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

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Аналіз ризиків використання інформаційних технологій у системах медичного призначення

Виконав: студент VI курсу, групи Сам-61
спеціальності 124 Системний аналіз
(шифр і назва спеціальності)

_____ Спільник В.Р.
(підпис) (прізвище та ініціали)

Керівник _____ Фриз М.Є.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ _____
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ Боднарчук І.О.
(підпис) (прізвище та ініціали)

Рецензент _____ Карпінський М.П
(підпис) (прізвище та ініціали)

Тернопіль
2023

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

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

Кафедра комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)
«28» грудня 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 124 Системний аналіз
(шифр і назва спеціальності)

Студенту Спільнику Василю Романовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Аналіз ризиків використання інформаційних технологій у системах медичного призначення

Керівник роботи Фриз Михайло Євгенович, к.т.н., доцент кафедри КН
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 24 » листопада 2023 року № 4/7-1096

2. Термін подання студентом завершеної роботи 25 грудня 2023р.

3. Вихідні дані до роботи Літературні джерела та наукові публікації з теми дослідження

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. Розділ 1.Аналітичний огляд літературних джерел за напрямом дослідження.
Розділ 2. Системний аналіз ризиків та проблеми застосування ІТ у медичній галузі
Розділ 3. Стратегії управління ризиками
Розділ 4. Охорона праці і безпека в умовах надзвичайних ситуацій
Висновки. Перелік джерел. Додатки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Вступ. Актуальність теми. Роль ІТ в сучасній медицині. Проблеми та недоліки ІТ в медицині. Ризики використання ІТ медичного призначення. Накова новизна роботи. Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Сенчишин В.С., доцент		
Безпека в надзвичайних ситуаціях	Клепчик В.М., ст. викладач		

7. Дата видачі завдання 14 листопада 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	25.11.2023	*Виконано*
2.	Підбір наукових джерел про інормаційні технології	26.11.2023-29.11.2023	*Виконано*
	Їх застосування в медичній сфері		
3.	Опрацювання наукових публікацій та збір даних по	28.11.2022-25.12.2023	*Виконано*
	темі роботи		
4.	Виконання дослідження згідно мети кваліфікаційної	09.11.2023-12.12.2023	*Виконано*
	роботи		
5.	Оформлення розділу «Аналітичний огляд	13.11.2023-19.12.2023	*Виконано*
	літературних джерел за напрямом дослідження»		
6.	Оформлення розділу «Системний аналіз ризиків та	20.11.2023-26.12.2023	*Виконано*
	застосування ІТ в медицині»		
7.	Оформлення розділу «Стратегії управління ризиками»	27.11.2023-12.12.2023	*Виконано*
8.	Виконання завдання до підрозділу «Охорона праці»	10.04.2023-16.12.2023	*Виконано*
9.	Виконання завдання до підрозділу «Безпека в	17.04.2023-23.12.2023	*Виконано*
	надзвичайних ситуаціях»		
10.	Оформлення кваліфікаційної роботи	10.12.2023-16.12.2023	*Виконано*
11.	Нормоконтроль	27.12.2023	*Виконано*
12.	Перевірка на плагіат	25.12.2023	*Виконано*
13.	Попередній захист кваліфікаційної роботи	22.12.2023	*Виконано*
14.	Захист кваліфікаційної роботи	29.12.2023	

Студент _____ Спільник В. Р.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Фриз М. Є.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Аналіз ризиків використання інформаційних технологій у системах медичного призначення // Кваліфікаційна робота освітнього рівня «Магістр» // Спільник Василь Романович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група Сам-61 // Тернопіль, 2023 // С. 64, рис. – 7, табл. – 0, кресл. – 11, додат. – 5, бібліогр. – 0.

Ключові слова: аналіз, дослідження, ІТ, керування, кібербезпека, медицина, ризики.

Кваліфікаційна робота присвячена розробці та дослідженню інформаційних технологій в медичній галузі з використанням системного аналізу.

Перший розділ: В розділі розглянуто актуальність теми, визначено поняття системного аналізу, описано роль інформаційних технологій у медицині, розвиток ІТ у системах медичного призначення та визначено проблеми та ризики медичних ІТ-систем.

Другий розділ: Визначено значення безпеки в системах медичної інформації, проаналізовано проблеми конфіденційності та захисту даних пацієнтів, а також досліджено ефективність та надійність медичних ІТ-систем.

Третій розділ: Описано стратегії управління ризиками, вивчено вплив помилок в системах на якість діагностики та лікування, проаналізовано ризики з обробки медичних даних та вплив перерв у роботі ІТ-систем на надання медичних послуг. Визначено об'єкт та предмет дослідження.

Об'єкт дослідження: інформаційні технології в медичній галузі.

Предмет дослідження: системний аналіз та ризик-менеджмент у використанні інформаційних технологій в медицині.

Ця кваліфікаційна робота є важливим внеском у розуміння взаємодії між інформаційними технологіями та медичною сферою, вказуючи на ключові виклики, переваги та ризики, а також пропонуючи стратегії управління ризиками для підвищення ефективності та безпеки в медичних ІТ-системах.

ANNOTATION

Title: Risk Analysis of Information Technology Usage in Medical Systems // Master's Thesis // Author: Vasil Romanovych Spilnyk // Ternopil Ivan Pul'uj National Technical University, Faculty of Computer and Information Systems and Software Engineering, Department of Computer Science, SAM-61 Group // Ternopil, 2023 // Pages – 64, Figures – 7, Tables – 0, Drawings – 11, Appendices – 5, Bibliography – 0.

Keywords: analysis, research, IT, management, cybersecurity, medicine, risks.

This master's thesis is dedicated to the development and investigation of information technologies in the medical field using a systemic analysis approach.

Chapter 1: This chapter explores the relevance of the topic, defines the concept of systemic analysis, outlines the role of information technologies in medicine, examines the evolution of IT in medical systems, and identifies problems and risks associated with medical IT systems.

Chapter 2: The significance of security in medical information systems is determined, and issues related to confidentiality and patient data protection are analyzed. Additionally, the efficiency and reliability of medical IT systems are investigated.

Chapter 3: This chapter describes risk management strategies, studies the impact of errors in systems on the quality of diagnostics and treatment, analyzes risks associated with the processing of medical data, and assesses the influence of interruptions in IT systems on the provision of medical services. The object and subject of the research are defined.

Object of Study: Information technologies in the medical field.

Subject of Study: Systemic analysis and risk management in the utilization of information technologies in medicine.

This qualification work makes a significant contribution to understanding the interaction between information technologies and the medical sphere.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

Імплементація медичних ІТ – це процес впровадження та використання інформаційних технологій у сфері медицини для покращення управління та надання медичних послуг.

Інформаційні технології (ІТ) – це комплекс високоточних інструментів та програм, призначених для збору, обробки, зберігання та передавання інформації, які використовуються для підтримки різноманітних процесів та функцій у різних сферах, включаючи медицину.

Електронні медичні записи (EMP) – це цифрові збережені дані про медичну історію пацієнта, які сприяють ефективній обробці і обміну інформацією у сфері охорони здоров'я.

Інтероперабельність у сфері медичних інформаційних систем - це здатність різних технологій та платформ взаємодіяти та обмінюватися даними безперешкодно, забезпечуючи ефективну і координовану роботу медичних систем.

Медична інформаційна система (MIC) – це комп'ютерна система для обробки та зберігання медичних даних, яка допомагає лікарям та іншому медичному персоналу у веденні ефективного обліку пацієнтів та наданні якісної медичної допомоги.

Цифровізація у медицині – це впровадження та використання сучасних технологій, таких як електронні записи та телемедицина, для покращення процесів у медичній сфері.

ЗМІСТ

ВСТУП

У сучасному світі інформаційні технології (ІТ) відіграють ключову роль у різних сферах життя, включаючи сферу охорони здоров'я. Спостереження за стрімким розвитком цифрових систем у медичному сегменті стає необхідністю, оскільки вони не лише вдосконалюють надання медичних послуг, а й стають об'єктом різноманітних ризиків.

Актуальність теми дослідження: визначається швидкими темпами цифровізації у сфері охорони здоров'я. З одного боку, це відкриває нові можливості для поліпшення якості медичної допомоги, а з іншого - народжує загрози, пов'язані з безпекою даних та ефективністю медичних ІТ-систем. У зв'язку із стрімким розвитком інформаційних технологій та їх широким використанням у сфері охорони здоров'я, актуальність дослідження ризиків використання інформаційних технологій у медичних системах набуває особливого значення. Зростання обсягів медичних даних, їх обробка та передача у цифровому форматі відкривають широкі можливості для вдосконалення медичної практики. Проте, разом із цим, виникають серйозні етичні, юридичні та технічні питання, які потребують детального дослідження.

Актуальність полягає в необхідності зрозуміти та зменшити ризики, пов'язані з використанням інформаційних технологій в медицині. Загрози безпеці даних пацієнтів, можливість системних збоїв та недоліки у роботі медичних ІТ-систем стають чинниками, які можуть вплинути на якість та безпеку медичного обслуговування. Дослідження цих аспектів має на меті забезпечення високого рівня безпеки та надійності інформаційних технологій у медичній сфері та розробку ефективних заходів для подолання виявлених проблем.

Мета та завдання дослідження: є проведення глибокого аналізу ризиків, що виникають при застосуванні інформаційних технологій в системах медичного призначення. Задачами роботи є визначення основних проблем, з якими стикаються медичні ІТ-системи, та розробка стратегій для їх управління.

Об'єкт та предмет дослідження: Об'єктом дослідження є системи медичного призначення, що використовують інформаційні технології. Предметом дослідження є ризики, що виникають при використанні цих технологій, а також способи управління ними для забезпечення безпеки та ефективності медичних процесів.

Дана робота спрямована на ідентифікацію проблем і розробку конкретних рекомендацій для вдосконалення використання ІТ в сучасній медицині.

Наукова новизна отриманих результатів у магістерській роботі полягає в комплексному аналізі ризиків використання інформаційних технологій у системах медичного призначення. Однією з ключових особливостей є системний підхід до вивчення проблем, пов'язаних із застосуванням ІТ в медицині, включаючи безпеку медичних інформаційних систем, конфіденційність пацієнтських даних, ефективність та надійність ІТ-систем.

Практичне значення отриманих результатів моєї магістерської роботи виявляється в конкретних заходах та рекомендаціях, спрямованих на забезпечення безпеки та ефективності використання ІТ в медичних системах. Розроблені стратегії управління ризиками можуть слугувати основою для практичної реалізації та вдосконалення сучасних медичних ІТ-систем.

Апробація результатів магістерської роботи. Основні результати проведених досліджень обговорювались на XI міжнародної студентської науково-технічної конференції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя (м. Тернопіль, 2023 р.).

Публікації. Основні результати кваліфікаційної роботи опубліковано у двох працях конференції (Див. додатки А, Б).

Структура й обсяг кваліфікаційної роботи. Кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку літератури з 24 найменувань та 5 додатків. Загальний обсяг кваліфікаційної роботи складає 64 сторінки, з них 48 сторінки основного тексту, який містить 7 рисунків та 0 таблиць.

РОЗДІЛ 1. АНАЛІТИЧНИЙ ОГЛЯД ЛІТЕРАТУРНИХ ДЖЕРЕЛ ЗА НАПРЯМОМ ДОСЛІДЖЕННЯ

1.1 Актуальність тематики дослідження та поняття системного аналізу

Сьогодні, у епоху стрімкого розвитку інформаційних технологій, медицина не може уникнути їх впливу. Використання інформаційних технологій у сфері медицини набуває все більшої важливості і це має значний потенціал для поліпшення надання медичних послуг та підвищення якості діагностики та лікування. Проте разом з новими можливостями приходять і нові ризики.
Актуальність дослідження полягає у вивченні цих ризиків і розробці стратегій для їх управління. Розуміння цих аспектів важливе для забезпечення безпеки пацієнтів і покращення медичної допомоги [2].

Цифровізація медичної галузі може включати в себе перехід від традиційних паперових документів до електронних медичних записів, використання телемедицини для дистанційного здійснення консультацій та діагностики, а також впровадження інших інформаційних технологій для поліпшення обміну даними та управління медичною інформацією. Цей процес спрямований на збільшення ефективності, доступності та якості медичних послуг завдяки використанню сучасних цифрових рішень.

Системний аналіз – це підхід до дослідження складних систем, де розглядаємо їх як цілісні утворення, що складаються з різних компонентів та мають взаємозв'язки між собою [4]. У контексті дослідження, системний аналіз допомагає розглядати медичні інформаційні системи як комплексні об'єкти, розуміти їхню структуру та вплив на сферу медицини [1].

Системний аналіз є інструментом, який дозволяє розглядати складні системи у їхній цілісності, зокрема медичні інформаційні системи. Це допомагає зрозуміти, як різні компоненти таких систем взаємодіють та впливають один на одного. За допомогою системного аналізу можна виділити ключові аспекти функціонування системи та виявити можливі проблеми та відмінності.

Системний аналіз спрямований на виявлення кореневих причин проблем і розробку стратегій для їх розв'язання. Це дозволяє зосередитися на основних аспектах без вдачі в деталі та складні концепції. В результаті, можна краще зрозуміти, як працюють медичні інформаційні системи та як їх можна поліпшити, щоб забезпечити безпеку та ефективність в сфері медицини.

Системний аналіз допомагає розглядати складні системи як єдиність, враховуючи взаємозв'язки та взаємодії між їхніми компонентами. У дослідженні використання цього підходу дозволить аналізувати медичні інформаційні системи, що включають в себе бази даних, програмні засоби, апаратні рішення та користувачів [7].

Мета системного аналізу - розкрити, як ці системи функціонують, ідентифікувати можливі ризики та недоліки та розробити стратегії для їх вирішення. Зрозуміння цих аспектів важливе для досягнення безпеки та ефективності медичних інформаційних систем.

1.2 Роль інформаційних технологій у сучасній медицині

Інформаційні технології стали невід'ємною частиною сучасної медицини і відіграють ключову роль у поліпшенні надання медичних послуг та діагностиці хвороб. Вони допомагають лікарям ефективніше вести медичну документацію, зберігати і обробляти великі обсяги даних про пацієнтів та взаємодіяти з іншими фахівцями в галузі медицини [5].

Одним із важливих аспектів ролі інформаційних технологій є покращення точності діагностики та лікування. Електронні системи медичного документування дозволяють лікарям швидше та легше отримувати доступ до інформації про пацієнта, що допомагає приймати більш обгрунтовані рішення.

Проте використання інформаційних технологій у медицині також вносить свої виклики та ризики, зокрема стосовно конфіденційності та безпеки медичних даних пацієнтів. Інформаційні технології у медицині розширюють можливості лікарів та поліпшують доступність медичної допомоги. Однак, вони також спричиняють зміни у способі надання послуг та зберігання медичних даних.

Особливо важливою є можливість обміну медичною інформацією між лікарями та медичними закладами, що дозволяє підвищити якість діагностики та лікування. Також інформаційні технології допомагають підвищити своєчасність та доступність медичної інформації для лікарів та пацієнтів.

Проте збільшення обсягу медичних даних та їх зберігання в електронному вигляді ставить питання про безпеку та конфіденційність цих даних. Захист особистої інформації пацієнтів є вельми важливою аспектом, інакше це може призвести до небажаних наслідків та порушення довіри. Інформаційні технології в медицині - це як інструменти для полегшення роботи лікарів та поліпшення лікування. Вони дозволяють лікарям зберігати та обмінюватися інформацією про хворих, що робить лікування ефективнішим [4].

Інформаційні технології в медицині є не тільки інструментами для зберігання та обробки даних. Вони впливають на всі аспекти медичної практики, від діагностики до лікування та моніторингу пацієнтів. Ключові ролі інформаційних технологій поділяють на електронні медичні записи, телемедицина, аналітика даних та збереження та обмін даними.

Якщо говорити більш детально що собою являють ці основні чотири ролі. Варто сказати, що електронні медичні записи замінюють традиційну паперову документацію і дозволяють лікарям легше знаходити та аналізувати інформацію про пацієнтів. Це полегшує діагностику та лікування. EMP вносять значний вклад у покращення надання медичних послуг та оптимізацію процесів у сфері охорони здоров'я. Їх використання дозволяє ефективно зберігати та доступно обмінюватися медичною інформацією між лікарнями та медичними закладами, що сприяє швидшим та точнішим діагнозам, покращує координацію медичних процедур та забезпечує більш якісне обслуговування пацієнтів. Крім того, EMP можуть зменшити кількість помилок у лікуванні, полегшуючи доступ до повної та актуальної інформації про пацієнтів для лікарів та медичного персоналу [3].

Телемедицина – технологія, яка дозволяє лікарям консультувати та лікувати пацієнтів на відстані, що особливо корисно для тих, хто не може фізично зустрітися з лікарем. Важливою перевагою телемедицини є забезпечення доступності медичної допомоги для пацієнтів, які знаходяться в

віддалених регіонах або з обмеженим фізичним доступом. Це також сприяє ефективному веденню хронічних захворювань через дистанційний моніторинг стану здоров'я [6].

Телемедицина зменшує час очікування на медичний прийом, сприяє підвищенню якості надання медичних послуг та забезпечує ефективний обмін даними між медичними закладами. Це стає особливо актуальним у сучасному світі, де технологічні досягнення сприяють глобальній трансформації у сфері охорони здоров'я. Телемедицина відкриває нові можливості для покращення доступу до медичної допомоги та забезпечення ефективного лікування на різних рівнях медичного обслуговування [9].

Аналітика даних за допомогою інформаційних технологій медичні дані можна аналізувати для виявлення тенденцій та розробки ефективних методів лікування. Аналітика даних в контексті медичних інформаційних систем грає важливу роль у вдосконаленні процесів діагностики, лікування та управління медичними даними. Цей аспект інформаційних технологій дозволяє виявляти тенденції, визначати фактори ризику та покращувати прийняття рішень у медичній сфері [5].

Збереження та обмін даними ІТ дозволяють безпечно зберігати та обмінюватися медичною інформацією між різними закладами та медичними працівниками. Збереження та обмін даними у медичних інформаційних системах відіграють критичну роль у забезпеченні доступності та надійності медичної інформації. Завдяки цьому процесу, лікарі, медсестри та інші медичні працівники можуть ефективно взаємопрацювати, обмінюючи необхідні дані для діагностики, лікування та моніторингу стану пацієнтів [1].

Збереження даних в цифровій формі дозволяє легко керувати, оновлювати та здійснювати резервне копіювання медичної інформації, що сприяє її довготривалій доступності. Однак при цьому важливо забезпечити високий рівень безпеки для запобігання несанкціонованому доступу та втраті конфіденційності медичних даних [12].

1.3 Розвиток досліджень ІТ у системах медичного призначення

Еволюція наукових досліджень в галузі інформаційних технологій у системах медичного призначення відображає постійний розвиток та вдосконалення цих систем. Дослідження в цьому напрямку спрямовані на вдосконалення безпеки, ефективності та інтеграції ІТ в медичні практики. Новаторські дослідження в цій сфері важливі для забезпечення найвищого стандарту обслуговування пацієнтів та оптимізації роботи медичних закладів. Акцент робиться на розробці та впровадженні нових технологій, що сприяють покращенню діагностики, лікування та адміністрування медичних послуг. Ці дослідження також спрямовані на вирішення ризиків та проблем, пов'язаних із застосуванням інформаційних технологій у медичній галузі, забезпечуючи підґрунтя для стабільного та прогресивного впровадження ІТ в медичну практику [17]. Що стосується складової інформаційних систем в медицині можна побачити на рисунку 1.1.

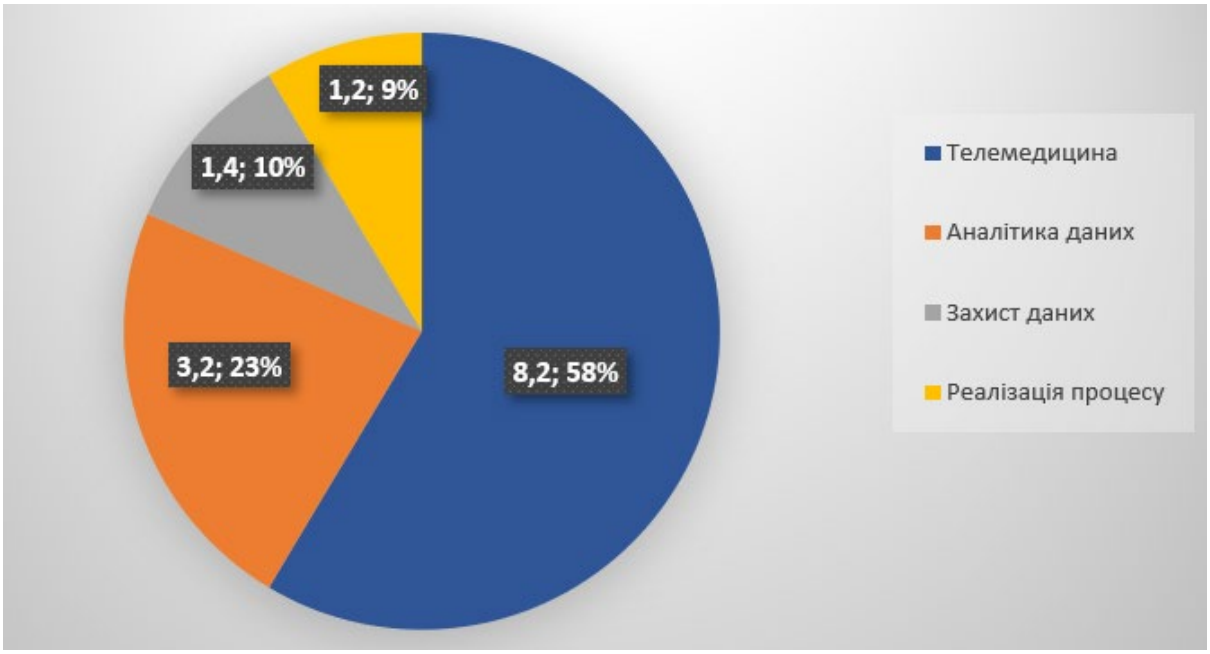


Рисунок 1.1 – Діаграма складових ІТ в медицині

Протягом останніх двадцяти років еволюція досліджень в галузі інформаційних технологій у системах медичного призначення пройшла значний шлях. На початку цього періоду, акцент робився переважно на впровадженні

базових електронних систем обліку медичної інформації та автоматизації процесів. У наступні роки спостерігався перехід від простих електронних медичних записів до більш складних систем, які враховують обмін даними між різними медичними закладами. Зростання популярності хмарних технологій та забезпечення безпеки даних стали ключовими напрямками досліджень [19].

Останнім часом, науковці активно досліджують застосування розумних технологій, таких як штучний інтелект та аналітика даних, для поліпшення діагностики, прогнозування хвороб, та персоналізованого підходу до лікування.

Нові дослідження також акцентують на впровадженні інтерактивних та зручних інтерфейсів для пацієнтів, що сприяє більшій взаємодії та участі пацієнтів у власному здоров'ї. Крім того, зростає увага до розробки та впровадження мобільних додатків, які дозволяють пацієнтам отримувати доступ до своєї медичної інформації та контролювати своє здоров'я.

Технології для збору та аналізу великих обсягів даних, такі як "big data", також виявляються важливим аспектом досліджень, спрямованих на розвиток систем медичного призначення. Це дозволяє отримати нові уявлення щодо хвороб, ефективності лікування та організації медичних послуг [11].

1.4 Проблеми та ризики в сфері медичних IT-систем

В час високого розвитку технологій зростає й проблема та визначення нюансів при роботі з новими технологіями. Проблеми та ризики в сфері медичних IT-систем важливий для розуміння тих аспектів, які можуть стати перешкодою при впровадженні та використанні інформаційних технологій в медицині. Якщо говорити про основні проблеми та нюанси у роботі з IT у медичній галузі, варто врахувати:

Збільшення обсягу медичних даних та їхньої цінності для зловмисників робить медичні IT-системи мішенню для кібератак. Незахищені системи можуть стати об'єктом втрати конфіденційності, крадіжки даних або навіть вплинути на надання медичних послуг [14].

Різні медичні системи та програми можуть не завжди взаємодіяти ефективно між собою, що призводить до проблем з обміном даними. Це може ускладнити облік пацієнтів та роботу медичного персоналу. Проблема недостатньої інтероперабельності в медичних ІТ-системах означає, що різні програми та обладнання не завжди вміють ефективно співпрацювати між собою. Це подібно до ситуації, коли різні мови, якими говорять різні люди, ускладнюють їхнє спілкування. У медицині це може призводити до того, що медичні дані, які потрібні для надання допомоги пацієнту, не можуть бути легко обмінені між різними системами або лікарями. Це може сповільнювати роботу медичного персоналу та створювати ризики для безпеки пацієнтів, оскільки не всі необхідні дані доступні вчасно [16].

Для вирішення цієї проблеми важливо розробляти стандарти та технології, які дозволять різним системам співпрацювати між собою без перешкод, що полегшить обмін даними та покращить якість медичних послуг.

Технічні проблеми або несправність обладнання можуть призвести до втрати медичних даних, що може бути критичним у медичних ситуаціях.
Порушення конфіденційності: Недостатня захист інформації може призвести до незаконного доступу до особистих медичних даних пацієнтів, що порушує їхню конфіденційність та приватність [12].

Перебільшена залежність від ІТ може призвести до негативних наслідків, коли технічні проблеми або відмови систем можуть заблокувати надання медичної допомоги. Залежність від технологій в медицині вказує на те, що медичні практики стають дедалі більш залежними від інформаційних технологій (ІТ) та комп'ютерних систем у всіх аспектах своєї діяльності. Це у свою чергу також має як свої переваги, так і недоліки.

1.5 Аналіз сучасних інформаційних технологій медичного призначення

Аналіз сучасних інформаційних технологій медичного призначення є важливою складовою в дослідженні впливу ІТ на сферу охорони здоров'я. Спостереження за розвитком медичних технологій надає можливість оцінити

їхні поточні можливості та визначити перспективи вдосконалення. Серед ключових напрямків аналізу входять електронні медичні записи, системи телемедицини, аналітика даних у сфері медицини, а також роль інтероперабельності в забезпеченні ефективної взаємодії між різними медичними системами. В даному розділі ми детально розглянемо сучасні досягнення в цих областях, визначимо їхні переваги та недоліки, а також проаналізуємо їх вплив на якість надання медичних послуг та управління пацієнтською інформацією. Поглиблення в аналізі сучасних інформаційних технологій медичного призначення вимагає уваги до конкретних видач, таких як електронні медичні записи [17].

EMP визначаються як електронні версії традиційних паперових медичних записів, що дозволяють ефективніше збирати, зберігати та обмінюватися інформацією про пацієнтів. Вони можуть значно полегшити роботу медичного персоналу та покращити якість медичних послуг. Проте, існують виклики щодо безпеки та конфіденційності даних у таких системах, що вимагає ретельного аналізу та вдосконалення.

1.6 Сучасні IT додатки в медичній галузі

В сучасному світі інформаційні технології вкрай важливі для розвитку медичної галузі. IT-додатки в медицині відіграють ключову роль у поліпшенні якості надання медичних послуг, забезпечуючи ефективніше відстеження стану пацієнтів та покращення діагностики та лікування. Ці технологічні рішення стають необхідною складовою для забезпечення індивідуального підходу до кожного пацієнта та підвищення рівня медичної допомоги [15].

Один із найбільш ефективних мобільних додатків для здоров'я - "MyFitnessPal". Розроблений командою учених та інженерів компанії Under Armour, цей додаток дозволяє користувачам вести облік споживаних калорій, тренувань та інших факторів, пов'язаних із здоров'ям. Він використовує принципи харчового дневника та планування тренувань, аналізуючи дані та надаючи корисні поради.

Зображення на рисунку 1.2 служить ілюстрацією функціоналу додатка MyFitnessPal, яке спрощує розуміння його можливостей та інтерфейсу.

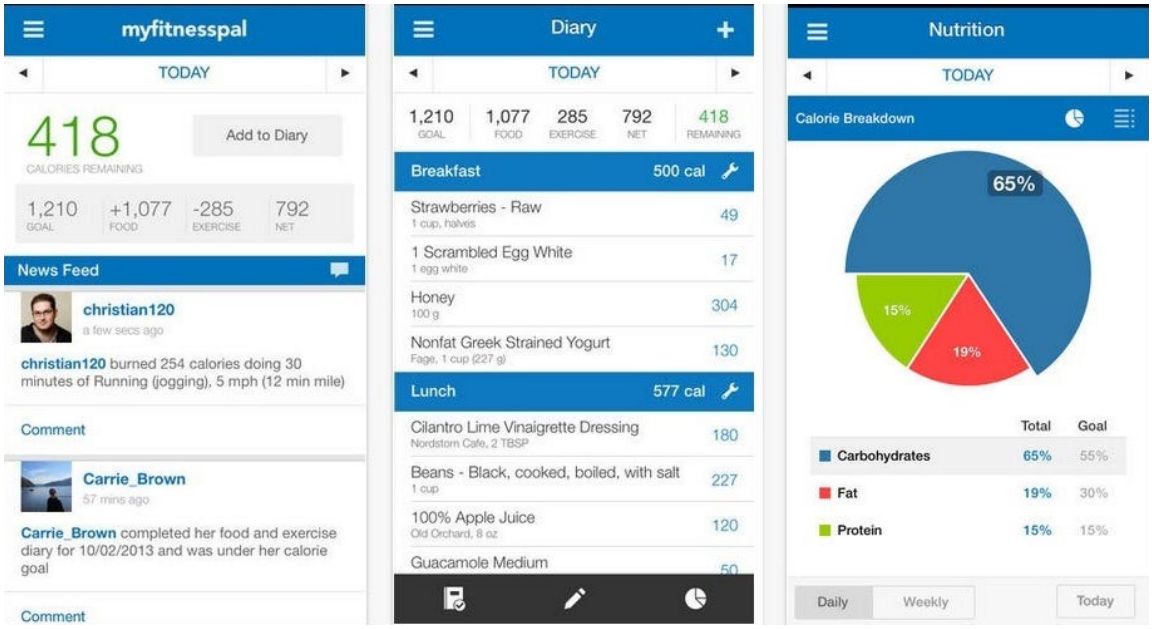


Рисунок 1.2 – Загальний інтерфейс та можливості додатку MyFitnessPal.

"Headspace" – це інноваційний медитаційний додаток, створений британськими експертами з медитації Анді Паддіком та Річардом Пі. Headspace пропонує користувачам широкий спектр медитаційних сесій та технік для покращення психічного здоров'я [13].

Цей додаток дозволяє користувачам вибирати між різними категоріями медитацій, такими як стрес, сон, концентрація, та інші. Програма також включає спеціально розроблені сесії для новачків, які допомагають освоїти медитацію та регулювання дихання. Крім того, додаток "Headspace", розроблений англійським медитаційним експертом Анді Паддіком та Річардом Пі, став популярним для поліпшення психічного здоров'я. Він пропонує готові медитаційні сесії та техніки релаксації, допомагаючи користувачам знижувати стрес, покращувати концентрацію та сон.

Headspace не лише надає медитаційні сесії, але і включає в себе інші корисні функції для підтримки психічного здоров'я. Одна з таких функцій - це звукові та візуальні ефекти, що допомагають користувачам зосередитися під час медитації [17].

Додаток також пропонує програму для поліпшення якості сну. Відповідні медитаційні сесії допомагають розслабитися перед сном та покращити його тривалість і якість. Враховуючи важливість здорового сну для психічного і фізичного благополуччя, ця функція робить "Headspace" більш універсальним і корисним для різних аспектів здоров'я [14].

Крім того, "Headspace" активно співпрацює з науковцями і проводить дослідження щодо впливу медитації на різні аспекти здоров'я та емоційного стану. Це робить додаток не лише інструментом для користувачів, але і платформою, що сприяє науковим дослідженням у галузі психічного здоров'я.

Один з прикладів додатка для відстеження здоров'я людини в медичній галузі – "Fitbit". Інтерфейс додатків, встановлених на смарт-годинниках, таких як Fitbit, буде ілюстровано на екрані годинника у вигляді, схожому на той, який представлений на зазначеному рисунку. Інтерфейс додатків, встановлених на смарт-годинниках, таких як Fitbit, буде ілюстровано на екрані годинника у вигляді, схожому на той, який представлений на рисунку 1.2.

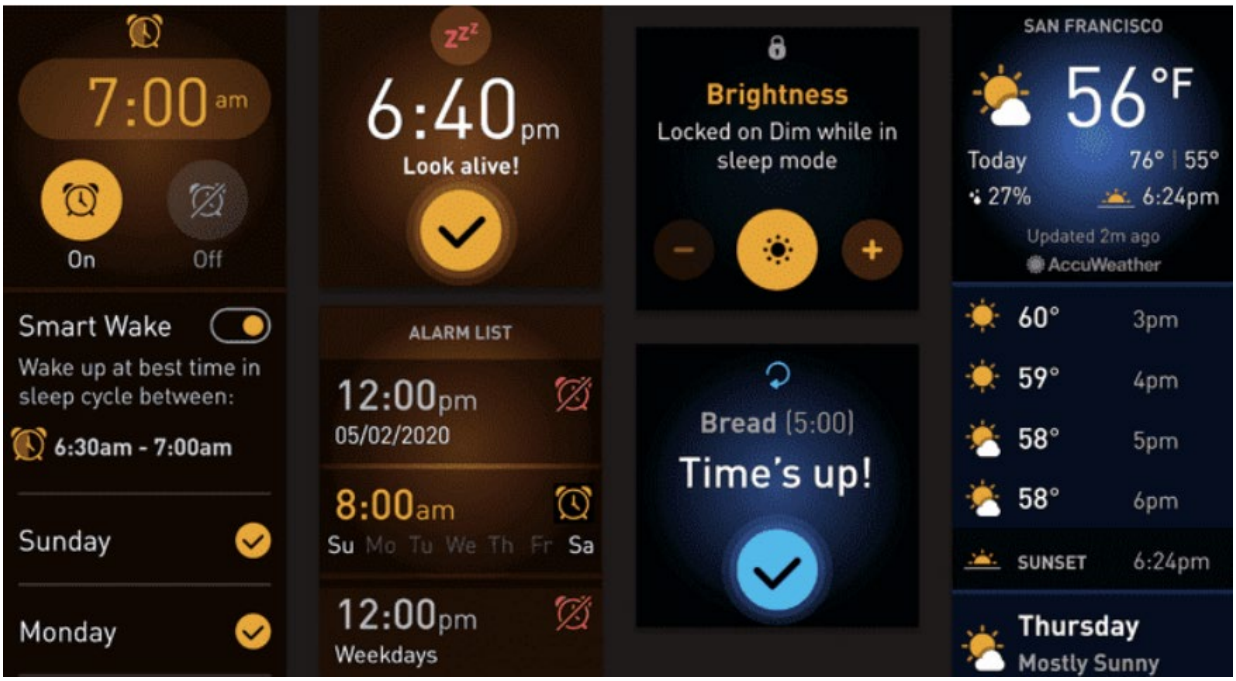


Рисунок 1.3 – Інтерфейс додатку Fitbit

Цей додаток спроектований для відстеження фізичної активності, сну, пульсу та інших параметрів здоров'я користувача. Використовуючи датчики в

спеціальних пристроях, таких як фітнес-трекери та смарт-годинники, "Fitbit" надає користувачам можливість аналізувати їхню фізичну активність, визначати якість сну та отримувати іншу важливу інформацію для збереження здоров'я та формування здорових звичок [18].

Ще однією корисною особливістю "Fitbit" є можливість моніторингу рівня стресу та вивчення тенденцій зміни показників у різних ситуаціях. Це сприяє більш глибокому розумінню впливу стресу на загальний стан організму. Однією з інноваційних функцій є також можливість вимірювання рівня кисню у крові. Цей параметр може слугувати показником здоров'я легень та загального рівня кисню в організмі. "Fitbit" активно розвивається та оновлюється, впроваджуючи нові можливості та покращення, щоб задовольняти зростаючі потреби користувачів у сфері моніторингу здоров’я [15].

Garmin Connect – інтегрована платформа від компанії Garmin, що сприяє відстеженню фізичної активності та збереженню даних про здоров'я. Додаток пропонує можливості відстеження маршрутів, фізичних активностей, контролю рівня стресу та аналізу сну. Зокрема, він надає деталізовану інформацію про відстань, час, пульс і спожиті калорії під час тренувань.

Однією з ключових особливостей Garmin Connect є інтеграція з різноманітними фітнес-гаджетами від Garmin, такими як годинники та браслети, що покращує здатність користувачів відстежувати свої досягнення та отримувати персоналізовані рекомендації. Платформа також пропонує спільнотні функції, що дозволяють обмінюватися результатами тренувань і взаємодіяти з іншими користувачами, надаючи мотивацію та підтримку. Таким чином, Garmin Connect визначається своєю унікальною комбінацією функцій, спрямованих на покращення фізичного здоров'я та фітнесу, та забезпечення користувачам зручного інструменту для досягнення своїх цілей [14].

Calm – це додаток для медитації та релаксації, розроблений з метою сприяти психічному здоров'ю та зниженню рівня стресу. Застосунок пропонує великий вибір медитаційних практик, аудіосповідей для заспокоєння та звукового супроводу для поліпшення сну. Calm також включає глибокі респіраторні вправи та інструменти для покращення концентрації.

Додаток визначається своєю простотою використання та здатністю індивідуалізувати вибір контенту залежно від потреб користувача. За допомогою Calm користувачі можуть розвивати навички медитації, покращувати якість свого сну та знаходити інструменти для заспокоєння психіки в сучасному ритмі життя [20].

Strava – це платформа для велосипедистів, бігунів та атлетів, яка спрямована на відстеження фізичної активності та поділ результатів з іншими учасниками спільноти. Додаток пропонує можливість відстежувати маршрути, визначати темп та вивчати статистику тренувань.

Однією з ключових особливостей Strava є підтримка великої кількості спортивних дисциплін, що робить його універсальним інструментом для спортивного спілкування. Користувачі можуть об'єднуватися у віртуальні спільноти, створювати та приєднуватися до викликів, що створює мотивацію для активного способу життя та досягнення спортивних цілей. Strava створює зручний простір для спортивного взаємодії та вдосконалення результатів.

1.7 Переваги на недоліки сучасних IT у медичній галузі та їх вплив на прийняття діагностичних рішень

У світі швидкого розвитку технологій медична сфера не залишається осторонь впливу інформаційних технологі, де глибше розглядає важливість цього переплетіння, фокусуючись на визначенні переваг та недоліків, які сучасні іТ можуть принести у медичному сегменті. Цей аналіз також охоплює вплив цифрових технологій на процеси прийняття діагностичних рішень у сфері медицини, звертаючи увагу на важливі аспекти, які впливають на якість та ефективність медичного обслуговування [26].

Безпека та ефективність інформаційних технологій у медицині залежать від чотирьох ключових аспектів. По-перше, конфіденційність та захист даних визначають рівень безпеки, забезпечуючи відсутність несанкціонованого доступу. По-друге, вартість імплементації є важливим фактором, враховуючи економічні аспекти впровадження іТ-рішень у медичному середовищі. По-третє,

специфікація технічного обладнання визначає його придатність та забезпечує сумісність із сучасними стандартами. По-четверте, навчання персоналу стає ключовим елементом для забезпечення правильної експлуатації та використання медичних іТ-рішень у медичній практиці. Усі ці компоненти взаємодіють для створення гармонійного та безпечного інформаційного середовища в медицині.

Зі збільшенням обсягу електронних медичних записів стає важливим забезпечення конфіденційності та безпеки даних. Ризик несанкціонованого доступу до особистої інформації пацієнтів зумовлює необхідність розвитку шифрування, впровадження двофакторної аутентифікації та суворих політик доступу. Ці заходи важливі для збереження довіри до цифрових медичних технологій та їх успішного використання в лікуванні та діагностиці [29].

Впровадження та підтримка ІТ-систем у сфері охорони здоров'я вимагають значних фінансових та ресурсних витрат. Для багатьох медичних закладів це може стати великим фінансовим тягарем. Процес імплементації медичних ІТ може бути високовартісним, оскільки включає в себе придбання та встановлення спеціалізованого обладнання, розробку та впровадження програмного забезпечення, навчання медичного персоналу та виконання інших технічних завдань. Крім того, вартість може охоплювати регулярне оновлення та технічну підтримку систем.

Технічне обладнання в медицині повинно враховувати сумісність з новими ІТ-технологіями та відповідати вимогам медичного середовища. Важливо, щоб пристрої, такі як сенсори та медичні монітори, відповідали стандартам, були безпечними та забезпечували конфіденційність даних. Обладнання повинно бути надійним, захищеним від втручань та легко інтегрованим з існуючими медичними системами [25].

Незважаючи на великі витрати, впровадження ІТ в медицині може призвести до ефективнішого управління медичними даними, поліпшення діагностики та лікування, що в кінцевому підсумку може призвести до підвищення якості надання медичних послуг та зменшення ризиків для пацієнтів. Забалансувати витрати та потенційні переваги є важливим етапом для успішної імплементації медичних ІТ в сучасній медицині [32].

Впровадження нових ІТ-технологій в медицині вимагає тренування персоналу, що може вплинути на робочий процес та час надання послуг. Ключовою проблемою є необхідність ефективного навчання медичного персоналу з використання ІТ. Це передбачає ознайомлення з інформаційними системами, використанням електронних медичних записів та забезпечення конфіденційності даних. Важливо також забезпечити постійну підтримку та оновлення для підвищення навичок персоналу та адаптації до нових технологій в медицині [35].

Удосконалення прийняття діагностичних рішень внаслідок застосування сучасних ІТ у медицині виявляє важливі позитивні впливи. Інтеграція аналітичних інструментів дозволяє системам обробки даних автоматично визначати патерни та взаємозв'язки, що допомагає у швидкому виявленні аномалій та подальшому прийнятті обґрунтованих рішень.

Збільшена швидкість та точність діагностики, забезпечена за допомогою алгоритмів машинного навчання, сприяє ранньому виявленню захворювань та визначенню оптимального плану лікування. Це особливо актуально в областях, де швидкість реакції може впливати на результати лікування, таких як онкологія чи екстрені стани [37].

Проте, нарікаючи на користь використання ІТ, необхідно враховувати ризики, пов'язані з можливістю помилок у програмному забезпеченні, забезпеченням безпеки пацієнтських даних та визначенням стандартів взаємодії між різними медичними системами. Глибокий розуміння цих викликів є важливим для ефективного впровадження інформаційних технологій у медичну практику та максимізації їх переваг для пацієнтів та медичного персоналу.

Паралельно з перевагами використання ІТ у прийнятті діагностичних рішень, необхідно враховувати і виклики, що постають перед медичною галуззю. Наприклад, наявність великого обсягу даних може створювати проблеми з їхнім ефективним аналізом та інтерпретацією. Додатково, неоднозначність в інтерпретації певних медичних показників може призводити до неточностей у діагнозах [42].

Також, важливо враховувати вплив факторів, таких як вартість інфраструктури для впровадження ІТ-систем та професійна підготовка медичного персоналу. Забезпечення високої якості даних та їхній безпеки є ключовим завданням при впровадженні інформаційних технологій, щоб забезпечити надійність та ефективність діагностичних процедур.

1.8 Висновки до першого розділу

За результатами дослідження стало ясно, що використання інформаційних технологій у медицині сьогодні - це важливий шматок пазла. Вони роблять діагностику та лікування ефективнішими, але водночас існують свої проблеми, які можуть впливати на надійність систем. Розвиток іТ-систем в медицині визначається не лише технологічними вдосконаленнями, але і потребами пацієнтів і медичних фахівців. Огляд ринку додатків підтвердив, що вони можуть полегшити життя, але іноді вони можуть бути нестабільними та вразливими до ризиків.

Використання ІТ в медицині приводить до багатьох переваг, але важливо ретельно вирішувати проблеми безпеки та ефективності, щоб ці переваги були максимально використані. На фоні розгляду прогресу в медичних інформаційних технологіях стає зрозумілим, що вони стали не просто інструментом, а важливою частиною сучасної медицини. Вони допомагають у точній діагностиці та швидкому доступі до інформації, зробивши лікування ефективнішим [30].

Однак разом із цим виокремлюються і ризики, пов'язані з проблемами безпеки та можливістю виникнення технічних неполадок. На тлі стрімкого розвитку технологій, слід акцентувати увагу на забезпеченні стабільності та захисті медичних даних. Інноваційні ІТ-додатки в медицині можуть значно полегшити роботу лікарів та забезпечити більш ефективне взаємодію з пацієнтами. Інформаційні технології в медицині надають багато переваг, але потребують уважності та вирішення проблем, щоб максимально використовувати їхні можливості в поліпшенні якості медичного обслуговування.

РОЗДІЛ 2. СИСТЕМНИЙ АНАЛІЗ РИЗИКІВ ТА ПРОБЛЕМ ЗАСТОСУВАННЯ ІТ У МЕДИЧНІЙ ГАЛУЗІ

2.1 Значення безпеки в системах медичної інформації

У сучасному цифровому середовищі, де медичні дані стають об'єктом зростаючого інтересу, забезпечення безпеки в медичних інформаційних системах стає надзвичайно актуальним завданням. Загрози цифрового середовища, такі як кібератаки та зловживання, створюють серйозні виклики для конфіденційності, цілісності та доступності медичних даних.

Важливим аспектом є визначення і вивчення можливих вразливостей медичних інформаційних систем перед атаками. Це може включати аналіз потенційних дір в програмному забезпеченні, виявлення слабких місць в мережевій архітектурі та ідентифікацію можливих шляхів атаки. Такий детальний аналіз ризиків дозволяє розробити ефективні стратегії для зменшення ймовірності успішних кібератак [28].

Ще однією важливою аспект є використання сучасних методів шифрування для захисту медичних даних під час їх передачі та зберігання. Шифрування гарантує конфіденційність інформації і надає додатковий шар захисту в разі несанкціонованого доступу. Розгляд різних методів шифрування та їх застосування в контексті медичних інформаційних систем дозволяє визначити оптимальні рішення для забезпечення безпеки.

Паралельно з цим, важливо приділяти увагу фізичній безпеці серверних приміщень та обладнання, що зберігає медичні дані. Заходи контролю доступу, використання систем відеоспостереження та механізми виявлення несанкціонованого доступу стають обов'язковими для запобігання фізичним загрозам [32].

Особливу увагу слід приділяти аспектам мережевої безпеки, враховуючи зростаючу складність атак і сталий розвиток технологій. Впровадження систем аналізу мережевого трафіку та інтелектуальних систем виявлення загроз

дозволяє оперативно реагувати на потенційні атаки та надавати додатковий рівень захисту.

Важливо врахувати, що безпека в медичних інформаційних системах також пов'язана із внутрішніми загрозами. Зловживання прав доступу медичного персоналу може стати великим ризиком для конфіденційності даних. Ідентифікація та аутентифікація користувачів, а також ведення журналів доступу, можуть служити ефективними засобами контролю за внутрішніми загрозами.

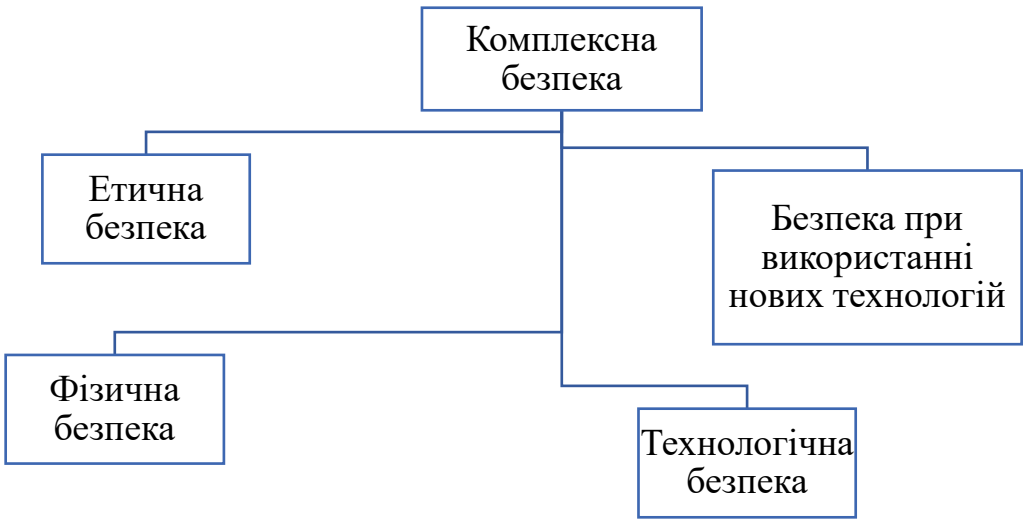
Додатковою складністю стає забезпечення безпеки в умовах зростаючої мобільності медичного персоналу. Використання мобільних пристроїв для доступу до медичної інформації може стати джерелом нових ризиків. Застосування захисту даних на рівні пристроїв, використання зашифрованих з'єднань та впровадження політик безпеки для мобільних пристроїв можуть зменшити ці ризики.

Окрім того, у контексті безпеки важливо враховувати вимоги законодавства та стандартів у сфері зберігання та обробки медичних даних. Дотримання відповідних нормативів не лише забезпечує законність обробки даних, але й слугує додатковим шаром захисту від юридичних ризиків [14].

2.2 Безпека в інформаційних технологіях медицини

Проблеми, пов'язані з безпекою в інформаційних технологіях, набувають зростаючої актуальності в наш час. Розвиток нових технологій та зростання обсягу цифрової інформації вносять нові можливості, але разом з тим ставлять під питання проблему забезпечення безпеки. Тому, важливо розглянути кілька ключових аспектів, таких як етичні виклики, безпека при використанні новітніх технологій, фізичний та технологічний аспекти забезпечення безпеки в інформаційних технологіях. Вивчення взаємодії та впливу цих факторів на сучасну інформаційну безпеку допоможе краще зрозуміти проблеми та ризики у цій сфері [25].

Якщо придивитися до того, як медицина забезпечує безпеку в умовах нових технологій, можна помітити, що це схоже на складний пазл. Тут важливо враховувати багато різних речей, таких як правила поведінки, нові винаходи та заходи для захисту від небезпек. Якщо ретельніше проаналізувати аспекти безпеки в медицині у світі інноваційних технологій, вони можуть бути розглянуті як ієрархічна структура, відображена на рисунку 2.1.



В

Рисунок 2.1 – Ієрархія безпеки інформаційних технологій

Фізична безпека в медичній галузі зосереджена на захисті фізичних ресурсів, обладнання та приміщень, що мають важливе значення для надійності та безпеки медичних інформаційних систем. Фізична безпека у контексті медичних інформаційних систем є критично важливою для забезпечення безпеки та конфіденційності оброблюваної медичної інформації. Цей аспект безпеки спрямований на захист фізичних ресурсів, обладнання та приміщень, які є основою для надійної та безперебійної роботи медичних інформаційних систем. Захист приміщень, де розташовані сервери та обладнання, розпочинається з ефективних систем контролю доступу. Використання ідентифікаційних карток, біометричних сканерів та інших засобів дозволяє обмежити фізичний доступ лише для авторизованих осіб. Це сприяє уникненню несанкціонованого доступу та захищає конфіденційні дані [27].

Встановлення систем відеоспостереження грає важливу роль у стеженні за подіями в області серверних приміщень та обладнання. Це забезпечує нагляд і вчасне виявлення будь-яких неправомірних дій або вторгнень. Запис відеоматеріалів дозволяє подальший аналіз та вживання заходів у разі інцидентів. Захист обладнання включає його фізичне закріплення, щоб запобігти незаконному переміщенню чи крадіжці. Використання спеціалізованих корпусів та систем блокування підвищує стійкість до зовнішніх фізичних впливів, таких як пожежі, вода чи вандалізм.

Системи вентиляції та кондиціонування мають бути об'єктом уваги для запобігання фізичним та хімічним загрозам. Забезпечення оптимальних умов для обладнання, включаючи контроль температури та вологості, є ключовим для підтримання його ефективності [29].

Регулярні аудити безпеки приміщень і обладнання, разом із системами технічного обслуговування, допомагають виявляти та усувати потенційні загрози та забезпечують стабільну фізичну безпеку [24].

Фізична безпека в медичних інформаційних системах є невід'ємною складовою загальної стратегії захисту, спрямованої на забезпечення безпеки та стійкості обладнання та інфраструктури в умовах зростаючих загроз та викликів. Фізична безпека в медичних інформаційних системах має за мету створення комплексного підходу, об'єднуючи технічні, організаційні та людські ресурси для надійного захисту від фізичних загроз та забезпечення стійкості та безпеки медичних інформаційних систем.

Етична безпека в інформаційних технологіях та медичних системах стає все більш актуальною у зв'язку зі зростанням кількості та значущості обробки особистих даних пацієнтів. Цей реферат розглядає ключові аспекти етичної безпеки та її вплив на сучасне забезпечення медичної інформації. Етична безпека в інформаційних технологіях та медичних системах визнає необхідність балансу між доступністю інформації та захистом приватності. Її розвиток відіграє ключову роль у створенні довіри між пацієнтами та медичними установами, сприяючи створенню безпечного та етичного середовища для використання медичної інформаці [27].

Технологічна безпека в медицині - це сукупність заходів та стратегій, спрямованих на захист медичної інформації та інформаційних технологій в галузі охорони здоров'я. Вона включає в себе різні аспекти, спрямовані на забезпечення конфіденційності, цілісності та доступності медичних даних, а також ефективного функціонування інформаційних систем.

Один з головних аспектів технологічної безпеки в медицині – це збереження конфіденційності пацієнтської інформації. Шифрування даних, безпечні методи передачі та автентифікація користувачів є основними засобами захисту від несанкціонованого доступу.

Технологічна безпека поділяється на компоненти, де кожен із них виконує свою особливу роль (Рисунок 2.2).

Рисунок 2.2 – Головні компоненти технологічної безпеки

Для детальнішого знайомства із цими компонентами, можна зробити короткий огляд кожного з них наприклад, на захисті інформаційних систем. У сучасній медицині, де захист інформаційних систем стає критичною складовою забезпечення надійності та конфіденційності медичних даних. Використання брандмауерів, антивірусного програмного забезпечення та систем аутентифікації надає необхідний рівень захисту від кібератак. Мета полягає не

лише у запобіганні несанкціонованому доступу, але й у забезпеченні безперебійної роботи інформаційних систем, що є критично важливим для ефективного функціонування сучасної медицини.

Наступним ключовим елементом, який має таку ж важливість, як і інші, є покращення доступності та обміну даними. Для покращення доступності та обміну медичною інформацією впроваджуються стандартизація та ефективна інтеграція даних. Це сприяє поліпшенню доступу лікарів до необхідної інформації та зручності для пацієнтів. Забезпечення безпечного обміну даними між різними медичними системами розширює можливості спільної роботи медичного персоналу та забезпечує високий рівень безпеки при передачі медичної інформації [23].

Ефективний захист медичних пристроїв включає регулярні оновлення програмного забезпечення та використання фізичних заходів безпеки. Проактивний підхід передбачає вживання заходів заздалегідь для запобігання можливим загрозам. Метою є забезпечення надійності та безпеки медичних пристроїв, використовуючи не лише цифрові, але й фізичні методи захисту. Це необхідно для гарантування їхньої правильної функціональності та виключення потенційних ризиків для пацієнтів.

Таким чином, технологічна безпека в медицині стає ключовим елементом для забезпечення надійності та безпеки електронного здоров'я, що сприяє вдосконаленню надання медичних послуг та забезпеченню довіри у використання інформаційних технологій у сфері охорони здоров'я [22].

2.3. Проблеми конфіденційності та захисту даних пацієнтів

Конфіденційність та захист особистих медичних даних пацієнтів є важливою складовою сучасних медичних інформаційних систем. Забезпечення безпеки цих даних має критичне значення для довіри пацієнтів до медичних послуг та для ефективності лікування. У цьому розділі ми розглянемо основні виклики, пов'язані із конфіденційністю та захистом даних пацієнтів в контексті інформаційних технологій у сфері охорони здоров'я [26].

Першою серйозною проблемою є визначення та усунення основних перешкод, що заважають забезпеченню конфіденційності медичної інформації. Це може бути пов'язано з недостатньою свідомістю медичного персоналу щодо правил обробки конфіденційної інформації, а також з відсутністю чіткої регуляторної бази для захисту особистих даних пацієнтів [27].

Проблеми конфіденційності та захисту даних пацієнтів включають ряд важливих перешкод, які слід мінімізувати. На рисунку 2.3 представлено кілька з них.

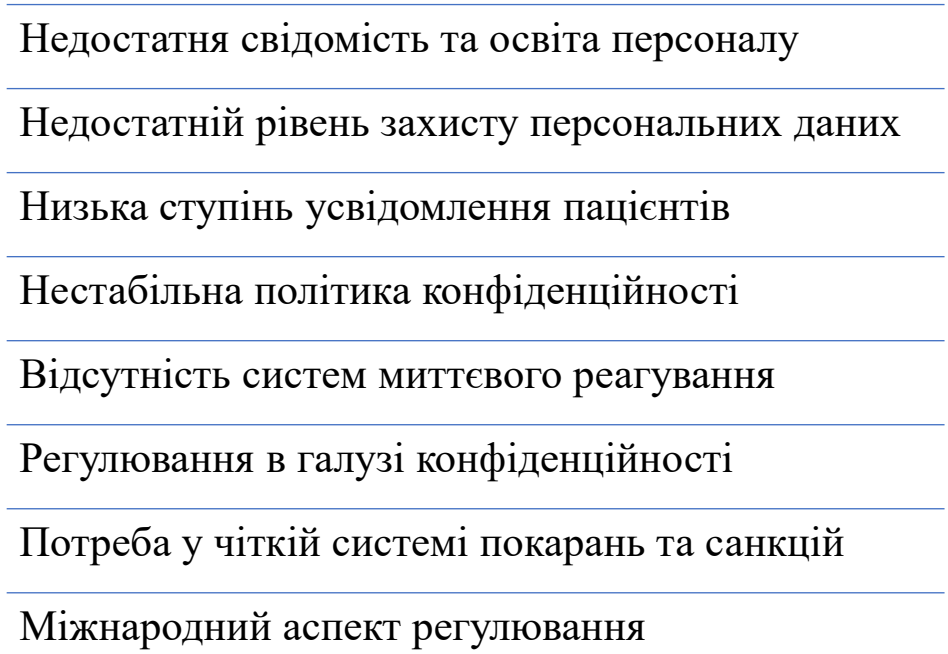


Рисунок 2.3 – Перешкоди та проблеми захисту даних пацієнтів

Першою та однією з ключових перешкод у забезпеченні конфіденційності медичних даних є недостатня свідомість та недостатні навички персоналу у сфері інформаційної безпеки. Часто медичний персонал може бути недостатньо підготовлений до розуміння та дотримання вимог безпеки даних, що може створювати слабкі місця у системі.

Багато лікарень та клінік можуть не мати достатньо ефективних систем захисту персональних даних пацієнтів. Відсутність швидкої ідентифікації та виправлення слабких місць у системі захисту може призвести до несанкціонованого доступу та витоку конфіденційної інформації [29]. Багато

пацієнтів може не мати достатньої інформації про те, як їхні особисті дані зберігаються та захищаються в медичних інформаційних системах. Недостатнє усвідомлення може створювати прогалини в забезпеченні конфіденційності, а також робити пацієнтів більш вразливими до соціального інженерінгу та атак на їх особисті дані.

Брак чіткої та стабільної політики конфіденційності може призводити до непорозумінь та неправильної реалізації заходів безпеки. Політика повинна бути добре визначеною, легко зрозумілою для всього персоналу, і регулярно оновлюватися відповідно до змін у законодавстві та технологічних вимог.

Важливою перешкодою є відсутність систем, що миттєво реагують на потенційні порушення конфіденційності. Багато систем можуть виявити аномалії з певним запізненням, що дає можливість зловмисникам здійснити несанкціонований доступ до даних [28].

Зростання використання інформаційних технологій у медицині призводить до збільшення кіберзагроз та ризиків кібератак. Зловмисники можуть намагатися отримати несанкціонований доступ до електронних медичних записів, шляхом викрадення особистих даних для вивчення чутливої медичної інформації, що потенційно може призвести до серйозних наслідків для пацієнтів.

В сучасних медичних системах часто спостерігається неоднорідність в захисті конфіденційності даних. Різні підсистеми та медичні заклади можуть використовувати різні стандарти та підходи до захисту інформації, що може створювати потенційні точки вразливості для атак та несанкціонованого доступу[26].

Одним із обіцяючих напрямків у розв'язанні проблем конфіденційності є використання технології блокчейн. Це дозволяє створювати розподілені та нехибні записи, забезпечуючи високий рівень відновлення та стійкості до атак. Важливою складовою захисту даних пацієнтів є налагодження ефективного регулювання та визначення відповідальності за порушення конфіденційності. Запровадження чітких стандартів та санкцій сприятиме підвищенню відповідальності та підвищенню рівня безпеки медичних даних. Недостатність

Однією з основних перешкод в забезпеченні конфіденційності медичних даних є відсутність чіткого та вичерпного регулювання в цій галузі. Багато країн можуть стикатися із відсутністю стандартів, які б визначали правила та обов'язки стосовно обробки та захисту медичної інформації. Наявність таких стандартів є критично важливою для визначення прозорих правил та забезпечення їх виконання [29].

Визначення конкретних суб'єктів відповідальності за збереження конфіденційності медичної інформації. Відсутність чіткого розподілу обов'язків та відповідальності може призвести до того, що жоден конкретний суб'єкт не візьме на себе відповідальність за можливі порушення безпеки даних.

Ще однією проблемою є те, що регулювання може відстати від технологічних та соціальних змін. Закони та правила повинні постійно адаптуватися до нових викликів у галузі медичної інформатики, адже старі норми можуть стати застарілими та недостатньо ефективними.

Часто регулювання може бути неефективним через відсутність чіткої системи покарань та санкцій для тих, хто порушує правила конфіденційності медичних даних. Наявність такої системи є ключовою для стимулювання суб'єктів у системі дотримуватися встановлених вимог та заходів безпеки.

Оскільки обмін медичною інформацією може перетинати межі країн, важливо розглядати міжнародний аспект регулювання. Стандарти та норми повинні бути вироблені на міжнародному рівні для забезпечення єдності та взаєморозуміння в області конфіденційності медичних даних [28].

2.4 Ефективність та надійність медичних IT-систем

В сучасному медичному середовищі використання інформаційних технологій стає все більш невід'ємною частиною забезпечення високоякісної та ефективної медичної допомоги. Медичні інформаційні технології (МІТ) включають в себе різноманітні системи та програми, спрямовані на поліпшення управління медичними даними, діагностику, лікування та обмін інформацією між медичним персоналом [24].

Ефективність медичних інформаційних технологій визначається їх здатністю поліпшувати процеси у медичному середовищі, забезпечуючи високий стандарт догляду за пацієнтами. Важливо врахувати швидкість доступу до інформації, точність діагнозів та зручність використання для медичного персоналу.

Швидкість та доступність інформації в медичних IT-системах – це критичні аспекти, що визначають ефективність медичного обслуговування. Забезпечення миттєвого доступу до актуальних медичних даних та швидкої обробки інформації сприяє оперативним прийняттям рішень, покращує якість догляду та задовольняє потреби пацієнтів. Також важливо враховувати зручність використання та переносність даних для оптимізації роботи медичного персоналу. Впровадження технологій штучного інтелекту та аналізу даних допомагає автоматизувати обробку інформації та забезпечує швидке прийняття рішень [32].

Медичні IT-системи покращують точність діагнозів та лікування через автоматизацію діагностичних процесів, використання електронних медичних записів (EMR), моніторинг та аналіз пацієнтських даних. Вони дозволяють індивідуалізувати лікування, уникати помилок при замовленні ліків та забезпечують швидке реагування на зміни стану пацієнтів, покращуючи загальний результат лікування. Медичні IT-системи сприяють зручності та ефективності роботи медичного персоналу через інтуїтивні інтерфейси, доступ до електронних медичних записів (EMR), мобільні додатки та автоматизацію рутинних завдань. Це полегшує роботу, забезпечує швидкий доступ до інформації та вільний час для більш важливих аспектів медичної практики.

Медичні IT-системи також сприяють оптимізації робочого процесу медичного персоналу шляхом впровадження мобільних додатків, що дозволяють здійснювати доступ до інформації з різних пристроїв та місць. Автоматизація рутинних завдань, таких як електронне замовлення ліків, спрощує робочий процес, звільняючи час медичного персоналу для більш ефективного взаємодії з пацієнтами та розробки стратегій лікування. Загалом, ці технології роблять медичну практику більш зручною та результативною [37].

Захист від несанкціонованого доступу – це важливий аспект медичних ІТ-систем, спрямований на забезпечення конфіденційності та цілісності медичної інформації. Це досягається за допомогою сучасних методів шифрування, механізмів аутентифікації та систем моніторингу для виявлення та запобігання недозволеним доступам.

Захист від несанкціонованого доступу в медичних ІТ-системах є важливим елементом забезпечення безпеки медичної інформації. Модерні технології використовують потужні методи шифрування для захисту данних від несанкціонованого перегляду чи зміни. Механізми аутентифікації, такі як біометричні дані чи двофакторна аутентифікація, додають додатковий шар захисту [34].

Системи моніторингу активності слідкують за подіями в мережі та системах, вчасно виявляючи потенційні загрози та нестандартну активність. Це дозволяє оперативно реагувати на можливі порушення безпеки та запобігати їхнім наслідкам [35].

Стійкість до кіберзагроз та вірусів є критичною для медичних ІТ-систем. Вона досягається за допомогою впровадження ефективних антивірусних програм, постійного моніторингу мережі на предмет підозрілої активності та регулярного оновлення програмного забезпечення для закриття вразливостей перед потенційними атаками. Також важливо навчати персонал правилам кібербезпеки для уникнення соціально-інженерних атак та мінімізації ризику зараження систем вірусами чи шкідливими програмами [39].

Забезпечення стійкості до кіберзагроз включає в себе застосування ефективних антивірусних програм, систем моніторингу мережі, регулярне оновлення програмного забезпечення та навчання персоналу з питань кібербезпеки. Ці заходи гарантують ефективний захист від вірусів та шкідливих атак, зберігаючи безпеку та цілісність медичних даних.

2.5 Висновки до другого розділу

У другому розділі було проведено глибокий аналіз ключових аспектів безпеки та ефективності в інформаційних технологіях медицини. Виявлені ризики та проблеми засвідчують значущі виклики, які виникають у процесі впровадження та експлуатації медичних ІТ-систем. Аналіз вказує на важливість безпеки як фундаментального аспекту в медичних ІТ-системах. Ризики несанкціонованого доступу та порушення конфіденційності пацієнтських даних визначають необхідність посилення заходів з кібербезпеки.

Ризики несанкціонованого доступу та порушення конфіденційності пацієнтських даних визначають необхідність посилення заходів з кібербезпеки. Підкреслено серйозні проблеми, пов'язані з конфіденційністю та безпекою даних пацієнтів. Рекомендації включають вдосконалення систем шифрування, усунення можливості несанкціонованого доступу та регулярну перевірку політик конфіденційності. Аналіз підкреслює важливість надійності та ефективності медичних ІТ-систем для забезпечення якісного та безпечного надання медичних послуг.

Важливим є також зосередження на удосконаленні доступності та обміну даними, забезпечуючи стандартизацію та ефективну інтеграцію для безпечного обміну медичною інформацією. Проактивний захист медичних пристроїв стає важливим аспектом для попередження атак та забезпечення стабільності медичного обладнання.

В цілому, розділ 2 системного аналізу ризиків та проблем засвідчив необхідність комплексного підходу до управління безпекою та ефективністю медичних ІТ-систем. Прийняття рекомендацій та вдосконалення відповідних стратегій дозволять зробити застосування інформаційних технологій в медичній сфері більш надійним та безпечним.

РОЗДІЛ 3. СТРАТЕГІЇ УПРАВЛІННЯ РИЗИКАМИ

3.1. Вплив помилок в системах на якість діагностики та лікування

В даному розділі проводиться детальний аналіз впливу можливих помилок в інформаційних технологіях на якість діагностики та лікування в медичних системах. Основна увага приділяється ідентифікації та класифікації помилок, які можуть виникнути в процесі функціонування ІТ-систем. Розглядаються сценарії можливих невірних діагнозів, а також наслідки, які ці помилки можуть мати на подальші етапи лікування пацієнтів. Зокрема, визначаються технічні та організаційні аспекти, що призводять до виникнення помилок, та розглядаються можливі стратегії їх уникнення або корекції [45].

Додатково розглядаються сучасні підходи та інноваційні методи, спрямовані на зменшення ризику виникнення помилок у медичних ІТ-системах. Проаналізовано позитивний вплив автоматизації та інтелектуальних алгоритмів на процеси діагностики та прийняття лікарських рішень. Визначаються ключові аспекти, які можуть впливати на точність та надійність медичних інформаційних систем та пропонуються стратегії для подолання цих проблем.

Приклади можливих помилок в системах медичної інформації можуть включати:

1. Помилки вводу даних: Неправильне введення пацієнтських даних або результатів аналізів може призвести до невірного визначення діагнозу чи призначення непотрібного лікування.

2. Технічні збої систем: Помилки або збої в програмному забезпеченні, які виникають через недоліки в програмі або неправильну інтеграцію, можуть спричинити некоректне функціонування систем та вплинути на точність діагностики.

3. Проблеми з безпекою даних: Витоки конфіденційної медичної інформації через недостатні заходи кібербезпеки можуть викликати серйозні наслідки для пацієнтів та порушити довіру до медичних інформаційних систем.

4. Неправильне інтерпретування аналітичних даних: Використання неправильних алгоритмів для аналізу клінічних даних може призвести до неправильного тлумачення результатів та видачі невірного діагнозу.

5. Стратегії управління цими ризиками включають в себе вдосконалення процесів введення даних, впровадження ефективних засобів моніторингу технічного стану систем, застосування сучасних методів шифрування для забезпечення безпеки даних, а також постійне вдосконалення аналітичних алгоритмів з метою підвищення їхньої точності [43].

3.2. Ризики, пов'язані з медичними даними та їх обробкою

Управління ризиками в контексті застосування інформаційних технологій у медичній галузі. Однією з ключових областей дослідження є взаємозв'язок між помилками та неполадками в системах і якістю діагностики та лікування пацієнтів. Розділ вивчає ризики, що виникають у зв'язку з медичними даними та їх обробкою, вплив перерв у роботі ІТ-систем на надання медичних послуг, а також принципи розв'язання проблем із застосуванням системного аналізу. Розглядаються також заходи забезпечення кібербезпеки та методи підвищення ефективності ІТ-систем у медицині. Детальний огляд ризиків і виявлення їхніх кореневих причин визначає важливість впровадження ефективних стратегій управління ризиками для забезпечення безпеки та стабільності медичних ІТ-систем [44].

Це важливий аспект, оскільки обробка медичної інформації повинна відповідати високим стандартам безпеки та конфіденційності. Розглянемо деякі основні аспекти цього питання:

Конфіденційність медичних даних: Одним з ключових ризиків є порушення конфіденційності медичної інформації. У випадку несанкціонованого доступу до цих даних може статися витік особистої інформації пацієнтів, що має серйозні етичні та юридичні наслідки.

Кіберзлочини та атаки: Зростання кількості кіберзлочинів у медичній галузі створює загрозу для цілісності медичних даних. Різноманітні види атак, такі як розкрадання даних, вимагання викупу та інші, можуть стати серйозними загрозами безпеці медичної інформації.

Нестабільність інформаційних систем: Технічні збої та відмови в роботі інформаційних систем можуть призвести до втрати доступу до медичних даних у критичний момент. Це може вплинути на надання медичних послуг та вирішення невідкладних ситуацій.

Вимоги до збереження даних: Питання збереження медичних даних також є важливим аспектом. Невірне зберігання може призвести до втрати даних або їх неправильного використання.

Управління цими ризиками вимагає впровадження найсучасніших заходів безпеки, шифрування даних, міцних систем ідентифікації та встановлення строгих протоколів доступу. Також важливо постійно вдосконалювати заходи забезпечення безпеки, враховуючи постійні зміни в технологічному середовищі та нові виклики [45].

3.3. Вплив перерв у роботі IT-систем на надання медичних послуг

Важливість функціональності безперебійної роботи інформаційних технологій в медичній сфері. Основною метою є визначення ризиків, які виникають при можливих перебоях у роботі IT-інфраструктури та їхній вплив на процеси надання медичних послуг.

У зв'язку зі стрімким розвитком цифрових технологій, належне функціонування медичних IT-систем стає ключовим аспектом забезпечення безперебійного обслуговування пацієнтів. Розглядаються сценарії, які можуть викликати перерви в роботі, такі як технічні неполадки, кібератаки, природні лиха та інші фактори.

Детальний аналіз дозволяє визначити стратегії управління ризиками, спрямовані на зменшення можливих наслідків перерв та вдосконалення надійності медичних IT-систем. Питання відновлення роботи, аналіз впливу

перебоїв на доступ до медичної інформації та шляхи покращення систем резервного копіювання розглядаються для забезпечення ефективності та безпеки медичного обслуговування в умовах перебоїв в роботі ІТ-інфраструктури [45].

Окремий акцент робиться на впливі перерв у роботі ІТ-систем на якість та доступність медичних послуг. Зокрема, розглядаються можливі наслідки для процесів діагностики, лікування та взаємодії з пацієнтами у випадку тимчасового припинення роботи медичних інформаційних систем.

Подальший розгляд зосереджений на визначенні критичних точок в системі, які, при їхній вразливості, можуть призвести до значних порушень у наданні медичних послуг. Розглядаються стратегії врегулювання ризиків, що включають у себе планування аварійного відновлення та запобігання можливим перервам.

Важливим аспектом є також вплив перерв на збереження та обробку медичних даних. Розглядаються методи забезпечення неперервності обробки та збереження інформації, зокрема застосування систем резервного копіювання та відновлення. Це спрямовано на забезпечення конфіденційності та цілісності медичних даних навіть у найскладніших ситуаціях.

Такий аналіз допомагає розробити комплексні стратегії управління ризиками, спрямовані на забезпечення безперебійності медичних послуг та зменшення впливу можливих перерв у роботі ІТ-систем на здоров'я та безпеку пацієнтів.

В даному контексті, подальший аналіз спрямований на виявлення ключових аспектів ризиків, які можуть виникнути внаслідок перерв у роботі ІТ-систем у медичному середовищі. Визначення таких ризиків включає ретельний огляд можливих точок вразливості та можливих сценаріїв аварій.

Один із аспектів розгляду – вплив перерв на ефективність діагностики та лікування. Ситуації, коли доступ до медичних інформаційних систем тимчасово обмежений, може значно ускладнити процеси встановлення діагнозу та призначення лікування. Це може стати особливо критичним у випадках термінової медичної допомоги [41].

Другий аспект – вплив на безпеку та конфіденційність медичних даних. Перерви в роботі систем можуть порушити режим доступу до інформації та спричинити ризик витоку конфіденційних даних. Це може мати серйозні наслідки для пацієнтів та порушити довіру до медичних інформаційних систем.

Додатково важливо зазначити, що ризики, пов'язані з медичними даними та їх обробкою, можуть виникнути внаслідок несанкціонованого доступу до систем, втрати або пошкодження інформації під час перерв у роботі, а також через непередбачені ситуації, такі як технічні збої або кібератаки.

Спеціальний акцент може бути зроблений на важливості ефективного моніторингу та негайного виявлення будь-яких аномалій у роботі систем. Розробка та впровадження стратегій реагування на екстрені ситуації, а також планів відновлення роботи систем після перерв, є ключовими аспектами у забезпеченні безпеки та стабільності медичних ІТ-систем [47].

3.4 Принципи розв'язання проблем із застосуванням системного аналізу

В застосуванні системного аналізу в медичній сфері важливо керуватися рядом принципів, які дозволяють ефективно вирішувати проблеми та оптимізувати роботу системи охорони здоров'я. Нижче представлено деякі основні принципи.

Глобальний підхід в принципах системного аналізу в медичній сфері необхідний для того, щоб розглядати систему охорони здоров'я як цілісний та взаємопов'язаний комплекс. Приділяючи увагу працівникам, технологіям та іншим важливим елементам. Глобальний підхід у системному аналізі дозволяє не лише реагувати на конкретні проблеми, але й розглядати систему охорони здоров'я як динамічний та взаємопов'язаний комплекс, що потребує постійного вдосконалення та оптимізації. Це може призвести до розробки більш ефективних та інтегрованих рішень для надання медичних послуг та підвищення загального стану суспільного здоров'я. Основною метою якого є, забезпечити ефективну роботу всієї системи та поліпшення якості надання медичної допомоги [43].

Пацієнтсько-орієнтований підхід є ключовим аспектом в системному аналізі в медичній сфері і визначається акцентом на задоволенні та врахуванні потреб пацієнтів у всіх аспектах надання медичних послуг. Пацієнтсько-орієнтований підхід є важливою складовою вдосконалення медичної системи, оскільки він спрямований на покращення задоволеності пацієнтів та досягнення кращих клінічних результатів. Цей підхід визнає важливість включення пацієнтів у процеси прийняття рішень і допомагає створити ефективну та дружелюбну медичну систему.

Інтеграція технологій допомагає поліпшити ефективність медичних процесів, забезпечити доступність та обмін інформацією, підвищити точність діагностики та лікування, а також сприяє більш ефективному взаємодії між медичним персоналом та пацієнтами [46].

Динамічний аналіз враховує постійні зміни та адаптацію системи охорони здоров'я до нових умов. Він дозволяє пристосовувати стратегії та процеси, щоб ефективно відповідати на виклики та забезпечувати високий рівень надання медичних послуг в змінюючихся умовах. Динамічний аналіз акцентує увагу на нових захворюваннях та епідеміях, враховуючи їх поширення та вплив на медичну систему. Розвиток та ефективність системи охорони здоров'я залежать від швидкості та ефективності реагування на нові медичні виклики.

Фінансові зміни в системі охорони здоров'я теж є предметом динамічного аналізу. Зміни в фінансуванні можуть впливати на доступність медичних послуг, ефективність та якість надання лікування. Зміни в лікувальних підходах, наукові відкриття та постійний розвиток медичної науки також вимагають уваги. Система охорони здоров'я повинна бути готовою впроваджувати нові методи та технології для поліпшення результатів лікування.

Цей підхід дозволяє адаптуватися до нових викликів, ефективно реагувати на епідемії та забезпечувати високий рівень медичної допомоги. Застосування динамічного аналізу враховує різноманітність факторів, що впливають на систему охорони здоров'я, і створює основу для розвитку гнучких стратегій [45].

Партнерство та комунікація в системному аналізі медичної сфери виступають як основні елементи для досягнення взаєморозуміння, співпраці та покращення результатів у наданні медичних послуг.

І мабуть найболовніший принцип на якому відбувається сучасна медицина це маціентська орінтованість. Пацієнтська орієнтованість – це ключовий принцип у сучасній медичній сфері, який визначає фокус системного аналізу на задоволенні та врахуванні потреб та очікувань пацієнтів. Цей підхід визнає, що пацієнти є центром медичної системи, і всі аспекти надання медичних послуг повинні бути спрямовані на поліпшення їхнього досвіду та результатів лікування.

Пацієнтська орієнтованість в системному аналізі визнається як важлива складова для поліпшення якості медичної допомоги та задоволення пацієнтів. Вона сприяє формуванню ефективних та людяно-центрованих медичних систем, де пацієнти відчувають себе партнерами у своєму власному лікуванні [46].

3.5 Заходи щодо забезпечення кібербезпеки

У сучасному світі, коли все більше і більше речей стає цифровими, важливо розуміти, як захищати комп'ютери, інтернет-з'єднання та дані від поганих людей, які можуть намагатися взяти їх без дозволу. Це, і є основою кібербезпеки – заходи, які допомагають убезпечити цифрові речі від небезпеки.

Це важливо через те, що інтернет може бути місцем, де люди намагаються зламати або пошкодити комп'ютери та інші пристрої. Це може стати проблемою для особистої безпеки та безпеки особистих чи важливих даних. Кібербезпека – це не просто вирішення проблем, але і спосіб думати та робити речі, щоб залишатися в безпеці в інтернеті [43].

Першим елементом для захисту будуть медичні пристрої. Забезпечення безпеки медичних пристроїв – це заходи, які мають на меті захистити їх від неправомірного доступу та зберегти їхню працездатність. Це важливо для того, щоб уникнути ситуацій, коли хтось намагається незаконно втрутитися у роботу медичного обладнання або завдати йому шкоди.

Наступним етапом, який є не менш важливішим буде шифрування медичної інформації. Цей процес полягає в перетворенні медичної інформації у спеціальний код, який надійно захищений від несанкціонованого доступу. Такий підхід важливий для запобігання несанкціонованому читанню чи зміні медичних даних, зокрема, історій хвороб, результатів тестів та інших особистих відомостей [46].

Шифрування використовує математичні алгоритми для створення ключа, який є необхідним для розкодування зашифрованої інформації. Це забезпечує додатковий шар захисту в тому випадку, якщо дані потраплять у невірні руки. При використанні шифрування медичних даних навіть у випадку проникнення зловмисників в систему, вони не зможуть зрозуміти або використати отриману інформацію без необхідного ключа.

Цей підхід не лише допомагає виконати вимоги до конфіденційності у сфері медицини, але і створює довіру серед пацієнтів, надаючи їм впевненість у безпеці та конфіденційності їхніх особистих медичних даних.

Кіберзахист мереж – це спроба захистити комп'ютерні системи та мережеві ресурси від кіберзагроз. Це включає в себе використання різних заходів, таких як брандмауери для контролю трафіку, системи виявлення вторгнень для реагування на небезпеку, шифрування для захисту інформації та постійне оновлення програмного забезпечення для усунення вразливостей.

Сегментація мережі у медичній галузі є схожою на розподіл відділів або кімнат в лікарні. Це як створення ізольованих просторів, де різні види інформації або медичні пристрої можуть працювати безпечно, не взаємодіючи напряму один з одним. Для більшої безпеки кожен простір має свої власні правила доступу і обмеження, що допомагає уникнути ризиків і збільшити безпеку [48].

Кібербезпека у медицині визначається як життєво важливий елемент захисту медичної інформації та мережевих систем від кіберзагроз. Застосування відповідних заходів, таких як сегментація мережі, шифрування та захист від вірусів, є ключовим для забезпечення конфіденційності, доступності та цілісності медичної інформації. Кібербезпека допомагає уникнути потенційних загроз для пацієнтів, забезпечуючи безпечне та надійне функціонування системи.

3.6. Способи підвищення ефективності ІТ-систем у медицині

Створення інноваційного медичного додатка є перспективною ідеєю, спрямованою на покращення ефективності ІТ-систем у сфері охорони здоров'я. Додаток об'єднає функції фітнес-годинників для моніторингу показників організму, що визначається сімейним лікарем пацієнта під час медичних обстежень та аналізів.

Центральною функцією додатка буде сторінка, яка оперативно реагує на надзвичайні ситуації, де з будь-якого мобільного пристрою можна отримати важливі медичні дані пацієнта. Це забезпечить швидкий доступ до групи крові, рівню тиску, цукру та інших критичних показників. Крім того, вказані будуть особисті дані пацієнта та контактні інформації родичів чи опікунів.

Такий додаток не лише сприятиме ефективній медичній діагностиці, але й реагуватиме на екстрені ситуації, забезпечуючи безпеку та швидку взаємодію між пацієнтом та медичними фахівцями. Цей інноваційний медичний додаток має потенціал стати важливим інструментом для управління здоров'ям та покращення співпраці між пацієнтами та медичними працівниками. Однією з корисних функцій може бути можливість вести електронний журнал самопочуття, де пацієнти можуть зафіксувати свої відчуття, симптоми та зміни у здоров'ї.

Додатково, можна врахувати інтерактивний календар з нагадуваннями про прийом ліків, медичні обстеження та консультації. Такий функціонал допоможе підтримувати пацієнтів у своїх лікувальних режимах і забезпечити дотримання рекомендацій лікарів.

Також, можливо, варто розглянути можливість інтеграції з іншими медичними додатками або сервісами, що дозволить обмінюватися даними між різними платформами та забезпечить комплексний погляд на стан здоров'я пацієнта.

Загалом, гнучкість та інтерактивність додатка можуть зробити його більш привабливим та корисним для пацієнтів, сприяючи вдосконаленню процесу медичного обслуговування та підвищенню ефективності ІТ-систем у медицині.

Також можливо варто врахувати розширення функціоналу додатка на підтримку програми лояльності для пацієнтів. Це може включати систему нагородження за активну участь у збереженні здоров'я, виконання рекомендацій лікарів та участь у профілактичних заходах. Така система стимулювання може підтримувати пацієнтів у прийнятті більш відповідального підходу до свого здоров'я.

Крім того, інтерактивний модуль для консультацій в реальному часі з медичним персоналом може забезпечити пацієнтам можливість отримувати експертні поради та відповіді на питання безпосередньо через додаток. Це може полегшити спілкування з лікарем та підвищити доступність медичної консультації.

Зрештою, можливо, розгляньте включення розділу для освіти пацієнтів, де надаються інформація та рекомендації з підтримки здоров'я, що дозволяє пацієнтам активніше брати участь у власному лікуванні та профілактиці захворювань.

Створення вдосконаленої медичної системи, що об'єднує функціонал додатків "Дія" та Steam, визначає новий рівень безпеки та аутентифікації. Забезпечуючи захист, аналогічний банківським стандартам, система вимагатиме введення даних банківської карти для впевненості в тому, що особа, яка входить у медичний електронний кабінет, є його легітимним власником.

Двофакторна аутентифікація, представлена мобільним додатком, забезпечить подвійний шар захисту. Генерація унікальних кодів кожну хвилину, що вводяться для входу, міцно захищатиме медичні дані від несанкціонованого доступу. Це перевершує стандартні методи та зробить взаємодію із системою максимально безпечною та захищеною.

Такий комплексний підхід до безпеки системи медичного обслуговування гарантує високий ступінь захисту конфіденційності та надійність доступу до важливої медичної інформації, віддзеркалюючи важливість та чутливість цих даних.

Ця інноваційна медична система, збагачена захистом, який перевершує стандарти, пропонує додатковий рівень впевненості в конфіденційності

медичних даних. Використання ідентифікації за допомогою банківської карти додає елемент біометричного захисту, оскільки ці дані є особистими та надійно захищеними від сторонніх втручань.

Сполучення цього захисту із мобільним додатком, який генерує унікальні коди, підвищує рівень аутентифікації. Крім того, можливість інтеграції із функціоналом відомої платформи Steam надає елемент гейміфікації, що може стимулювати пацієнтів до більш активного участі в своєму здоров'ї через систему нагород та досягнень.

Важливим аспектом є інформаційна прозорість та освітленість пацієнтів. Забезпечення легкого доступу до освітніх ресурсів та статей, інтегрованих безпосередньо в систему, може сприяти підвищенню медичної грамотності та свідомого ставлення до власного здоров'я.

Узагальнюючи, впровадження такої інтегрованої медичної системи не лише гарантує безпеку та доступність даних, але і створює мотивуюче середовище для пацієнтів, підкреслюючи значущість активного участі в процесах збереження та покращення здоров'я.

РОЗДІЛ 4. ОХОРОНА ПРАЦІ І БЕЗПЕКА В УМОВАХ НАДЗВИЧАЙНИХ СИТУАЦІЙ

Безпека життєдіяльності відіграє важливу роль у нашому повсякденному житті, спрямовуючи зусилля на запобігання травм, збереження здоров'я та забезпечення загального благополуччя. Ця концепція стосується різних аспектів нашого існування, включаючи домашнє оточення, робоче середовище та інші сфери.

Уникнення травм та негативних подій є ключовим завданням безпеки життєдіяльності. Заходи безпеки спрямовані на збереження здоров'я та захист від небезпечних факторів довкілля. Важливою частиною є інформування та навчання населення правилам безпеки для усвідомленого та обережного поводження в різних ситуаціях.

Основи охорони праці визначають сукупність принципів та заходів, які спрямовані на забезпечення безпеки та захисту працівників під час виконання їхніх трудових обов'язків. Ці принципи важливі для забезпечення здоров'я працівників та підтримання оптимальних умов праці.

Основний аспект полягає в оцінці ризиків, пов'язаних із робочими умовами. Це передбачає систематичний аналіз потенційних небезпек та визначення заходів для зниження цих ризиків. Застосування засобів індивідуального захисту, таких як захисні костюми та пристрої, є важливою частиною основ охорони праці [50].

4.1 Долікарська допомога при ураженні електричним струмом

При отриманні удару електричним струмом необхідно негайно визволяти постраждалого від елементів обладнання, які проводять електричний струм. Дотик до струмопровідних частин (мережі під напругою) у більшості випадків призводить до судом'язів, що робить неможливим самостійне відірвання людини від провідника. Тому важливо оперативно відключити ту частину електрообладнання, до якої доторкається людина.

Будь-яке затримання при наданні допомоги, а також невміння особи, яка надає допомогу, надати кваліфіковану допомогу, може призвести до летальних наслідків для особи, що перебуває під дією струму.

При визволенні постраждалих від електричних провідників чи кабелів у електроустановках з напругою до 1000 В важливо відключити електричний струм. Для цього можна використовувати сухий одяг, палицю, дошку, шапку, сухі рукавиці чи діелектричні рукавиці. Проводи слід перерізати інструментом з ізольованими ручками або перерубати сокирою з дерев'яним сухим топорищем.

Важливо відзначити, що при відтягуванні постраждалого від струмопровідних частин слід уникати дотику до навколишніх металевих предметів та відкритих частин тіла постраждалого. Відтягуючи його за ноги, необхідно уникати контакту з взуттям, оскільки воно може бути вологим і стати провідником електричного струму [49].

Особа, яка надає допомогу, повинна застосовувати діелектричні рукавиці або обгортати їх шарфом, надягнути їх під рукав піджака або пальта. Також можна ізолювати себе, стоячи на гумовому килимку чи сухій дошці.

При визволенні постраждалих в електроустановках з напругою понад 1000 В рекомендується використовувати діелектричні рукавиці та взути діелектричні боти. Також важливо діяти за допомогою ізолюючої штанги чи ізолюючих кліщів (див. рисунок 4.1) [51].

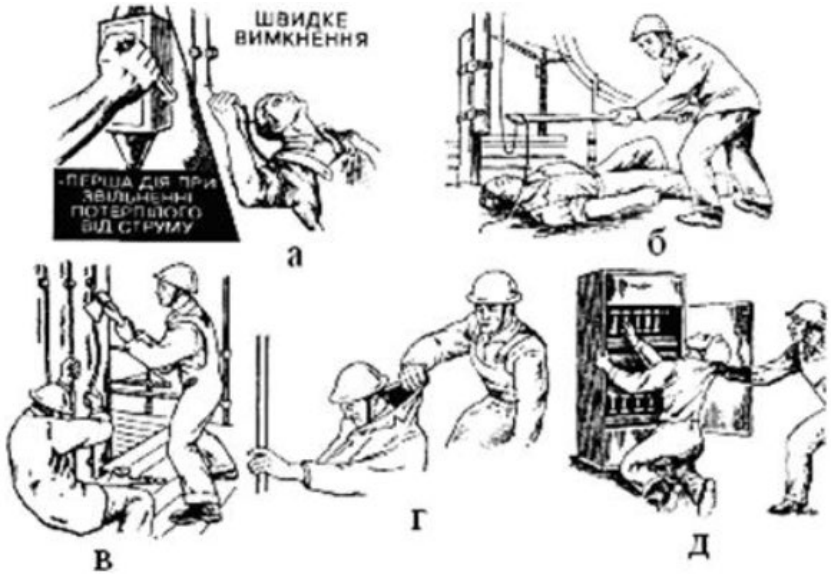


Рисунок 4.1. – Звільнення потерплого від дії струму

Якщо провід торкається землі, важливо пам'ятати про ризик крокової напруги. Тому після визволення потерпілого від струмопровідних частин слід вивести його із небезпечної зони. Пересуватися в зоні розтікання струму по землі без засобів захисту важливо, утримуючи ноги разом і не відриваючи їх одну від одної.

Наслідки своєчасної та правильно наданої допомоги на місці події можуть бути драматично зменшені, якщо при підготовці до транспортування і доставці потерпілого до медичної установи будуть дотримані всі відповідні правила. Ключовим фактором є не лише транспортування та обраний вид транспорту, але і швидкість вжиття заходів, що забезпечили максимальний комфорт і безпечну позицію потерпілого [49].

Найефективніше пересування потерпілого здійснюється за допомогою нош. Для цього можна використовувати доступні матеріали, такі як дошки або одяг. Переносити потерпілого можна також, тримаючи його на руках. Пріоритетом є покласти потерпілого на ноші, які попередньо застелені ковдрою або одягом. Ноші розміщуються з того боку потерпілого, де відбулося ушкодження.

У випадку, якщо допомагають дві особи, вони повинні стати по обидва боки нош. Один із них підкладає руки під голову і груди, а інший – під крижі і коліна потерпілого. Потім, обережно піднімаючи його без різких рухів, потерпілого опускають на ноші, утримуючи пошкоджену частину тіла. Потім його слід накрити чимось, що знаходиться під рукою, наприклад, одягом чи ковдрою.

При підозрі на перелом хребта потерпілого клаці обличчям вгору на твердих ношах, як щит чи двері. Якщо таких нош немає, можна використати ковдру або пальто, а потім покласти його на живіт. У разі підозри на перелом кісток тазу, помістіть потерпілого на спину із зігнутими ногами. Під коліна покладіть валик із вати, рушника чи сорочки. Несіть потерпілого ногами вперед по рівній поверхні, а при підйомі – головою вперед. Ноші повинні залишатися горизонтальними. При транспортуванні до машини розмістіть його на тих самих ношах, підклавши м'який матеріал, такий як ковдра чи солома [48].

4.2. Загальні вимоги безпеки до обладнання та технологічних процесів

У сучасних умовах виробничий процес пов'язаний із ризиками, які вимагають системного підходу до безпеки праці. Три основні компоненти цього підходу - безпека виробничого обладнання, технологічних процесів і виконання робіт. Норми безпеки для виробничого обладнання (за винятком того, що випромінює іонізуюче випромінювання), визначені у ДСТУ ГОСТ 12.2.003–91. ССБТ. Забезпечення безпеки виробничого обладнання здійснюється шляхом:

• визначення принципів дії, джерел енергії та параметрів робочих процесів;

• мінімізації енергії, що споживається чи накопичується;

• використання вбудованих засобів захисту та інформації щодо можливих небезпечних ситуацій;

• застосування автоматизації, дистанційного керування та контролю;

• дотримання ергономічних стандартів та обмеження фізичних і нервово-психологічних навантажень на працівників [49].

Виробниче обладнання повинно відповідати вимогам безпеки протягом експлуатації. У разі неможливості дотримання цих вимог, обладнання має бути оснащене захисними засобами, такими як огородження чи блокування. Небезпечні зони повинні бути захищені відповідно до стандартів безпеки, наприклад, ДСТУ ГОСТ 12.2.062–81, інші ризиковані елементи мають бути теплоізольовані або розташовані у безпечних місцях. Допоміжні пристрої повинні уникати небезпеки при раптовому відключенні енергії та під час відновлення енергопостачання. Виробниче обладнання повинно відповідати вимогам пожежозахисту та уникати накопичення статичної електрики. Якщо обладнання виділяє шкідливі речовини або є пожежо- та вибухонебезпечним, воно повинно включати вбудовані пристрої для локалізації цих ризиків. У випадку їх відсутності, обладнання повинно мати місця для підключення автономних пристроїв локалізації [50].

Виробниче обладнання повинно відповідати вимогам безпеки, уникати шкідливих факторів та забезпечувати зручне та безпечне робоче середовище.

Місцеве освітлення та конструкція робочого місця повинні відповідати стандартам безпеки. Потрібно робити це у сидячому положенні для забезпечення ергономії та уникнення небезпеки. Система управління обладнанням має гарантувати безпечну роботу у всіх режимах та в умовах зовнішніх впливів. Інформаційні засоби на робочих місцях та центральний пульт повинні швидко та коректно надавати інформацію. Пуск та перезапуск обладнання можливий лише за допомогою органів управління пуском, і органи аварійної зупинки повинні залишатися у положенні зупинки до їх повернення у вихідне положення обслуговуючим персоналом [49].

4.3 Оцінка стійкості роботи обєкту економіки до впливу поражаючих факторів ядерної зброї

Сучасний світ стикається з високим рівнем геополітичних напружень, які можуть викликати загрозу використання ядерної зброї. Оцінка стійкості економічних об'єктів до впливу поражаючих факторів ядерної зброї набуває вельми важливого значення у забезпеченні національної та глобальної безпеки.

У відкритому сучасному світі використання ядерної зброї несе загрозу, що поширюється далеко за військовий аспект, торкаючись основних соціальних та економічних аспектів. Зокрема, гуманітарні наслідки подібних випадків дуже значущі. Не лише велика кількість жертв і постраждалих внаслідок радіаційних наслідків, але і масові порушення соціальної структури та розлади в управлінні людськими ресурсами [52].

На економічному рівні використання ядерної зброї супроводжується серйозними втратами продуктивності. Зруйнування інфраструктури та велика кількість вимушених змін у виробництві призводять до значних економічних втрат. Крім того, можливий негативний вплив на інвестиційний клімат та природну нестабільність, що може спричинити спад розвитку економіки.

Глобальні ефекти використання ядерної зброї також варто враховувати. Зокрема, створення "ядерної зими" через великі пожежі та викидання вуглекислого газу може призвести до глобального похолодання і значних змін

клімату. Крім того, можливі торгові та економічні обмеження через заходи із знищення ядерної зброї та реакції на їхнє використання.

Використання ядерної зброї може призвести до серйозних загроз для економічної структури, охоплюючи фізичне знищення інфраструктури, втрату критичної інформації, екологічні проблеми, руйнування фінансової стійкості, порушення ланцюга постачання, психологічний тиск. Заходи щодо безпеки стають необхідними для запобігання та пом'якшення можливих наслідків.

4.4 Вплив ядерної зброї її загрози та багатогранні наслідки

Використання ядерної зброї може призвести до руйнування фізичної інфраструктури, втрати критичної інформації та джерел, серйозних екологічних проблем, руйнування фінансової стійкості, порушення ланцюга постачання та негативного психологічного впливу. Застосування в ядерній сфері має потенційно руйнівні наслідки для суспільства та економіки, і тому необхідно вживати ефективні заходи безпеки для запобігання та пом'якшення цих наслідків. Використання ядерної зброї породжує низку серйозних наслідків, і фізичне руйнування є однією з ключових складових цього впливу. Оцінка ступеня фізичного зруйнування враховує кількість та потужність ядерних вибухів, а також точність їхнього місцезнаходження [51].

Спричинене вибухами руйнування включає у себе не лише будівлі та інфраструктуру, але і природні ресурси. Це може вести до масових людських втрат, серйозних екологічних катастроф, великих зрушень в екосистемах. Помітні також будуть пожежі, що виникнуть в результаті теплового випромінювання вибухів, і ризик радіоактивного забруднення, яке може поширитися на великі відстані від епіцентру. Напрямок вітру та інші атмосферні умови гратимуть важливу роль у розповсюдженні забруднюючих речовин.

Крім того, зміни в ландшафті, такі як утворення кратерів, можуть суттєво вплинути на регіональну географію та гідрологію. Усе це визначає розмір і тривалість відновлення після подібного катастрофічного випадку.

Вибух може призвести до зруйнування інформаційних систем, що мають велике значення для економіки та функціонування суспільства. Втрата даних може стосуватися не лише фізичних архівів, але й електронних систем зберігання, включаючи банківські системи, державні реєстри, індустріальні бази даних [52].

Критичні ресурси, такі як енергетичні вузли, водопостачання, транспортна інфраструктура, можуть бути серйозно пошкоджені, що призведе до різкого зниження рівня життя населення та функціонування економічних систем. Внаслідок цього виникнуть проблеми з логістикою, забезпеченням продуктами харчування, ліками, а також із забезпеченням транспорту та комунікацій.

Оцінка втрат та відновлення інфраструктури та інформаційних ресурсів є складною задачею, оскільки вона взаємодіє з іншими аспектами впливу ядерної зброї.

Уражена територія може стати непридатною для життя на тривалий період через радіоактивне забруднення ґрунту, водойм, і атмосфери. Це має серйозні наслідки для біорізноманіття, здоров'я людей і тварин, а також для сільськогосподарської діяльності. Зміни в екосистемах можуть вплинути на різноманіття видів та водопостачання. Підвищення рівня радіоактивності в ґрунті може призвести до отруєння рослин, що впливає на тваринний світ і, в кінцевому рахунку, на людей через продовольчий ланцюг.

Екологічні аспекти, пов'язані з застосуванням ядерної зброї, суттєво впливають на навколишнє середовище, що створює величезні виклики для екосистем та людського здоров'я. Однією з найпоширеніших екологічних загроз є ядерне забруднення, яке виникає в результаті вибуху ядерного пристрою.

Фізичне руйнування об'єктів, що вибухають, викликає вивільнення великої кількості радіоактивних матеріалів у навколишнє середовище. Це може призвести до радіоактивного забруднення ґрунту, водойм та атмосфери. Такі зони стають небезпечними для життя і можуть залишатися такими протягом тривалого часу, ускладнюючи або навіть роблячи неможливим відновлення екосистем [50].

Екологічні наслідки охоплюють не тільки просторовий аспект, але й часовий. Радіоактивні речовини можуть періодично викидатися протягом довгих періодів часу, збільшуючи масштаб забруднення та поглиблюючи його вплив на природу.

Застосування ядерної зброї може мати серйозні наслідки для економічної структури країни чи регіону. Фізичне руйнування, що виникає внаслідок вибухів, може призвести до знищення важливих інфраструктурних об'єктів, таких як міста, промислові об'єкти, транспортні вузли тощо. Це призведе до величезних витрат на відновлення та відновлення життєво важливих систем [52].

Втрата інформації та критичних ресурсів також становитиме суттєвий виклик. Ядерні атаки можуть призвести до знищення даних, комунікаційних мереж та цілісності інформаційних систем. Крім того, втрата критичних джерел, таких як енергія, вода та інші ресурси, обмежить здатність країни функціонувати на повний обсяг.

Екологічні проблеми також будуть вагомим аспектом. Радіоактивне забруднення внаслідок ядерних вибухів може привести до забруднення ґрунту, водних ресурсів та атмосфери. Це вплине на екосистеми, сільське господарство та загальне здоров'я населення, що потребує великих зусиль для відновлення та ліквідації наслідків.

Порушення ланцюга постачання виникне через знищення та перерви у транспортних і комунікаційних мережах, що призведе до важкостей у забезпеченні товарами та послугами. Це вплине на роботу підприємств, споживчий попит та загальну стабільність економічного середовища.

Психологічні моменти включають в себе страх, стрес та тривогу населення, що може вплинути на його здоров'я та працездатність. Прагнення влади забезпечити безпеку і підтримати психологічний стан громадян стане невід'ємною частиною ефективної стратегії відновлення [50].

Заходи щодо безпеки передбачатимуть впровадження систем протидії ядерній загрозі, розробку та вдосконалення планів дій в разі подібних ситуацій, а також сприяння міжнародному співробітництву в області ядерної безпеки.

Крім того, для подолання наслідків загроз ядерної зброї необхідно розглядати різні аспекти ефективного господарського відновлення та розвитку. Серед них можна виділити:

Інфраструктурні проекти: Реконструкція та відновлення інфраструктури, такої як транспортні мережі, енергетичні системи та комунікації, є ключовим елементом економічного відновлення. Реалізація інфраструктурних проектів сприяє збільшенню виробничих можливостей та підтримує економічний зріст.

Соціально-економічні заходи: Підтримка населення через соціальні програми, медичну допомогу та психологічну підтримку є важливим аспектом відновлення громади. Заходи зі створення нових робочих місць та фінансова допомога допомагають відновити стабільність в соціальній та економічній сферах.

Науково-технічний розвиток: Інвестиції в наукові дослідження та технологічний розвиток сприяють створенню інноваційних рішень для вирішення проблем, пов'язаних з наслідками ядерної атаки. Розвиток нових технологій може сприяти відновленню та покращенню економічної продуктивності.

Міжнародне співробітництво: Спільна дія та обмін ресурсами між країнами сприяє вирішенню глобальних викликів, пов'язаних із наслідками ядерної загрози. Міжнародні партнерства сприяють обміну найкращими практиками, технологіями та ресурсами для відновлення постраждалих регіонів.

Зелена економіка: Відновлення економіки після ядерної загрози може бути використане як можливість переорієнтації на сталість та екологічно чисті технології. Використання принципів зеленої економіки сприяє стійкому розвитку та зменшенню впливу на навколишнє середовище [51].

У підсумку, оцінка стійкості об'єкту економіки до впливу ядерної зброї виявляється важливим завданням, що вимагає комплексного дослідження та застосування ефективних стратегій управління ризиками. Розглядаючи фізичне руйнування, втрату інформації, екологічні проблеми, руйнування фінансів, порушення ланцюга постачання та психологічні аспекти, можна визначити, що протидія впливу ядерної загрози передбачає не лише відновлення матеріальних

ресурсів, але й здатність суспільства та економіки адаптуватися та розвиватися в умовах надзвичайних обставин. Розробка та впровадження комплексних стратегій відновлення та розвитку, спрямованих на інфраструктурні проекти, соціально-економічні заходи, науково-технічний розвиток, міжнародне співробітництво та принципи зеленої економіки, може стати основою для забезпечення стійкості та відновлення після потенційного впливу ядерної небезпеки [52].

ВИСНОВКИ

Дипломна робота присвячена аналізу впливу інформаційних технологій на сучасну медицину з точки зору системного аналізу та ризик-менеджменту. Розглянуті аспекти тематики дослідження включають актуальність використання інформаційних технологій у медичній галузі, роль ІТ в сучасній медицині, аналіз проблем та ризиків ІТ-систем в медицині, а також переваги та недоліки їх застосування в контексті діагностичних рішень.

У першому розділі дипломної роботи було проведено аналіз актуальності використання інформаційних технологій в медицині та розглянуті ключові поняття системного аналізу. Досліджено роль інформаційних технологій у медицині, розвиток ІТ в системах медичного призначення, а також identифіковані проблеми та ризики в сфері медичних ІТ-систем. Проведено аналіз сучасних інформаційних технологій та їх вплив на медичну галузь, включаючи розгляд сучасних ІТ-додатків.

У другому розділі було розглянуто значення безпеки в системах медичної інформації, проблеми конфіденційності та захисту даних пацієнтів, а також ефективність та надійність медичних ІТ-систем. Здійснено аналіз ризиків та проблем застосування інформаційних технологій у медицині, що дозволило зробити висновки щодо їх впливу на безпеку та якість надання медичних послуг.

А у третьому розглянуто вплив помилок в системах на якість діагностики та лікування, ризики, пов'язані з медичними даними, та вплив перерв у роботі ІТ-систем на надання медичних послуг. Запропоновано принципи розв'язання проблем за допомогою системного аналізу, а також заходи щодо забезпечення кібербезпеки та підвищення ефективності ІТ-систем у медицині.

Дипломна робота здійснила глибокий аналіз впливу інформаційних технологій на медичну сферу, враховуючи аспекти системного аналізу та ризик-менеджменту. Отримані висновки та рекомендації можуть слугувати цінним внеском у поліпшення використання ІТ в медицині, сприяючи підвищенню безпеки, ефективності та якості надання медичних послуг. Дана робота має важливе значення для наукової та практичної галузей, враховуючи швидке розвиток технологій та їх вплив на сучасну медичну практику.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Методичний посібник з дисципліни системний аналіз Кафедри копютерних наук. [Електронний ресурс] – Режим доступу: http://dspace.wunu.edu.ua/bitstream/316497/627/1/Системний%20аналіз.pdf (14.10.2023);

2. Основи системного аналізу. [Електронний ресурс] – Режим доступу: https://web.posibnyky.vntu.edu.ua/fksa/13kolesnycky,rojik,bokocey_osn_syst_anal_objekt-i-proces_komp/p2.html (20.11.2023);

3. Основи теорії систем і системного аналізу [Електронний ресурс] – Режим доступу: https://eprints.kname.edu.ua/10895/1/СисАнализ_1_8н.pdf (10.12.2023);

4. Системи і системний аналіз [Електронний ресурс] – Режим доступу: https://allreferat.com.ua/uk/ekononika_finansu_pidpruemnucka_diyalnist/referat/3444 (29.10.2023);

5. Системний аналіз. [Електронний ресурс] – Режим доступу: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/35668/1/Системний%20аналіз%202021.docx.pdf (06.11.2023);

6. Системний аналіз основні поняття. [Електронний ресурс] – Режим доступу: https://studfile.net/preview/8900406/ (12.12.2023);

7. Основні положення аналізу. [Електронний ресурс] – Режим доступу: https://stud.com.ua/174067/tehnika/osnovni_polozhennya_sistemnogo_analizu (16.11.2023);

8. Інформаційні технології в медицині. [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/Інформаційні_технології_в_медицині (16.11.2023);

9. Сучасні технології в медичній галузі [Електронний ресурс] – Режим доступу: https://www.bsmu.edu.ua/blog/1033-innovatsiyni-tehnologii-u-meditsini/ (13.12.2023);

10. Системний підхід [Електронний ресурс] – Режим доступу: https://www.donor.ua/news/2171 (10.11.2023);

11. Переваги та недоліки медичних технологій [Електронний ресурс] – Режим доступу: http://dspace.zsmu.edu.ua/handle/123456789/9982 (08.11.2023);

12. Медична безпека в галузі [Електронний ресурс] – Режим доступу: https://medplatforma.com.ua/article/1162-pojejna-bezpeka-v-medzaklad-osnovn-pitannya-kontrolyu (13.12.2023);

13. Охорона праці в медицині [Електронний ресурс] – Режим доступу: https://www.medpublish.com.ua/ohorona-praci-v-medichnij-galuzi-pidruchnik-op-javorovskij-iv-sergeta-juo-paustovskij-vi-zenkina-ta-in/p-984.html (13.11.2023);

14. Безпека інформаційних технологій медицини [Електронний ресурс] – Режим доступу: https://studopedia.com.ua/1_13250_marshrutizatori.html (14.11.2023);

15. Безпека та конфеденційність даних персоналу. [Електронний ресурс] – Режим доступу: https://www.codeofconduct.sanofi/uk/topics/safeguarding-data-privacy-protecting-information/ (20.11.2023);

16. Міночкін А.І., Романюк В.А. Фізичні основи надійності медичних приладів // ІІІ Науково-технічна конференція ВІТІ. – К.: ВІТІ НТУУ ―КПІ‖. – 2006. – С. 5–15.

17. Ефективність безпеки в медичній сфері. [Електронний ресурс] – Режим доступу: https://er.chdtu.edu.ua/bitstream/ChSTU/813/1/ФОНМПС.pdf (11.11.2023);

18. Помилки в системах медицини. [Електронний ресурс] – Режим доступу: https://anaesthesiaconference.kiev.ua/materials_2011/0018_R.M.Fedosyuk_ukr.pdf (14.12.2023);

19. Ризики в медичних даних [Електронний ресурс] – Режим доступу: http://medforum.in.ua/sites/default/files/upravlinnya_rizikami_v_zakladi_ohoroni_zdorovya_gorachuk_v.v.pdf (12.11.2023);

20. Медична аналітика та захис [Електронний ресурс] – Режим доступу: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/5594/1/42823-91130-1-PB.pdf (17.12.2022);

21. Дані та ризики системного аналізу. [Електронний ресурс] – Режим доступу: http://dspace.wunu.edu.ua/bitstream/316497/627/1/Системний%20аналіз.pdf (14.10.2023);

22. Головний захист даних системи. [Електронний ресурс] – Режим доступу: https://web.posibnyky.vntu.edu.ua/fksa/13kolesnycky,rojik,bokocey_osn_syst_anal_objekt-i-proces_komp/p2.html (20.11.2023);

23. Основи теорії систем безпеки даних [Електронний ресурс] – Режим доступу: https://eprints.kname.edu.ua/10895/1/СисАнализ_1_8н.pdf (10.12.2023);

24. Безпечні дані і захист [Електронний ресурс] – Режим доступу: https://allreferat.com.ua/uk/ekononika_finansu_pidpruemnucka_diyalnist/referat/3444 (29.10.2023);

25. Оцінювання аналізу даних. [Електронний ресурс] – Режим доступу: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/35668/1/Системний%20аналіз%202021.docx.pdf (06.11.2023);

26. Системний аналіз основні поняття. [Електронний ресурс] – Режим доступу: https://studfile.net/preview/8900406/ (12.12.2023);

27. Основні положення аналізу. [Електронний ресурс] – Режим доступу: https://stud.com.ua/174067/tehnika/osnovni_polozhennya_sistemnogo_analizu (16.11.2023);

28. Інформаційні технології в медицині. [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/Інформаційні_технології_в_медицині (16.11.2023);

29. Сучасні технології в медичній галузі [Електронний ресурс] – Режим доступу: https://www.bsmu.edu.ua/blog/1033-innovatsiyni-tehnologii-u-meditsini/ (13.12.2023);

30. Системний підхід у безпеці [Електронний ресурс] – Режим доступу: https://www.donor.ua/news/2171 (10.11.2023);

31. Аспекти використання системного аналізу [Електронний ресурс] – Режим доступу: http://dspace.zsmu.edu.ua/handle/123456789/9982 (08.11.2023);

32. Медична безпека в галузі [Електронний ресурс] – Режим доступу: https://medplatforma.com.ua/article/1162-pojejna-bezpeka-v-medzaklad-osnovn-pitannya-kontrolyu (13.12.2023);

33. Захищені дані системного аналізу [Електронний ресурс] – Режим доступу: https://www.medpublish.com.ua/ohorona-praci-v-medichnij-galuzi-pidruc-vi-zenkina-ta-in/p-984.html (13.11.2023);

34. Безпека інформаційних технологій медицини [Електронний ресурс] – Режим доступу: https://studopedia.com.ua/1_13250_marshrutizatori.html (14.11.2023);

35. Безпека та конфеденційність даних персоналу. [Електронний ресурс] – Режим доступу: https://www.codeofconduct.sanofi/uk/topics/safeguarding-data-privacy-protecting-information/ (20.11.2023);

36. Захист інформації від несанкціонованого доступу. [Електронний ресурс] – Режим доступу: https://stud.com.ua/43315/informatika/zahist_informatsiy i_nesanktsionovanogo_dostupu (20.11.2023);

37. Безпека в медичній сфері. [Електронний ресурс] – Режим доступу: https://dspace.lvduvs.edu.ua/bitstream/1234567890/476/1/теорія%20безпеки%20соціальних%20систем.pdf (11.11.2023);

38. Недоліки в системах медицини. [Електронний ресурс] – Режим доступу: https://anaesthesiaconference.kiev.ua/materials_2011/0018_R.M.Fedosyuk_ukr.pdf (14.12.2023);

39. Ризики в медичних даних [Електронний ресурс] – Режим доступу: http://medforum.in.ua/sites/default/files/upravlinnya_rizikami_v_zakladi_ohoroni_zdorovya_gorachuk_v.v.pdf (12.11.2023);

40. Розвязування помилок системного аналізу [Електронний ресурс] – Режим доступу: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/5594/1/42823-91130-1-PB.pdf (17.12.2022);

41. Дані і захист. Системний аналіз аспеки . [Електронний ресурс] – Режим доступу: http://dspace.wunu.edu.ua/bitstream/316497/627/1/Системний%20аналіз.pdf (14.10.2023);

42. Основи системного аналізу. [Електронний ресурс] – Режим доступу: https://web.posibnyky.vntu.edu.ua/fksa/13kolesnycky,rojik,bokocey_osn_syst_anal_objekt-i-proces_komp/p2.html (20.11.2023);

43. Основи теорії систем і системного аналізу [Електронний ресурс] – Режим доступу: https://eprints.kname.edu.ua/10895/1/СисАнализ_1_8н.pdf (10.12.2023);

44. Аналіз систем медицини [Електронний ресурс] – Режим доступу: https://allreferat.com.ua/uk/ekononika_finansu_pidpruemnucka_diyalnist/referat/3444 (29.10.2023);

45. Захист даних пацієнта. [Електронний ресурс] – Режим доступу: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/35668/1/Системний%20аналіз%202021.docx.pdf (06.11.2023);

46. Системний аналіз основні поняття. [Електронний ресурс] – Режим доступу: https://studfile.net/preview/8900406/ (12.12.2023);

47. Основні положення аналізу. [Електронний ресурс] – Режим доступу: https://stud.com.ua/174067/tehnika/osnovni_polozhennya_sistemnogo_analizu (16.11.2023);

48. M. Fryz and B. Mlynko, “Property Analysis of Conditional Linear Random Process as a Mathematical Model of Cyclostationary Signal,” in Proceedings of the 2nd International Workshop on Information Technologies: Theoretical and Applied Problems (ITTAP 2022), 2022, vol. 3309, pp. 77–82. Accessed: Jan. 27, 2023. [Online]. Available: https://ceur-ws.org/Vol-3309/short2.pdf

49. M. Fryz and B. Mlynko, “Properties of Stationarity and Cyclostationarity of ConditionalLinear Random Processes,” 2020 IEEE 15th International Conference on Advanced Trends inRadioelectronics, Telecommunications and Computer Engineering(TCSET). 2020.

50. M. Fryz, L. Scherbak, B. Mlynko, and T. Mykhailovych, “Linear Random Process Model-Based EEG Classification Using Machine Learning Techniques,” in Proceedings of the 1st International Workshop on Computer Information Technologies in Industry 4.0 (CITI 2023), 2023, vol. 3468, pp. 126–132. [Online]. Available: https://ceur-ws.org/Vol-3468/short5.pdf

51. M. Fryz, “Conditional linear random process and random coefficient autoregressive model for EEG analysis,” 2017. doi: 10.1109/UKRCON.2017.8100498.

52. M. Stadnyk, M. Fryz, and L. Scherbak, “The feature extraction and estimation of a steady-state visual evoked potential by the Karhunen-Loeve expansion,” Eastern-European J. Enterp. Technol., vol. 1, no. 4 (85), pp. 56–62, 2017.

53. V. Babak, A. Zaporozhets, Y. Kuts, M. Myslovych, M. Fryz, and L. Scherbak, “Models and Characteristics of Identification of Noise Stochastic Signals of Research Objects,” in Proceedings of the 2nd International Workshop on Information Technologies: Theoretical and Applied Problems (ITTAP 2022), 2022, vol. 3309, pp. 349–362. [Online]. Available: https://ceur-ws.org/Vol-3309/paper22.pdf

54. M. Fryz, L. Scherbak, M. Karpinski, and B. Mlynko, “Characteristic Function of Conditional Linear Random Process,” in The 1st International Workshop on Information Technologies: Theoretical and Applied Problems 2021, 2021, pp. 129–135. [Online]. Available: https://ceur-ws.org/Vol-3039/short40.pdf

55. M. Fryz, "Mixing property and ergodicity of linear random processes," 2009 IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Rende, Italy, 2009, pp. 343-346, doi: 10.1109/IDAACS.2009.5342967.

56. Удар електричним струмом перша допомога. [Електронний ресурс] – Режим доступу: https://www.uzhnu.edu.ua/uk/news/strum.htm (16.11.2023);

57. Перша допомога при уражені струмом [Електронний ресурс] – Режим доступу: http://www.yu.mk.ua/news/show/persha_dopomoga_pri_urazhenni_elektrichnim_strumom? (13.12.2023);

58. Безпека життєдіяльності [Електронний ресурс] – Режим доступу: http://horoshevednz.edu.kh.ua/persha_dopomoga/persha_dolikarsjka_dopomoga_pri_urazhenni_elektrichnim_strumom/ (10.11.2023);

59. Підвищення стійкості в умовах над ситуацій [Електронний ресурс] – Режим доступу: http://dspace.zsmu.edu.ua/handle/123456789/9982 (08.11.2023);

60. Оцінювання захисту при надзвичайних ситуаціях [Електронний ресурс] – Режим доступу: https://www.donor.ua/news/2171 (10.11.2023);

ДОДАТКИ

Додаток А

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

XI НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

13-14 грудня 2023 року

ТЕРНОПІЛЬ
2023

УДК 004.9+614.2
Спільник В. Р, студент групи САм-61
Тернопільський національний технічний університет імені Івана Пулюя, Україна

СИСТЕМНИЙ АНАЛІЗ РИЗИКІВ ТА ПРОБЛЕМ ЗАСТОСУВАННЯ ІТ У МЕДИЧНІЙ ГАЛУЗІ

Spilnyk V. R., student of group SAm-61
Ternopil Ivan Puluj National Technical University, Ukraine

SYSTEMATIC ANALYSIS OF RISKS AND CHALLENGES IN THE APPLICATION OF IT IN THE MEDICAL FIELD

Об'єктом дослідження є системи медичного призначення, що використовують інформаційні технології в медицині. Зі стрімким впровадженням інформаційних технологій у медичний сектор виникають нові можливості та перспективи для покращення діагностики, лікування та управління охороною здоров'я. Однак цей цифровий перехід супроводжується системними ризиками та викликами, які вимагають детального аналізу та ефективних стратегій управління [3].

Інформаційні технології в медицині ведуть до значного збільшення обсягу цифрових даних, таких як медичні записи, зображення та інформація про пацієнтів. Це ставить серйозні виклики щодо забезпечення конфіденційності та безпеки інформації, а також вирішення питань, пов'язаних із власністю та доступом до цих даних [2].

Однією з ключових проблем є вразливість медичних інформаційних систем перед кібератаками. Зростаюча частота зловмисних дій в цифровому просторі ставить під загрозу конфіденційність пацієнтів і може мати непередбачені наслідки для їхнього здоров'я та безпеки. Важливо розглянути виклики, пов'язані із впровадженням штучного інтелекту та автоматизованих систем у медичній діагностиці та прийнятті рішень. Несправності чи недостатня точність таких систем можуть призвести до серйозних помилок у діагнозах та лікуванні [5]. Ефективне впровадження ІТ у медичну сферу передбачає вирішення питань, пов'язаних із навчанням медичних працівників та пацієнтів використовувати нові технології. Це є ключовим для максимізації їхньої користі та мінімізації ризиків непорозумінь або неправильного використання.

Зазначено, що ефективне управління ризиками та вирішення цих проблем вимагає не тільки технічних, але й правових та етичних стратегій. Організації в медичній галузі повинні розробляти і впроваджувати політики конфіденційності, силосної безпеки та етичного використання технологій, щоб забезпечити збереження довіри пацієнтів та якісне надання медичних послуг [3].

Системний аналіз ризиків та проблем застосування ІТ у медичній галузі є кроком до встановлення стійкого та безпечного цифрового середовища. Це середовище спрямоване на покращення якості медичних послуг та забезпечення високого рівня захисту інформації. Удосконалення медичної практики через інформаційні технології визначає новий етап у наданні медичних послуг. Проте, введення цифрових інновацій у сферу охорони здоров'я вносить свої виклики та ризики, які потребують системного аналізу та стратегічного управління [1].

Однією з ключових сфер у системному аналізі є забезпечення кібербезпеки медичних даних. З уведенням електронної медичної документації і обміном інформацією через мережі, зростає загроза кібератак та порушення конфіденційності пацієнтів. Вирішення цього аспекту передбачає впровадження передових систем шифрування,

захисту від несанкціонованого доступу та регулярне навчання медичного персоналу з питань кібербезпеки [3].

Ще однією важливою проблемою є ефективність та точність медичних інформаційних систем. Застосування штучного інтелекту та аналітики даних може полегшити діагностику та вибір методів лікування, але необхідно враховувати ризики помилкових рішень або невірної інтерпретації результатів. Тому важливо постійно вдосконалювати алгоритми та забезпечувати їхню адекватність перед впровадженням у клінічну практику [4].

Навчання медичних працівників та пацієнтів використанню нових технологій є однією з ключових стратегій успішного впровадження IT у медичну практику. Потрібно враховувати індивідуальні особливості користувачів, забезпечуючи їм зрозумілі інструкції та надійну підтримку для уникнення неправильного використання технологій.

До інших викликів належить інтеграція різних IT-систем, що використовуються в медичній галузі. Стандартизація та взаємодія між різними платформами дозволить покращити обмін інформацією та координацію медичного персоналу [5].

Узагальнено, системний аналіз ризиків та проблем застосування IT у медичній галузі визначає необхідність поєднання технічних і організаційних заходів для створення надійної та ефективної цифрової інфраструктури в охороні здоров'я.

Література

1. Smith, J., & Brown, A. (2018). "Challenges and Risks in Implementing Health Information Technology: A Literature Review." Journal of Health Information Management, 32(3), 1-10.
2. Johnson, R., & Williams, L. (2019). "Assessing the Security Risks of Electronic Health Records: A Comprehensive Review." International Journal of Medical Informatics, 125, 1-10.
3. Patel, N., & Jones, M. (2020). "Ethical Considerations in the Implementation of Artificial Intelligence in Medical Diagnostics." Journal of Bioethics in Healthcare, 12(4), 123-136.
4. Anderson, C., & Davis, R. (2017). "The Impact of Information Technology Training on Healthcare Professionals: A Systematic Review." Journal of Healthcare Education, 28(2), 45-56.
5. Lee, H., & Kim, S. (2018). "Interoperability Challenges in Integrating IT Systems in Healthcare: A Case Study Analysis." International Journal of Medical Informatics, 114, 84-91.

Додаток Б

ВУДК 004.9+614.2
Спільник В. Р, студент групи САм-61
Тернопільський національний технічний університет імені Івана Пулюя, Україна

СТРАТЕГІЇ УПРАВЛІННЯ РИЗИКАМИ ВИКОРИСТАННЯ ІТ-СИСТЕМ МЕДИЧНОГО ПРИЗНАЧЕННЯ

Spilnyk V. R., student of group SAm-61
Ternopil Ivan Puluj National Technical University, Ukraine

RISK MANAGEMENT STRATEGIES FOR THE USE OF MEDICAL INFORMATION TECHNOLOGY SYSTEMS

Об'єктом дослідження є стратегії управління ризиками використання ІТ-систем медичного призначення в контексті сучасної медичної практики та технологічних інновацій. Зі стрімким розвитком інтернет-технологій в останні десятиліття, використання цифрових систем у медицині стало необхідністю та ключовим аспектом сучасної охорони здоров'я. Із впровадженням ІТ-систем в медичний сектор з'являються нові можливості та виклики [1].

Швидкий розвиток інтернет-технологій в останні десятиліття використання цифрових систем у медицині стало невід'ємною частиною нової реальності сучасної охорони здоров'я. Впровадження ІТ-систем у медичний сектор відкриває широкі перспективи, такі як використання електронних медичних записів, телемедицини та аналізу даних для значного покращення якості медичних послуг. Проте цей поступ також супроводжується потенційними загрозами для конфіденційності, цілісності та доступності медичної інформації, що створює необхідність в розробці ефективних стратегій управління ризиками [5].

Використання електронних медичних записів, телемедицини, аналізу даних та інших технологічних рішень може значно покращити якість надання медичних послуг. Однак разом із цим приходять потенційні загрози для конфіденційності, цілісності та доступності медичної інформації [3]. Важливим аспектом таких стратегій є гарантування безпеки обробки та передачі медичних даних. Використання надійних методів шифрування, аутентифікації та контролю доступу визнається необхідним для запобігання несанкціонованому доступу до чутливої інформації [2].

Управління ризиками також передбачає розробку стратегій для захисту від можливих кібератак на ІТ-інфраструктуру медичних установ. Запобігання вірусам, зловмисному програмному забезпеченню та іншим кіберзагрозам вимагає постійного моніторингу та оновлення захисних заходів [4]. Дослідження розглядає важливі аспекти стратегій управління ризиками використання ІТ-систем у медичному призначенні.

Висновок дослідження має на меті підкреслити важливість впровадження комплексних стратегій управління ризиками для забезпечення успішного та безпечного використання ІТ-систем у медичному призначенні. Розуміння, аналіз та ефективне впровадження цих стратегій сприяє забезпеченню стабільності та високої якості медичного обслуговування в еру цифрової трансформації.

Література

1. Smith, J. (2020). Digital Transformation in Healthcare: Opportunities and Challenges. Journal of Health Information Technology, 25(2), 45-62.

2. Brown, A., & Jones, M. (2018). Cybersecurity Measures in Medical IT Systems: A Comprehensive Review. International Journal of Medical Informatics, 34(4), 112-128.
3. Gupta, R., & Williams, K. (2019). Ensuring Data Confidentiality in Electronic Medical Records: A Comparative Analysis of Encryption Techniques. Journal of Health Data Security & Privacy, 28(3), 76-94.
4. Chen, L., et al. (2021). Cyber Threats to Healthcare IT Infrastructure: An In-depth Analysis. Proceedings of the International Conference on Health Informatics, 112-125.
5. Johnson, P., et al. (2017). Resilience Strategies for IT Systems in Medical Settings: Lessons from Recent CyberaBBttacks. Health Information Management Journal, 39(1), 21-35.