акцентом на критичність ризиків, пріоритетність ресурсів і реальний вплив на стійкість бізнесу. Саме в цьому контексті на перший план виходить ризик-орієнтований підхід, який все частіше розглядається як метод побудови дійсно ефективної та адаптивної системи кіберзахисту.

Ризик-орієнтований підхід водночас виконує дві важливі задачі. По-перше, він визначає зменшення ризику як головну мету. Це дає змогу організації правильно розставляти пріоритети для інвестицій, зокрема у вирішення практичних питань впровадження, орієнтуючись на те, наскільки ефективно кіберпрограма знижує ризики. По-друге, цей підхід трансформує цілі керівництва щодо зниження ризиків у чіткі, практичні плани впровадження, які мають зрозуміле відображення від директорів до виконавців. Завдяки ризик-орієнтованому підходу компанія припиняє впроваджувати контролі всюди. Натомість увага зосереджується на впровадженні саме тих засобів контролю, які здатні захистити від найсерйозніших вразливостей і найнебезпечніших загроз, що загрожують найбільш критичним для бізнесу сферам.

ISO/IEC 27005, частина ширшої серії ISO 27000, пропонує структуровану методологію для оцінки кіберризиків. У фокусі знаходяться ідентифікація активів, оцінка ризиків, вибір та реалізація заходів управління ризиками. Цей стандарт широко застосовується в регульованих галузях і допомагає узгоджувати кіберзахист із вимогами нормативної відповідності.

Іншим прикладом є модель FAIR (Factor Analysis of Information Risk), яка впроваджує кількісний підхід до управління ризиками. Вона дозволяє розкласти ризик на вимірювані компоненти, такі як частота втрати та потенційні збитки, і оцінювати ризики у фінансовому вимірі. Це значно покращує розуміння ризиків на рівні керівництва та дозволяє ухвалювати обґрунтовані рішення щодо інвестицій у безпеку.

У сфері охорони здоров’я й медичних пристроїв регулятори, такі як FDA (США) та ENISA (ЄС), також впроваджують власні ризик-орієнтовані стандарти. Наприклад, у 2014 році FDA зобов’язала виробників медичних пристроїв включати моделювання загроз і оцінку ризиків у передреєстраційні документи. ENISA у звітах (наприклад, Threat Landscape for eHealth, 2021) акцентує на пріоритезації загроз і контекстному підборі заходів контролю для середовищ медичного IoT.

1.2.3 Порівняння підходів до управління ризиками

На рисунку 1.4 наведено порівняння двох підходів до кібербезпеки: підходу, заснованого на зрілості, та ризик-орієнтованого підходу.

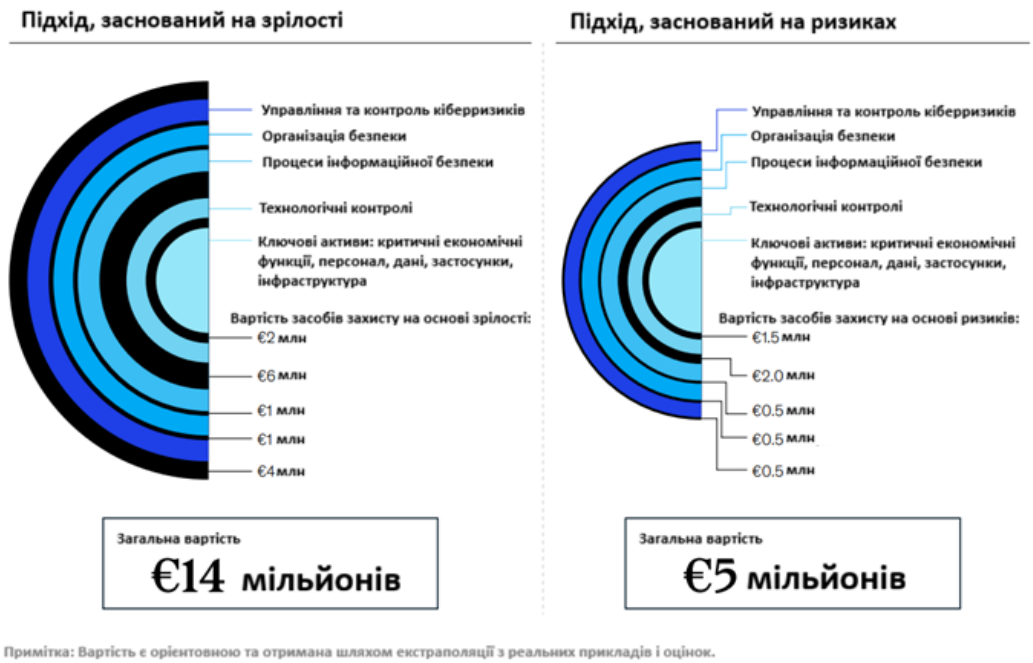

Рисунок 1.4 – Порівняння підходів моделі зрілості та ризик-орієнтованої моделі[7]

Зліва показано, що підхід зрілості передбачає максимальний рівень захисту для всіх компонентів системи: від управління ризиками та організації безпеки до технологічних контролів і найважливіших активів. Це означає, що кошти

розподіляються широко, охоплюючи всі елементи, часто незалежно від їх реального рівня ризику. В результаті загальні витрати на кіберзахист за цим підходом можуть бути значно вищими.

Справа представлений ризик-орієнтований підхід, який оптимізує захисні шари, концентруючись на найбільш критичних вразливостях. Тут увага і ресурси спрямовані на ті елементи, які несуть найбільшу загрозу для бізнесу. Такий підхід дозволяє досягти ефективного захисту з меншими загальними витратами, підвищуючи при цьому продуктивність і цінність витрачених коштів.

З прикладу видно, що загальні витрати за зрілісним підходом становлять 14 мільйонів євро, тоді як за ризик-орієнтованим лише 5 мільйонів євро. Це ілюструє, наскільки економічно вигіднішим і стратегічно виправданим є фокус на ключових ризиках, а не на максимальному контролі над усім.

Таким чином, ця схема наочно демонструє, чому сучасні організації дедалі частіше обирають ризик-орієнтований підхід як основу для побудови ефективної, адаптивної і економічно раціональної системи кібербезпеки.

Отже, ризик-орієнтований підхід до кібербезпеки є динамічним інструментом, який підтримує стратегічне прийняття рішень. Він зосереджений на бізнес-цінності, ґрунтується на спільній мові між усіма зацікавленими сторонами та напряму пов’язує корпоративні ризики із заходами контролю. Такий підхід дозволяє ефективно трансформувати управлінські рішення щодо зниження ризиків у конкретні дії з впровадження контролів.

Його ключова перевага - це здатність оптимізувати зменшення ризику за будь-якого рівня інвестицій. Крім того, підхід залишається гнучким, оскільки може адаптуватися до змін у стратегії допустимого ризику в міру розвитку організації.

Попри те, що підходи, засновані на зрілості, та ризик-орієнтовані моделі є важливими основами для управління кібербезпекою, вони здебільшого залишаються стратегічними або операційними інструментами, зосередженими на процесах, управлінні або виборі заходів контролю. Проте жоден із цих

підходів не забезпечує системного способу моделювання того, як загрози насправді виникають і взаємодіють із компонентами системи з часом.

У складних і динамічних середовищах, як наприклад, у системах із підключеними медичними IoT-пристроями, цього вже недостатньо. Важливо вийти за межі статичних каталогів контролів і суб'єктивних експертних оцінок. Щоб ухвалювати дійсно ефективні рішення, організація має розуміти, як конкретні вектори атак впливають на критичні активи системи, які наслідки це може спричинити, і як різні стратегії захисту змінюють загальний рівень ризику.

У цьому контексті стає необхідним досліджувати сучасні підходи та стратегії кібербезпеки, що застосовуються у медичних інформаційних системах. Вони дозволяють систематично оцінювати ризики, впроваджувати ефективні заходи захисту та зменшувати ймовірність негативного впливу кібератак на дані пацієнтів і критичні медичні сервіси. Аналіз таких підходів допомагає зрозуміти, які методи та технології є найбільш дієвими в умовах постійно змінюваного кіберсередовища та обмежених ресурсів організацій.

1.3 Сучасні підходи та стратегії кібербезпеки у медичних інформаційних системах

У боротьбі з постійно еволюціонуючими кіберзагрозами медичні організації застосовують комплексні стратегії для посилення власної безпеки. Регуляторні органи, такі як HIPAA (Health Insurance Portability and Accountability Act) та GDPR (General Data Protection Regulation), встановлюють стандарти безпеки для захисту інформації пацієнтів. Медичні організації зобов'язані дотримуватися цих нормативних вимог, впроваджуючи протоколи безпеки даних, повідомлення про інциденти та заходи з охорони приватності. Виконання нормативних вимог не лише забезпечує правову відповідність, але й сприяє формуванню культури обізнаності з кібербезпеки [8].

Аналіз ризиків є основою ефективної кібербезпеки. Медичні установи систематично ідентифікують вразливості та потенційні загрози у своїй

технологічній інфраструктурі. Отримані результати дозволяють пріоритизувати ресурси, впроваджувати потрібні заходи безпеки та формувати надійні стратегії управління ризиками. Регулярні оцінки забезпечують адаптивність до нових загроз.

Шифрування є потужним механізмом захисту від несанкціонованого доступу до даних пацієнтів. Використання наскрізного шифрування гарантує, що інформація залишається недоступною для зловмисників навіть у разі порушення безпеки. Методи токенізації замінюють чутливі дані на замасковані значення, що робить їх непридатними для кіберзлочинців. Послідовне застосування різних протоколів шифрування створює ефективний бар'єр проти компрометації даних.

Людський фактор залишається суттєвою вразливістю у сфері кібербезпеки. Медичні організації усвідомлюють необхідність навчання персоналу найкращим практикам кібербезпеки. Комплексні програми підготовки та підвищення обізнаності допомагають співробітникам розпізнавати фішингові атаки, уникати соціальної інженерії та безпечно працювати в цифровому середовищі. Формування обізнаного персоналу посилює захист від потенційних порушень безпеки.

Враховуючи неминучість кіберінцидентів, медичні установи посилюють свої стратегії реагування та відновлення. Швидке виявлення, локалізація та мінімізація наслідків атак є критично важливими для зменшення шкоди. Організації розробляють заздалегідь сплановані плани реагування, визначаючи ролі, канали комунікації та кроки для усунення порушень і відновлення роботи. Аналіз після інцидентів дозволяє вдосконалювати протоколи та підвищувати ефективність майбутніх реакцій.

Медичні організації також усвідомлюють цінність колективного захисту від кіберзагроз. Спільні платформи сприяють обміну інформацією про загрози, що дозволяє раніше ідентифікувати нові ризики. Обмін даними про методи атак, тактики та вразливості допомагають галузі передбачати загрози та розробляти проактивні заходи захисту.

У сучасному динамічному середовищі кібербезпеки необхідний комплексний підхід. Медичні організації мають інтегрувати нормативну відповідність, управління ризиками, шифрування, навчання персоналу та ефективне реагування на інциденти, формуючи таким чином надійний захисний механізм. Ці стратегії створюють взаємопов'язану систему захисту, що охороняє дані пацієнтів і забезпечує безперервність якісного надання медичних послуг.

1.4 Наслідки кіберзагроз для безпеки пацієнтів

Складний взаємозв'язок між охороною здоров'я та технологіями відкрив нову еру надання медичної допомоги, проте разом із цим виникла низка нових кіберзагроз. Кіберзагрози безпосередньо впливають на два критично важливі аспекти: конфіденційність даних та порушення приватності пацієнтів. Особиста медична інформація, яка раніше вважалася захищеною в межах установ охорони здоров'я, сьогодні ризикує бути отриманою несанкціонованими особами. Такий компроміс шкодить довірі між пацієнтами та медичними працівниками та може призвести до викрадення особистих даних, фінансового шахрайства й психологічної травми.

Наслідки виходять за межі окремих осіб і зачіпають самі медичні організації, які можуть зазнати штрафів або судових позовів за неналежний захист даних пацієнтів. Для захисту від таких загроз установи охорони здоров'я мають пріоритетно впроваджувати надійне шифрування, контролі доступу та протоколи моніторингу даних для забезпечення конфіденційності пацієнтів.

Кіберзлочинці часто порушують роботу медичних установ, виводячи з ладу критичні системи, медичні пристрої та комунікаційні мережі. Такі порушення можуть паралізувати робочі процеси лікарень, затримувати надання медичної допомоги, порушувати роботу служб екстреної допомоги та підривати клінічне прийняття рішень, ставлячи під загрозу безпеку пацієнтів. У зв'язку з цим організації впроваджують превентивні заходи, зокрема резервування систем,

сегментацію мереж і плани відновлення після надзвичайних ситуацій, щоб захистити критично важливі послуги та безпеку пацієнтів.

Через тісну інтеграцію медичних технологій будь-яке порушення може мати далекосяжні наслідки для лікування пацієнтів. Кіберзлочини можуть змінювати плани лікування, редагувати електронні рецепти або модифікувати діагностичні дані, що потенційно загрожує життю пацієнтів. Тому установи охорони здоров'я застосовують суворі контролі доступу, ведення аудиту та інвестують у захищені платформи комунікацій, щоб забезпечити безпечний процес лікування та захист медичної інформації.

Кіберзагрози також мають значні фінансові наслідки: витрати на відновлення систем та даних, юридичні послуги та потенційні штрафи можуть істотно впливати на обмежені ресурси установи. Постраждалі пацієнти можуть подавати позови про відшкодування шкоди через порушення безпеки або перебої в наданні послуг. У зв'язку з цим установи охорони здоров'я мають інвестувати в заходи кібербезпеки, орієнтовані на запобігання, раннє виявлення та швидку реакцію, щоб мінімізувати можливі наслідки інцидентів.

Кібербезпека у сфері охорони здоров'я постійно регулюється, що підкреслює необхідність дотримання норм і готовності організацій. Вони мають дотримуватися законів і регламентів, таких як HIPAA та Загальний регламент ЄС щодо захисту даних (GDPR), щоб захистити медичну інформацію та приватність пацієнтів. Недотримання цих вимог може призвести до значних штрафів і юридичної відповідальності. Судові позови пацієнтів, які зазнали шкоди через кіберінциденти, додатково демонструють правові ризики для організацій.

Таким чином, кіберзагрози безпеці пацієнтів мають широкий вплив на всі аспекти надання медичної допомоги, тобто від компрометації даних і порушення роботи систем до безпосереднього ризику для пацієнтів і фінансових наслідків для установ. У сучасному технологічно керованому середовищі кібербезпека повинна розглядатися не лише як технічне завдання, а й як обов'язкові заходи для захисту пацієнтів.

1.5 Висновки до першого розділу

У даному розділі було здійснено огляд сучасного стану кібербезпеки та управління ризиками у медичних інформаційних системах. Проаналізовано підходи до управління ризиками, сучасні стратегії захисту даних, а також наслідки кіберзагроз для пацієнтів. Було показано, що кіберзагрози можуть не лише порушувати конфіденційність та цілісність даних, а й безпосередньо впливати на безпеку та життя пацієнтів, особливо у складних системах із підключеними медичними IoT-пристроями.

Виявлено, що у сучасних підходах до управління ризиками існує суттєвий пробіл: відсутні методи, які б інтегрували оцінку шкоди для пацієнта разом із фінансовими аспектами. Традиційні методи ризик-менеджменту не дозволяють організаціям ухвалювати обґрунтовані рішення щодо пріоритетності заходів захисту та оптимізації витрат на безпеку.

У результаті проведеного аналізу постає потреба подальшої роботи над методами оцінки ризиків, що б дозволило кількісно оцінити вплив загроз на критичні активи та безпеку пацієнтів, порівняти різні стратегії захисту та допомогти організаціям із прийняттям рішень щодо впровадження заходів захисту, базуючись на відношенні «ризик-витрати».

РОЗДІЛ 2 МОДЕЛЬ ОЦІНЮВАННЯ РИЗИКІВ КІБЕРБЕЗПЕКИ МЕДИЧНОЇ СИСТЕМИ

Метою моделювання є дослідження інтегрованої медичної інформаційної системи, призначеної для моніторингу стану пацієнта в реальному часі. Модель створена для прийняття рішень при розробці заходів захисту медичної системи, враховуючи прийнятний залишковий ризик та ціну на впровадження та підтримку контролів. Таким чином, це дозволяє розглянути можливі набори заходів захисту, що відповідають заданим параметрам (ризику та ціні). Модель забезпечує моделювання загроз з використанням підходу STRIDE, а також оцінку залишкового ризику загроз. Модель дозволяє оцінити вплив ефективності заходів зменшення ризиків, а також дозволяє пріоритезувати заходи захисту в системі зважаючи на вплив успішної реалізації загроз на здоров'я пацієнт.

Моделювання дотримується структурованого процесу, який об'єднує ідентифікацію загроз, кількісну оцінку ризиків та пошук компромісу між витратами на кіберзахист та ризиками. Це проілюстровано на рисунку 2.1, де представлено покроковий процес, що використовується для оцінки та вибору оптимальних стратегій мінімізації наслідків. На діаграмі також позначено вхідні та вихідні дані у вигляді умовних позначень, які дозволяють відстежити, яку саме інформацію використовує та генерує кожен етап. Ці позначення детально розшифровані на рисунку 2.2.

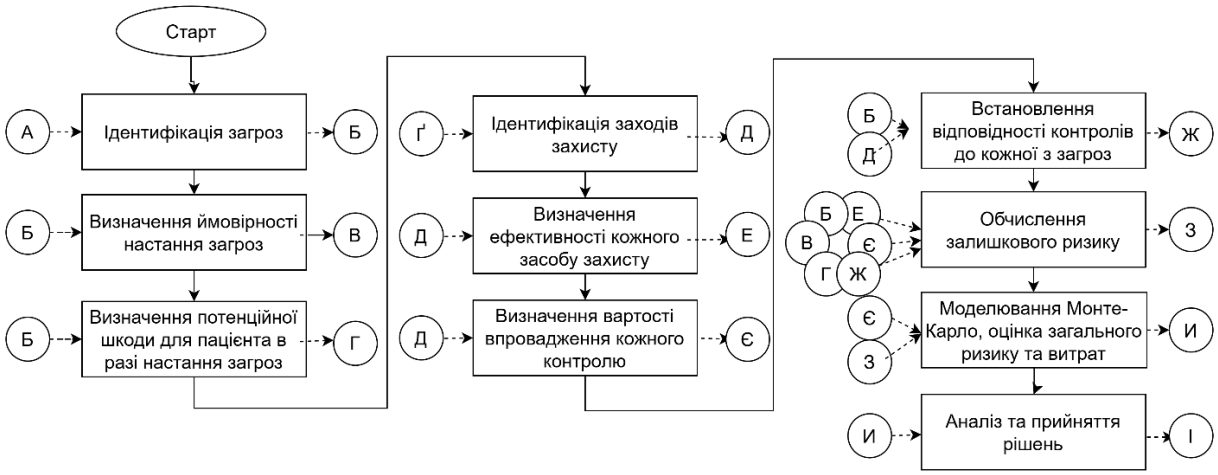

Рисунок 2.1 – Алгоритм моделювання ризиків

Умовні позначення вхідних та вихідних даних			
А	Архітектура системи, її активи	Е	Значення ефективності кожного контролю
Б	Список загроз	Є	Ціна впровадження кожного з контролів
В	Значення ймовірностей настання для кожної загрози	Ж	Відповідність між загрозами та контролями
Г	Значення шкоди пацієнту від кожної загрози	З	Значення залшкового ризику кожної загрози
Ґ	Каталог засобів контролю безпеки (NIST SP 800-53, ISO 27001), можливості системи	И	Загальний ризик, вартість для кожної підмножини контролів, що в межах прийнятного значеня ризикику
Д	Список заходів захисту (контролів)	І	Вибрана найкраща множина заходів захисту для даної системи

Рисунок 2.2 – Умовні позначення вхідних і вихідних даних моделі

Наведена діаграма слугує основою розробленої моделі, пов'язуючи аналіз загроз з плануванням заходів зменшення ризиків з урахуванням витрат.

2.1 Опис системи

Система, що розглядається, є багатокомпонентною цифровою платформою, що збирає, відображає і обробляє терапевтичні дані пацієнта, а також надає користувачу можливість слідкувати за своїм станом та контролювати його, відображаючи показники у мобільному додатку. Система, що розглядається, допомагає проводити терапію з використанням пристрою-актуатора, а також надає сповіщення про критичні рівні терапевтичних даних та здійснює нагадування щодо здійснення терапії.

Архітектура системи побудована на основі таких ключових компонентів та комунікацій між ними:

1. Сенсор для вимірювання показників терапії, що постійно вимірює стан пацієнта в реальному часі.
2. Пристрій-актуатор, що дозволяє пацієнту здійснювати терапію (автоматично, або за потребою самостійно)
3. Мобільний додаток, що отримує дані від сенсора через Bluetooth, показує пацієнту вимірювання і надсилає дані до бекенд-сервера.

4. Бекенд-сервер для обробки та зберігання історичних терапевтичних даних.

Діаграма потоків даних (Data Flow Diagram, DFD), яка відображає архітектуру, основні процеси та комунікації описаної системи, зображена на рисунку 2.3. Позначення елементів діаграми наведено на рисунку 2.4.

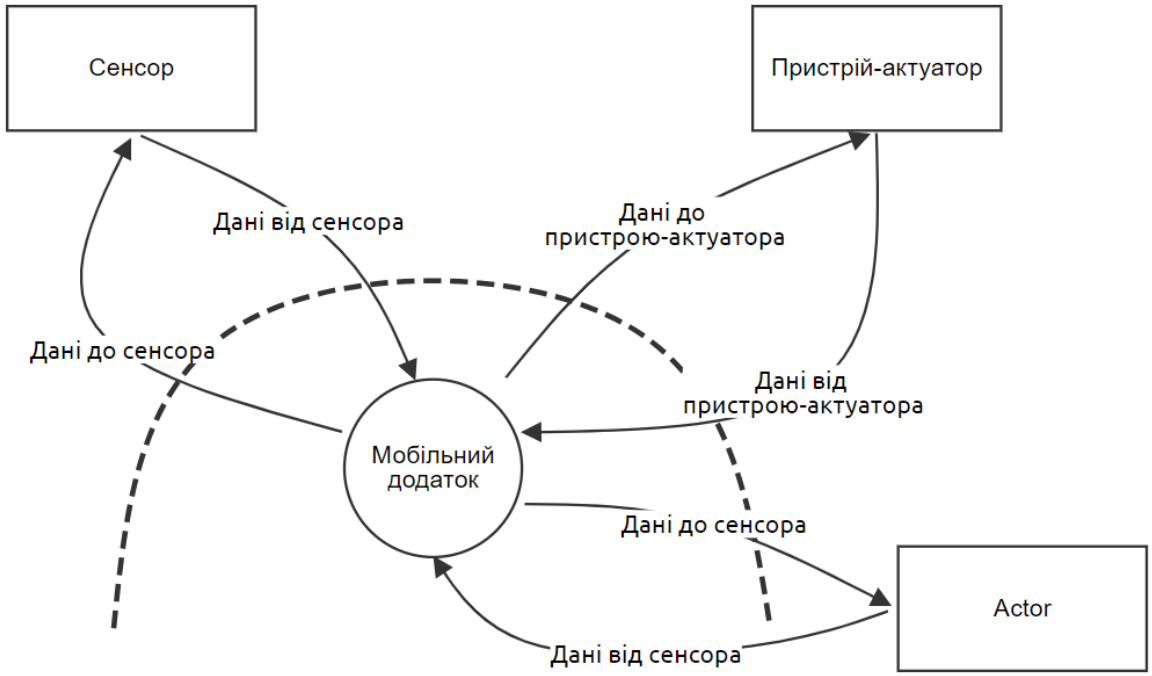

Рисунок 2.3 – Діаграма потоків даних медичної інформаційної системи

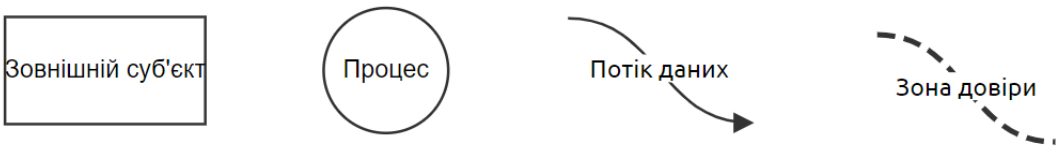

Рисунок 2.4 – Умовні позначення елементів діаграми потоків даних

Дизайн системи передбачає встановлення зон довіри системи. Це дозволяє визначити відповідальності в рамках системи, уточнити які дані передаються між рівнями та забезпечити безпечну роботу кожної частини системи. Зона довіри відділяє мобільний додаток від BLE-пристроїв та від сервера.

Для моделювання потенційних загроз та більш чіткого визначення заходів захисту розглядатимуться інтерфейси між компонентами системи, наведені у таблиці 2.1. Комунікація додатку з сенсором та пристроєм-актуатором здійснюється через BLE протокол, що призначений для бездротової передачі даних між пристроями з низьким енергоспоживанням та на коротких відстанях. HTTPS (TLS 1.2/1.3) забезпечує безпечну передачу даних між мобільним додатком і сервером.

Таблиця 2.1 – Інтерфейси медичної інформаційної системи

Інтерфейс	Призначення	Протокол
Мобільний додаток↔Сенсор	– Надсилання терапевтичних показників від сенсора – Надсилання контрольних команд до сенсора	BLE
Мобільний додаток↔Пристрій-актуатор	– Надсилання контрольних команд до пристрою-актуатора – Надсилання підтверджень до мобільного додатку про виконання команд	BLE
Мобільний додаток↔Сервер	– Надсилання терапевтичних історичних даних – Надсилання відповідей та фонових команд мобільному додатку	HTTPS

Комунікації на стороні хмари, APIs третіх сторін, прошивки BLE-девайсів, їх фізична безпека, а також поведінка користувачів знаходяться поза розглядом даної системи через брак засобів захисту та їх складність.

Модель приймає на вхід інформацію, як про характеристики загроз, так і про параметри засобів захисту. На вхід подається ймовірнісний розподіл для загроз, що представляє ймовірність появи загрози у заданій системі. Також кожен контроль (засіб протидії) має ймовірнісний розподіл для ефективності дії цього контролю. Ще одним параметром на вхід є ціна впровадження засобу захисту. Це дозволяє аналізувати залежність «ризик-втрати» під час симулювання.

Зрештою, на вхід моделі надається ризик-апетит, тобто максимально допустимий рівень ризику, або найвища допустима оцінка для системи.

2.2 Ідентифікація загроз і засобів контролю

2.2.1 Виявлення загроз у системі

Моделювання загроз у контексті медичної інформаційної системи дозволяє визначити необхідні вимоги безпеки, виявити потенційні вразливості та оцінити їхній вплив, що дає змогу обґрунтовано пріоритезувати заходи захисту [9].

Для визначення загроз використовувався фреймворк STRIDE. Вибір STRIDE мотивований кількома причинами: це системний підхід, який аналізує кіберзагрози для кожного компонента системи на основі його технічних знань, він є комплексним та аналізує такі властивості безпеки, як автентифікація, авторизація, конфіденційність, цілісність, невідмовність та доступність для кожного компонента системи, та він забезпечує чітке розуміння впливу вразливості компонента на всю систему та допомагає забезпечити безпеку системи на рівні компонента.

Метод STRIDE запропоновано компанією Microsoft і являє собою мнемоніку для шести різних типів загроз безпеці.

1. Spoofing - маскування легітимного користувача, процесу або системного елемента,
2. Tampering - модифікація/редагування легітимної інформації,
3. Repudiation - заперечення або відмова від певної дії, виконаної в системі,
4. Information disclosure - витік даних або несанкціонований доступ до конфіденційної інформації,
5. Denial of Service (DoS) переривання обслуговування для легітимних користувачів,

6. Elevation of privilege - отримання доступу з вищими привілеями до системного елемента користувачем з обмеженими повноваженнями.

Кожен тип елемента діаграми потоків даних вразливий лише до кількох або всіх загроз STRIDE, як показано в таблиці 2.2.

Таблиця 2.2. – Загрози STRIDE, застосовні до елементів DFD діаграми

Елемент діаграми потоків даних	S	T	R	I	D	E
Зовнішній суб'єкт	✓		✓			
Процес	✓	✓	✓	✓	✓	✓
Потік даних		✓		✓	✓	

Наступним кроком є ідентифікація загроз STRIDE для кожного системного компонента з діаграми потоків даних. Виходячи з кожного системного компонента та його функціональності, певні загрози STRIDE можуть бути не застосовні до нього. Рисунок 2.5 графічно представляє підхід STRIDE для аналізу загроз.

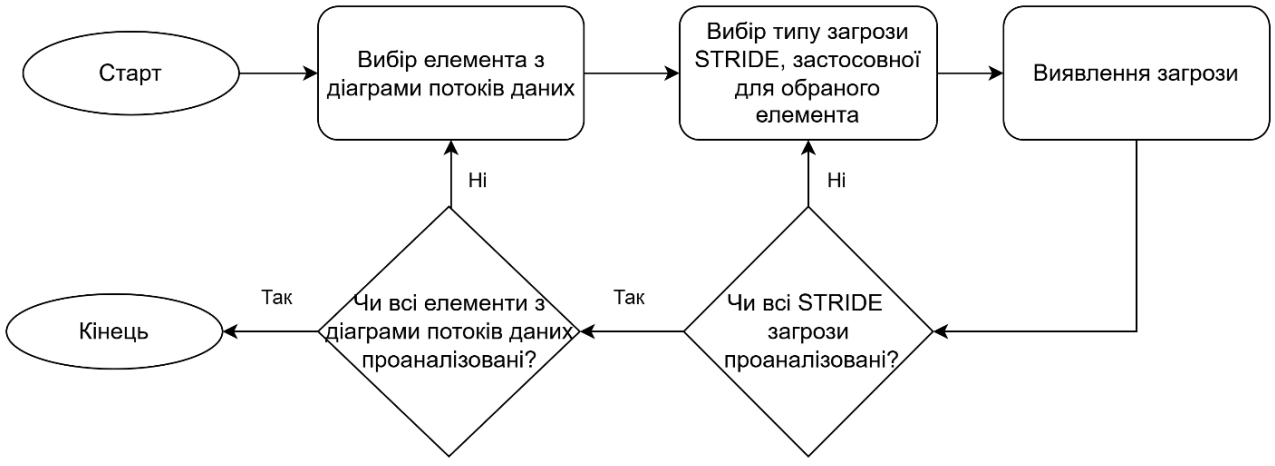

Рисунок 2.5 – Процес ідентифікації загроз методом STRIDE

При моделюванні була виявлена 31 загроза. Результати наведено у Додатку Б (стовпці «ІД» та «Опис»).

Кожна загроза має присвоєне значення ймовірності виникнення. Крім того, кожна загроза пов'язана зі значенням шкоди для пацієнта, що відображає потенційний вплив на користувачів. Це враховує одну з вимог для медичних систем FDA регуляторики, що зазначає потребу в оцінці тяжкості шкоди, завданої пацієнту.

2.2.2 Визначення заходів контролю та їх відповідність загрозам

Пом’якшувальні заходи визначаються як засоби контролю безпеки або контрзаходи, що зменшують ймовірність або вплив конкретних загроз.

Для вибору заходів контролю було обрано організаційно-зумовлений підхід, що, відповідно до рекомендацій NIST SP 800-53, є виправданий для систем, що є вузькоспеціалізованими (наприклад, система зброї або медичний пристрій), має обмежене призначення або сферу застосування, потребує захисту від певного набору загроз або характер обробки даних створює певні типи ризиків для конфіденційності [10]. Такий підхід передбачає формування набору заходів безпеки не на основі заздалегідь визначеного базового переліку, а виходячи зі специфіки досліджуваної системи, характеру даних та ідентифікованих загроз.

Засоби захисту для медичної системи наведені у Додатку Б (стовпці «ІД», «Елемент», «Тип STRIDE» та «Опис».

Кожен контроль характеризується ефективністю та ціною, що включає вартість впровадження та підтримка рішення впродовж року.

Ідентифіковані загрози зіставленні з відповідними засобами захисту. При чому кожній загрозі може відповідати декілька контролів.

Відповідність між загрозами та контролями наведена на рисунку 2.6.

	М-1	М-2	М-3	М-4	М-5	М-6	М-7	М-8	М-9	М-10	М-11	М-12	М-13	М-14
Т-1	✓													
Т-3	✓													
Т-4		✓	✓											
Т-5	✓			✓	✓									
Т-6						✓	✓							
Т-7								✓	✓	✓	✓			
Т-8		✓	✓											
Т-9								✓						
Т-10								✓					✓	✓
Т-12						✓								
Т-13		✓	✓											
Т-14				✓										
Т-15				✓										
Т-16														✓
Т-17				✓										
Т-18				✓										
Т-19														✓
Т-20				✓										
Т-21				✓										
Т-22														✓
Т-23				✓										
Т-24				✓										
Т-25														✓
Т-26							✓							
Т-27							✓							
Т-28													✓	
Т-29							✓							
Т-30							✓							
Т-31													✓	

Рисунок 2.6 – Відповідність між загрозами та заходами захисту

2.3 Ймовірнісне моделювання

2.3.1 Невизначеність у моделюванні ризиків

Характеристики кіберпростору, кількість й різноманіття користувачів та комунікацій сприяють його невизначеності. Кіберпростір вважається одною із надзвичайно складних систем. Через цю велику складність у ньому набагато складніше встановити й визначити ймовірності на наслідки щодо ризиків. На відміну від деяких інших сфер, кібербезпека не має напрацювань із створення єдиного набору даних, де зібрано майже всі загрози, вразливості чи ризики, як це

використовується, до прикладу, в авіації. У сфері кібербпезпеки інциденти є складними, дуже варіюються, а також регулярно з’являються нові інциденти. Також спостерігається неповне звітування, оскільки організації, що постраждали від атак, часто обирають приховування інформації, наприклад побоюючись за репутацію. Більше того, наразі не існує єдиною структури для централізованої звітності. Кібербезпека – відносно нова наука, тому все ще вивчається, які є вразливості. Оскільки кіберпростір розширюватиметься в нових напрямках, може пройти багато часу, перш ніж проблеми з безпеки будуть досліджені.

Зрештою, моделювання є відносно складним у контексті кіберпростору. У віртуальних середовищах інциденти не призводять до реальних пошкоджень систем чи людей. Тому постає питання як змоделювати частину кіберпростору таким чином, щоб вона дійсно імітувала реальні умови. Незважаючи на те, що значний прогрес був досягнутий у галузі дослідження сценаріїв інцидентів на основі моделювання все ще залишається складним створити симуляції, які дійсно відображають складність та зв'язок у реальних контекстах кіберпростору.

У сукупності ці три критичні зауваження – складність кіберпростору, нестача даних та нестача можливостей для моделювання – демонструють складність управління ризиками та пояснюють проблему невизначеності.

Загалом, метрики кібербезпеки значною мірою залежать від експертних оцінок. Ця проблема добре відома і вважається одною із найважливіших у кібербпезпеці, як показано у дослідницькій книзі Національного центру кіберзпезпеки Великобританії (NCSC) де питання «Як створити та прийняти значущі заходи кібербезпеки?» є однією із основних піднятих проблем. На вищезазначене питання немає узгодженої відповіді та відносно мало робіт з цієї теми.

Таким чином, у даній сфері набагато складніше визначити ймовірності та вплив кіберзагроз і, відповідно, їх ризиків.

Невизначеність у медичних системах у кіберпросторі пов'язана з потенційною шкодою для пацієнта внаслідок успішної реалізації загроз. На відміну від традиційних IT-систем, де вплив порушення часто обмежується

втратою даних, фінансовими чи репутаційними збитками, медичні системи несуть додатковий ризик прямої шкоди для здоров'я та безпеки пацієнтів. Це робить невизначеність особливо критичною, оскільки навіть за впроваджених заходів контролю результати не завжди можна точно передбачити.

Таким чином медична система, що розглядається, має параметри з невизначеністю.

Однією із проблемних задач у кібербезпеці є визначення ефективності заходів контролю. Постає питання: як виміряти ефективність контролю, якщо він ніколи не був порушений. Чи правильно вважати, що його ефективність 100%, чи він ще не був перевірений достатньо складною атакою. Таким чином, відсутність інцидентів не обов’язково вказує на високу ефективність, що створює парадокс у вимірюванні [11].

Ціні на впровадження заходів захисту, що включає і вартість річної підтримки реалізованих рішень, також притаманна невизначеність. Навіть за наявності достатнього бюджету, інвестування в кібербезпеку все ще є складним завданням через мінливий характер загроз, що створює певні невизначеності під час оцінювання ризиків. Тому прийняте рішення щодо вкладень з часом може виявитися неефективним, оскільки можуть з’являтися нові виявлені вразливості, що вимагають виправлень, або оцінка ризиків могла бути проведена помилково, що може призвести до неправильних оптимальних стратегій кібербезпеки системи [12]. Ще одним фактором, що враховується, це ціна робочої години спеціаліста на імплементацію, що варіюється в залежності від досвіду та регіону, де створюється певне рішення.

Невизначеність притаманна і до параметра, що позначає шкоду пацієнту, оскільки рівень шкоди може залежати від пацієнта індивідуально, як-от від віку. Система не може передбачити рівень шкоди пацієнту наперед. Більш того, вплив на пацієнта залежить і від ситуації, наприклад від терміновості у здійсненні терапії чи наявності альтернатив у лікуванні. Таким чином, врахування невизначеності для даного параметру демонструє реальність медичних систем, де наслідки інцидентів залежать і від пацієнтів, і від інших обставин.

Методом, що використовується для представлення невизначеності вимірювань, є використання ймовірнісних розподілів.

2.3.2 Вибір ймовірнісних розподілів для вхідних параметрів системи

Методи кількісної оцінки ймовірностей спираються на вибір відповідного розподілу ймовірностей, щоб відобразити очікувану поведінку значення оціненої змінної в реальному світі. Вибір розподілу ймовірностей ґрунтується на припущеннях щодо поведінки змінної. Малоймовірно, що вибраний розподіл буде точно відповідати змінній, але в більшості випадків достатньо наближення розподілу.

2.3.2.1 Ціна на впровадження заходів захисту

Для ціни імплементації певного контролю системи використовуватиметься Логнормальний розподіл, який характерний для величин, що зазвичай є результатом кількох незалежних факторів (наприклад, роботи, матеріалів, навчання, інтеграції), кожен з яких мультиплікативно збільшує загальну величну, як-от вартість. Даний розподіл не може генерувати нульове чи від’ємне число, а здебільшого використовується для моделювання різноманітних величин, що переважно мають помірний масштаб, але можуть (але рідко) бути великими. Він має односторонній, або «скошений» характер та «хвіст» праворуч, що допускає можливість великих значень. Ось чому даний вид розподілу часто є реалістичним представленням ймовірнісних коштів, витрачених на створення кіберзахисту та його підтримки.

2.3.2.2 Ефективність заходів захисту

Наразі не існує одного правильного вибору розподілу для ефективності впроваджених заходів захисту. Проте дана величина варіюється від 0 (не

ефективний) та до 1 (ефективна у 100% випадків), забезпечуючи обмежені значення. Більш того, потрібно обрати тип розподілу, що дозволить керувати «відхиленнями» від очікуваного значення, оскільки ефективність контролю може варіюватися в різних діапазонах. Наприклад, якщо ефективність залежить (і може зменшуватися) від одного фактора, то цей діапазон «коливань» буде вузьким. Якщо існують багато факторів, що можуть знизити ефективність, то потрібен, що більше «відхиляється» від очікуваного значення. Інакше кажучи, поведінка цієї величини вимагає зміну рівня невизначеності.

Тому було обрано Бета розподіл, оскільки він добре підходить для цієї мети завдяки своїй гнучкості що дозволяє представляти широкий діапазон форм (однорідний, U-подібний, асиметричний) шляхом зміни та налаштування його двох параметрів на вхід. Таким чином, різні контролі захисту, можуть мати власний рівень невизначеності.

2.3.2.3 Шкода пацієнту

Вплив успішної реалізації кіберзагроз на пацієнта є відкритою проблемою. Наразі не існує одного правильного вибору розподілу для такої величини.

Вплив загрози на здоров’я пацієнта оцінюється від 0 (немає впливу) до 1 (найгірший плив, чи навіть смерть). Тому було обрано Бета розподіл, оскільки він добре підходить для цієї мети завдяки своїй гнучкості, емпіричній підтримці в медичних застосуваннях та при відсутності статистичних даних[13].

Існує припущення, що ризик для пацієнта відповідає розподілу Пуассона. Цей розподіл Пуассона підходить для цілочисельних оцінок, його гнучкість та відповідність даним часто обмежені. Натомість, бета-розподіл забезпечує більшу гнучкість для моделювання безперервних, обмежених результатів, таких як шкода, завдана пацієнту.

Дослідники розглядали безперервні оцінки ризику та застосовували бета-розподіл для моделювання комбінацій ризиків пацієнтів. Їхній підхід підкреслив здатність бета-розподілу представляти різні форми розподілу даних, що робить

його універсальним вибором для моделювання наслідків шкоди для пацієнтів [14]. Є роботи з оцінки кіберризиків, пов’язаних з медичною галуззю, де Бета розподіл успішно застосовується для моделювання параметру щодо якості життя, пов’язаним зі здоров’ям, які обмежені в діапазоні 0 та 1.

Бета розподіл має перевагу у гнучкості, що дозволяє представляти широкий діапазон форм (однорідний, U-подібний, асиметричний) шляхом налаштування його двох параметрів на вхід. Таким чином, для даної обмеженої величини використовуватиметься цей розподіл.

2.3.3 Джерела даних та експертні оцінки

2.3.3.1 Ймовірність настання загрози у системі

Для кіберінцидентів ймовірність їх виникнення важко оцінити на основі історичних та загальнодоступних даних, тому зазвичай використовуються експертні оцінки, які, однак, залишають простір для суб'єктивності [15].

Так як дизайн системи, з’єднання між елементами і поверхня атаки стабільні та зафіксовані, тоді ймовірність появи певної відомої загрози приблизно фіксована для обраного періоду для аналізу.

Чотири експерти з кібербезпеки в охороні здоров'я, які спеціалізуються на безпеці медичних виробів, оцінили загальну ймовірність кожної атаки [16]. Ці дані і використовуватимуться для моделювання ймовірності настання загроз.

Таким чином, у Додатку Б у стовпці «Ймовірність» наведено кількісні значення ймовірностей настання загроз.

2.3.3.2 Шкода пацієнту від успішної реалізації загрози

Оскільки не існує історичних даних щодо впливу різних кіберзагроз на здоров’я пацієнта у медичних системах, для обчислень використовуватимуться експертні оцінки шкоди пацієнту, що базуються на проаналізованій літературі.

Зважаючи на відсутність точних даних тестів (всі спроби та кількість успішних), що визначали б параметри на вхід, для обчислень альтернативних параметрів Бета розподілу, було визначено середнє, тобто очікуване значення шкоди, а також дисперсія, що позначає наскільки значення може відхилятися від очікуваного середнього. Кожна кіберзагроза має власне середнє значення та значення дисперсії. Значення, що використовуватимуться для моделювання, наведені у Додатку Б у стовпцях «Середнє шкоди пацієнта» та «Дисперсія шкоди пацієнта».

2.3.3.3 Ефективність заходів захисту

Оскільки не існує історичних даних щодо тестувань контролів, для обчислень використовуватимуться експертні оцінки ефективності, що базуються на проаналізованій літературі. Зважаючи на відсутність точних даних тестів (всі спроби та кількість успішних), що визначали б параметри на вхід, для обчислень альтернативних параметрів Бета розподілу, було визначено середнє, тобто очікуване значення ефективності, а також дисперсія, що позначає наскільки значення може відхилятися від очікуваного середнього. Кожен контроль має власне середнє значення та значення дисперсії. Значення, що використовуватимуться для моделювання, наведені у Додатку В у стовпцях «Середня ефективн.» та «Дисперсія ефективн.».

2.3.3.4 Ціна впровадження заходів безпеки

Ціна для кожного контролю обраховувалася як сума ціни на початкову імплементацію (що включає ціну роботи та розробки, а також вартість «непрямих» витрат, таких як ліцензії, додаткові інструменти, витрати на хмарне середовище), так і витрати на підтримку розробленого рішення на рік, що становить 25% від витрат на рік та враховує витрати на сервери, виправлення помилок, оновлення ОС тощо [17]. Значення, що використовуватимуться для

моделювання, наведені у Додатку В у стовпцях «Мін. Вартість» та «Макс. Вартість».

2.4 Математична модель оптимізації

Модель, що розглядається, дозволяє отримувати залишковий ризик за різних стратегій (наборів) мінімізації наслідків та підтримує визначення оптимальних підмножин, які мінімізують витрати, зберігаючи при цьому прийнятний рівень безпеки. Модель ґрунтується на встановлених принципах ймовірнісної оцінки ризиків та аналізу економічної ефективності.

Було визначено множину ідентифікованих загроз:

$$T = \{t_1, t_2, \dots, t_n\} \tag{2.1}$$

Кожна t_i загроза характеризується фіксованим значенням ймовірності її настання в даній системі $L_i \in [0, 1]$, а також ймовірнісним значенням шкоди пацієнту H_i, змодельованою як випадкова величина, отримана з бета-розподілу:

$$H_i \sim Beta(\alpha_i, \beta_i), \tag{2.2}$$

де α_i та β_i – додатні довільні фіксовані параметри, що обчислюються таким чином:

$$\alpha_i = \mu_i \left(\frac{\mu_i(1-\mu_i)}{var_i} - 1 \right) \tag{2.3}$$

$$\beta_i = (1 - \mu_i) \left(\frac{\mu_i(1-\mu_i)}{var_i} - 1 \right) \tag{2.4}$$

де μ_i, є середнім значенням шкоди пацієнту (очікуваним) та var_i, є дисперсією для значення шкоди пацієнту, при чому $var_i < \mu_i(1-\mu_i)$

Визначено множину контролів (пом'якшуючих заходів):

$$M = \{m_1, m_2, \dots, m_k\} \tag{2.5}$$

Кожен контроль m_j характеризується його ефективністю $E_j \in [0,1]$, отриманою з бета-розподілу:

$$E_j \sim Beta(\alpha_j, \beta_j) \tag{2.6}$$

Параметри α_j, β_j обчислюються з відомих величин μ_j, що є середнім значенням ефективності контролю (очікуваним) та var_j, що є дисперсією для ефективності контролю, при чому $var_j < \mu_j(1-\mu_j)$:

$$\alpha_j = \mu_j\left(\frac{\mu_j(1-\mu_j)}{var_j} - 1\right) \tag{2.7}$$

$$\beta_j = (1-\mu_j)\left(\frac{\mu_j(1-\mu_j)}{var_j} - 1\right) \tag{2.8}$$

Ефективність контролю позначає міру, наскільки даний контроль зменшує ймовірність настання загрози.

Кожен контроль m_j також характеризується ймовірнісним значенням ціни впровадження контролю C_j з метою відображення нерівномірного характеру витрат на впровадження на основі попередньо визначеної відповідності контролів загрозам. Ціна впровадження позначає ціну на розробку та підтримку рішення і має логнормальний розподіл:

$$C_j \sim Log(\mu_j, {\sigma_j}^2) \tag{2.9}$$

із щільністю ймовірності:

$$f(C) = \frac{1}{C\sigma\sqrt{2\pi}} exp\left(-\frac{(\ln C - \mu)^2}{2\sigma^2}\right), C > 0 \quad (2.10)$$

Припускається, що існує LB – нижня межа (5-й процентиль, позначає «рідко нижче цього значення»), UB – верхня межа (95-й процентиль, «рідко вище цього значення»). Це відповідає 90% довірчому інтервалу.

Параметри μ_j (середнє значення), σ_j (стандартне відхилення) обраховуються наступним чином:

$$\sigma = \frac{\ln UB - \ln LB}{\Phi^{-1}(0.95) - \Phi^{-1}(0.95)} \quad (2.11)$$

$$\mu = \ln LB - \sigma \cdot \Phi^{-1}(0.95) \quad (2.12)$$

де Φ^{-1} - квантиль стандартного нормального розподілу.

Кожна загроза t_i може бути пом’якшена за допомогою підмножини контролів $S_i \subseteq M$.

Тоді для будь-якої підмножини контролів системи $S \subseteq M$ залишковий ризик R_i^{res} для загрози t_i обчислюється, враховуючи шкоду пацієнту та ймовірність настання цієї загрози, враховуючи її зменшення ефективністю контролю:

$$R_i^{res}(S) = (L_i \cdot \prod_{m_j \in S_i \cap S} (1 - E_j)) \cdot H_i \quad (2.13)$$

Залишковий ризик моделюється за допомогою мультиплікативної формули, що відображає ймовірнісну природу виникнення загрози, сукупний ефект заходів протидії, а також потенційну шкоду пацієнту, якщо реалізація загрози буде успішна. Формула відображає залишкову імовірність після урахування всіх

застосовних заходів, де кожен із них зменшує імовірність виникнення загрози на певну частку.

Така структура ґрунтується на усталених методологіях оцінки ризиків, зокрема ISO 31000 та ISO 14971, де ризик визначається як комбінація імовірності та наслідків. У цій моделі вважається, що заходи захисту діють незалежно та знижують імовірність настання загрози, але безпосередньо не впливають на серйозність шкоди пацієнту. Тому ефективність кожного заходу застосовується лише до компоненти ймовірності.

Залишковий ризик кожної загрози $R_i^{res}(S)$ обраховується для оцінки того, чи він знаходиться в межах заданого на вхід прийнятого значення порогу $R_{threshold}$, тобто

$$R_i^{res}(S) \leq R_{threshold} \tag{2.14}$$

Під час розрахунку загального залишкового ризику R_{total}^{res} за обраної підмножини контролів $S \subseteq M$ для всієї системи, за умови, що кожна загроза $R_i^{res}(S)$ знаходиться в межах прийнятного значення, внесок кожної загрози масштабується за пов'язаною з нею шкодою:

$$R_{total}^{res}(S) = \sum_{i=1}^{n} R_i^{res}(S) \tag{2.15}$$

При обрахуванні загального залишкового ризику врахування шкоди H_i для пацієнта, що враховується у залишковому ризику R_i^{res} для кожної загрози, відграє роль ваг та гарантує, що загрози з вищою потенційною шкодою мають пропорційно більший вплив на загальне значення ризику. Таким чином загрози не розглядаються однакові, а пріоритезуються в залеженості від розміру шкоди пацієнту. Інтегруючи шкоду як ваговий коефіцієнт, модель забезпечує більш зважений підхід до прийняття рішень. Наприклад, загроза із помірною імовірністю, але високим рівнем шкоди може розглядатися як більш критична,

ніж часта, проте малозначна загроза. Такий механізм зважування допомагає ефективніше розподіляти ресурси, зосереджуючи зусилля на пом'якшенні саме тих ризиків, де це має найбільше значення.

Для кількісного порівняння залишкових ризиків різних рівнів вводиться індекс серйозності ризику (Risk Severity Index, RSI). Цей показник відображає сукупний рівень ризику системи після застосування заходів безпеки та дозволяє оцінити, наскільки значним залишається вплив імовірних загроз у цілому. Обчислення RSI здійснюється з урахуванням кількості загроз кожного рівня залишкового ризику та їхніх вагових коефіцієнтів за формулою (2.16):

$$RSI = \sum_{l \in L} r_l n_l \tag{2.16}$$

де $\mathrm{L} = \{\mathrm{low}, \mathrm{low} - \mathrm{medium}, \mathrm{medium}, \mathrm{medium} - \mathrm{high}, \mathrm{high}\}$ – множина рівнів ризику. r_l – значення вагового коефіцієнта для рівня ризику $l, r_l = \{0.1, 0.3, 0.5, 0.7, 0.9\}$, n_l – кількість загроз з залишковим рівнем ризику l.

Також обраховується загальна сума витрат на імплементацію C_{total} підмножини контролів $S \subseteq M$ за формулою (2.17):

$$C_{total}(S) = \sum_{m_j \in S} C_j \tag{2.17}$$

Ранжування підмножин $S \subseteq M$, що мають прийнятний залишковий ризик та найменші вкладення, дозволяють особам, що приймають рішення, вибирати з набору рішень той варіант, який балансує між зниженням ризиків та бюджетними обмеженнями.

2.5 Висновки до другого розділу

У даному розділі було представлено покроковий процес, що використовується для оцінки та вибору оптимальних стратегій мінімізації наслідків реалізації кіберзагроз. Було визначено та описано об’єкт моделювання – медична інформаційна система. Ідентифіковано елементи системи, інтерфейси. Загалом була отримано 31 загроза для всієї системи. Також визначено множину заходів захисту даної системи, що складається із 14 заходів захисту. Встановлено відповідність між загрозами та контролями. Визначено, що такі параметри системи, як ефективність та вартість контролю, а також шкода пацієнту, мають ймовірнісну природу. Обґрунтовано вибір ймовірнісних розподілів для них.

Представлено математичну модель для оцінювання ризиків. Визначено основні параметри, за якими буде здійснюватися вибір найкращого рішення, а саме: загальний рівень ризику, індекс серйозності ризику та загальна ціна впровадження набору заходів захисту.

РОЗДІЛ 3 СИМУЛЯЦІЙНІ ЕКСПЕРИМЕНТИ ТА АНАЛІЗ РЕЗУЛЬТАТІВ

3.1 Програмна реалізація моделі оцінювання ризиків

Для реалізації моделі оцінювання ризиків кібербезпеки було розроблено програмне забезпечення, що дозволяє проводити симуляційні експерименти з використанням методу Монте-Карло та оцінювати вартість та ризик за різних комбінацій заходів контролю. Для створення симуляційної моделі було обрано Python, що надає перелік засобів для статистичного моделювання, обробки даних та візуалізації результатів.

Основною бібліотекою для роботи з табличними даними використовувалася pandas, яка застосовувалася для імпорту вхідних даних із електронних таблиць, попередньої обробки, перетворення типів змінних, формування підсумкових таблиць результатів і збереження їх у форматі CSV. Завдяки зручним структурами даних та операціям фільтрації, групування й агрегації, pandas забезпечила ефективну роботу з великими наборами параметрів загроз, контролів і симуляційних результатів.

Для виконання швидких математичних операцій, генерації випадкових величин і роботи з багатовимірними масивами використовувалася бібліотека NumPy, яка лежить в основі статистичних обчислень у проєкті. У моделі NumPy застосовувався для обробки числових параметрів, генерування логнормальних випадкових значень вартості контролів, а також для прискореного опрацювання вибірок, що генеруються в процесі симуляцій.

Бібліотека SciPy, зокрема модуль *scipy.stats*, забезпечувала роботу з ймовірнісними розподілами, що є критично важливим для моделювання невизначеності ризиків у межах методу Монте-Карло. У моделі використовувалися розподіли ймовірностей, які застосовувалися для моделювання шкоди від загроз, ефективності заходів контролю та вартості.

Для формування всіх можливих комбінацій заходів контролю застосовувався модуль itertools, який забезпечує функції створення ітераторів. Зокрема, *chain* та *combinations* використовувалися для побудови всіх підмножин контролів, що необхідно для пошуку оптимальної стратегії зменшення ризиків і аналізу впливу різних наборів контролів на результати симуляцій.

Для побудови візуалізацій, зокрема підсумкового тривимірного графіка взаємозв'язку між загальним ризиком, сумарною вартістю контролів та індексом RSI, використовувалася бібліотека matplotlib.

В основу розрахунків було покладено метод Монте-Карло. Цей метод широко використовується для кількісної оцінки ризиків у системах, що мають невизначеність у вхідних парметрах. У контексті моделювання ризиків кібербезпеки він дозволяє моделювати велику кількість потенційних сценаріїв шляхом багаторазової вибірки значень з розподілів ймовірностей, які представляють ймовірність настання загроз, вартість та ефективність контролів. Запуск симуляції з використанням цього методу дозволяє отримати вибірку з можливих результатів замість одного результату, що дозволяє розглянути всі ймовірні результати та проаналізувати їх, що допомагає у прийнятті рішень [18].

У розробленому програмному забезпеченні моделювання Монте-Карло використовується для моделювання залишкового ризику для кожної загрози після застосування набору заходів протидії. Цей метод узгоджується з усталеними практиками кількісної оцінки ризиків, де, наприклад, моделювання Монте-Карло зазвичай застосовується в оцінці ризиків для здоров'я пацієнтів, де вхідні параметри, є невизначеними та ймовірнісними за своєю природою [19].

Після вибірки механізм моделювання агрегує результати в усіх ітераціях для обчислення ключових показників, таких як залишкового ризику, загальної вартості та індексу серйозності ризику (RSI). Аналізуючи отриманий розподіл цих показників, стає можливим визначити комбінації контролю, які мінімізують ризик за бюджетних обмежень, або навпаки, зрозуміти, який залишковий ризик можна терпіти для заданого рівня вкладень [20].

Однією з переваг використання Монте-Карло для кіберризиків є його гнучкість. На відміну від простих детерміністичних моделей або оцінок з фіксованими значеннями, метод враховує мінливість та непередбачуваність динаміки величин. Однак, точність таких симуляцій значною мірою залежить від того, наскільки добре розподіли вхідних даних відображають невизначеність реального світу. За умови ретельного впровадження, моделювання методом Монте-Карло стає інструментом підтримки рішень та дозволяє розглянути і найкращі, й найгірші сценарії.

Логіка функціонування розробленої симуляційної моделі базується на послідовному опрацюванні вхідних даних, що подані у вигляді Excel-файлу. Повний програмний код реалізації наведені у Додатку Г. Структура вхідного файлу складається із таблиць, наведених у Додатку Б та Додатку В, а також рисунку 2.6. Логіка роботи програми наведена на рисунку 3.1.

Розроблене програмне забезпечення умовно поділено на три етапи.

На першому етапі модель завантажує вхідні дані, що містять перелік загроз, перелік заходів контролю, таблицю відповідностей між ними, а також числові значення, що використовуватимуться для обрахування параметрів ймовірнісних розподілів шкоди пацієнту, ефективності та вартості контролів. Після зчитування даних здійснюється їх попередня обробка. Для показника «шкода пацієнту» (harm) кожної загрози та показника ефективності кожного контролю обчислюються параметри бета-розподілу. Це необхідно для подальшої генерації випадкових значень у моделюванні Монте-Карло.

Також на цьому етапі програмою формується повний набір можливих комбінацій контролів. Кожна комбінація буде проаналізована окремо, що дозволяє оцінити вплив різних стратегій мінімізації ризику на загальний рівень захищеності системи.

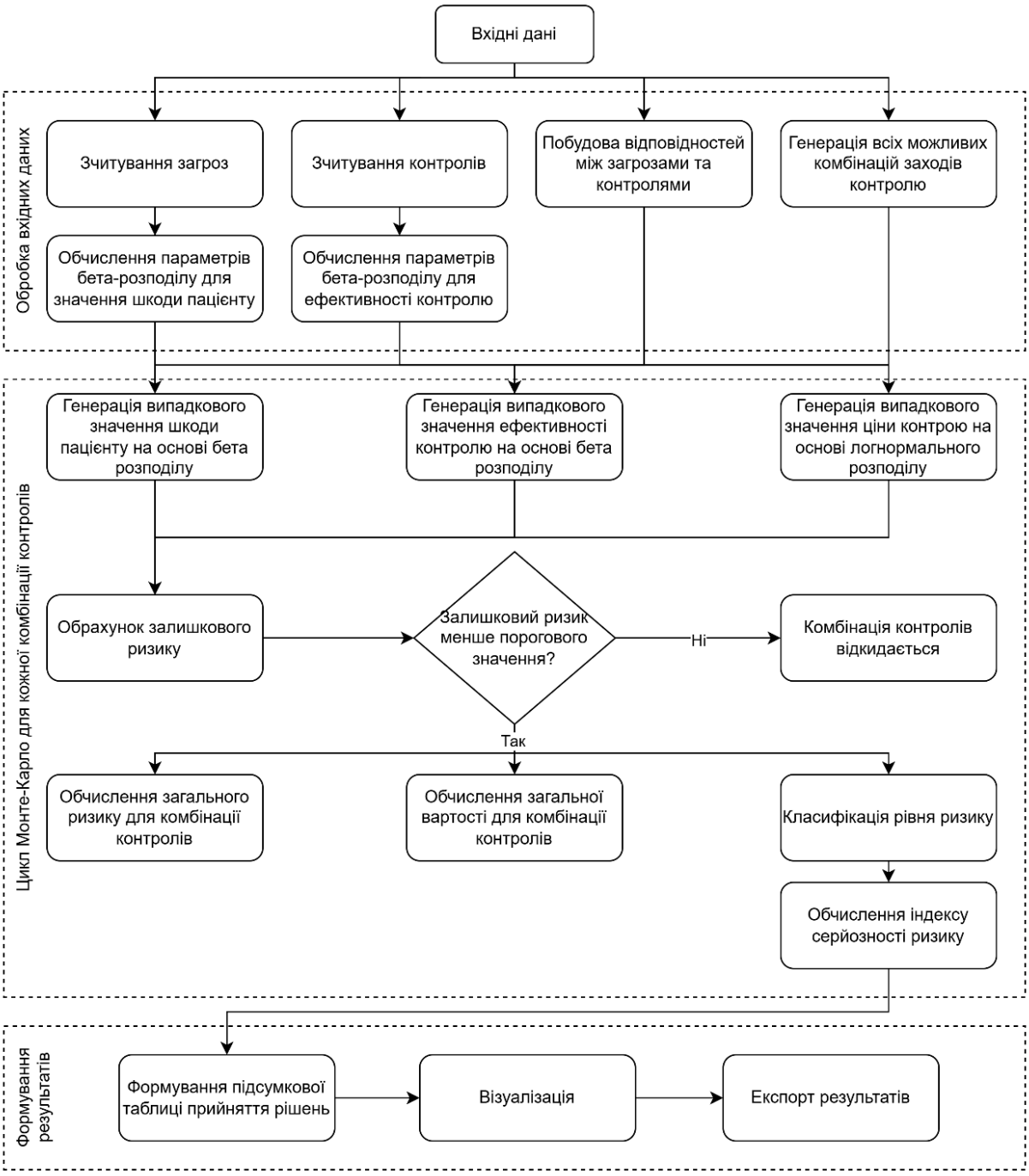

Рисунок 3.1 – Алгоритм роботи розробленої симуляційної моделі

Другий етап є центральним у роботі моделі та включає проведення численних симуляцій методом Монте-Карло. Для кожної комбінації заходів контролю виконується генерація випадкових величин. Після отримання вибіркових значень виконується обчислення залишкового ризику. Розрахований залишковий ризик порівнюється з визначеним пороговим значенням. Якщо

ризик перевищує поріг, дана комбінація контролів автоматично відкидається як неефективна.

У випадку, коли залишковий ризик є нижчим за порогове значення, модель переходить до подальших розрахунків. Визначається сумарний ризик для всіх загроз у межах цієї комбінації, обчислюється повна вартість контролів, виконується класифікація рівня ризику за категоріями та обчислюється індекс серйозності ризику (RSI), що є ваговим показником сукупного ризику.

Після завершення симуляцій для всіх можливих комбінацій контрольних заходів модель переходить до останнього етапу. На цьому етапі здійснюється формування підсумкової таблиці рішень, що включає значення сумарного ризику, вартості та RSI для кожної прийнятної комбінації.

Після цього результати експортуються у вигляді окремих CSV-файлів, що дозволяє проводити додатковий аналіз, повторну валідацію чи незалежну перевірку. Також виконується візуалізація даних, зокрема побудова 3D-графіка, який відображає взаємозв’язок між вартістю контролів, рівнем ризику та індексом серйозності (RSI). Цей етап забезпечує отримання структурованих аналітичних результатів, які можуть бути використані для прийняття оптимізованих рішень щодо впровадження заходів безпеки.

3.2 Проведення симуляційного моделювання

Першим кроком аналізу ризиків є вибір методологічного підходу до оцінювання рівня ризику. У медичній сфері особливо важливим є кількісний підхід, оскільки він дозволяє чисельно оцінити ймовірність події та шкоду для пацієнта, охоплюючи весь спектр можливих наслідків: від незначної шкоди до тяжкої травми чи летального результату.

На рисунку 3.2 представлений пркилад матриці ризиків, за якою організації визначають значення прийнятого ризику.

			Шкода для пацієнта				
			Кіберзагроза призводить до незначної травми або несприятливого впливу на здоров'я	Кіберзагроза призводить до помірної травми або несприятливого впливу на здоров'я	Кіберзагроза призводить до серйозної травми або несприятливого впливу на здоров'я	Кіберзагрза може призвести до серйозних травм чи інвалідності	Кіберзагроза, ймовірно, призведе до смерті пацієнта
			0.1	0.3	0.5	0.7	0.9
Ймовірність настання загрози	Кіберзагроза настане точно у даній системі (настає один раз чи декілька разів на місяць)	0.9	0.09	0.27	0.45	0.63	0.81
	Кіберзагроза очікується за більшості обставин у даній системі (настає декілька разів на рік)	0.7	0.07	0.21	0.35	0.49	0.63
	Кіберзагроза може настати за багатьох обставин у даній системі (настає один раз на 1-3 роки)	0.5	0.05	0.15	0.25	0.35	0.45
	Кіберзагроза може наставати, але не часто для даної системи (настає один раз на 3-5 років)	0.3	0.03	0.09	0.15	0.21	0.27
	Настання кіберзагрози не очікується в даній системі, але все ще є можливою (настає один раз на 5 або більше років, або не настає взагалі)	0.1	0.01	0.03	0.05	0.07	0.09

Рисунок 3.2 – Матриця ризиків [21]

Матриця поєднує два виміри: ймовірність настання загрози у заданій системі та шкоду для пацієнтів. Такий структурований підхід підтримує прозору пріоритезацію ризиків.

Вимір шкоди для пацієнта та вимір ймовірності представлено за п'ятибальною шкалою. Перетинаючи ці два виміри, кожну загрозу можна віднести до рівня ризику («Низький», «Нижче середнього», «Середній», «Вище середнього», «Високий»).

Отримана матриця ризиків дозволяє ввести поріг прийнятності ризику. Цей поріг визначається як вхідний параметр для моделі: ризики, що перевищують поріг, вважаються неприйнятними та потребують зменшення, тоді як ризики нижче порогу можуть бути допустимі.

Цей підхід узгоджується з усталеними рамками управління ризиками, пов'язаними з медичними виробами та кібербезпекою, включаючи ISO 14971:2019 та NIST SP 800-30 Rev.1.

На практиці при управлінні ризиками організації самостійно формують матриці ризиків із числовими пороговими значеннями та індикацією рівнів небезпеки: від прийнятного (зелений) до критичного (червоного) рівня.

Оскільки прийнятний рівень ризику залежить від політик, ресурсів та інших потреб конкретної організації, у подальшій роботі моделювання буде виконано для двох сценаріїв порогового значення, що відповідає зеленому рівню, та менш жорсткого порогу на рівні жовтої зони. Це дасть змогу порівняти, як зміна критеріїв прийнятності ризику впливає на результати симуляції, ефективність контролів та остаточні рішення щодо управління ризиками.

3.2.1 Моделювання для низького рівня прийнятного ризику

У рамках проведення моделювання ризиків було обрано низький рівень прийнятного ризику, який у багатьох організаціях використовується як базовий поріг для критичних активів. Вибір саме низького порогового значення пояснюється тим, що компанії прагнуть мінімізувати навіть незначні ймовірності інцидентів, оскільки навіть одинична подія може спричинити значну шкоду користувачам, що, відповідно, веде до репутаційних, фінансових або юридичних наслідків. У цьому дослідженні було використано значення, визначені на матриці ризику, поданій на рисунку 3.2, і для моделювання було обрано значення ризику 0,07, яке віднесено до категорії низького прийнятного рівня, позначеного зеленими кольорами).

Загальна кількість розглянутих комбінацій контрольних заходів склала 16 384 набори, що відповідає повному перебору всіх можливих підмножин наявних заходів. Серед них лише два набори контролів були класифіковані як прийнятні, тобто відповідали критерію залишкового ризику, менше встановленого порогового значення. Це демонструє, що при низькому порозі симуляція виявила жорсткі вимоги до комплектації заходів безпеки для забезпечення мінімізації ризику. Результати наведені в таблиці 3.1.

Таблиця 3.1 – Результати симуляції з низьким значенням прийнятного ризику

Номер набору	Загальна вартість	Загальний ризик	RSI
2	10256.90	0.355	8.1
1	19920.16	0.659	12.5

Перший прийнятний набір включав одинадцять заходів контролю (M-1, M-3, M-4, M-6, M-7, M-8, M-10, M-11, M-12, M-13, M-14). Загальна вартість цього набору становила 19 920.16, а сумарний залишковий ризик дорівнював 0.659. Значення показника RSI для цього набору склало 12.5, що відображає середньо-високий рівень залишкового ризику для розглянутих загроз. Розподіл ризиків по категоріях показав, що більшість загроз були низького та середнього рівня, проте окремі загрози відносилися до категорії високого ризику.

Другий прийнятний набір контролів складався з дванадцяти заходів (M-1, M-2, M-3, M-4, M-5, M-6, M-7, M-8, M-10, M-12, M-13, M-14). Його загальна вартість склала 10 256.9, сумарний залишковий ризик становить 0.355, а RSI дорівнював 8.1. Такий результат демонструє кращу економічну ефективність при збереженні допустимого рівня ризику, оскільки більшість загроз у цьому наборі були класифіковані як низькі або нижче середнього, а жодна з загроз не потрапила до категорії високого ризику.

З огляду на ці показники, набір під номером 2 було обрано як оптимальний для заданих конфігурацій системи, оскільки він забезпечує допустимий рівень залишкового ризику при кращій економічній ефективності порівняно з іншим прийнятним набором.

Вибір оптимального набору може базуватися як на мінімізації загальної вартості, так і на досягненні найнижчого залишкового ризику, залежно від пріоритетів організації.

Таким чином, моделювання для низького рівня прийнятного ризику продемонструвало, що забезпечення мінімального залишкового ризику вимагає комплексного підходу до вибору заходів контролю. Лише невелика кількість

комбінацій заходів (2 з 16 384) виявилася прийнятною, що свідчить про високу чутливість системи до невиконання навіть окремих контролів. При цьому аналіз показав, що оптимальні набори контролів можуть значно відрізнятися за економічними показниками, хоча обидва забезпечують допустимий рівень залишкового ризику. Отримані результати дозволяють оцінити баланс між вартістю заходів та ефективністю зменшення ризику, що є ключовим при прийнятті рішень щодо безпеки медичної інформаційної системи.

3.2.2 Моделювання для підвищеного рівня прийнятного ризику

Для порівняння було обрано підвищений рівень прийнятного ризику, який застосовується у багатьох організаціях, як компроміс між мінімізацією ризику та економічною ефективністю. Використання більш високого порогового значення пояснюється тим, що організації іноді готові приймати незначні ризики для зменшення витрат на заходи контролю або для збереження гнучкості системи.

У цьому моделюванні за основу взято значення ризику 0.27, яке відноситься до категорії підвищеного прийнятного рівня (позначеного жовтим кольором на матриці ризику, поданій на рисунку 3.2).

Загальна кількість розглянутих комбінацій контрольних заходів залишилася такою ж, тобто 16 384 набори, проте кількість прийнятних комбінацій значно зросла до 134. Це демонструє, що підвищення порогового значення дозволяє більшій кількості наборів контролів відповідати критерію залишкового ризику, що забезпечує гнучкість у виборі заходів безпеки та можливість оптимізувати витрати. Результати для перших 5 найкращих наборів наведені в таблиці 3.2.

Таблиця 3.2 – Результати симуляції з низьким значенням прийнятного ризику

Номер набору	Загальна вартість	Загальний ризик	RSI
89	13939.27	0.695	4.9

Продовження таблиці 3.2

46	16512.28	0.791	5.1
58	21192.73	0.734	5.1
33	48524.72	0.900	5.3
53	20255.93	0.715	5.3

Для наочності отримані результати були представлені у вигляді тривимірної поверхні RSI залежно від сумарної вартості та загального залишкового ризику кожного набору контролів. Графік дозволяє візуально порівняти ефективність різних комбінацій заходів безпеки, позначеними порядковими номерами наборів, та ідентифікувати оптимальні набори, що мінімізують залишковий ризик при оптимальній економічній вартості.

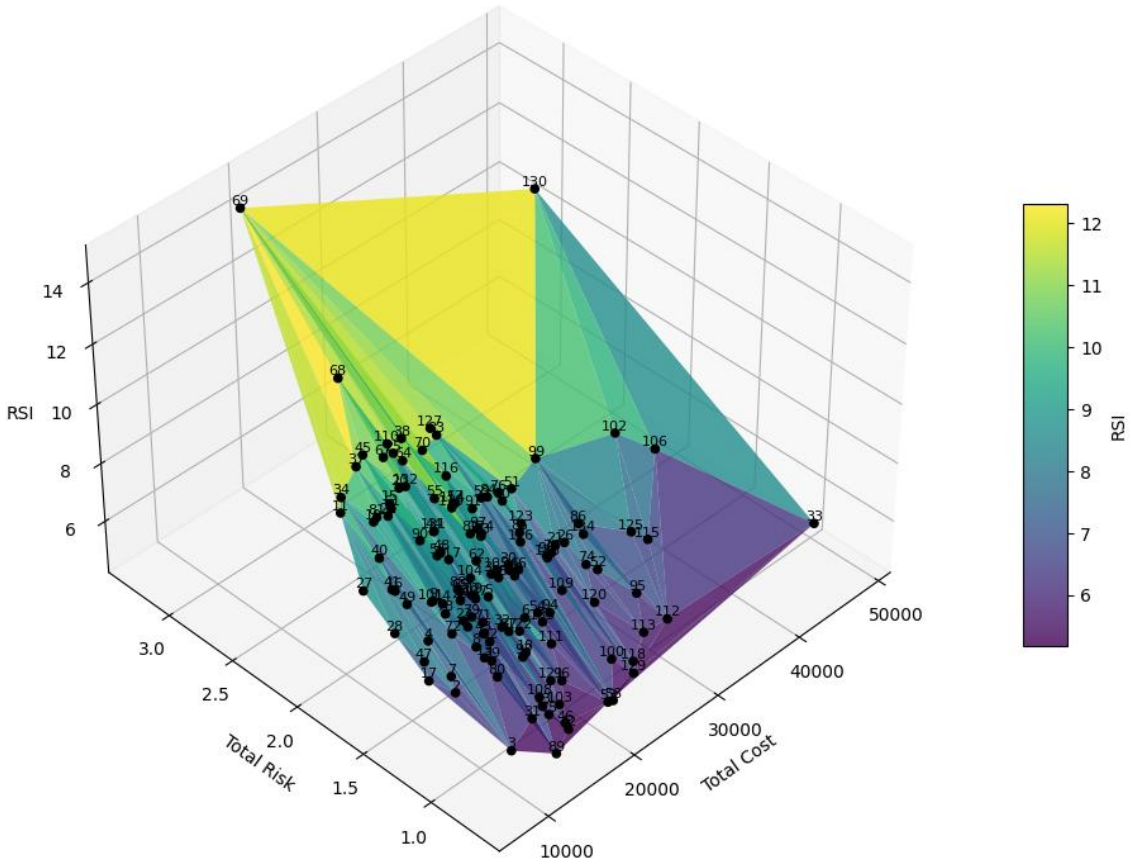

Рисунок 3.3 – Візуалізація результатів симуляції з низьким значенням прийнятного ризику

Серед прийнятних наборів контролів можна виділити оптимальний за набором контролів номер 89, який забезпечує найкращий баланс між економічною ефективністю та допустимим залишковим ризиком. Набір контролів складався з 11 заходів (M-1, M-2, M-4, M-5, M-6, M-7, M-9, M-10, M-12, M-13, M-14). Його загальна вартість склала 13939.27, сумарний залишковий ризик становить 0.695, а RSI дорівнював 4.9.

У порівнянні з моделюванням для низького рівня ризику, оптимальний набір для підвищеного рівня включає меншу кількість заходів, що дозволяє знизити загальні витрати при збереженні допустимого залишкового ризику для критичних загроз.

Обчислення залишкового ризику для кожної загрози показали, що більшість загроз у цьому наборі були класифіковані як низькі, кілька нижче середнього та середнього рівня, а кількість високоризикових загроз залишалася відсутньою. Це свідчить про ефективність комплектації заходів контролю навіть при більш гнучкому значенні прийнятного ризику.

Таким чином, моделювання для підвищеного рівня прийнятного ризику показало, що збільшення порогового значення дозволяє значно розширити вибір прийнятних комбінацій контролів, зберігаючи при цьому ефективність системи управління ризиками та оптимізуючи витрати на заходи безпеки. Це забезпечує організаціям гнучкість у прийнятті рішень щодо безпеки медичної інформаційної системи та дозволяє враховувати фінансові обмеження при плануванні заходів контролю.

3.3 Аналіз отриманих результатів

Отримані результати моделювання, наведені у Додатку Д, для вищого порогового значення ризику демонструють широкий спектр можливих комбінацій заходів безпеки, які суттєво відрізняються як за вартістю впровадження, так і за здатністю знижувати залишковий ризик. Помітно, що навіть у межах однієї кількості заходів загальний ефект може бути різним

залежно від їхнього змісту та взаємодії. Найнижчий зафіксований рівень залишкового ризику становить приблизно 0.625-0.718, що спостерігається у варіантах 42, 53, та 89. Вартість імплементації заходів контролю варіюється від 7400 до 48800. Це вказує на те, що досягнення прийнятного ризику не завжди відбувається за рахунок пропорційного збільшення інвестицій, а залежить від комбінування саме тих заходів, що адресують найкритичніші вразливості системи.

Результати демонструють, що надмірне додавання заходів не завжди є економічно виправданим. Деякі комбінації, які мають помірний рівень витрат, забезпечують набагато кращий баланс між витратами та ефективністю. Наприклад, набір №31, що має 10 заходів контролю, має залишковий ризик 0.815 та вартість близько 13000, показує кращу ефективність за співвідношенням «вартість–ризик», ніж набір №33, що також складається з 10 контролів, який забезпечує загальний ризик 0.9, але за значно вищої вартості близько 48500. Це підтверджується значенням RSI, яке для варіанту 33 є одним із найнижчих (5.3), але з урахуванням величезної вартості стає менш привабливим порівняно з комбінаціями, що коштують удвічі дешевше, але мають близькі значення ризику.

Значення RSI дає змогу побачити загальну ефективність комбінацій. Найнижчі RSI (приблизно 4.9 - 5.5) характерні для варіантів 33, 46, 53, 58, 75 та 89, але ці результати дуже різні за фінансовими витратами. Варіант 3, наприклад, має залишковий ризик 0.784 при вартості 10200, тоді як варіант 53 забезпечує ще нижчий ризик (0.715), але вже за понад 20000. Така різниця показує, що формально низький RSI не завжди означає оптимальність з позиції інвестування, а скоріше демонструє загальну технічну ефективність комбінації незалежно від бюджету. Натомість деякі варіанти з RSI близько 6-7 пропонують значно кращий компроміс між бюджетом і рівнем захисту.

У верхньому діапазоні RSI (10-14.5) опинилися набори, які хоч і охоплюють значну кількість заходів, але залишковий ризик знижується недостатньо, порівняно з витраченими коштами. Наприклад, варіант 69 має найвищий ризик (3.298) та RSI 14.5, попри витрати 18400. Це свідчить, що вибрані заходи не є

релевантними для тих типів загроз, які формують основну частку ризику, і демонструє типову проблему некоректної або надмірної алокації ресурсів. Такі комбінації розглядаються як неефективні та не повинні бути рекомендовані для впровадження, навіть у випадку доступного бюджету.

Загалом аналіз результатів підтверджує важливість не просто збільшувати кількість заходів, а ретельно підбирати їх у взаємодоповнювальні групи. Особливо результативними виявилися комбінації, що включають заходи М-1, М-3, М-4, М-6, М-7, М-8, М-12, М-13 та М-14 у різних поєднаннях, оскільки саме вони найчастіше формують збалансовані за вартістю та ефективністю набори. З іншого боку, заходи М-9, М-10 та М-11 вносять позитивний внесок лише в певних комбінаціях, а в інших суттєво підвищують вартість без пропорційного зменшення ризику. Це демонструє необхідність перевіряти внесок кожного контролю в умовах конкретної моделі ризиків медичної інформаційної системи.

Результати моделювання дозволили виділити найбільш збалансовані комбінації заходів, які забезпечують оптимальне співвідношення між залишковим ризиком та витратами. Такі набори не обов’язково мають найнижчий ризик, але вони найбільш економічно обґрунтовані для практичного впровадження.

Розроблена модель має обмеження, пов’язані із нестачею статистичних даних, необхідних для точного налаштування ймовірнісних розподілів, що використовувалися в моделі. Сфера кібербезпеки традиційно характеризується обмеженим доступом до реальних інцидентів, оскільки більшість організацій не публікують детальну інформацію про атаки, масштаби завданої шкоди чи частоту загроз. Це пов’язано як із вимогами конфіденційності та законодавчими обмеженнями, так і з репутаційними ризиками, які виникають у разі розголошення фактів компрометації систем.

Додаткову складність становить те, що для медичної галузі доступність статистики ще нижча. Медичні інформаційні системи є критично чутливими, обробляють дані підвищеної конфіденційності (PHI) та підпадають під суворе регулювання (HIPAA, GDPR). Через це медичні установи майже ніколи не

надають публічних звітів із деталізацією наслідків конкретних атак. Крім того, кіберзагрози для медичних систем мають специфічну природу: вони включають не лише витоки даних, але й ризики прямого впливу на безпеку пацієнтів. Через унікальність таких загроз історичні вибірки даних є надто малими, у результаті чого модель вимушено ґрунтується на експертних оцінках, відкритих джерелах та літературних даних, що створює певну невизначеність у точності параметрів.

Також необхідно зазначити, що результати симуляції залежать від припущень щодо кореляцій між загрозами та ефективністю контролів. Реальні системи можуть демонструвати іншу динаміку. Наприклад, деякі контролі можуть по-різному впливати на взаємопов’язані загрози. Через брак експериментальних даних це неможливо було врахувати повною мірою. Тому результати дослідження слід інтерпретувати не як абсолютні значення ризику, а як відносні показники, що допомагають порівняти стратегії захисту для прийняття зважених рішень.

Створена модель має універсальний характер і може бути адаптована для використання різними медичними організаціями з урахуванням їхніх власних умов, конфігурацій систем та рівнів ризик-апетиту. Для запуску моделювання установі необхідно ввести перелік актуальних загроз та їх базові ймовірності, перелік доступних заходів контролю, їхню вартість і ефективність, а також прийнятний рівень залишкового ризику, який визначається політиками безпеки організації.

Також модель дає змогу медичній організації самостійно визначити стратегічний пріоритет: мінімізацію залишкового ризику або мінімізацію витрат. Для закладів, які працюють із критичними клінічними процесами і мають низький ризик-апетит, оптимальним буде відбір наборів контролів із найнижчим рівнем ризику навіть за вищої вартості. Для закладів із суворо обмеженим бюджетом, навпаки, модель дозволяє знайти комбінації, що забезпечують достатній рівень захисту за мінімально можливих витрат. Завдяки повному перебору або вибірковому пошуку модель формує список прийнятних

комбінацій, після чого організація може вибрати той набір, що найкраще відповідає її потребам та можливостям.

У результаті запропонована модель може бути використана як планувальний інструмент під час формування бюджету на інформаційну безпеку, розроблення політик безпеки, планування впровадження контролів або оцінювання альтернативних варіантів модернізації системи.

3.4 Висновки до третього розділу

У даному розділі було здійснено програмну реалізацію моделі оцінки ризиків медичної інформаційної системи, що була протестована на двох рівнях прийнятного ризику. Аналіз отриманих результатів показав, що просте накопичення заходів контролю не завжди забезпечує ефективність, а й може бути економічно необґрунтованим. Частина комбінацій, хоча й забезпечує прийнятний рівень ризику, може включати заходи, що не є релевантними до основних загроз, що формують значну частку ризику, і таким чином ілюструє типову проблему некоректної або надмірної алокації ресурсів.

Результати підтверджують, що для ефективного управління інформаційною безпекою важливо підбирати заходи у взаємодоповнювальні групи. Запропонована модель може бути використана медичними організаціями як інструмент планування та прийняття рішень щодо інформаційної безпеки, дозволяючи обирати параметри на вхід моделі відповідно до пріоритетів організації: балансування між ризиком і витратами, а також підбір контролів, що відповідають специфіці їхніх систем та вимогам безпеки.

Реалізація моделі має певні обмеження, пов’язані з недостатньою кількістю статистичних даних для точного налаштування ймовірнісних розподілів. Це обмеження обумовлене специфікою медичної галузі та кібербезпеки, де публічно доступна інформація про інциденти є обмеженою або відсутня, що може впливати на точність оцінки ризиків.

РОЗДІЛ 4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Сучасний розвиток технологій і автоматизація виробничих процесів забезпечують підвищення ефективності роботи підприємств. Комп'ютерна техніка є невід'ємною складовою медичних інформаційних систем, проте її масове використання висуває низку вимог до охорони праці. Законодавство України встановлює норми безпеки для працівників, які працюють із комп'ютерними пристроями, з метою забезпечення їхнього здоров'я та комфорту [22].

Згідно НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями», на робочі місця працівників з електронними пристроями поширюються такі вимоги:

1. Ергономіка робочого місця. Конструкція має забезпечувати підтримання оптимальної пози працівника, знижуючи фізичне навантаження та перевтому.

2. Рівень випромінювання. Випромінювання від екранних пристроїв повинно бути зведене до гранично допустимих рівнів для мінімізації впливу на здоров'я [23].

3. Ергономічність організації простору. Усі елементи робочого місця мають відповідати антропологічним, психофізіологічним і ергономічним вимогам [24].

4. Освітлення. Освітлення робочого місця повинно забезпечувати належний контраст між екраном і навколишнім середовищем відповідно до вимог ДБН В.2.5-28:2018.

5. Мікроклімат приміщень. Температурний режим, вологість і чистота повітря повинні відповідати вимогам ДСН 3.3.6.042-99, затвердженим головним державним санітарним лікарем [25].

Приміщення, в яких встановлюються комп’ютери, мають відповідати проектній документації, затвердженій державними органами. Враховуються:

1. Санітарні норми освітлення.
2. Параметри мікроклімату (температура, вологість).
3. Рівень шуму, вібрації та інших фізичних факторів.
4. Безпека щодо електромагнітних, ультрафіолетових і інфрачервоних полів.

Робочі місця не допускається облаштовувати у підвальних або цокольних приміщеннях. Заборонено використовувати матеріали, що виділяють шкідливі хімічні речовини [23].

Згідно з ДБН В.2.5-28:2018 "Природне і штучне освітлення", приміщення з постійним перебуванням людей мають бути забезпечені природним освітленням. Для штучного освітлення рекомендується використовувати енергоефективні джерела світла, такі як світлодіодні лампи.

Працівники зобов’язані проходити інструктажі з охорони праці, які включають навчання надання першої допомоги та дій у разі аварійних ситуацій. Інструктажі поділяються на такі види:

1. Вступний. Проводиться з усіма новими працівниками, а також із працівниками сторонніх організацій, які беруть участь у виробничому процесі.
2. Первинний. Здійснюється безпосередньо перед початком роботи на новому місці.
3. Повторний. Проводиться регулярно, з урахуванням умов праці (не рідше одного разу на 6 місяців).
4. Позаплановий. Організовується у разі змін у нормативно-правових актах, після аварій або порушень правил безпеки.
5. Цільовий. Проводиться перед виконанням робіт із підвищеною небезпекою або в умовах надзвичайних ситуацій.

4.2 Фактори ризику та можливі порушення здоров'я користувачів комп'ютерної мережі

Комп'ютерні мережі є невід'ємною частиною сучасного життя, забезпечуючи ефективність роботи у різних галузях, в тому числі і в медичній. Однак, тривала взаємодія з інформаційно-комунікаційними технологіями може негативно впливати на здоров'я користувачів.

Основні фактори ризику, пов'язані з використанням комп'ютерних мереж:

1. Фізіологічні фактори.
2. Психоемоційні фактори.
3. Ергономічні фактори.

Фізіологічні фактори ризику пов'язані із сидячим способом життя та тривалою роботою за комп'ютером. Перебування у фіксованій позі протягом тривалого часу призводить до перенапруження м'язів, появи болю у спині, шиї та плечах, а також до порушень кровообігу, що підвищує ризик розвитку варикозного розширення вен та інших судинних захворювань [26]. Значну небезпеку становить і напруження зору, спричинене постійною роботою з моніторами. Воно може викликати синдром комп'ютерного зору, що проявляється сухістю очей, порушенням фокусування та головним болем. Додаткове навантаження на органи зору створює неправильна освітленість робочого місця [27]. Окремо слід зазначити вплив шумового забруднення, адже постійний фоновий шум від комп'ютерного обладнання може спричиняти підвищену втомлюваність, стрес та зниження працездатності.

Психоемоційні фактори ризику зумовлені надмірним використанням комп'ютерних мереж та високою інтенсивністю інформаційних потоків. Постійна робота за комп'ютером може призводити до психологічного перевантаження та емоційного вигорання, а часті технічні збої або проблеми з програмним забезпеченням підвищують рівень стресу. Крім того, тривале перебування в онлайн-середовищі часто сприяє соціальній ізоляції, що проявляється зниженням рівня безпосереднього міжособистісного спілкування.

Ергономічні фактори ризику пов’язані з неправильним облаштуванням робочого місця. Недостатня або надмірна висота стільця, неправильний кут нахилу монітора, відсутність підставки для ніг створюють додаткове навантаження на опорно-руховий апарат та можуть спричиняти хронічні больові відчуття [26]. Погане освітлення робочої зони, зокрема надто яскраве або, навпаки, недостатнє світло, також негативно впливає на стан зору та викликає його перевтому [27].

Наслідком тривалого впливу зазначених факторів можуть бути різноманітні порушення здоров’я. Найпоширенішими серед них є порушення зору, зокрема синдром сухого ока та прогресування міопії. Також часто виникають захворювання опорно-рухового апарату, такі як остеохондроз або синдром карпального каналу, що пов’язаний із тривалою роботою з мишею та клавіатурою. Окрім цього, можливий розвиток психологічних розладів, серед яких хронічний стрес, підвищена тривожність та порушення сну, зумовлені змінами добового ритму внаслідок роботи у нічний час.

Фактори ризику, пов’язані з використанням комп’ютерних мереж, суттєво впливають на здоров’я користувачів. Вони включають як фізіологічні, так і психоемоційні аспекти, що вимагають комплексного підходу до їх усунення. Для мінімізації негативних наслідків необхідно дотримуватися низки рекомендацій, які охоплюють організацію робочого місця, раціональний режим роботи, регулярну фізичну активність і підтримку психоемоційного балансу. Зокрема, ефективна ергономіка дозволяє знизити навантаження на опорно-руховий апарат, а перерви та вправи для очей зменшують втому і напруження зору. Крім того, важливо використовувати техніки релаксації для запобігання стресу і організовувати завдання за пріоритетами для уникнення когнітивного перевантаження. Такий інтегрований підхід не лише сприяє збереженню здоров’я користувачів комп’ютерних мереж, але й забезпечує підвищення їхньої продуктивності та загального благополуччя.

ВИСНОВКИ

У даній дипломній роботі було проаналізовано сучасний стан кібербезпеки медичних систем, підкреслено важливість управління ризиками для захисту не лише даних пацієнтів, а й їх життя. Досліджено існуючі підходи до управління ризиками, проведено порівняльний аналіз ризик-орієнтованих та зрілісних моделей. Розглянуто сучасні стратегії кібербезпеки, які застосовуються у медичних інформаційних системах. Визначено, що в існуючих методах управління ризиками відсутні ті, які б інтегрували оцінку шкоди для пацієнта разом із фінансовими аспектами.

З цією метою запропоновано модель оцінки ризиків кібербезпеки медичних інформаційних систем із використанням методу Монте-Карло, яка дозволяє аналізувати різні комбінації заходів захисту з урахуванням їх вартості, ефективності та впливу на ризики. Розроблена модель дозволяє ідентифікувати сценарії, за яких певні комбінації заходів контролю стають надмірними або недостатньо ефективними.

В роботі визначено та описано медичну інформаційну систему як об’єкт моделювання, ідентифіковано ключові загрози та заходи контролю, які відповідають специфіці її функціонування. Було розроблено симуляційну модель оцінювання ризиків, що враховує невизначеність вхідних параметрів, таких як шкода пацієнту, ціна та ефективність контролю, та дозволяє оптимізувати вибір заходів, забезпечуючи баланс між рівнем прийнятного ризику та ресурсами організації.

Програмна реалізація моделі була протестована на двох рівнях прийнятного ризику (низькому на середньому). Проведений аналіз результатів показав, що накопичення заходів контролю не завжди забезпечує ефективність і може бути економічно необґрунтованим. Результати підтвердили, що ефективне управління інформаційною безпекою потребує підбору заходів у взаємодоповнювальні групи, орієнтуючись на баланс між ефективністю та витратами, а не лише на загальну кількість контролів. Визначено, що навіть при наявності достатнього

бюджету, надмірна реалізація заходів не гарантує пропорційного зменшення ризику, і може призводити до неефективного використання ресурсів. Це підтверджує необхідність інтегрованого підходу до планування заходів безпеки, який враховує специфіку загроз та пріоритети організації.

Дослідженню обмеження, пов’язані з недостатністю статистичних даних у сфері кібербезпеки медичних систем та необхідністю застосування експертних оцінок для формування ймовірнісних розподілів. Нестача відкритих даних обмежує точність оцінки ймовірностей, тому результати моделювання слід розглядати як орієнтовні та адаптувати під специфіку конкретної організації.

Розроблена модель дозволяє організаціям приймати обґрунтовані рішення, обираючи параметри на вході моделі відповідно до своїх пріоритетів: баланс між ризиком та витратами, а також набір загроз і заходів контролю, що відповідає їхнім системам та вимогам безпеки. Модель сприяє підвищенню обізнаності керівників про реальні ризики та допомагає формувати більш зважену стратегію кібербезпеки, беручи до увагу не лише фінансові чи репутаційні наслідки кіберризиків, а й вплив на здоров’я та життя пацієнтів. Застосування методу Монте-Карло забезпечує ймовірнісну оцінку ризиків, що дозволяє моделювати невизначеність і варіативність впливу загроз на критичні процеси та безпеку пацієнтів, надаючи організаціям ефективний інструмент для прийняття обґрунтованих рішень щодо інформаційної безпеки.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Yevseiev S., Ponomarenko V., Laptiev O., Milov O., Korol O., Milevskyi S. et. al. Synergy of building cybersecurity systems. Kharkiv: PC TECHNOLOGY CENTER, 2021. 188 p.

2. Gary M. The True Cost of Cybercrime: Why Global Damages Could Reach $1.2 – $1.5 Trillion by End of Year 2025. Cyber Defense Media Group. URL: https://www.cyberdefensemagazine.com/the-true-cost-of-cybercrime-why-global-damages-could-reach-1-2-1-5-trillion-by-end-of-year-2025/.

3. Israelski E. W., Muto W. H. Human Factors Risk Management as a Way to Improve Medical Device Safety: A Case Study of the Therac 25 Radiation Therapy System. The Joint Commission Journal on Quality and Safety. 2004. Vol. 30, no. 12. P. 689–695.

4. Skorenkyy Y., Kozak R., Zagorodna N., Kramar O., Baran, I. Use of augmented reality-enabled prototyping of cyber-physical systems for improving cybersecurity education. Journal of Physics: Conference Series. 2021. Vol. 1840, No. 1.

5. Poster Abstract: Analysis of Cyber-Security Vulnerabilities of Interconnected Medical Devices / Y. Xu et al. 2019 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE), Arlington, VA, USA, 25–27 September 2019. 2019.

6. Development of methodological foundations for designing a classifier of threats to cyberphysical systems / O. Shmatko et al. Eastern-European Journal of Enterprise Technologies. 2020. Vol. 3, no. 9 (105). P. 6–19.

7. The risk-based approach to cybersecurity / J. Boehm et al. McKinsey & Company. URL: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-risk-based-approach-to-cybersecurity.

8. Ревнюк О. А., Загородна Н. В. МЕТОДОЛОГІЯ КІЛЬКІСНОЇ ОЦІНКИ ЗАХИЩЕНОСТІ ВЕБДОДАТКУ ЕЛЕКТРОННОЇ КОМЕРЦІЇ НА ЕТАПІ

ЕКСПЛУАТАЦІЇ. Scientific Bulletin of Ivano-Frankivsk National Technical University of Oil and Gas. 2024. № 2(57). С. 107–119.

9. Lupenko, S., Orobchuk, O., Kateryniuk, I., Kozak, R., & Lypak, H. (2023). Secure information system for Chinese Image medicine knowledge consolidation.

10. Selecting Security and Privacy Controls: Choosing the Right Approach. NIST. URL: https://www.nist.gov/blogs/cybersecurity-insights/selecting-security-and-privacy-controls-choosing-right-approach.

11. Zhang Y., Malacaria P. Dealing with uncertainty in cybersecurity decision support. Computers & Security. 2024. P. 104153.

12. Risk Assessment Uncertainties in Cybersecurity Investments / A. Fielder et al. Games. 2018. Vol. 9, no. 2. P. 34.

13. Fente J., Schexnayder C., Knutson K. Defining a Probability Distribution Function for Construction Simulation. Journal of Construction Engineering and Management. 2000. Vol. 126, no. 3. P. 234–241.

14. Loke C. K., Gan F. F. Joint Monitoring Scheme for Clinical Failures and Predisposed Risks. Quality Technology & Quantitative Management. 2012. Vol. 9, no. 1. P. 3–21.

15. MAGIC: A Method for Assessing Cyber Incidents Occurrence / M. Battaglioni et al. IEEE Access. 2022. P. 1.

16. A Cyber-Security Risk Assessment Methodology for Medical Imaging Devices: the Radiologists' Perspective / T. Mahler et al. Journal of Digital Imaging. 2022.

17. App Development Costs 2025: Complete Pricing Guide & Calculator. Topflight. URL: https://topflightapps.com/ideas/app-development-costs/.

18. Dou M. Principle and Applications of Monte-Carlo Simulation in Forecasting, Algorithm and Health Risk Assessment. Highlights in Science, Engineering and Technology. 2024. Vol. 88. P. 406–414.

19. Van Devender M., McDonald J. T. A Quantitative Risk Assessment Framework for the Cybersecurity of Networked Medical Devices. International Conference on Cyber Warfare and Security. 2023. Vol. 18, no. 1. P. 402–411.

20. Severt M., Casado-Vara R., Martín del Rey A. M. d. A Comparison of Monte Carlo-Based and PINN Parameter Estimation Methods for Malware Identification in IoT Networks. Technologies. 2023. Vol. 11, no. 5. P. 133.

21. Risk Analysis in Healthcare Organizations: Methodological Framework and Critical Variables / G. Pascarella et al. Risk Management and Healthcare Policy. 2021. Volume 14. P. 2897–2911.

22. Orobchuk, O. (2019). Methodology of development and architecture of ontooriented system of electronic learning of Chinese image medicine on the basis of training management system. Вісник Тернопільського національного технічного університету, 92(4), 83-90.

23. Karpinski M., Khoma V., Dudvkevych V., Khoma Y., Sabodashko D. Autoencoder neural networks for outlier correction in ECG-based biometric identification. In 2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS). 2018. P. 210-215.

24. Lupenko, S., Orobchuk, O., & Xu, M. (2019, September). Logical-structural models of verbal, formal and machine-interpreted knowledge representation in Integrative scientific medicine. In Conference on Computer Science and Information Technologies (pp. 139-153).

25. Derkach, M., Matiuk, D., Skarga-Bandurova, I., Biloborodova, T., & Zagorodna, N. (2024, October). A Robust Brain-Computer Interface for Reliable Cognitive State Classification and Device Control. In 2024 14th International Conference on Dependable Systems, Services and Technologies (DESSERT) (pp. 1-9). IEEE.

26. Lechachenko, T., Gancarczyk, T., Lobur, T., & Postoliuk, A. (2023). Cybersecurity Assessments Based on Combining TODIM Method and STRIDE Model for Learning Management Systems. In CITI (pp. 250-256).

27. Matiuk D., Skarga-Bandurova I., Derkach M. (2025) EMG pattern recognition for thumb muscle states using wearable sensing and adaptive neural network. Scientific Journal of TNTU (Tern.), vol 119, no 3, pp. 5–11.

28. Lupenko, S., Tomaszewski, M., Bryniarska, A., Pavlyshyn, A., & Orobchuk, O. (2025). Conceptual modeling of the subject area'Aseptic Wound'for AI-based medical systems.

29. Palamar, A., Palamar, M., & Osukhivska, H. (2023, November). Real-time Health Monitoring Computer System Based on Internet of Medical Things. In ITTAP (pp. 106-115).

30. Babakov, R. M., et al. "Internet of Things for Industry and Human Application. Vol. 3." (2019): 1-917.

31. Zagorodna, N., Skorenkyy, Y., Kunanets, N., Baran, I., & Stadnyk, M. (2022). Augmented Reality Enhanced Learning Tools Development for Cybersecurity Major. In ITTAP (pp. 25-32).

32. Skarga-Bandurova, I., Biloborodova, T., Skarha-Bandurov, I., Boltov, Y., & Derkach, M. (2021). A Multilayer LSTM Auto-Encoder for Fetal ECG Anomaly Detection. Studies in health technology and informatics, 285, 147-152.

33. Про затвердження Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями : Наказ М-ва соц. політики України від 14.02.2018 № 207. URL: https://zakon.rada.gov.ua/laws/show/z0508-18.

34. Про охорону праці : Закон України від 14.10.1992 № 2694-XII : станом на 12 верес. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2694-12.

35. Про затвердження Правил пожежної безпеки в Україні : Наказ М-ва внутр. справ України від 30.12.2014 № 1417 : станом на 14 серп. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/z0252-15.

36. Державний комітет ядерного регулювання України. (2008). Проект консультацій щодо підвищення безпеки джерел іонізуючого випромінювання в Україні. Київ.

37. ISO. (2010). ISO 9241-210:2010. Ergonomics of human-system interaction —Principles and requirements for designing ergonomic systems.

38. Сидоренко, Є. В. (2019). Основи ергономіки та безпеки життєдіяльності. Київ: Наукова думка.

Додаток А – Тези наукової конференції

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

М А Т Е Р І А Л И

XIII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

17-18 грудня 2025 року

ТЕРНОПІЛЬ
2025

Продовження додатку А

УДК 004.056.53
Дарія Косарик, студентка гр. СБмз-61, Руслан Козак, к.т.н., доцент
(Тернопільський національний технічний університет імені Івана Пулюя)

ЗАСТОСУВАННЯ МЕТОДУ МОНТЕ-КАРЛО ДЛЯ МОДЕЛЮВАННЯ КІБЕРЗАГРОЗ У МЕДИЧНИХ СИСТЕМАХ

Dariia Kosaryk, student of gr. СБмз-61, Ruslan Kozak, Ph.D., Assoc. Prof.

APPLICATION OF THE MONTE CARLO METHOD FOR MODELING CYBERTHREATS IN MEDICAL SYSTEMS

Кібербезпека медичних інформаційних систем є критично важливою, адже вона забезпечує не лише захист конфіденційних даних пацієнтів, а й безпосередньо впливає на їхнє життя та здоров'я. Актуальність цієї проблеми стала підґрунтям для проведення дослідження, яке охопило аналіз сучасних підходів до управління ризиками, здійснення порівняльного аналізу ризик-орієнтованих моделей, а також виявлення прогалини у методах, які б поєднували оцінку потенційної шкоди для пацієнта з фінансовими наслідками. Запропоновано модель оцінки ризиків кібербезпеки медичних систем із використанням методу Монте-Карло, яка враховує вартість, ефективність та вплив заходів контролю на рівень ризику, дозволяючи ідентифікувати сценарії надмірної чи недостатньої ефективності заходів.

Ключовим об'єктом моделювання у дослідженні є медична інформаційна система, для якої ідентифіковано основні загрози [1] та відповідні засоби захисту [2]. За допомогою симуляційної моделі враховано невизначеність параметрів, таких як шкода пацієнту, ціна та ефективність засобу, і здійснено оптимізацію вибору засобів захисту, дотримуючи балансу між рівнем прийнятного ризику та ресурсами організації [3].

Випробування програмої реалізація моделі показало, що накопичення контролів не завжди підвищує ефективність і може бути економічно необґрунтованим. Ефективність досягається завдяки формуванню взаємодоповнювальних груп заходів, а не їх кількісному збільшенню. Практичне значення моделі полягає у допомозі організаціям приймати обґрунтовані рішення щодо вибору заходів безпеки, забезпечуючи баланс між ризиком та витратами. Вона підвищує обізнаність керівників про реальні ризики, враховуючи не лише фінансові чи репутаційні наслідки, а й вплив на життя пацієнтів.

Дослідження мало деякі обмеження, пов'язані з недостатністю статистичних даних у сфері кібербезпеки медичних систем та необхідністю застосування експертних оцінок для формування ймовірнісних розподілів. Нестача відкритих даних обмежує точність оцінки ймовірностей, тому результати моделювання варто розглядати як орієнтовні та адаптувати під специфіку конкретної організації чи бізнесу.

Розроблена модель може бути застосована для ймовірнісної оцінки ризиків та оптимізації заходів та засобів захисту в медичних інформаційних системах, а також дає змогу сформувати інтегровані стратегії безпеки, що враховують специфіку загроз, пріоритети організації та критичний вплив на пацієнтів.

Література

1. Xu, Yanchen & Tran, Daniel & Tian, Yuan & Alemzadeh, Homa. (2019). Poster Abstract: Analysis of Cyber-Security Vulnerabilities of Interconnected Medical Devices. 23-24.
2. Almohri, Hussain & Cheng, Long & Yao, Danfeng Daphne & Alemzadeh, Homa. (2017). On Threat Modeling and Mitigation of Medical Cyber-Physical Systems.
3. Aven, Terje & Zio, Enrico. (2013). Foundational Issues in Risk Assessment and Risk Management. Risk analysis : an official publication of the Society for Risk Analysis. 34.

Додаток Б – Список ідентифікованих загроз

ІД	Опис	Ймовірність	Середнє шкоди пацієнта	Дисперсія шкоди пацієнта
Т-1	Зловмисник може видати себе за сенсор, що призведе до надсилання підробленої інформації до мобільного додатку. В результаті, неправдиві дані можуть ввести пацієнту в оману щодо його показників терапії чи призвести до прийняття неправильних рішень щодо лікування.	0.6	0.6	0.02
Т-2	Така загроза виключена, оскільки сенсор є фізичним пристроєм, що не ініціює дії самостійно, і відповідно, не може спростувати факт виконання дії.	0.6	0.85	0.01
Т-3	Зловмисник може видати себе за пристрій-актуатор, що призведе до надсилання мобільному додатку фальшивого підтвердження виконання певної терапевтичної дії, хоча насправді ця дія не була виконана. В результаті, неправидиві дані можуть ввести пацієнта в оману і призвести до прийняття неправильних рішень щодо лікування.	0.55	0.25	0.02
Т-4	Пристрій-актуатор може виконати певну терапевтичну дію, а згодом заперечити її виконання. Це може спричинити втрату довіри до зідйснених терапевтичних дій, ускладнити розслідування інцидентів або виявлення зловмисних дій, а також затримати відновлення належних параметрів лікування.	0.75	0.8	0.015
Т-5	Зловмисник може створити фальшивий мобільний додаток і встановити з'єднання з BLE-пристроями, що дозволяє скомпрометувати будь-які дані, що передаються від або до пристроїв. У результаті, некоректні команди можуть бути надіслані до пристроїв, або пацієнтські дані отримані з пристроїв будуть розкриті.	0.75	0.78	0.02
Т-6	Зловмисник може створити фальшивий мобільний додаток і встановити з'єднання з сервером, що дозволяє скомпрометувати будь-які дані, що передаються між мобільним додатком та сервером. У результаті, можливе несанкціоноване завантаження терапевтичних даних, підміна записів, а також зміна чи витік персольних даних пацієнта.	0.75	0.82	0.02
Т-7	Зловмисник може внести несанкціоновані зміни в мобільний додаток, проінстальований на телефоні, що має увімкнений режим розробника, або ж з підвищеними правами доступу, що дозволяє модифікувати APK/IPA-файл, або вставоляти шкідлвий код, порушуючи цілісність додатку. Зловмисник може керувати інформацією, що показана на екрані пацієнта, або надсилати підроблені команди підключеним пристроям, чи серверу. Це може ввести пацієнта в оману і призвести до прийняття неправильних рішень щодо лікування.	0.55	0.55	0.03
Т-8	Мобільний додаток може автоматично або у фоновому режимі виконувати певні дії, а згодом не залишити доказів їх виконання. Це може спричинити втрату довіри до зідйснених терапевтичних дій, ускладнити розслідування інцидентів, а також затримати відновлення належних параметрів лікування.	0.75	0.7	0.025
Т-9	Зловмисник може інсталювати додаткове програмне забезпечнення з метою перехоплення даних мобільного додатку шляхом створення знімків екрану чи отримання несанкціонованого доступу до внутрішньої пам'яті мобільного додатку. В результаті, терапевтичні дані, пароль пацієнта та внутрішні секрети мобільного додатку можуть бути розкриті.	0.6	0.75	0.03

Продовження додатку Б

T-10	Зловмнисник може запобігти виконання мобільного додатку шляхом зашифрування пристрою програмою-вимагачем, встановленням додаткового програмного забезпечення, що блокуватме додаток від функціонування, або ж блокування BLE, Wi-Fi чи мобільного зв'язку. В результаті, пацієнт не зможе використовувати мобільний додаток, чи мобільний додаток не зможе конумікувати з підключеними пристроями або сервером.	0.6	0.88	0.012
T-11	Мобільний додаток має лише один рівень доступу - звичаного користувача (пацієнт). Відповідно, підвищення привілеїв є неможливим, оскільки в межах додатку відсутні інші ролі або функції з вищими правами доступу.	0.55	0.2	0.02
T-12	Зловмисник може створити підроблений сервер, або перехопити трафік мобільного додатку, видаючи себе за легітимний сервер, що дозволить зломиснику надсилати підроблені чи шкідливі терапевтичні дані мобільному додатку. В результаті користувач може бути введений в оману через неправильні налаштування, що може призвести до прийняття неправильних рішень щодо лікування.	0.725	0.9	0.010
T-13	Сервер може виконати певну дію (таку як передати команду, чи обробити запит), а згодом заперечити її виконання. Це може спричинити втрату довіри до зідйснених дій сервером, ускладнити розслідування інцидентів або виявлення зловмисних дій, а також затримати відновлення належних параметрів системи.	0.75	0.4	0.03
T-14	Зловмисник може модифікувати терапевтичні дані, що передаються від сенсора до мобільного додатку. В результаті, терапевтичні показники можуть бути змінені, що може призвести до неправильних рішень щодо лікування.	0.55	0.5	0.035
T-15	Зловмисник може перехопити BLE-комунікацію між сенсором та мобільним додатком з метою отримання терапевничних показників користувача. В результаті, пацієнтські дані можуть бути розкриті.	0.725	0.92	0.008
T-16	Зловмисник може здійснити атаку відмови в обслуговуванні шляхом заглушення BLE-з'єднання, захоплення BLE-з'єднання, перевантаження сенсора чи телефону BLE-запитами, що може порушити комунікацію між пристроями. В результаті, користувач не зможе приєднатися до сенсору і отримувати терапевтичні показники.	0.75	0.45	0.03
T-17	Зловмисник може модифікувати терапевтичні команди чи налаштування, що передаються від мобільного додатку до сенсора. В результаті, сенсор може виконувати підроблені команди чи мати некоректні налаштування, що може призвести до неправильних рішень щодо лікування.	0.55	0.5	0.035
T-18	Зловмисник може перехопити BLE-комунікацію між сенсором та мобільним додатком з метою отримання команд чи налаштувань пристрою. В результаті,команди чи налаштування сенсору можуть бути розкриті.	0.725	0.88	0.012
T-19	Зловмисник може здійснити атаку відмови в обслуговуванні шляхом заглушення BLE-з'єднання, захоплення BLE-з'єднання, перевантаження сенсора чи телефону BLE-запитами, що може порушити комунікацію між пристроями. Користувач не зможе приєднатися до сенсору, налаштовувати сенсор чи надсилати йому команди.	0.75	0.45	0.03
T-20	Зловмисник може модифікувати відповіді пристрою-актуатора щодо підтвердження здійснених дій чи статусу пристрою, що передаються мобільному додатку. В результаті, пацієнт може отримати підроблені відповіді пристрою-актуатора щодо його стану чи підтверджень виконання дій, що може призвести до неправильних рішень щодо лікування.	0.55	0.5	0.035

Продовження додатку Б

Т-21	Зловмисник може перехопити BLE-комунікацію між пристроєм-актуатором та мобільним додатком з метою отримання відповідей чи статусу пристрою. В результаті, відповіді щодо факту виконання дій пристрою-актуатора чи його статус можуть бути розкриті.	0.725	0.94	0.006
Т-22	Зловмисник може здійснити атаку відмови в обслуговуванні шляхом заглушення BLE-з'єднання, захоплення BLE-з'єднання, перевантаження пристрою-актуатору чи телефону BLE-запитами, що може порушити комунікацію між пристроями. В результаті, користувач не зможе приєднатися до пристрою-актуатора, чи отримувати від нього відповіді та стутс-повідомлення.	0.75	0.45	0.03
Т-23	Зловмисник може модифікувати терапевтичні команди чи налаштування, що передаються від мобільного додатку до пристрою-актуатора. В результаті, сенсор може виконувати підроблені команди чи мати некоректні налаштування, що може призвести до неправильних рішень щодо лікування.	0.55	0.5	0.035
Т-24	Зловмисник може перехопити BLE-комунікацію між пристроєм-актуатором та мобільним додатком з метою отримання команд чи налаштувань пристрою. В результаті,команди чи налаштування пристрою-актуатора можуть бути розкриті.	0.725	0.9	0.01
Т-25	Зловмисник може здійснити атаку відмови в обслуговуванні шляхом заглушення BLE-з'єднання, захоплення BLE-з'єднання, перевантаження пристрою-актуатору чи телефону BLE-запитами, що може порушити комунікацію між пристроями. В результаті, користувач не зможе приєднатися до пристрою-актуатору, налаштовувати його чи надсилати команди.	0.75	0.55	0.03
Т-26	Зловмисник може модифікувати відповіді сервера до мобільного додатку, що може призвести до надсилання мобільному додатку неправильних відповідей чи команд сервера. В результаті, це може призвести до неправильних рішень щодо лікування.	0.55	0.6	0.035
Т-27	Зловмисник може перехопити комунцікацію між мобільним додатком та сервером з метою отримання відповідей чи команд, що сервер надсилає мобільному додатку. В результататі, відповіді сервера та команди можуть бути розкиті.	0.725	0.85	0.02
Т-28	Зловмисник може заглушити Wi-Fi мережу між мобільним додатком та сервером, що може порушити комункацію між ними. В результаті, сервер не зможе надсилати відповіді та команди до мобільного додатку.	0.75	0.5	0.03
Т-29	Зловмисник може модифікувати терапевтичні дані пацієнта надіслані від мобільного додатку, що може призвести до надсилання серверу неправильної інформації. В результаті, це може призвести до неправильних рішень щодо лікування.	0.55	0.55	0.035
Т-30	Зловмисник може перехопити комунцікацію між мобільним додатком та сервером з метою отримання терапевтичних даних пацієнта, що надсилаються на обробку та зберігання серверу. В результататі,пацієнтські дані можуть бути розкиті.	0.6	0.6	0.02
Т-31	Зловмисник може заглушити Wi-Fi мережу між мобільним додатком та сервером, що може порушити комункацію між ними. В результаті, мобільний додаток не зможе надсилати терапевтичні дані пацієнта серверу.	0.6	0.85	0.01

Додаток В – Список ідентифікованих заходів захисту

ІД	Опис	Мін. вартість	Макс. вартість	Середня ефективн.	Дисперсія ефективн.
М-1	Мобільний додаток має здійснювати автентифікацію шляхом використання криптографічних методів, таких як унікальні серійні номери, для підтвердження їх достовірності.	500.00	6250.00	0.9	0.05
М-2	Мобільний додаток має здійснювати журналювання усіх терапевтичних подій, здійснених у фоновому режимі, ініційованих користувачем та підключеними пристроями.	375.00	2813.00	0.85	0.01
М-3	Мобільний додаток має забезпечити безпечне зберігання журналів подій.	1250.00	11250.00	0.88	0.008
М-4	Канал комунікації з BLE-пристроями має бути зашифрований з використанням AES-128.	338.00	2038.00	0.85	0.01
М-5	Мобільний додаток має підтримувати механізми атестації програмного забезпечення(такі як DeviceCheck(iOS), Google Play Integrity API (Android)) для підтвердження своєї автентичності.	590.00	6325.00	0.8	0.02
М-6	Мобільний додаток повинен автентифікувати сервер перед встановленням з'єднання шляхом перевірки дійсності сертифіката.	130.00	3249.00	0.92	0.004
М-7	Весь трафік що, передається при комунікації з сервером, повинен шифруватися за допомогою TLS v1.3.	364.00	7000.00	0.95	0.002
М-8	Мобільний додаток повинен забороняти користувачу його використання, якщо телефон має підвищені права доступу (rooted(Android)/jailbroken(iOS)).	750.00	3440.00	0.8	0.02
М-9	Мобільний додаток повинен перевіряти свою цілісність до запуску і блокувати виконання у разі виявлення змін.	1000.00	5315.00	0.82	0.02
М-10	Вихідний код мобільного додатку має бути обфусковано для ускладнення реверс-інжинірингу та зміни логіки додатку.	300.00	1625.00	0.65	0.03
М-11	Мобільний додаток повинен реалізовувати механізми виявлення спроб втручання в процесі виконання і блокування під час виявлення змін	625.00	4065.00	0.7	0.03
М-12	Мобільний додаток повинен блокувати виконання, якщо на пристрої не встановлений пароль блокування екрану.	50.00	1625.00	0.78	0.02
М-13	Мобільний додаток повинен сповіщати користувача, коли Wi-Fi з'єднання, або мобільний зв'язок відсутній.	100.00	3250.00	0.6	0.04
М-14	Мобільний додаток повинен показувати стан підключення BLE-пристроїв.	150.00	3000.00	0.75	0.02

Додаток Г – Лістинг файлу risk_assessment.py

```
import pandas as pd
import numpy as np
from scipy.stats import beta, norm
from itertools import chain, combinations
import matplotlib.pyplot as plt
from mpl_toolkits.mplot3d import Axes3D
def read_threat_data(file_path, sheet_name='Threats'):
    df = pd.read_excel(file_path, sheet_name=sheet_name)
    df.replace('-', np.nan, inplace=True)
    df['Likelyhood']       =       pd.to_numeric(df['Likelyhood'],
errors='coerce')
    df['Harm    mean']     =     pd.to_numeric(df['Harm    mean'],
errors='coerce')
    df['Harm   varience']   =   pd.to_numeric(df['Harm   varience'],
errors='coerce')return df
def read_mitigation_data(file_path, sheet_name='Mitigations'):
    df = pd.read_excel(file_path, sheet_name=sheet_name)
    df.replace('-', np.nan, inplace=True)
    df['Cost min'] = pd.to_numeric(df['Cost min'], errors='coerce')
    df['Cost max'] = pd.to_numeric(df['Cost max'], errors='coerce')
    df['Effectiveness   mean']   =   pd.to_numeric(df['Effectiveness
mean'], errors='coerce')
    df['Effectiveness varience'] = pd.to_numeric(df['Effectiveness
varience'], errors='coerce') z_95 = norm.ppf(0.95)
    df['Cost  sigma'] = (np.log(df['Cost  max']) - np.log(df['Cost
min'])) / (2 * z_95)
    df['Cost mu'] = np.log(df['Cost min']) + df['Cost sigma'] * z_95
    return df
def read_mapping_data(file_path, sheet_name='Mapping'):
    df = pd.read_excel(file_path, sheet_name=sheet_name)
    df.replace('-', np.nan, inplace=True)
    return df
def threat_to_mitigations_map(mapping_df):
```

Продовження додатку Г

```
return
mapping_df.groupby('Threat')['Mitigation'].apply(list).to_dict()

def beta_params(mu, var):

    if pd.isna(mu) or pd.isna(var) or mu <= 0 or mu >= 1 or var <=
0:

        return np.nan, np.nan

    common_term = (mu * (1 - mu)) / var - 1

    alpha = mu * common_term

    beta_param = (1 - mu) * common_term

    return alpha, beta_param

def add_beta_parameters(df, mean_col, var_col, prefix):

    df[[f'{prefix} Alpha', f'{prefix} Beta']] = df.apply(lambda row:
pd.Series(beta_params(row[mean_col], row[var_col])),axis=1)

    return df

def sample_beta(row, alpha_col, beta_col):

    alpha = row[alpha_col]

    beta_val = row[beta_col]

    if pd.isna(alpha) or pd.isna(beta_val) or alpha <= 0 or beta_val
<= 0:

        return np.nan

    return beta.rvs(alpha, beta_val)

def add_beta_samples(df, alpha_col, beta_col, sample_col):

    df[sample_col]   =   df.apply(lambda   row:   sample_beta(row,
alpha_col, beta_col), axis=1)

    return df

def sample_lognormal_cost(row):

    mu = row['Cost mu']

    sigma = row['Cost sigma']

    if pd.isna(mu) or pd.isna(sigma) or sigma <= 0:

        return np.nan

    return np.random.lognormal(mean=mu, sigma=sigma)

def add_lognormal_cost_samples(df, sample_col='Sampled Cost'):

    df[sample_col] = df.apply(sample_lognormal_cost, axis=1)

    return df
```

Продовження додатку Г

```
def all_mitigation_subsets(mitigation_ids):
    return list(chain.from_iterable(combinations(mitigation_ids, r)
for r in range(len(mitigation_ids) + 1)))
def classify_risk_level(risk, threshold):
    percent = risk / threshold
    if percent < 0.1:
        return 'low'
    elif percent < 0.3:
        return 'low-medium'
    elif percent < 0.5:
        return 'medium'
    elif percent < 0.7:
        return 'medium-high'
    else:
        return 'high'
def calculate_residual_risk(threats_df, mitigations_df, threat_map,
selected_mitigations, threshold):
    effectiveness_lookup = mitigations_df.set_index('ID')['Sampled
Effectiveness'].to_dict()
    results = []
    for _, threat in threats_df.iterrows():
        threat_id = threat['ID']
        L_i = threat['Likelyhood']
        H_i = threat['Sampled Harm']
        mapped_mitigations = threat_map.get(threat_id, [])
        active_mitigations = [m for m in mapped_mitigations if m in
selected_mitigations]
        mitigation_factor = 1.0
        for m_id in active_mitigations:
            E_j = effectiveness_lookup.get(m_id, 0)
            mitigation_factor *= (1 - E_j)
        R_res = L_i * mitigation_factor * H_i
        if R_res > threshold:
            return None
```

Продовження додатку Г

```
results.append({ 'Threat ID': threat_id, 'Likelyhood': round(L_i, 3), 'Sampled Harm': round(H_i, 3), 'Residual Risk': round(R_res, 3) })

    return results

def plot_rsi_3d_surface(df):

    fig = plt.figure(figsize=(10, 7))

    ax = fig.add_subplot(111, projection='3d')

    x = df['Total Cost']

    y = df['Total Risk']

    z = df['RSI']

    surf = ax.plot_trisurf(x, y, z, cmap='viridis', edgecolor='none', alpha=0.8)

    ax.scatter(x, y, z, color='black', s=20, alpha=1.0, label='Mitigation Sets')

    for i in range(len(df)):

        ax.text(x[i], y[i], z[i] + 0.03, str(df.loc[i, 'Index']), fontsize=8, ha='center', va='bottom')

    ax.set_xlabel('Total Cost')

    ax.set_ylabel('Total Risk')

    ax.set_zlabel('RSI')

    ax.set_title('3D Surface: RSI vs Cost and Risk')

    fig.colorbar(surf, ax=ax, shrink=0.5, aspect=10, label='RSI')

    ax.view_init(elev=40, azim=-135)

    plt.tight_layout()

    plt.show()

def monte_carlo_simulation(file_path, threshold, output_csv):

    threats_df = read_threat_data(file_path)

    mitigations_df = read_mitigation_data(file_path)

    mapping_df = read_mapping_data(file_path)

    threat_map = threat_to_mitigations_map(mapping_df)

    threats_df = add_beta_parameters(threats_df, 'Harm mean', 'Harm varience', 'Harm')

    mitigations_df = add_beta_parameters(mitigations_df, 'Effectiveness mean', 'Effectiveness varience', 'Effectiveness')

    mitigation_ids = mitigations_df['ID'].dropna().tolist()
```

Продовження додатку Г

```
 subsets = all_mitigation_subsets(mitigation_ids)
    output_rows = []
    summary_rows = []
    total_simulations = 0
    successful_simulations = 0
    for subset in subsets:
        total_simulations += 1
        sampled_threats = add_beta_samples(threats_df.copy(), 'Harm
Alpha', 'Harm Beta', 'Sampled Harm')
        sampled_mitigations                                        =
add_beta_samples(mitigations_df.copy(),   'Effectiveness   Alpha',
'Effectiveness Beta', 'Sampled Effectiveness')
        sampled_mitigations                                        =
add_lognormal_cost_samples(sampled_mitigations, 'Sampled Cost')
        residuals    =    calculate_residual_risk(sampled_threats,
sampled_mitigations, threat_map, subset, threshold)
        if residuals is not None:
            successful_simulations += 1
            subset_str = ', '.join(str(m) for m in subset) if subset
else 'None'
            total_cost                                             =
sampled_mitigations[sampled_mitigations['ID'].isin(subset)]['Sampl
ed Cost'].sum()
            total_risk = sum(r['Residual Risk'] for r in residuals)
            risk_levels = {'low': 0, 'low-medium': 0, 'medium': 0,
'medium-high': 0, 'high': 0}
            for r in residuals:
                level  =  classify_risk_level(r['Residual  Risk'],
threshold)
                risk_levels[level] += 1
            lambda_weights   =   {'low':   0.1,'low-medium':   0.3,
'medium': 0.5,  'medium-high': 0.7, 'high': 0.9 }
            rsi = sum(lambda_weights[level] * count for level, count
in risk_levels.items())
            summary_rows.append({  'Index': successful_simulations,
'Mitigation Subset': subset_str,  'Total Cost': round(total_cost,
2), 'Total Risk': round(total_risk, 3), 'RSI': round(rsi, 3), 'Risk
Breakdown':  risk_levels,  'Mitigations':  subset,    'Threats':
residuals })
```

Продовження додатку Г

```
   for m_id in subset:

                m_row                                                    =
sampled_mitigations[sampled_mitigations['ID'] == m_id].iloc[0]

                output_rows.append({'Simulation              Index':
successful_simulations,'Mitigation   Subset':   subset_str,'Type':
'Mitigation','ID':          m_id,'Sampled          Effectiveness':
round(m_row['Sampled    Effectiveness'],    3),'Sampled    Cost':
round(m_row['Sampled  Cost'],  2),'Likelyhood':  '','Sampled  Harm':
'','Residual Risk': ''})

            for row in residuals:

                level  =  classify_risk_level(row['Residual  Risk'],
threshold)

                output_rows.append({'Simulation              Index':
successful_simulations,  'Mitigation  Subset':  subset_str,'Type':
'Threat','ID':   row['Threat   ID'],   'Sampled   Effectiveness':
'','Sampled  Cost':  '','Likelyhood':  row['Likelyhood'],'Sampled
Harm':   row['Sampled   Harm'],'Residual   Risk':   row['Residual
Risk'],'Risk Level': level})

    pd.DataFrame(output_rows).to_csv(output_csv, index=False)

    summary_df  =  pd.DataFrame([{'Index':  row['Index'],'Mitigation
Subset': row['Mitigation Subset'],'Total Cost': row['Total Cost'],
'Total  Risk':  row['Total  Risk'],  'RSI':  row['RSI'],'Low  Risk':
row['Risk    Breakdown']['low'],'Low-Medium    Risk':    row['Risk
Breakdown']['low-medium'],      'Medium      Risk':      row['Risk
Breakdown']['medium'],'Medium-High         Risk':         row['Risk
Breakdown']['medium-high'],'High          Risk':          row['Risk
Breakdown']['high'] } for row in summary_rows])

    summary_df.to_csv('simulation_summary.csv', index=False)

    print("\nРезультати симуляції")

    print(f"Загальна       кількість       наборів       контролів:
{total_simulations}")

    print(f"Прийнятні набори контролів: {successful_simulations}")

    for row in summary_rows:

        print(f"\n--- Прийнятний набір контролів №{row['Index']} --
-")

        print(f"Множина контролів: {row['Mitigation Subset']}")

        print(f"Значення загальної вартості: {row['Total Cost']}")

        print(f"Значення загального ризику: {row['Total Risk']}")

        print(f"RSI: {row['RSI']}")

        print("Категорії ризиків у поточному наборі контролів:")
```

Продовження додатку Г

```
 print(f"  - Низький: {row['Risk Breakdown']['low']}")
        print(f"  - Нижче середнього: {row['Risk Breakdown']['low-
medium']}")
        print(f"  - Середній: {row['Risk Breakdown']['medium']}")
        print(f"  - Вище середнього: {row['Risk Breakdown']['medium-
high']}")
        print(f"  - Високий: {row['Risk Breakdown']['high']}")
        print("Загрози:")
        for t in row['Threats']:
            print(f"  - Загроза {t['Threat ID']}: Залишковий ризик
= {t['Residual Risk']}")
    decision_table = []
    for row in summary_rows:
        breakdown = row['Risk Breakdown']
        decision_table.append({'Номер набору контролів':
row['Index'],'Значення загальної вартості': row['Total Cost'],
'Значення загального ризику': row['Total Risk'], 'RSI': row['RSI'],
'Низький': breakdown['low'],'Нижче середнього': breakdown['low-
medium'],'Середній': breakdown['medium'], 'Вище середнього':
breakdown['medium-high'], 'Високий': breakdown['high'] })
    decision_df = pd.DataFrame(decision_table)
    if decision_df.empty:
        return
    decision_df_sorted                                          =
decision_df.sort_values(by='RSI').reset_index(drop=True)
    decision_df_sorted.to_csv('rsi_decision_table.csv',
index=False)
    print("\nОптимальні набори контролів")
    if decision_df_sorted.empty:
        print("Немає прийнятних наборів контролів.")
    else:
        print(decision_df_sorted.iloc[:5].to_string(index=False))
        decision_df_sorted = decision_df_sorted.rename(columns={
        'Номер набору контролів': 'Index',
        'Значення загальної вартості': 'Total Cost',
        'Значення загального ризику': 'Total Risk'})
```

Продовження додатку Г

```
  if len(decision_df_sorted) < 3:
            pass
        else:
            plot_rsi_3d_surface(decision_df_sorted)
if __name__ == "__main__":
    file_path = 'ThreatsMitigations_v1.xlsx'
    threshold = 0.07
    output_csv = 'residual_risk_detailed_low.csv'
    print("Запуск симуляції: Низький рівень прийнятного ризику")
    monte_carlo_simulation(file_path, threshold, output_csv)
    threshold = 0.27
    output_csv = 'residual_risk_detailed_medium.csv'
    print("Запуск симуляції: Середній рівень прийнятного ризику")
    monte_carlo_simulation(file_path, threshold, output_csv)
```

Додаток Д – Результати симуляції

№	Комбінація заходів контролю	Вартість	Ризик	RSI
1	M-1, M-2, M-4, M-6, M-7, M-8, M-13, M-14	13641.73	1.319	7.3
2	M-1, M-3, M-4, M-6, M-7, M-8, M-11, M-14	8911.1	1.106	6.7
3	M-1, M-3, M-4, M-6, M-7, M-8, M-13, M-14	10186.62	0.784	5.5
4	M-1, M-4, M-6, M-7, M-11, M-12, M-13, M-14	9237.12	1.323	7.7
5	M-1, M-2, M-3, M-4, M-6, M-7, M-8, M-9, M-14	16372.64	1.343	7.7
6	M-1, M-2, M-3, M-4, M-6, M-7, M-8, M-13, M-14	18673.48	1.223	6.9
7	M-1, M-2, M-3, M-4, M-6, M-7, M-10, M-12, M-14	9051.81	1.145	7.1
8	M-1, M-2, M-4, M-5, M-6, M-7, M-8, M-13, M-14	12917.76	1.212	7.1
9	M-1, M-2, M-4, M-5, M-6, M-7, M-9, M-12, M-13	12867.71	1.522	7.7
10	M-1, M-2, M-4, M-6, M-7, M-8, M-9, M-13, M-14	11169.81	1.842	9.7
11	M-1, M-2, M-4, M-6, M-7, M-8, M-10, M-13, M-14	8550.54	1.909	10.3
12	M-1, M-2, M-4, M-6, M-7, M-8, M-11, M-13, M-14	15054.33	1.379	7.9
13	M-1, M-2, M-4, M-6, M-7, M-8, M-12, M-13, M-14	12492.56	1.124	7.1
14	M-1, M-2, M-4, M-6, M-7, M-9, M-10, M-12, M-14	12179.37	1.407	8.1
15	M-1, M-2, M-4, M-6, M-7, M-9, M-12, M-13, M-14	13631.98	1.885	9.7
16	M-1, M-2, M-4, M-6, M-7, M-10, M-12, M-13, M-14	9539.35	1.582	8.5
17	M-1, M-2, M-4, M-6, M-7, M-11, M-12, M-13, M-14	7422.93	1.202	7.1
18	M-1, M-3, M-4, M-5, M-6, M-7, M-8, M-11, M-14	16750.85	1.094	6.5
19	M-1, M-3, M-4, M-5, M-6, M-7, M-8, M-13, M-14	15182.51	1.37	7.9
20	M-1, M-3, M-4, M-5, M-6, M-7, M-9, M-12, M-14	15011.36	1.905	9.9
21	M-1, M-3, M-4, M-6, M-7, M-8, M-9, M-13, M-14	25201.4	1.41	7.5
22	M-1, M-3, M-4, M-6, M-7, M-8, M-10, M-13, M-14	12486.9	1.822	9.7
23	M-1, M-3, M-4, M-6, M-7, M-8, M-11, M-13, M-14	13409.82	1.336	7.5
24	M-1, M-3, M-4, M-6, M-7, M-8, M-12, M-13, M-14	19350.49	1.38	7.9
25	M-1, M-3, M-4, M-6, M-7, M-10, M-11, M-12, M-14	15639.98	1.986	10.7
26	M-1, M-4, M-5, M-6, M-7, M-8, M-10, M-13, M-14	25492	1.361	7.7
27	M-1, M-4, M-5, M-6, M-7, M-9, M-12, M-13, M-14	7752.88	1.698	8.5
28	M-1, M-4, M-6, M-7, M-9, M-10, M-12, M-13, M-14	7952.8	1.483	7.7
29	M-1, M-2, M-3, M-4, M-6, M-7, M-8, M-9, M-10, M-14	14452.25	1.424	7.7
30	M-1, M-2, M-3, M-4, M-6, M-7, M-8, M-9, M-13, M-14	19777.64	1.413	7.9
31	M-1, M-2, M-3, M-4, M-6, M-7, M-8, M-11, M-13, M-14	13041.93	0.815	5.9
32	M-1, M-2, M-3, M-4, M-6, M-7, M-8, M-12, M-13, M-14	16568.41	1.256	6.9
33	M-1, M-2, M-3, M-4, M-6, M-7, M-10, M-12, M-13, M-14	48524.72	0.9	5.3
34	M-1, M-2, M-3, M-4, M-6, M-7, M-11, M-12, M-13, M-14	10889.67	2.063	9.9
35	M-1, M-2, M-4, M-5, M-6, M-7, M-8, M-9, M-13, M-14	18107.08	1.378	7.9
36	M-1, M-2, M-4, M-5, M-6, M-7, M-8, M-10, M-12, M-14	18490.89	1.456	7.7
37	M-1, M-2, M-4, M-5, M-6, M-7, M-8, M-10, M-13, M-14	12857.36	2.079	10.5
38	M-1, M-2, M-4, M-5, M-6, M-7, M-8, M-11, M-13, M-14	18957.26	2.145	10.1
39	M-1, M-2, M-4, M-5, M-6, M-7, M-8, M-12, M-13, M-14	13134.86	1.113	6.9
40	M-1, M-2, M-4, M-5, M-6, M-7, M-9, M-12, M-13, M-14	9929.93	1.721	9.1
41	M-1, M-2, M-4, M-5, M-6, M-7, M-10, M-12, M-13, M-14	9507.17	1.602	8.5
42	M-1, M-2, M-4, M-6, M-7, M-8, M-9, M-10, M-13, M-14	15705.88	0.718	5.3
43	M-1, M-2, M-4, M-6, M-7, M-8, M-10, M-11, M-12, M-14	13460.46	1.194	7.5

Продовження додатку Д

44	M-1, M-2, M-4, M-6, M-7, M-8, M-10, M-11, M-13, M-14	16292.95	1.738	8.7
45	M-1, M-2, M-4, M-6, M-7, M-8, M-10, M-12, M-13, M-14	13737.75	2.087	10.7
46	M-1, M-2, M-4, M-6, M-7, M-8, M-11, M-12, M-13, M-14	16512.28	0.791	5.1
47	M-1, M-2, M-4, M-6, M-7, M-9, M-10, M-12, M-13, M-14	8247.04	1.288	7.3
48	M-1, M-2, M-4, M-6, M-7, M-9, M-11, M-12, M-13, M-14	14408.68	1.562	8.9
49	M-1, M-2, M-4, M-6, M-7, M-10, M-11, M-12, M-13, M-14	10096.38	1.532	8.1
50	M-1, M-3, M-4, M-5, M-6, M-7, M-8, M-9, M-10, M-13	19682.93	1.361	7.7
51	M-1, M-3, M-4, M-5, M-6, M-7, M-8, M-9, M-11, M-14	24045.91	1.659	8.9
52	M-1, M-3, M-4, M-5, M-6, M-7, M-8, M-9, M-12, M-13	27102.25	1.216	6.9
53	M-1, M-3, M-4, M-5, M-6, M-7, M-8, M-11, M-13, M-14	20255.93	0.715	5.3
54	M-1, M-3, M-4, M-5, M-6, M-7, M-8, M-12, M-13, M-14	19351.48	1.171	7.1
55	M-1, M-3, M-4, M-5, M-6, M-7, M-9, M-12, M-13, M-14	17151.61	1.785	9.5
56	M-1, M-3, M-4, M-5, M-6, M-7, M-10, M-11, M-12, M-14	14930.06	1.624	8.5
57	M-1, M-3, M-4, M-6, M-7, M-8, M-9, M-10, M-11, M-14	18995.22	1.752	9.1
58	M-1, M-3, M-4, M-6, M-7, M-8, M-9, M-10, M-13, M-14	21192.73	0.734	5.1
59	M-1, M-3, M-4, M-6, M-7, M-8, M-9, M-11, M-13, M-14	20436.17	1.652	9.3
60	M-1, M-3, M-4, M-6, M-7, M-8, M-9, M-12, M-13, M-14	22415.44	1.624	8.9
61	M-1, M-3, M-4, M-6, M-7, M-8, M-10, M-11, M-13, M-14	13796.93	1.885	9.5
62	M-1, M-3, M-4, M-6, M-7, M-8, M-10, M-12, M-13, M-14	17227.87	1.486	8.3
63	M-1, M-3, M-4, M-6, M-7, M-8, M-11, M-12, M-13, M-14	14669.21	0.843	5.9
64	M-1, M-3, M-4, M-6, M-7, M-9, M-10, M-11, M-12, M-14	17070.08	2.013	10.1
65	M-1, M-3, M-4, M-6, M-7, M-9, M-10, M-12, M-13, M-14	14184.8	1.41	8.1
66	M-1, M-3, M-4, M-6, M-7, M-9, M-11, M-12, M-13, M-14	20418.05	1.379	7.7
67	M-1, M-3, M-4, M-6, M-7, M-10, M-11, M-12, M-13, M-14	16762.33	2.137	9.9
68	M-1, M-4, M-5, M-6, M-7, M-8, M-10, M-11, M-13, M-14	15880.55	2.406	11.9
69	M-1, M-4, M-5, M-6, M-7, M-8, M-11, M-12, M-13, M-14	18457.27	3.298	14.5
70	M-1, M-4, M-5, M-6, M-7, M-9, M-10, M-11, M-12, M-14	19640.9	2.035	9.9
71	M-1, M-4, M-6, M-7, M-8, M-9, M-10, M-12, M-13, M-14	14876.08	1.289	7.3
72	M-1, M-4, M-6, M-7, M-8, M-9, M-11, M-12, M-13, M-14	11173.87	1.275	7.7
73	M-1, M-2, M-3, M-4, M-5, M-6, M-7, M-8, M-10, M-13, M-14	19139.89	1.572	8.5
74	M-1, M-2, M-3, M-4, M-5, M-6, M-7, M-8, M-11, M-12, M-14	26367.58	1.255	7.1
75	M-1, M-2, M-3, M-4, M-5, M-6, M-7, M-8, M-11, M-13, M-14	15322.75	0.836	5.5
76	M-1, M-2, M-3, M-4, M-5, M-6, M-7, M-8, M-12, M-13, M-14	22386.13	1.652	9.1
77	M-1, M-2, M-3, M-4, M-5, M-6, M-7, M-9, M-12, M-13, M-14	23325.45	1.32	7.9
78	M-1, M-2, M-3, M-4, M-5, M-6, M-7, M-10, M-12, M-13, M-14	12461.28	1.406	7.7
79	M-1, M-2, M-3, M-4, M-6, M-7, M-8, M-9, M-11, M-13, M-14	13724.61	1.294	7.7
80	M-1, M-2, M-3, M-4, M-6, M-7, M-8, M-9, M-12, M-13, M-14	14057.01	1.13	6.1
81	M-1, M-2, M-3, M-4, M-6, M-7, M-8, M-11, M-12, M-13, M-14	11255.63	1.822	9.9
82	M-1, M-2, M-3, M-4, M-6, M-7, M-9, M-11, M-12, M-13, M-14	17713.75	1.559	8.9
83	M-1, M-2, M-3, M-4, M-6, M-7, M-10, M-11, M-12, M-13, M-14	21285.89	2.035	10.1
84	M-1, M-2, M-4, M-5, M-6, M-7, M-8, M-9, M-11, M-12, M-14	21909.25	1.701	8.9
85	M-1, M-2, M-4, M-5, M-6, M-7, M-8, M-9, M-11, M-13, M-14	22185.71	1.483	8.3
86	M-1, M-2, M-4, M-5, M-6, M-7, M-8, M-9, M-12, M-13, M-14	27999.43	1.414	7.7
87	M-1, M-2, M-4, M-5, M-6, M-7, M-8, M-10, M-11, M-13, M-14	16590.84	1.207	6.9
88	M-1, M-2, M-4, M-5, M-6, M-7, M-8, M-11, M-12, M-13, M-14	14747.65	1.463	7.9
89	M-1, M-2, M-4, M-5, M-6, M-7, M-9, M-10, M-12, M-13, M-14	13939.27	0.695	4.9

Продовження додатку Д

90	M-1, M-2, M-4, M-5, M-6, M-7, M-9, M-11, M-12, M-13, M-14	14741.05	1.737	8.7
91	M-1, M-2, M-4, M-6, M-7, M-8, M-9, M-10, M-11, M-13, M-14	19501.88	1.658	9.1
92	M-1, M-2, M-4, M-6, M-7, M-8, M-9, M-10, M-12, M-13, M-14	14630.73	1.222	6.9
93	M-1, M-2, M-4, M-6, M-7, M-9, M-10, M-11, M-12, M-13, M-14	15721.6	1.051	6.7
94	M-1, M-3, M-4, M-5, M-6, M-7, M-8, M-9, M-10, M-13, M-14	20071.16	1.129	7.1
95	M-1, M-3, M-4, M-5, M-6, M-7, M-8, M-9, M-11, M-13, M-14	27811.65	0.975	6.7
96	M-1, M-3, M-4, M-5, M-6, M-7, M-8, M-9, M-12, M-13, M-14	17445.79	0.876	6.1
97	M-1, M-3, M-4, M-5, M-6, M-7, M-8, M-10, M-11, M-12, M-13	20097.43	1.654	8.3
98	M-1, M-3, M-4, M-5, M-6, M-7, M-8, M-10, M-11, M-13, M-14	22786.49	1.322	7.9
99	M-1, M-3, M-4, M-5, M-6, M-7, M-8, M-10, M-12, M-13, M-14	27612.13	1.707	9.1
100	M-1, M-3, M-4, M-5, M-6, M-7, M-8, M-11, M-12, M-13, M-14	22655.09	0.838	5.9
101	M-1, M-3, M-4, M-5, M-6, M-7, M-9, M-10, M-12, M-13, M-14	12166.36	1.489	7.9
102	M-1, M-3, M-4, M-5, M-6, M-7, M-10, M-11, M-12, M-13, M-14	35711.87	1.622	8.7
103	M-1, M-3, M-4, M-6, M-7, M-8, M-9, M-10, M-11, M-12, M-14	16777.9	0.85	5.5
104	M-1, M-3, M-4, M-6, M-7, M-8, M-9, M-10, M-11, M-13, M-14	15430.39	1.414	8.3
105	M-1, M-3, M-4, M-6, M-7, M-8, M-9, M-10, M-12, M-13, M-14	18678.16	1.425	7.9
106	M-1, M-3, M-4, M-6, M-7, M-8, M-9, M-11, M-12, M-13, M-14	38804.96	1.512	7.9
107	M-1, M-3, M-4, M-6, M-7, M-8, M-10, M-11, M-12, M-13, M-14	15474.28	1.379	7.7
108	M-1, M-3, M-4, M-6, M-7, M-9, M-10, M-11, M-12, M-13, M-14	15262.89	0.902	5.9
109	M-1, M-4, M-5, M-6, M-7, M-8, M-10, M-11, M-12, M-13, M-14	23211.69	1.235	6.9
110	M-1, M-4, M-6, M-7, M-8, M-9, M-10, M-11, M-12, M-13, M-14	16624.67	2.096	10.5
111	M-1, M-2, M-3, M-4, M-5, M-6, M-7, M-8, M-9, M-10, M-13, M-14	18489.58	1.017	6.7
112	M-1, M-2, M-3, M-4, M-5, M-6, M-7, M-8, M-9, M-11, M-13, M-14	30446	0.905	5.5
113	M-1, M-2, M-3, M-4, M-5, M-6, M-7, M-8, M-9, M-12, M-13, M-14	26848.1	0.862	5.9
114	M-1, M-2, M-3, M-4, M-5, M-6, M-7, M-9, M-10, M-12, M-13, M-14	18720.82	1.752	9.1
115	M-1, M-2, M-3, M-4, M-5, M-6, M-7, M-9, M-11, M-12, M-13, M-14	32763.29	1.195	6.9
116	M-1, M-2, M-3, M-4, M-5, M-6, M-7, M-10, M-11, M-12, M-13, M-14	18769.12	1.802	9.9
117	M-1, M-2, M-3, M-4, M-6, M-7, M-8, M-9, M-10, M-11, M-13, M-14	14264.14	1.495	8.9
118	M-1, M-2, M-3, M-4, M-6, M-7, M-8, M-10, M-11, M-12, M-13, M-14	24224.46	0.777	5.7
119	M-1, M-2, M-4, M-5, M-6, M-7, M-8, M-9, M-10, M-11, M-13, M-14	17862.99	1.704	9.3
120	M-1, M-2, M-4, M-5, M-6, M-7, M-8, M-9, M-10, M-12, M-13, M-14	25078.7	1.112	6.5
121	M-1, M-2, M-4, M-5, M-6, M-7, M-8, M-9, M-11, M-12, M-13, M-14	16822.61	0.917	6.1
122	M-1, M-2, M-4, M-5, M-6, M-7, M-8, M-10, M-11, M-12, M-13, M-14	18230.51	1.232	6.5
123	M-1, M-2, M-4, M-5, M-6, M-7, M-9, M-10, M-11, M-12, M-13, M-14	23088.03	1.528	8.3
124	M-1, M-3, M-4, M-5, M-6, M-7, M-8, M-9, M-10, M-11, M-13, M-14	19409.64	1.586	8.5

Продовження додатку Д

125	M-1, M-3, M-4, M-5, M-6, M-7, M-8, M-9, M-10, M-12, M-13, M-14	30877.89	1.204	7.5
126	M-1, M-3, M-4, M-5, M-6, M-7, M-8, M-10, M-11, M-12, M-13, M-14	21444.26	1.429	8.3
127	M-1, M-3, M-4, M-5, M-6, M-7, M-9, M-10, M-11, M-12, M-13, M-14	21525.5	2.098	10.1
128	M-1, M-3, M-4, M-6, M-7, M-8, M-9, M-10, M-11, M-12, M-13, M-14	23669.79	1.371	7.5
129	M-1, M-2, M-3, M-4, M-5, M-6, M-7, M-8, M-9, M-10, M-12, M-13, M-14	23730.82	0.743	5.5
130	M-1, M-2, M-3, M-4, M-5, M-6, M-7, M-8, M-9, M-11, M-12, M-13, M-14	42801.55	2.669	12.7
131	M-1, M-2, M-3, M-4, M-5, M-6, M-7, M-8, M-10, M-11, M-12, M-13, M-14	15346.6	1.671	9.1
132	M-1, M-2, M-3, M-4, M-6, M-7, M-8, M-9, M-10, M-11, M-12, M-13, M-14	15523.24	1.891	9.9
133	M-1, M-2, M-4, M-5, M-6, M-7, M-8, M-9, M-10, M-11, M-12, M-13, M-14	19845.79	1.167	6.7
134	M-1, M-2, M-3, M-4, M-5, M-6, M-7, M-8, M-9, M-10, M-11, M-12, M-13, M-14	27851.49	1.368	7.5