

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**

ІНЖЕНЕРНИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ

**КАФЕДРА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ
АВТОМАТИЗОВАНИХ СИСТЕМ**

Кваліфікаційна робота

другий (магістерський)

(рівень вищої освіти)

на тему **Інформаційна система закладу охорони здоров'я.**

Виконав: студент 2 курсу, групи 8.1219-пзс
спеціальності 121 Інженерія програмного
забезпечення

(код і назва спеціальності)


освітньої програми Інженерія програмного забезпечення
(код і назва освітньої програми)



Гурська Г.В.

(ініціали та прізвище)

Керівник доцент, к. т. н.  І. А. Скрипник
(посада, вчене звання, науковий ступінь, підпис, ініціали та прізвище)

Рецензент Директор ТОВ «Дісітел»  П.О. Лютий
(посада, вчене звання, науковий ступінь, підпис, ініціали та прізвище)

Запоріжжя
2020

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ___ енергетики, електроніки та інформаційних технологій_
Кафедра _____ програмного забезпечення автоматизованих систем
Рівень вищої освіти _____ другий (магістерський) _____
Спеціальність ___ 121_ Інженерія програмного забезпечення _____
(код та назва)
Освітня програма ___ Інженерія програмного забезпечення _____
(код та назва)

ЗАТВЕРДЖУЮ

Завідувач кафедр _____ *В.Г. Вербицький* В.Г. Вербицький
“_01_” ___ вересня _____ 2020_ року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТОВІ

Гурська Ганна Вікторівна

(прізвище, ім'я, по батькові)

1. Тема роботи ___ **Інформаційна система закладу охорони здоров'я.**

керівник роботи Скрипник Ірина Анатоліївна, доцент, канд. технічних наук
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом ЗНУ від “_25_” травня_2020_ року № 600-с _____

2. Строк подання студентом кваліфікаційної роботи ___ 30.11.2020 ___

3. Вихідні дані магістерської роботи

- комплект нормативних документів ;
- технічне завдання до роботи.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

- огляд та збір літератури стосовно теми кваліфікаційної роботи;
- огляд та аналіз існуючих рішень та аналогів;
- дослідження проблеми розпізнавання мов та розробка методів її вирішення;
- створення програмного продукту та його опис;
- перелік вимог для роботи програми;
- дослідження поставленої проблеми та розробка висновків та пропозицій.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
10 слайдів презентації


6. Консультанти розділів магістерської роботи


Розділ	Прізвище, ініціали та посада Консультанта	Підпис, дата
		Завдання прийняв

7. Дата видачі завдання 01.09.2020

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1	Аналіз предметної області	02.09-10.09.20	виконано
2	Формулювання основної задачі дипломної роботи та узгодження її з науковим керівником	11.09-12.09.2020	виконано
3	Аналіз існуючих методів рішення	13.09-17.09.20	виконано
4	Дослідження області медичних інформаційних систем	18.09-24.09.20	виконано
5	Узгодження подальших дій з науковим керівником	25.09-26.09.20	виконано
6	Аналіз теоретичних відомостей	27.09-15.10.20	виконано
7	Проектування інтерфейсу	15.10-23.10.20	виконано
8	Узгодження інтерфейсу з науковим керівником	23.10-24.10.20	виконано
9	Реалізація функціоналу	25.10-14.11.20	виконано
10	Представлення отриманих результатів науковому керівнику і узгодження плану подальшого дослідження	15.11-16.11.20	виконано
11	Реалізація функціоналу	16.11-23.11.20	виконано
12	Проведення аналізу можливостей розроблених програмних за стосунків	24.11-09.12.20	виконано
13	Оформлення звіту	10.12-28.12.20	виконано

Студентка _____  _____ Гурська Г.В.
(підпис) (прізвище та ініціали)

Керівник роботи _____  _____ Скрипник І.А.
(підпис) (прізвище та ініціали)

Нормоконтроль пройдено

Нормоконтролер _____  _____ Скрипник І.А.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Сторінок: 68

Рисунків: 6

Таблиць: 1

Джерел: 19

Кваліфікаційна робота для здобуття ступеня вищої освіти магістра за спеціальністю 121 – Інженерія програмного забезпечення, науковий керівник І.А. Скрипник. Інженерний інститут ЗНУ. Факультет енергетики, електроніки та інформаційних технологій, 2020.

Мета роботи полягає у створенні онлайн застосунку медичної інформаційної системи. Аналіз системи захисту даних.

Для виконання роботи було використано Visual Studio 2019 мова програмування C#.

У результаті роботи було розроблено комплексну систему, функціями, якої є: шифрування даних за допомогою різноманітних алгоритмів, генерація та надання ключів доступу для користувачів, перевірка ключів доступу до інформації за допомогою надання різних прав доступу.

Ключові слова:, UDP, HTTPS, захист персональних даних, медичні інформаційні системи, електронний талон, адміністративна панель, веб-сервіс, система управління контентом, система управління реляційними базами даних

SUMMARY

Pages: 68

Figures: 6

Tables: 1

Sources: 19

NAME. Personal data protection system in medical information systems

Qualification work for obtaining a master's degree in specialty 121 - Software Engineering, supervisor IA Violinist. ZNU Engineering Institute. Faculty of Energy, Electronics and Information Technology, 2020.

The purpose of the work is to create an online application of medical information system. Data protection system analysis. Visual Studio 2019 C # programming language was used to perform the work.

As a result, a comprehensive system was developed, the functions of which are: data encryption using various algorithms, generation and provision of access keys for users, re-verification of access keys to information by granting various access rights.

Keywords :, UDP, HTTPS, personal data protection, medical information systems, electronic coupon, administrative panel, web service, content management system, relational database management system

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1 АНАЛІЗ ПРОБЛЕМИ	14
1.1 Історія початку використання Медичної інформаційної системи	14
1.2 Область використання Медичної інформаційної системи.....	14
1.3 Дослідження впровадження МІС на території України	17
1.4 Розгляд існуючих рішень.....	17
1.5 Перспективи розвитку інформаційних технологій в охороні здоров'я України	19
1.6 Телемедичні технології.....	21
1.7 Проблеми Медичної інформаційної системи	22
1.8 Переваги використання Медичної інформаційної системи.....	23
1.9 Класифікація медичних інформаційних систем.....	24
1.10 Інформаційна безпека та захист персональних даних в медичних інформаційних системах.....	24
1.10.1 Шифрування даних	27
1.10.2 Двохфакторна аутентифікація	29
1.10.3 Використання ЕЦП	30
1.10.3.1 Переваги використання ЕЦП	31
РОЗДІЛ 2 ЗАХИСТ ПЕРСОНАЛЬНОЇ ІНФОРМАЦІЇ	33
2.1 Актуальність проблеми захисту інформації в інформаційних системах	33
2.2 Кіберзлочинність	35
2.3 Захист персональної інформації в медичних системах	36
2.4 Безпека зберігання медичних даних в електронному вигляді.....	37
2.5 Проблема повторюваності помилок при копіюванні даних	37
2.6 Підвищення безпеки для пацієнтів.....	38
2.7 Лікарська таємниця	38
2.8 Шифрування діагнозу за допомогою класифікаторів	39

	7
РОЗДІЛ 3 ПРОЕКТ медичної інформаційної системи.....	42
3.1 Основні аспекти інформатизації медичної діяльності	42
3.2 Етапи створення і основні характеристики медичних інформаційних систем	43
3.2 Етапи створення і проектування баз даних	44
3.3 Специфікація.....	45
3.4 Інформаційне забезпечення системи.....	48
3.5 Побудова інфологічної моделі бази даних	49
3.6 Опис програмних модулів	51
3.7 Опис інтерфейсу	51
3.8 Опис контрольного прикладу реалізації проекту.....	54
РОЗДІЛ 4. ПРОГРАМНА РЕАЛІЗАЦІЯ.....	57
4.1. Програмна реалізація проекту.....	57
4.2. Модуль роботи з інтерфейсом Razor Pages.....	57
4.3. ASP.NET Core MVC	58
3.6 Вимоги до апаратного забезпечення	60
3.7 Опис функціональних можливостей	60
ВИСНОВКИ.....	66
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	67

ВСТУП

Актуальність теми

Наш час це період активного розвитку інформаційних технологій в абсолютно усіх галузях людства. Життя сучасних людей неможливе без автоматизованих систем керування. Системи обробки інформації це одні з найважливіших показником якості керування, від яких залежать якість роботи в кожному підприємстві.

Для сучасної людини питання медицини та медичного обслуговування має дуже велике значення, особливо у час пандемії. В Україні існує багато закладів охорони здоров'я, які цілодобово стоять на варті нашого здоров'я, але робота медичного персоналу не завжди є швидкою та продуктивною в сенсі автоматизації роботи. По сей час більшість лікарень використовують паперову документацію, що відбирає багато часу в лікаря та пацієнта.

В людей часто виникають проблеми зі здоров'ям і їм потрібна консультації з лікарями. Тому реорганізація процесу запису людей на прийом, проведення прийому в електронному режимі та зберігання інформації на одному сервері завжди буде актуальною задачею.

Значні обсяги інформації з джерел, що повинні формуватися кожним суб'єктом контролю якості за результатами його проведення, мають відповідати певним вимогам: своєчасності збору, обробки і передачі на вищий рівень управління, достатнього обсягу, надійності (відсутності помилок), цінності (здатності досягати мети).

Саме тому важливе місце серед дієвих засобів підвищення якості контролю займає автоматизація процедур контролю з використанням комп'ютерної техніки та спеціального програмного забезпечення. Зазначеним вимогам відповідають медичні інформаційні системи – комплекс методологічних прийомів, технічних засобів і алгоритмів керування, призначених

для збору, зберігання, обробки й передачі інформації з питань контролю якості медичної допомоги на різні рівні управління.

Саме тому створення програмного забезпечення зберігання, обробки та захисту персональних даних в медичних інформаційних системах є актуальною задачею для зниження ймовірності висвітлення за межами медичного закладу конфіденційної інформації, захисту зв'язку, шифрування даних та забезпечення стабільної роботи медичних інформаційних систем.

Медичні дані, що зберігатимуться в електронній системі охорони здоров'я, мають бути більш захищеними, у порівнянні з існуючими картками пацієнтів на паперових носіях в закладах охорони здоров'я.

Інформаційна система закладів охорони здоров'я в Україні з'явилась не так давно. Ще досі не має жодної системи, яка б повністю автоматизувала лікарню, тому весь час системи набувають нових стандартів.

Мета і завдання дослідження

Метою є дослідження та детальний аналіз вже існуючих варіантів медичних інформаційних систем. Проектування програмного коду для забезпечення захищеності та шифрування даних. Створення бази даних та інформаційної системи автоматизації роботи лікарів.

Об'єкт дослідження

Об'єкт дослідження — проектування бази даних, створення інформаційної системи автоматизації роботи закладу охорони здоров'я.

Предмет дослідження

Основним предметом дослідження є проектування бази даних, створення інформаційної системи автоматизації обліку пацієнтів, їх інформації та їх лікування.

Методи дослідження

Для розв'язання поставлених завдань використовуються такі методи дослідження:

- для визначення актуальності та розробленості теми застосовано системно-діяльнісний підхід, як загальнонауковий принцип дослідження;
- в процесі проектування на зовнішньому рівні та під час написання курсової роботи були використані методи якісного та кількісного аналізу, елементи контент-аналізу;
- при створенні інфологічної моделі та в процесі виконання проектування БД на датологічному рівні був використаний метод моделювання.

Наукова новизна одержаних результатів

Під час аналізу предметної області було проаналізована наступні програми «Helsi.me» та «Medstar». На даний час це найпоширеніші програми, що використовуються в лікарнях України. Під час роботи з «Helsi.me» були помилки в дублюванні пацієнтів, не має підтвердження дій, що привело до збою роботи в усьому закладі, не має форм та довідок.

Через збій роботи в системі «Helsi.me» підприємство перейшло на «Medstar», що призвело до проблем з базами даних. В цій програмі існує довідки та форми для заповнення огляду пацієнта. Але при переносі декларацій виникли проблеми з інформацією в деклараціях, що призвело до призупинення роботи.

Практичне значення одержаних результатів

Розроблена система надає можливість використовувати медичну інформаційну систему у будь-якому браузері, має гнучку систему налаштування.

Має різні ролі для користувачів, що забезпечує доступ до різних рівнів отримання інформації.

Апробація результатів кваліфікаційної роботи магістра

Результати досліджень, викладені у кваліфікаційній роботі магістра були представлені на XXV науково-технічній конференції студентів, магістрантів, аспірантів, молодих вчених та викладачів [34] і опубліковані в збірнику наукових праць студентів, аспірантів і молодих вчених «Молода наука - 2020» [33].

Глосарій

Медична інформаційна система — це інструмент, який дає змогу визначати і планувати всі ресурси закладу охорони здоров'я шляхом застосування спеціалізованого програмного забезпечення, засобів обчислювальної техніки, необхідного медичного обладнання, засобів зв'язку, і підтримує лікувально діагностичну, фінансову, адміністративно-господарську, облікову та сервісну діяльність установи для надання якісних медичних послуг пацієнтам. Медична інформаційна система може бути універсальною або спеціалізованою/[15]

Back-end — програмно-адміністративна частина застосунку.

Front-end — це інтерфейс для взаємодії між користувачем і back-end. Front-end та back-end можуть бути розподілені між однією або кількома системами.

PDF (щільність неперервної випадкової величини) — це функція, що визначає ймовірнісну міру відносної правдоподібності, того що значення випадкової величини буде відповідати заданій події, для кожної окремої події (або точки) у просторі подій (множини всіх можливих значень, які може приймати випадкова величина).

Графічний інтерфейс користувача (GUI, Graphical user interface) — тип інтерфейсу, який дозволяє користувачам взаємодіяти з електронними пристроями через графічні зображення та візуальні вказівки, на відміну від текс-

тових інтерфейсів, заснованих на використанні тексту, текстовому наборі команд та текстовій навігації.

Дедлайн — це остаточний, затверджений термін здачі проекту. Також цим терміном позначають кінцеву дату або час, коли дія мала завершитися, інакше, якщо прострочити і заступити за цю межу, то дія вже не матиме сенсу.

Клієнт в інформатиці (client) — апаратний або програмний компонент обчислювальної системи, який надсилає запити серверу.

Людино-машинний інтерфейс (Human machine interface) — широке поняття, що охоплює інженерні рішення, котрі забезпечують взаємодію оператора з керованими ним машинами.

Мель — психофізична одиниця висоти звуку, застосовується в музикальній акустиці.

Облік — належним чином організована система збору, нагромадження, обробки, групування, узагальнення і реєстрації (фіксації) необхідної інформації або її сукупних даних, що відображають кількісну чи якісну характеристику подій, явищ, фактів, процесів, об'єктів тощо. Є важливою складовою соціального (в т. ч. державного) регулювання суспільних відносин та управління процесами (насамперед економічними) й відповідними об'єктами. Відіграє значну роль при прийнятті правових, економічних, управлінських та інших рішень повноважними органами або компетентними особами.

Сервер або серверне програмне забезпечення в інформатиці (server) — програмний компонент обчислювальної системи, що виконує сервісні (обслуговуючі) функції за запитом клієнта, надаючи йому доступ до певних ресурсів або послуг.

Словник — лексикографічний продукт, який містить впорядкований перелік мовних одиниць (слів, словосполучень тощо) з короткими їх характеристиками або характеристиками позначених ними понять, або з перекладом на іншу мову.

Фреймворк (Framework) — інфраструктура програмних рішень, що полегшує розробку складних систем. Спрощено дану інфраструктуру можна вважати своєрідною комплексною бібліотекою.

Авторизація - надання Користувачеві прав на використання ресурсів Програми відповідно до його статусом і на основі даних, отриманих при реєстрації.

РОЗДІЛ 1 АНАЛІЗ ПРОБЛЕМИ

1.1 Історія початку використання Медичної інформаційної системи

Початок використання медичної інформаційної системи почалось у 2008 році, коли двоє студентів **ММІФ КПІ** захищали спільну дипломну роботу. Кафедра, на якій навчались студенти, співпрацювала з компанією InterSystems, яка посприяла для отримання призового місця на міжнародному конкурсі у США. Це стало початком автоматизації медичної галузі.

В 2010 році створено перше підприємство, що і стало початком работ над МІС. Компанія зробила багато напрацювань в т.ч. Електронна медична картка, диспансеризація, онлайн запис на прийом, смс / viber нагадування про візит, CRM, інтеграція з Vinotel та Asterisk, протоколи лікування ICPC-2, власний DICOM сервер, кейси з повністю безпаперовими офісами (медичний документообіг), інтеграцію каси с фіскальними реєстраторами, HR модуль з підключенням до біометричних систем, декілька режимів керування зарплатою мед. персоналу, бізнес-аналітику, бюджет з урахуванням всіх фактичних та запланованих витрат, списання матеріалів, страхові компанії та мобільні додатки. Якщо необхідно підписати з пацієнтом інформовану згоду на лікування, то nHealth може автоматично генерувати шаблон для педіатрії в залежності від налаштувань та віку пацієнта. Турбота та високий рівень сервісів для пацієнта. Підтримка міжнародних стандартів медичних даних. Управлінське списання матеріалів та наявність доступних інтеграцій з бухгалтерським ПЗ. Можливість динамічного формування статистичних звітів. Обмін даними між робочими місцями у реальному часі. Регламентовано швидка реакція технічної підтримки. МІС має онлайн та оффлайн версії.

1.2 Область використання Медичної інформаційної системи

У будь-якому медичному закладі знайомство починається з реєстратури. До обов'язків реєстратора відносяться врегулювання потоків пацієнтів,

яким потрібен талон, чи карточка, чи просто отримати відповідь на запитання. Також можна врегульовувати через телефон, журнал самозапису, системи попереднього запису, тощо.

При використанні талонної системи в деяких клініках, черги починають утворюватись задовго до початку робочого дня. Чекаючи своєї черги, люди будуть піддаватися різним інфекційним та хронічним захворюванням, тим самим підвищуючи рівень інфекційних захворювань. Через кілька годин після відкриття кількість людей стає все меншою і меншою, але купонів може не бути. Якщо немає сильного болю або температури, тоді ви не можете дозволити собі звернутися до лікаря.

Реєстратори виконують такі обов'язки [16]:

- Пояснити місцезнаходження конкретних лікарів;
- Інформувати пацієнтів про графік роботи лікаря-спеціаліста;
- Організувати екстрену медичну допомогу для пацієнтів з високою температурою та гострим болем;
- Забезпечити видачу консультаційних путівок лікарів;
- Забезпечити приплив амбулаторних карток.

У таблиці проведено аналіз використання талонної системи у закладах охорони здоров'я (табл. 1.1)

Таблиця 1.1

Аналіз використання талонної системи у закладах охорони здоров'я

Функція	Недолік	Перевага
Запис пацієнта на прийом по телефону	Працівник реєстратури може не правильно почути та записати дані пацієнта	Пацієнт може записатися до лікаря не виходячи з будинку
Запис пацієнти на прийом через реєстра-	Потрібно стояти в черзі, що може призвес-	Працівник реєстратури може надати будь-

туру в закладі охорони здоров'я	ти до зараження	яку інформацію, яка цікавить пацієнта.
Запис пацієнти на прийом через журнал самозапису	Оскільки ведення журналу самозапису відбувається в паперовому вигляді, то можливі дублювання та втрата даних	Пацієнт може записатися на прийом самостійно, без допомоги працівника реєстратури

Сьогодні майже всі медичні заклади мають власні веб-сторінки, де пацієнти можуть знайти потрібну інформацію. Крім того, деякі мають функцію реєстрації пацієнтів для призначення лікарів.

Метою цієї статті є розробка веб-програми, яка забезпечить функції запису та зберігання інформації про пацієнтів у зашифрованому вигляді.

Проектування медичної інформаційної системи надасть користувачам такі можливості:

- Пацієнт зможе вибрати бажаного лікаря з великої кількості лікарів, зареєстрованих у системі.

- В кабінеті реєстрації немає черги на отримання талону сімейного лікаря.

- В кабінеті лікаря немає черги, що зменшує ризик зараження.

- Електронний самозапис або запис реєстратором швидше.

- Статистка роботи лікаря відображається в медичній інформаційній системі.

- Пацієнти можуть записатися на прийом до відповідних лікарів, не виходячи з дому, що не вимагає додаткового часу.

1.3 Дослідження впровадження МІС на території України

Останнім часом країни СНД активно проводять інформатизацію медицини та охорони здоров'я. Однак усі країни, що належать до Радянського Союзу, перебувають у стані радянської медичної реформи, тому важко систематизувати цю сферу. Розробка "Електронної медичної системи та міжнародної системи телемедицини" розпочалась у 2006 році. Очевидно, важко говорити про суворі прецеденти у галузі автоматизації медицини, поки система охорони здоров'я країни не набере формальних та чітких рис, передбачених законодавством та адміністративними розпорядженнями та законопроектами.

В Україні проводиться велика робота в напрямку інформатизації охорони здоров'я: приймаються відповідні державні нормативні акти та складаються плани. Розроблено проект концепції управління якістю медичної допомоги в українському секторі охорони здоров'я. Запропонований проект розроблений відповідно до виконання Указу Президента України від 27.04.2011 № 504/2011 "Про Національний план дій на 2011 рік щодо впровадження Програми економічних реформ 2010 – 2014 роки "Заможне суспільство, конкурентоспроможна економіка, ефективна держава".

Ринок ІТ-технологій в Україні досить насичений, велика кількість компаній виробляє ІС, але більшість із цих постачальників - дуже маленькі компанії. Більше того, між цими компаніями мало співпраці чи координації.

1.4 Розгляд існуючих рішень

Основною ідеєю інформатизації в галузі охорони здоров'я України є створення єдиного медичного інформаційного простору. Створення такого простору допоможе забезпечити процеси управління медичною допомогою та надійну статистику.

Аналіз інформаційних потреб лікарів показує, що збір, накопичення та обробка інформації про пацієнтів в електронному вигляді дозволяє ефективно обробляти великі обсяги даних без ручного втручання.

Електронні медичні записи забезпечують облік операційних витрат,

пов'язаних з процедурами діагностики та лікування, використанням наркотиків та матеріалів та оплатою медичних послуг. Це є запорукою впровадження страхової медицини.

Станом на 26.11.2018 рекомендований Міністерством охорони здоров'я України перелік медичних інформаційних систем включає [17]:

- **Helsi** — система для керування медичним закладом. Система розроблена з урахуванням вимог та специфіки роботи МОЗ.
- **Поліклініка без черг** — це система яка призначена для управління потоком пацієнтів в лікувальних закладах. Дана МІС може інтегруватися із модулями для роботи з електронною картою пацієнта, обліковими системами і електронним рецептом.
- **EMCiMED** — медична інформаційна система, яка розроблена відповідно до стандартів ISO та МОЗ України, та містить: медичні документи, електронну медичну картку пацієнта, статистику та звіти МОЗ, мобільний додаток пацієнта, онлайн запис до лікаря.
- **MEDSTAR** — хмарна медична інформаційна система, яка містить модуль запису пацієнтів, електронну медичну картку, довідник ліків та інші модулі.
- **MEDICS** — це хмарна медична інформаційна система.
- **Доктор Елекс** — система, що забезпечує автоматизацію процесів медичної установи, наприклад, ведення історії хвороби в електронному режимі, формування звітності та документації згідно з вимогами МОЗ.
- **Health24** — повнофункціональна хмарна медична інформаційна система, що об'єднує в собі функціональні сервіси, які забезпечують роботу лікаря і медичного закладу відповідно існуючих стандартів медичного документообігу.
- **MedCard Plus** — медична інформаційна система головним компонентом якої є електронна медична карта пацієнта. Дана МІС використовує процесний підходу до автоматизації роботи медичного закладу.

- Asker.net — це хмарна міжнародна платформа для автоматизації процесів медичних закладів та може інтегруватися із сторонніми сервісами та технікою.
- МІС «Каштан» - система, що має компоненти для оцінки рівня складності, ефективності та якості обслуговування пацієнтів, обліку витрат та розрахунку вартості медпослуг.
- UASMART — хмарна МІС, у якій високий рівень захисту інформації.
- Облік медичних кадрів України та пацієнтів — МІС, що складається із робочого місця працівника кадрової служби, та програмного комплексу для амбулаторно-поліклінічних закладів і стаціонарів.
- МедЕйр — повнофункціональна медична інформаційна система, яка розроблена для лікарів.

1.5 Перспективи розвитку інформаційних технологій в охороні здоров'я України

Для поліпшення керованості сучасного управління охороною здоров'я та медичної допомоги, перш за все, необхідно впровадити основні групи інформаційних систем:

-Забезпечити інформаційну підтримку процесу управління службами охорони здоров'я медичних закладів регіону;

-Забезпечити інформаційну підтримку заходів щодо профілактики, діагностики та лікування конкретних людей.

Поки ці конкретні завдання вирішуються, ці плани можуть бути реалізовані [18].

-Враховуючи реальність та стратегію соціально-економічного розвитку країни, а також основний напрям розвитку інформатизації держави, реалізувати план інформаційного відділу охорони здоров'я;

-Сформувати сучасну галузеву інфраструктуру охорони здоров'я, що включає постійне вдосконалення та модернізацію галузевої комп'ютерної мережі та системи галузей баз даних на основі застосування сучасних теле-

комунікаційних технологій та створення в окремому місці базової сфери інформатизації охорони здоров'я. Найбільш підготовлений регіон країни;

-Розробити метод формування комп'ютерної мережі, яка об'єднає МОЗ України з іншими міністерствами;

-Створити серверний комплекс, присвячений певним галузям медицини, щоб забезпечити інформаційну підтримку роботи вчених, лікарів, студентів-медиків та громадськості;

-Створити конкурентний засіб інформатизації процесу діагностики, який буде накопичувати наукові досягнення в країні та за кордоном;

-Розробка сучасних інформаційно-аналітичних систем для моніторингу стану здоров'я та демографічного стану населення України;

-Розробити типову лікарняну інформаційну систему; "

-Створити систему аналізу інформації для аналізу стану медичного та медичного обслуговування людей;

-Розробити системи аналізу інформації для забезпечення наукових досліджень у медичній галузі;

-Встановити інформаційно-довідкові системи для забезпечення навчального процесу в певних галузях медицини;

-Встановити сучасні інформаційні технології, забезпечити бібліотеки та послуги з ліцензування патентів у медичній галузі;

-Створити систему аналізу інформації для аналізу даних переписів населення України, яка допоможе сформулювати відповідні стратегії підтримки здоров'я населення та швидко вирішити поточні проблеми управління охороною здоров'я.

Поява існуючої інформації вирішить проблему координації політики різних відділів у галузі охорони здоров'я, забезпечить швидкий доступ до найновішої та ефективної інформації про медичні технології, принципово вплине на здоров'я пацієнтів, швидкість та якість даних про методи лікування, а також профілактичні та освітні медичні заходи . Це інформаційне середовище створить необхідні передумови для подальшого реформування сис-

теми охорони здоров'я, поліпшення здоров'я людей, підвищення ефективності процесів лікування та діагностики та профілактичних заходів.

1.6 Телемедичні технології

В останні роки популяризація мультимедійних комп'ютерів та комунікаційних технологій призвела до бурхливого розвитку телемедицини. Технологія телемедицини також корисна для великих регіональних медичних установ, а також регіональних лікарень та кабінетів сімейних лікарів.

За їх допомогою на базі регіонального профільного науково-дослідного закладу або медичного закладу організовується консультативний центр телемедицини для надання послуг усім установам регіону. Використовуючи функції цього центру, ви можете проконсультувати пацієнтів у будь-якому провідному медичному центрі та за кордоном. Коли реєстрація діагностичних показників (ЕКГ, ЕЕГ, діаграма R) виконується медичним персоналом у декількох кабінетах або відділеннях в декількох кабінетах або відділеннях, технологія телемедицини також може використовуватися в окремих медичних закладах, а також їх аналіз та обробка Результат діагностики - кваліфікований фахівець. Центральна лабораторія або відділення функціональної діагностики.

В Україні існують також телеконсультаційні медичні центри (Харків, Житомир, Запоріжжя, Вінниця), телемедичні центри для "патологоанатомів" (Київ), ЯМР-томографія для електрокардіографії по телефону Віддалений консультаційний центр (Київ). Очевидно, цього недостатньо.

Технологія телемедицини значно покращила організацію авіаційних служб охорони здоров'я, збільшила рівень кваліфікованої допомоги сільському населенню та повністю використала клінічний потенціал медичних науково-дослідних установ та вищих навчальних закладів.

Телекомунікаційні технології були впроваджені в основній медицині та в аспірантурі.

Телекомунікаційні технології все ще не повністю використовуються для наукових досліджень. Пріоритетом у цьому плані є розширення міжнародного досвіду в організації та проведенні наукових телеконференцій на регіональному та національному рівнях.

1.7 Проблеми Медичної інформаційної системи

Хоча доступні кваліфіковані програмні рішення, в Україні майже немає досвіду повного переходу від медичних закладів до принципів електронного зберігання та обробки інформації. Тому при впровадженні медичної інформаційної системи особливо важливими стають проблемні питання, які можна розділити на кілька категорій:

- Наша існуюча законодавча база не забезпечує належного рівня правового захисту медичного персоналу, який використовує інформаційні технології у щоденній практиці;

- Фінансові ресурси більшості медичних установ поки що не можуть дозволити їм придбати достатньо комп'ютерного обладнання та дорогого програмного забезпечення для інтегрованої автоматизації. Тому процес успішний лише в певних місцях, які, як правило, знаходяться далеко від медичного напрямку, лікарняного відділення: статистики, бухгалтерії, автоматизації адміністративної роботи тощо.

- В Україні майже немає шкіл, які б могли навчити вищих фахівців розробці та впровадженню складних медичних інформаційних систем. Для того, щоб створити сімейну школу в цій галузі, творчій команді необхідно обмінятися думками та думками щодо розробки програмного забезпечення, щоб накопичити досвід та сформувані потенційні сфери переваг для пошуку ефективних напрямків для розвитку та реалізації інтегрованих прав інтелектуальної власності;

- Крім того, в Україні використовується близько 500 різних медичних форм, таких як F-003 для госпіталізації та F-066 для статистики. Форма F-003 заслуговує на особливу увагу, оскільки вона містить багато інформації, яка

повинна зберігатися в електронній медичній картці (ЕМС), наприклад, ліки, результати лабораторних досліджень та записи лікарів.

Ці форми «передаються у спадок» і більшість із них застосовуються в статистичному обліку. Основна проблема цих форм полягає в тому, що їх потрібно заповнювати та подавати вручну (форми, створені в електронних формах, не приймаються). Заповнення цих форм займало близько 40% часу лікаря. Більше того, цінність багатьох форм сумнівна, оскільки вони в основному використовуються для статистичного обліку. Якщо так, ці форми (та статистична інформація в них) повинні заповнюватися та оброблятися в електронному вигляді. В даний час вирішуються проблеми, пов'язані із впровадженням інформаційних технологій у медицину, що дає змогу забезпечити вирішення найбільш актуальних проблем у актуальній медицині в рамках існуючої медичної інфраструктури та обмежених коштів.

У теперішніх умовах є можливим використання локальних проектів з інформатизації медицини, а для більш глобального застосування необхідним є дотримання єдиних вимог які ґрунтуються на застосуванні світових стандартів збору, збереження, обробки та обміну електронного варіанту медичної інформації. В сучасних умовах місцеві проекти можуть бути використані для медичної інформатизації. Для більш широкого кола застосувань необхідно дотримуватися уніфікованих вимог, заснованих на застосуванні світових стандартів щодо збору, зберігання, обробки та обміну електронною медичною інформацією.

1.8 Переваги використання Медичної інформаційної системи

Основними перевагами впровадження МІС в медичних закладах є:

- "Прозорість" - це єдина база даних, яка дозволяє відстежувати всі ресурси (матеріальні, людські, фінансові). Результатом є планування, аналіз ефективності та оптимізація використання наявних ресурсів.

-Покращити потенціал медичних установ за допомогою постійних ресурсів (за рахунок оптимізації процесів введення даних, пошуку, редагування

та аналізу; пришвидшити взаємодію між відділеннями; планувати навантаження лікарів, кабінетів та обладнання).

-Поліпшити якість допомоги пацієнтам (скоротити час очікування завдяки плануванню; збільшити ефективний час перебування пацієнта в лікарні) і, отже, збільшити задоволеність пацієнта.

-За допомогою електронних медичних протоколів можна розрахувати ефекти лікування та зменшити ймовірність медичних помилок, покращуючи тим самим якість надання медичних послуг.

-Можливість швидко генерувати будь-який звіт для прийняття розумних управлінських рішень (кількість наданих послуг, навантаження лікарів та кабінетів, статистика пацієнтів за діагнозом, вік, стать тощо)

-Ефективне управління запасами ліків та витратних матеріалів шляхом автоматизації процесу замовлення та скасування та підтримання найкращого балансу.

-Поліпшити безпеку та конфіденційність інформації, запровадивши політику прав доступу до різних даних та інформації, що входять в систему за допомогою паролів або відбитків пальців.

1.9 Класифікація медичних інформаційних систем

Класифікація МІС основана на ієрархічному принципі та відповідає багаторівневій системі охорони здоров'я:

- МІС базового рівня
- Рівень профілактично-лікувальних установ

1.10 Інформаційна безпека та захист персональних даних в медичних інформаційних системах

Відповідно до "Закону про захист персональних даних" в Україні, персональні дані-інформація або група інформації про ідентифіковану або ідентифіковану особу. Підпишіть заяву про вибір лікаря, підтвердьте, що пацієнт

розуміє мету збору та обробки своїх персональних даних, і погоджуйтесь, що дані будуть доступні в MIS для подальшої обробки. Лише персонал, призначений медичними установами, може вносити особисті дані пацієнтів в медичні електронні системи. На них поширюється законодавство України щодо медичної конфіденційності та вони повинні забезпечувати захист таких персональних даних.

Відповідальна особа може нести адміністративну відповідальність за порушення законодавства та встановлених процедур захисту персональних даних та інформації, що призвело до незаконного доступу або порушення прав пацієнта як суб'єкта персональних даних. Кожна система електронного охорони здоров'я та медична інформаційна система повинні бути розроблені для обробки конфіденційних та персональних даних відповідно до практики та правил захисту даних. Інформаційна безпека - це стан безпеки інформаційного середовища. Захист інформації - це процес, спрямований на запобігання витоку захищеної інформації та здійснення несанкціонованого та ненавмисного впливу на захищену інформацію, тобто процес, спрямований на досягнення цього стану. Метою реалізації інформаційної безпеки будь-якого об'єкта є створення системи інформаційної безпеки об'єкта [7].

Об'єктом інформаційної безпеки є інформація, яка зачіпає національні, офіційні, комерційні, інтелектуальні та особисті інтереси, а також засоби та інфраструктура, що впливають на її обробку та передачу [8] Для того, щоб описати основні атрибути інформації як об'єкта захисту, зазвичай використовується модель ЦРУ [9]:

-Погроза конфіденційності, пов'язана з несанкціонованим доступом до інформації, є загрозою конфіденційності;

-Цілісність-загрози, пов'язані з несанкціонованим зміною інформації, є загрозами цілісності;

-Доступність-Погрози, пов'язані з можливістю порушення використання комп'ютерних систем або обробки інформації, є загрозою доступності.

Відповідно до українського законодавства [10], вирішення питань інформаційної безпеки повинно бути:

- Створити надійну національну інформаційну інфраструктуру та забезпечити захист її ключових елементів;

- Підвищити рівень координації національних установ щодо виявлення, оцінки та прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення усунення їх наслідків, а також здійснення заходів з міжнародного співробітництва з цих питань;

- Вдосконалити нормативно-правову базу щодо інформаційної безпеки, особливо захисту інформаційних ресурсів, боротьби з комп'ютерними злочинами, захисту персональних даних та правоохоронної діяльності в інформаційному полі;

- Розгорнути та розробити державну таємну систему зв'язку як сучасну та безпечну транспортну базу, яка може інтегрувати регіонально розподілені інформаційні системи, які обробляють конфіденційну інформацію.

Отже, для забезпечення інформаційної безпеки існують такі принципи [11]: систематичний, всебічний та постійний захист інформації; гнучкість управління та застосування; відкритість алгоритмів та механізмів захисту; простота використання захисних засобів та заходів.

Існує кілька основних методів захисту інформації [11]:

- Ідентифікація та сертифікація суб'єктів інтелектуальної власності;

- Дозвіл на розподіл ресурсів інтелектуальної власності;

- Контроль цілісності даних;

- Забезпечити конфіденційність даних;

- Аудиторські події, що відбуваються в інформаційній системі;

- Надмірність ресурсів та компонентів ІВ.

Вимоги до захисту інформації в медичних інформаційних системах:

- Система повинна надавати доступ лише уповноваженим користувачам.

-Система повинна записати всі дії користувача перед зміною інформації. Інформація про дію повинна бути детальною (визначити, які властивості змінилися та значення інших властивостей).

-Система повинна записати всі дії користувача для доступу до персональних даних.

-Система повинна мати вбудований механізм, який може використовувати електронний цифровий ключ центру сертифікації для підписання даних.

-Алгоритм, визначений у ДСТУ 4145-2002, використовується при формуванні та верифікації електронних цифрових підписів.

-Для обчислення сеансового ключа слід використовувати протокол розподілу ключів, що відповідає пункту 8.3 ДСТУ ISO / IEC 15946

-Рівень безпеки даних у системі повинен надавати можливість побудувати систему KSZI.

- Система повинна шифрувати дані, що зберігаються на центральному рівні, використовуючи бібліотеку шифрування, яка була належним чином сертифікована Державним бюро спеціальних служб.

1.10.1 Шифрування даних

В даний час розвиваються кібератаки, і люди розробляють нові методи, щоб справити враження на особисті дані користувачів Інтернету та викрасти конфіденційну інформацію. Щоб компенсувати цей негативний вплив, інформаційна безпека є незамінною частиною Інтернету. Шифрування даних - це метод захисту особистої інформації, яка може передаватися через мережу. В даний час розроблено багато складних алгоритмів шифрування.

Шифрування полягає в шифруванні даних відповідно до певного ключа, щоб захистити їх від доступу третіх сторін. Використовуваний метод кодування називається паролем. Основною вимогою до пароля є наявність ключа пароля.

Існують симетричні та асиметричні методи шифрування, кожен з яких має свої особливості.

Симетричне шифрування - це тип шифрування, при якому для кодування та декодування використовується один ключ. І користувач, і сервер повинні зберігати цей ключ шифрування в секреті і повинні досягти консенсусу щодо цього на початку обміну даними.

Цей метод має певні недоліки: коли частина вихідних даних перехоплюється, усі повідомлення можна розшифрувати. Тому в більшості паролів використовується складна комбінація ключів-заміни та перестановки. Симетричні шифри можуть виконуватися за кілька циклів (проходів), кожного разу, коли ключ пропуску використовується на початку нового циклу.

Основними особливостями та параметрами симетричного алгоритму шифрування є: довжина ключа, довжина блоку, що підлягає обробці, стабільність, складність апаратної та програмної реалізації, складність перетворення та кількість проходів.

До переваг симетричної системи шифрування належать: проста реалізація, швидка швидкість та відносно коротка довжина пароля.

Серед основних недоліків - складність управління кадрами шифру у великих мережах та недостатня здатність забезпечити надійну передачу ключів усім користувачам.

Асиметрична криптографія (асиметричне шифрування) - це процес шифрування, при якому відкриті ключі можуть передаватися через незахищені канали зв'язку і можуть використовуватися для шифрування (шифрування) повідомлень. Для них для декодування використовувався приватний ключ (секрет).

Тому через відкритий і закритий стани цю систему називають асиметричною системою. Для всіх, хто хоче надіслати повідомлення на сервер (або одержувача), надається відкритий ключ, а приватний ключ доступний і зберігається лише на сервері (у одержувача) і повинен бути конфіденційним та секретним .

Асиметричне шифрування має переваги, серед яких: не передача приватного ключа через канал зв'язку; на відміну від симетричного шифрування,

можливість збереження приватного ключа незмінним. Симетричне шифрування означає, що ключ змінюється після кожної передачі даних; у порівнянні з симетричною криптографією він використовує Менше ключів для асиметричного шифрування; вони зберігаються лише на одній стороні.

До недоліків можна віднести: використання відносно довгих ключів та асиметричних алгоритмів; використання відносно великих обчислювальних ресурсів;

Особливістю шифрування є те, що жоден ключ не можна використовувати протягом нескінченного періоду часу, оскільки чим довше використовується пароль, тим більша ймовірність доступу сторонніх осіб до інформації. Подібним чином розкриття ключа, який використовувався протягом тривалого часу, може призвести до витоку інформації, накопиченої протягом усього терміну служби ключа. Тому, вибираючи метод шифрування, пам'ятайте, що вам потрібно змінити ключ через певний проміжок часу.

1.10.2 Двофакторна аутентифікація

Запитуючи та перевіряючи два різні типи даних автентифікації, двійкова автентифікація є одним із методів ідентифікації користувачів у службі. Це може забезпечити два рівні більш ефективного захисту даних для запобігання несанкціонованому використанню. Насправді, як правило, двофакторна автентифікація має такі форми: перший фактор - це ім'я для входу та пароль, а другий фактор - це спеціальний код (SMS, набір вказаного номера) або електронна пошта на телефоні; запитуйте спеціальний USB-ключ або Біометричні дані користувача (відбитки пальців, сканування обличчя або рогівки тощо).

Двофакторна автентифікація забезпечує більш високий рівень безпеки процесу автентифікації, ускладнюючи зловмисникам доступ до даних користувачів або облікових записів в Інтернеті, оскільки одного пароля недостатньо для автентифікації.

Сертифікація обладнання стає все більш поширеною. Ідентифікація користувача базується на певному обладнанні, тобто на спеціальному елект-

ронному ключі, що належить користувачеві. Сьогодні найпоширенішими типами пристроїв є картки (смарт-карти, магнітні картки, безконтактні картки тощо) та маркери, які можна безпосередньо підключити до порту комп'ютера (як правило, USB-ключ).

Головна перевага апаратної ідентифікації - висока надійність та безпека, оскільки маркер може зберігати великий ключ, який важко знайти. Крім того, вони можуть також реалізувати додаткові механізми захисту.

Серед недоліків серйозною проблемою при використанні апаратної ідентифікації є викрадення, втрата, копіювання та передача зловмисниками карт або токенів зареєстрованим користувачам. Ще одним недоліком є використання коштів. Щоб використовувати апаратний захист для роботи двофакторної системи автентифікації, персональний ключ або картка повинна бути надана всім зареєстрованим користувачам.

1.10.3 Використання ЕЦП

Електронний цифровий підпис - це електронний підпис, отриманий шляхом криптографічного перетворення набору електронних даних, який може бути доданий до цього цифрового підпису або логічно поєднаний з ним, і дозволяє підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою персонального ключа та перевіряється за допомогою відкритого ключа. Гу знаходиться в Україні.

Електронні цифрові підписи за своєю функцією схожі на власноручні підписи, як правило, на папері, і мають усі основні переваги:

- Довести, що підписаний документ надходить від підписанта;
- Забезпечити цілісність файлу підпису (запобігти змінам);

Особа, яка підписує документ, не має права відмовлятися від зобов'язання, пов'язаного з підписанням документа.

Українське законодавство юридично прирівнює електронні документи, підписані ЕЦП, до документів із власноручним підписом або печатками, а

також закладає правову основу для використання ЕЦП та здійснення юридично значущих дій за допомогою електронного документообігу.

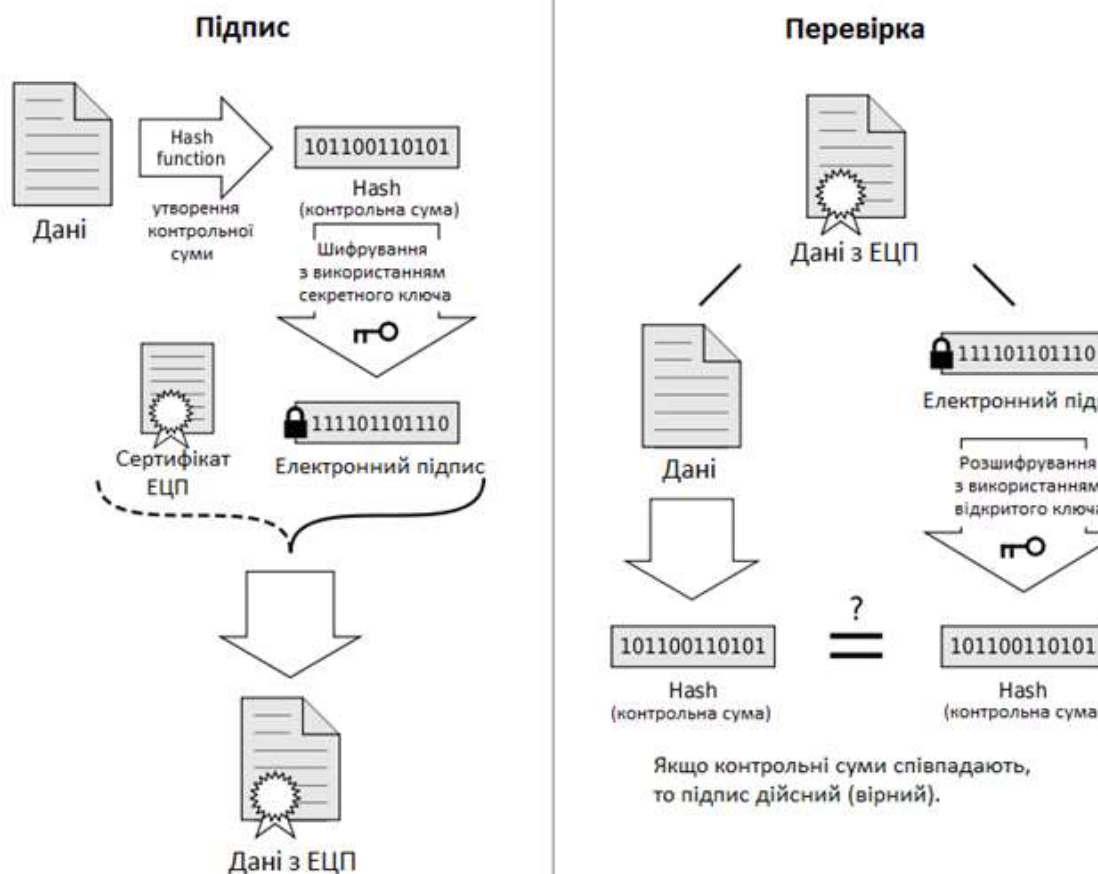
Безпека використання ЕЦП забезпечується тим, що метод, що використовується з ЕЦП, був перевірений та сертифікований Департаментом спеціальних систем телекомунікацій Українського агентства безпеки, який гарантує, що ЕЦП не можна зламати та підробити.

1.10.3.1 Переваги використання ЕЦП

Використання ЕЦП може значно скоротити час переміщення документів під час звітності та обміну документами. Документи, підписані EDS, будуть передані через Інтернет або локальну мережу протягом декількох секунд. Усі учасники електронного обміну документами, незалежно від відстані між собою, мають рівні можливості.

Використовуйте ЕЦП для: –

- Замініть традиційні печатки та підписи безпаперовим тиражем; –
- Поліпшити та зменшити витрати на процедури підготовки, доставки, обліку та зберігання документів для забезпечення достовірності документів;
- Значно скоротити час переміщення документа, пришвидшити та сприяти процесу схвалення документа кількома людьми;
- Використовувати ті самі засоби ЕЦП для обміну інформацією з усіма міністерствами та відомствами України;
- Створити систему компанії для обміну електронними документами;
- Забезпечити цілісність
- Переконайтесь, що інформація зараз існує в оригінальній формі, тобто не було внесено несанкціоновані зміни під час зберігання або передачі;
- Забезпечуючи конфіденційність обміну інформацією про документи (при використанні шифрування), ризик фінансових втрат зводиться до мінімуму.



Мал.1.1 Схеми роботи ЕЦП

Електронний цифровий підпис підтверджує справжність та цілісність документа. Якщо під час надсилання в документ будуть внесені будь-які зміни (або навіть абсолютно неактуальні), відбудеться заміна. Сертифікат відкритого ключа містить особисту інформацію про власника, що дозволяє однозначно ідентифікувати автора документа.

Отже, можна зробити висновок, що електронний цифровий підпис є невід'ємною частиною сучасного документообігу, оскільки його використання покращує захист переданої інформації, захищає її від шахрайства та спрощує різні операції (транзакції, Звіт державних установ), що значно економить витрати. час.

РОЗДІЛ 2 ЗАХИСТ ПЕРСОНАЛЬНОЇ ІНФОРМАЦІЇ

2.1 Актуальність проблеми захисту інформації в інформаційних системах

Зміст проблеми полягає в тому, що великі обсяги персональних даних часто обробляються (а іноді і передаються) під час користування Інтернетом або мобільними телефонами без явної згоди або навіть інформації про їх обробку.

Вагомим прикладом є пошукові системи: коли ви шукаєте готелі в іншому місті, Інтернет надасть вам різні готелі на інших веб-сайтах у формі реклами. Пам'ятайте, що наші онлайн-види спорту можуть полегшити життя. У той же час є і негативні наслідки: володіючи нашими даними, існує багато потенційних зловживань, які варіюються від безпосереднього визначення змісту нашої інформації, через цільову рекламу до навмисних та зловмисних маніпуляцій із вмістом та поведінкою, яку ми бачимо в Інтернеті, Це вплине на нашу обізнаність як споживачів.

Кібербезпека почала регулюватися на національному рівні. Нещодавно світ побачив новий український закон «Основні принципи української кібербезпеки». Метою закону є створення національної системи кібербезпеки, яка допоможе захистити важливі інтереси суспільства та країни. Виходячи з важливих концепцій, закон визначає основні об'єкти цього виду захисту та визначає ключових осіб, які повинні контролювати здійснення такого захисту. Однак після прочитання тексту закону виникає запитання: чи захищає закон інтереси певних осіб як фізичних осіб? Основна увага цього закону спрямована на захист прав суспільства та країни в кіберпросторі, але саме люди зазнають найбільшого негативного впливу в сучасному інформаційному просторі. Перш за все, важливою частиною таких проблем є нерозуміння того, що слід суворо захищати в середовищі захисту інформації людини.

Перша проблема, з якою стикається контролер персональних даних при реєстрації контролера персональних даних у реєстрі статусу бази персональних даних, полягає у визначенні, яка інформація належить до персональних даних, а яка інформація не належить до персональних даних.

Відповідно до ст. Стаття 11 Закону України "Про інформацію" від 2 жовтня 1992 р. Інформація про фізичну особу (персональні дані) - це інформація або група інформації про ідентифіковану або конкретно ідентифіковану особу. Конфіденційна інформація про осіб включає, але не обмежується ними, інформацію про їх національність, освіту, сімейний стан, релігійні переконання, стан здоров'я та місце проживання, дату та місце народження.

Відповідно до ст. 2 Люди, яких визнають або можуть бути спеціально визнаними.

21 грудня 2011 року Міністерство юстиції пояснило "Деякі питання практичного застосування українського законодавства, пов'язані із захистом персональних даних", що українське законодавство не встановлено, а також не може встановити чіткого переліку інформації, що дозволяє ідентифікувати особу. Це персональні дані, щоб положення цього закону могли застосовуватися до різних ситуацій, включаючи персональні дані в (автоматичній) базі даних та технологію обробки у файлах персональних даних, які можуть з'являтися в майбутньому через зміни в інформаційних технологіях, соціальних, економічних і інші сфери суспільного життя. Іншими словами, Міністерство юстиції було обізнане з проблемою і не відповіло на питання, яка інформація дозволена для ідентифікації осіб.

Веб-сайт нещодавно створеної в Україні Національної служби захисту персональних даних не надає конкретної відповіді на це питання. Він лише вважає, що визначення терміну „персональні дані” в українському законодавстві „про захист персональних даних” повністю відповідає Визначення позначених термінів, зазначених у Конвенції про автоматичну обробку персональних даних ”.

Конституційний Суд України офіційно інтерпретував частини першу та другу статті 32 Конституції України і вважає, що інформація про особисте та сімейне життя людини (про її персональні дані) є відповідною до того, що була визначена або може бути конкретно ідентифікована, а саме: національність, рівень освіти, сімейний стан, релігійні переконання, стан здоров'я, матеріальний стан, адреса, дата та місце народження, місце проживання та проживання тощо, дані про особисте майно та немайнові стосунки людини з іншими людьми, особливо з сім'єю. Взаємовідносини членів, а також інформація про події та явища, що відбулися або відбуваються в сім'ї, близькість, доброзичливість, професіоналізм, бізнес та інші сфери особистості, за винятком наведених нижче даних, що стосуються здійснення функцій держави або місцевого автономного відомства. Влада людини, яка займає посаду, здійснюється.

Така інформація про осіб та членів їх сімей є конфіденційною і може розповсюджуватися лише за дозволом закону та лише за їх згодою та лише з міркувань національної безпеки, економічного добробуту та прав людини [6].

2.2 Кіберзлочинність

Кіберзлочинність - це незаконні дії людей, які використовують інформаційні технології у злочинних цілях. До основних видів кіберзлочинності належать поширення шкідливого програмного забезпечення, злом паролів, крадіжка номерів кредитних карток та інших банківських реквізитів, а також розповсюдження незаконної інформації через Інтернет. Кіберзлочинність вважається злочинним діянням, яке передбачає несанкціоноване вторгнення в комп'ютерні мережі, комп'ютерні системи та програми для модифікації комп'ютерних даних. Одночасно комп'ютер виступає в ролі інформаційної безпеки суб'єкта та об'єкта злочину. Інциденти, пов'язані зі злочинністю, включають комп'ютер як інструмент злочину, порушення авторських прав, громадську безпеку, майнові права та мораль.

Класифікація кіберзлочинності:

1) Злочини, що загрожують конфіденційності, цілісності та доступності комп'ютерних даних та систем, особливо:

-Нелегальний доступ, наприклад, шляхом хакерських атак, обману та інших засобів;

-Незаконне перехоплення комп'ютерних даних;

-Втручання в дані, включаючи навмисне знищення, знищення, погіршення стану, зміну або приховування комп'ютерної інформації без права на це;

-Втручання в систему, включаючи навмисне спричинення серйозних перешкод для роботи комп'ютерної системи, наприклад, через розподілені атаки на критичну інформаційну інфраструктуру;

- Зловживання обладнанням, тобто виготовлення, продаж, придбання, використання, розповсюдження обладнання, комп'ютерних програм, комп'ютерних паролів або кодів доступу з метою кіберзлочинності

2) комп'ютерні злочини, включаючи підробку та комп'ютерне шахрайство;

3) злочини, пов'язані з інформаційним вмістом, особливо дитяча порнографія, расизм та ксенофобія;

4) Злочини, пов'язані з порушенням авторського права та суміжних прав, такі як незаконне копіювання та використання комп'ютерних програм, аудіо / відео та інших цифрових продуктів, баз даних та книг.

2.3 Захист персональної інформації в медичних системах

Основною складовою зберігання даних пацієнтів в інформаційній системі є електронна медична картка. В електронній медичній картці зберігається вся інформація: дані фізикального огляду, антропометричні дані, дані відеоспостереження, щоденники для динамічного моніторингу стану пацієнтів, вилучення та обстеження в інших клініках, мультимедіа Дані (рентгеногра-

фія, письмові зразки), фотографії) та інші важливі дані пацієнта. Одним із пріоритетів системи охорони здоров'я є створення єдиного медичного інформаційного простору для забезпечення ефективних управлінських рішень на всіх рівнях. Це дасть змогу створити ефективну систему бухгалтерського обліку для організації медичних закладів для впровадження сучасного менеджменту, отримувати своєчасну інформацію про останні події в медичній науці, використовувати всю медичну інформацію про пацієнтів (протягом усього життя) та накопичувати краще лікування на всіх рівнях медичної допомоги ефект.

2.4 Безпека зберігання медичних даних в електронному вигляді

У більшості випадків наслідки викрадення медичної інформації у інших проявляються у формі фінансових зловживань. Наприклад, злодій видає себе за пацієнта та безкоштовно отримує медичну допомогу (наприклад, ліки) для жертви. Після деяких експериментів ви також можете уявити переваги певних медичних послуг (зубних протезів). Алгоритми, що використовуються для захисту даних та шифрування, постійно вдосконалюються. Для великих "ножових поранень" у цій галузі можливостей стає все менше. Слід також зазначити, що захищеність паперової медичної інформації ще нижча. Будь-хто може ознайомитися з ними в своїх руках. Якщо ви перевірите, як зберігаються та переносяться медичні записи, рецепти або результати обстеження в сімейній лікарні, це може взяти кожен. Без конфіденційності, у випадку крадіжки паперу, вона назавжди зникне. Це зникнення є неприйнятним для електронної історії хвороби.

2.5 Проблема повторюваності помилок при копіюванні даних

У більшості випадків наслідки викрадення медичної інформації у інших проявляються у формі фінансових зловживань. Наприклад, злодії видають себе за пацієнтів та надають жертвам безкоштовні медичні послуги (на-

приклад, ліки). Після деяких експериментів ви також можете уявити переваги певних медичних послуг (накладні зуби). Алгоритми, що використовуються для захисту даних та шифрування, постійно вдосконалюються. Для великих "ножових поранень" у цьому районі шанси зменшуються. Слід також зазначити, що захищеність паперової медичної інформації ще нижча. Кожен може прочитати його самостійно. Якщо ви перевірите медичну документацію, як зберігаються та передаються рецепти чи результати перевірки в сімейній лікарні, це може взяти кожен. Без конфіденційності, якщо станеться крадіжка паперу, вона зникне назавжди. Це зникнення є неприйнятним для електронної історії хвороби.

2.6 Підвищення безпеки для пацієнтів

У більшості випадків наслідки викрадення медичної інформації у інших проявляються у формі фінансових зловживань. Наприклад, злодії видають себе за пацієнтів та надають жертвам безкоштовні медичні послуги (наприклад, ліки). Після деяких експериментів ви також можете уявити переваги певних медичних послуг (накладні зуби). Алгоритми, що використовуються для захисту даних та шифрування, постійно вдосконалюються. Для великих "порізаних ран" у цій області шанси зменшуються. Слід також зазначити, що захищеність паперової медичної інформації ще нижча. Кожен може читати сам. Якщо ви подивитесь, як зберігаються та передаються медичні записи, рецепти чи результати обстеження в сімейній лікарні, це може взяти кожен. Без конфіденційності, якщо папір вкрадуть, вона назавжди зникне. Це зникнення є неприйнятним для електронної історії хвороби.

2.7 Лікарська таємниця

Медична інформація про пацієнта дуже важлива: не виходити за межі медустанови: анамнез або дані про перебіг та прогноз конкретного пацієнта, патологія чи будь-який інший лабораторний та інструментальний діагностичний тест, результати операції, операції, реанімації тощо, а не "Вітік" для

незнайомців та широкої громадськості (як правило, у спотвореному вигляді). Це юридична норма.

Конфіденційність медичних послуг є частиною механізму захисту прав людини. Тому важливо висвітлити теоретичні аспекти визначення інформації, що становить медичну таємницю, та інших суміжних понять, щоб чітко розмежувати правову систему для конкретних видів інформації.

Тому медична таємниця має важливе медичне та юридичне практичне значення. Для лікарів та юристів надзвичайно важливо зрозуміти деталі медичної таємниці. Причинами порушення медичної таємниці є, насамперед, незнання закону та нерозуміння шкоди, яка може бути заподіяна порушенням конфіденційності. Тому досі має сенс змінити правила конфіденційності медиків.

2.8 Шифрування діагнозу за допомогою класифікаторів

Серфінг на плечах є одним із найпоширеніших методів отримання інформації, тому для шифрування даних використовуйте МКБ-10, ІСРС-2 для кодування захворювань.

В Україні, відповідно до Постанови Кабінету Міністрів № 326, Постанови 04.05.93 «Про створення Концепції української національної статистики та Національного плану переходу на міжнародну систему бухгалтерського обліку та статистики», МКБ-10 впроваджується в лікувально-профілактичні установи з 1999 року Роки відтоді.

Міжнародна статистична класифікація хвороб та пов'язаних з ними проблем зі здоров'ям є документом, що використовується як основа для основної статистики та класифікацій у системі охорони здоров'я. Регулярні огляди проводяться під егідою ВООЗ. МТП - це нормативний документ, який може забезпечити однаковість методологічних методів та міжнародну перевірку матеріалів. [14]

Мета ІСС - створити умови для запису процесів та проблем, пов'язаних зі здоров'ям, у коді, щоб зберігати, збирати та аналізувати дані.

Для всіх загальних епідеміологічних цілей та багатьох цілей, пов'язаних з управлінням системою охорони здоров'я, МКБ стала міжнародною стандартною діагностичною класифікацією. Ці цілі включають аналіз загального стану здоров'я населення та обчислення частоти та поширеності взаємозв'язку між захворюваннями та іншими проблемами, пов'язаними зі здоров'ям, та різними факторами.

Проводячи дослідження захворюваності на основі медичних вимог, розрізняють такі типи:

1. Загальний рівень захворюваності, що охоплює всі захворювання (гострі та хронічні), зареєстровані серед населення певної території протягом певного періоду;

Інфекційні хвороби - спеціальний облік гострих інфекційних захворювань, що вимагають швидких протиепідемічних заходів;

Через свою епідеміологічну та соціальну значущість (злоякісні пухлини, туберкульоз, венеричні хвороби, психічні захворювання тощо) захворюваність на найважливіші неепідемічні захворювання потребує спеціального пояснення;

Лікарняна або "госпіталізаційна" захворюваність дає можливість вивчити склад госпіталізованих пацієнтів;

Частота тимчасової втрати працездатності серед робітників та службовців відома своїм соціальним та економічним значенням.

Кожен із цих видів захворюваності вивчається за допомогою певних бухгалтерських документів та оцінюється за різними показниками

ICPC2 також використовується для опису діагнозу в Україні.

Міжнародна класифікація первинної медико-санітарної допомоги (ISRS) - найпоширеніша класифікація, що застосовується на низовому рівні в багатьох країнах / регіонах світу. Основним принципом цієї системи є розуміння того, що при ПМД важливим є не лише погляд (діагностика) проблеми пацієнта, а й причина лікування пацієнта, тому в ISRS-2 ви можете кодувати лікування пацієнта причина. [.gov.ua / icpc-2](http://gov.ua/icpc-2)]

Класифікація складена лікарями ПМД, тому вона може найбільшою мірою відображати їх роботу. Усі коди ISRS-2 підходять лише для двох сторінок паперу формату А4.

ICPC-2 містить приблизно 1300 кодів, що використовуються для опису найпоширеніших проблем (більше 1 на 1000 пацієнтів на рік). Рівень деталізації цих питань стосується первинної медичної допомоги. Крім того, ICPC-2 може бути скоригований відповідно до місцевих епідеміологічних потреб. Для порівняння: чинна Міжнародна класифікація хвороб (МКБ-10) містить від 14 000 до 140 000 кодів зі складними системами кодування, більшість з яких не використовуються в ПМД. Відповідно деталізований МКБ-10 можна використовувати в умовах стаціонару госпітальних стаціонарів, де відповідно до спеціалізації певного відділення використовується лише обмежена кількість кодів МКБ.

Основна концепція ISPS-2 - це процес надання медичної допомоги - взаємодія між пацієнтом та медичним закладом від першого візиту (візиту) до медичних працівників, а потім до останнього візиту (включаючи цей), що стикаються з однаковою Проблемою. При "об'єднанні" даних різних індивідуальних відвідувань медичної допомоги це дозволяє ефективно групувати медичну інформацію. Наприклад, пацієнти з хронічними захворюваннями часто відвідують заклади ПМСД і часто вказують на кілька різних проблем під час відвідування. ICPC-2 дозволяє лікарям складати медичні записи для пацієнтів на основі їх особистого стану хронічного захворювання. Це покращить якість медичної допомоги та оптимальне планування ресурсів ПМД з урахуванням потреб пацієнтів.

РОЗДІЛ 3 ПРОЕКТ МЕДИЧНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

3.1 Основні аспекти інформатизації медичної діяльності

Можна виділити такі аспекти інформатизації медичної діяльності: лікування, технологія.

Медичний аспект включає належну підготовку медичних даних та знань (формалізація, уніфікована термінологія, стандартизація), створення інтерфейсів для загальної структури інформаційної бази даних та побудову математичних моделей медичних та біологічних процесів (фізіології та патології).

Технічними аспектами проблеми є розробка теоретичних моделей даних та знань для вирішення супутніх медичних проблем та реалізація конкретного програмного та апаратного забезпечення на основі інформаційної бази даних розроблених моделей.

Технічний аспект відноситься до координації між встановленою технічною системою та технічним рішенням процесу медичної діагностики (наприклад, деякі "методи імплантації" системи в процесі медичної діагностики).

Медична інформаційна система (МІС) використовується для автоматизації роботи на кожному етапі діагностики та лікування. Відомо, щонайменше, два методи визначення ІСУ. Взагалі кажучи, медична інформаційна система - це форма організації медичної та медичної діяльності, яка поєднує в собі лікарів, інженерів та техніків із набором технічних засобів і забезпечує збір, зберігання, обробку та вивільнення в процесі. Різні архіви медичної інформації. -Не певні медичні та медичні завдання. У вузькому розумінні медична інформаційна система - це сукупність технічних засобів, призначених для збору та аналізу медичної та біологічної інформації та опублікування результатів у зручній для користувача формі.

3.2 Етапи створення і основні характеристики медичних інформаційних систем

Створюючи будь-яку інформаційну систему, вона залучає творців проблем, що представляють інтереси потенційних користувачів та розробників та програмістів, які випускають кінцевий продукт (програмне забезпечення).

Моделювання дає поняття предмета, спосіб вирішення проблеми та спосіб сформулювати бажаний результат.

Наступним етапом є усний опис вищевказаного змісту, який містить перелік необхідної вхідної інформації та необхідне подання інформації про джерело.

Далі подано офіційний опис вищезазначеного. Будь ласка, пам'ятайте, що чим глибший рівень офіційності, тим надійніші результати програміста.

Алгоритм рішення означає опис послідовності операцій, які потрібно виконати над вхідною інформацією для отримання бажаного результату на виході.

Останній крок - конкретна програмна та апаратна реалізація проекту.

Основні проблеми в розробці МІС можна узагальнити наступним чином:

- Розробити формат файлу, зручний для фіксації, пошуку та обробки медичної інформації;

- Виберіть розумний метод упорядкування медичних даних для забезпечення ефективного пошуку, зберігання, відновлення та пошуку інформації з пам'яті комп'ютера;

- Розробити набір програмного та апаратного забезпечення для забезпечення передачі даних всередині системи, обміну інформацією із зовнішніми системами та аналізу інформації;

- Впровадження та функціонування інформаційної системи управління. Систематичні вказівки щодо впровадження системи, процедури заповнення стандартизованих медичних документів та розробка інструкцій з експлуатації MIS.

Останнє питання є одним із найскладніших та найактуальніших, оскільки лише на практиці ми можемо перевірити ефективність ідей, впроваджених у розробку ІСУ.

Останнє питання є одним із найскладніших та гостріших, оскільки лише на практиці ми можемо перевірити ефективність ідей, впроваджених у розробку ІСУ. Тому завжди слід мати на увазі, що запровадження системи управління інформацією призведе не тільки до позитивних наслідків, але й до неминучих витрат.

3.2 Етапи створення і проектування баз даних

База даних (БД) - організована структура, призначена для зберігання інформації. Сучасні БД дозволяють розміщувати в своїх структурах не тільки дані, але і методи (тобто програмний код), за допомогою яких відбувається взаємодія зі споживачем або іншими програмно-апаратними комплексами.

Бази даних використовувалися в обчислювальній техніці з незапам'ятних часів. У перших комп'ютерах використовувалися два види зовнішніх пристроїв - магнітні стрічки та магнітні барабани. Ємність магнітних стрічок була досить велика. Пристрої для читання-запису магнітних стрічок забезпечували послідовний доступ до даних. Для читання інформації, яка перебувала в середині або кінці магнітної стрічки, необхідно було спочатку прочитати весь попередній ділянку. Наслідком цього було надзвичайно низька продуктивність операцій введення-виведення даних в зовнішню пам'ять. Магнітні барабани давали можливість довільного доступу, але мали обмежений об'єм інформації.

Зрозуміло, говорити про якусь систему управління даними у зовнішній пам'яті, в той момент не доводилося. Кожна прикладна програма, якою потрібно було зберігати дані в зовнішній пам'яті, сама визначала розташування кожного блоку на магнітній стрічці. Прикладна програма також брала на себе функції інформаційного обміну між оперативною пам'яттю і пристроями зовнішньої пам'яті за допомогою програмно-апаратних засобів низького рівня.

Такий режим роботи не дозволяє або дуже утрудняє підтримку на одному носії декількох архівів довго тривало зберігається.

Для розробки моделі бази даних була обрана реляційна модель даних. Він найкраще підходить для цього завдання, оскільки має безліч переваг:

-Незалежність програми та даних. Ідея використання баз даних та систем управління базами даних передбачає використання додаткових шарів між додатком та фактичними даними, щоб програмісти додатків могли абстрагуватися від реалізації самої бази даних та зосередитися на логіці обробки даних;

-Легко розробляти та моделювати інформаційні ресурси, щоб компенсувати деякі обмеження та уніфікацію в реалізації даних;

-Умови управління даними існують завдяки операціям над колекцією.

3.3 Специфікація

Для візуального зображення можливостей ПЗ використовується діаграма варіантів використання (мал.3.1)



Мал.3.1 Діаграма варіантів використання

Функція «Реєстрація в системі» вимагає від користувача процесу реєстрації на сайті. Для цього потрібно заповнити обов'язкові поля форми, такі як:

Ім'я користувача, електронна пошта, номер телефону, пароль.

Сценарій:

1. Перехід на сторінку реєстрації;
2. Заповнення полів форми;
3. Підтвердження

Функція «Авторизація користувача в системі» вимагає від користувача введення даних у форму авторизації, а саме поля ім'я користувача та пароль. Після авторизації пацієнт має доступ до функції «Перегляд попередніх талонів пацієнтів».

Сценарій:

1. Перехід на сторінку авторизації
2. Заповнення полів форми.
3. Підтвердження.

Функція “Перегляд списку медичних закладів” дає можливість користувачу переглянути список медичних закладів наявних в системі. На сторінці буде знаходитися список з назвами медичних закладів. Обравши якийсь з них користувач зможе переглянути детальну інформацію про медичний заклад та почати реєстрацію на прийом до лікаря обраного закладу.

Сценарій:

1. Перехід на головну сторінку сайту

Функція “Реєстрація на прийом до лікаря” дає змогу користувачу записатися на прийом до лікаря обравши потрібний йому медичний заклад, після чого перед користувачем з'явиться список спеціальностей лікарів даного закладу. Після обрання спеціальності користувачу буде показано список лікарів обраної спеціальності з подальшим вибором конкретної особи лікаря. На наступному кроці користувач заповнює форму, де потрібно заповнити такі поля: «Прізвище», «Ім'я», «По-батькові», «Рік, місяць та день народження»,

«Населений пункт», «Вулиця», «Будинок», «Квартира». Після заповнення останньої форми буде сформовано талон на прийом до лікаря з вказаною інформацією

Сценарій:

1. Перехід на сторінку реєстрації на прийом.
2. Вибір медичного закладу.
3. Вибір спеціальності лікаря.
4. Вибір особи лікаря.
5. Вибір дати і часу прийому.
6. Введення особистих даних
7. Підтвердження

Функція “Перегляд попередніх записів на прийом” дає можливість користувачу переглянути список талонів, які були замовлені на сайті з його аккаунта. На сторінці буде відображатися список талонів, відсортованих по даті, від новіших до старіших. Обравши який користувач зможе переглянути інформацію з талону.

Сценарій:

1. Перехід на особисту сторінку пацієнта.
2. Вибір списку попередніх записів.

Функція “Додавання медичного закладу в систему” дає змогу додати новий медичний заклад в базу даних системи. Дана функція доступна тільки адміністратору. Адміністратор в адміністративній панелі сайту при додаванні нового медичного закладу повинен вказати наступну інформацію: назву, адресу, контактні дані, також додати всіх лікарів даного медичного закладу з графіками робіт.

Сценарій:

1. Перехід в адмінпанель сайту.
2. Вибір посилання на сторінку додавання медичного закладу.
3. Введення інформації про медичний заклад.
4. Підтвердження.

5. Додавання персоналу медичного закладу.
6. Збереження

Функція “Видалення медичного закладу з системи”. Також адміністратор має можливість видаляти медичні заклади з системи, в разі необхідності.

Сценарій:

1. Перехід в адмінпанель сайту.
2. Вибір посилання на сторінку зі списком медичних закладів.
3. Вибір медичного закладу
4. Видалення.

Функція “Редагування інформації медичного закладу в системі”. Адміністратор при потребі має змогу редагувати інформацію про наявний в системі медичний заклад.

Сценарій:

1. Перехід в адмінпанель сайту.
2. Вибір посилання на сторінку зі списком медичних закладів.
3. Вибір медичного закладу
4. Перехід на сторінку редагування.
5. Внесення потрібних змін
6. Збереження.

Також у системі є дійова особа Лікар, яка має доступ до персональної інформації пацієнта, може редагувати її, заповнювати медичну документацію.

3.4 Інформаційне забезпечення системи

Основою інформаційної підтримки при розробці Інтернет-додатків є інформаційна бібліотека, що означає групу організованої інформації, яка використовується в роботі інформаційної системи, та взаємозв'язок між різними компонентами інформації. У той же час організований інформаційний набір відповідає компонентам та змісту розробленого проекту. Інформаційна база

впливає на ефективність роботи всієї системи та здатність вирішувати функціональні проблеми.

3.5 Побудова інфологічної моделі бази даних

Інфографічна модель повинна містити формальний опис предметної області, який легко зрозуміти не тільки експертам баз даних, а й замовникам проекту. Між сутностями.

Ми наголошуємо на наступних моментах:

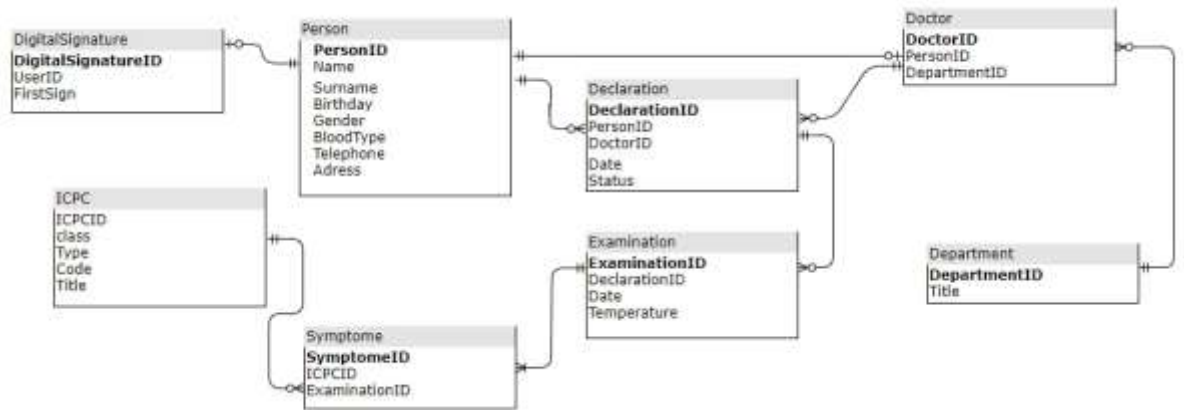
- Пацієнти
- Декларація
- Лікарі
- кафедра
- обстеження
- Міжнародна конвенція про захист рослин
- Скарги
- ЕЦП
- адміністратор

Логічна модель показує, як створювати структури даних та взаємозв'язки між таблицями. На відміну від логічної моделі, що визначає перспективу користувача, фізична модель визначає подання інформації в базі даних. Крім того, для кожного стовпця необхідно вказати тип даних, можливість пробілу символів тощо.

Після отримання моделі надлишкова інформація передаватиметься до мінімально можливої логіки, а модель буде відображатися до 3-х звичайних форм, так що:

- Зменшити потенційні невідповідності інформації, що зберігається в базі даних;
- Усунути виняток додавання, зміни та видалення;
- Цілісність даних.

Логічна модель представлена на **малюнку 3.1**.



Мал. 3.1 Логічна модель

Структура веб-сайту є основою для побудови порядку відображення та форми даних, доступних на веб-сайті. Завдяки правильній структурі веб-сайту користувачі можуть легко переходити від сторінки до сторінки та вивчати необхідну інформацію. [12]

Існують такі типи структур сайтів:

Лінійна структура. Якщо матеріали розташовані в логічний ланцюг, то сформується лінійна структура. Лінійний ланцюг повинен мати початкову і кінцеву точки. Зазвичай безглуздо починати переглядати веб-сайт посередині.

-Структура дерева-найпопулярніша структура для всіх типів сайтів. За винятком першої сторінки, вміст кожної сторінки включається як підрозділ на верхній сторінці

Лінійна з гілками - структура, яка може переходити від однієї гілки до основної «доріжки» сайту перегляду. Це зручно, коли вам потрібно направити користувачів на певні сторінки, і ви можете розмістити більш детальну інформацію в певних областях і куди ви хочете піти.

-Решітчаста структура. Він заснований на побудові системи навігації сайтами, коли існує взаємозв'язок між вертикальними сторінками та горизонтальними сторінками і може швидко переходити з однієї сторінки на іншу, не

відвідуючи проміжну сторінку. Така структура призводить до надмірного збільшення гіперпосилань, і її використання обмежується сайтами з великою кількістю сторінок. [13]

3.6 Опис програмних модулів

Модулі сайту - це невеликі програми або сценарії, написані різними мовами програмування та використовуються на сторінках Інтернет-ресурсів. Їх мета - розширити функціональність Інтернет-додатків, щоб збільшити зручність для відвідувачів під час перегляду та використання ресурсів.

Модуль реєстрації на сайті відображає форму з обов'язковими полями, де ви можете заповнити дані для ідентифікації клієнтів, здійснення покупок та повного використання всіх можливостей Інтернет-програми.

Модуль авторизації відображає форму з необхідними полями введення. Якщо клієнт зареєстрований та авторизований, він може зробити замовлення.

3.7 Опис інтерфейсу

Веб-інтерфейс - це набір спеціальних інструментів, за допомогою яких клієнт може взаємодіяти з Інтернет-програмами через браузер. "Проектування інтерфейсу - це дуже важливий етап створення веб-сайту. Без інтерфейсу неможливо розпочати компонування та програмування. [13]

Основні завдання, для вирішення яких він призначений:

- введення і відображення інформації (звук, зображення);
- управління окремими додатками;
- обмін даними з іншими пристроями;
- взаємодія з операційною системою.

Інтерфейс має на увазі взаємодію не тільки людини і техніки, а й комп'ютер-програма, програма-програма, комп'ютер-пристрій. Наприклад, коли

пристрої підключають до системного блоку комп'ютера, як спосіб взаємодії використовують роз'єм.

Одні види взаємодії дозволяють отримати більше контролю над комп'ютером або смартфоном, але вимагають додаткових навичок. Інші - більш комфортні, але надають менше можливостей. У кожного типу є свої особливості.

Через командний рядок можна виконати максимальну кількість операцій - це прямий спосіб спілкування з операційною системою. Щоб набрати команду, потрібно ввести текст на мові комп'ютера і натиснути Enter, комп'ютер почне виконувати.

Мінус способу в тому, що він підходить тільки підготовленим користувачам. У командному рядку немає допоміжних графічних елементів, для взаємодії доведеться освоїти мову, а щоб команди працювали - не можна допускати помилок.

Графіка спрощує взаємодію з комп'ютером, з нею працювати набагато легше і комфортніше, ніж з текстом. В ролі графічного інтерфейсу виступають такі елементи:

- іконки;
- меню;
- списки;
- малюнки і схеми;
- інші графічні елементи.

Наприклад, при взаємодії з Windows використовують іконки і вікна, для введення підключають миша. На смартфоні пристроєм введення служить сенсорний дисплей.

Текстовий інтерфейс не використовує зображення: команди віддаються за допомогою тексту і інформація надається в текстовому вигляді.

Жестова, голосовий, тактильний і нейронний

Жестової взаємодія дозволяє віддавати команди рухами пальців. Воно застосовується при роботі з сенсорним екраном смартфона. Наприклад, жест «вгору» змушує з'явитися спливаюче вікно.

Голосовий інтерфейс - це управління голосом. Гаджет розпізнає і виконує звукові команди.

Тактильний має на увазі взаємодію за допомогою дотику: вібрація або чутливість до сили натискання.

Нейронний інтерфейс передає команди прямо з мозку в комп'ютер, для цього в мозок вживляють електроди. Його застосовують в медицині: так паралізована людина може спілкуватися з навколишнім світом.

Спеціалізовані засоби для розробки інтерфейсу дозволяють спростити розробку користувальницького інтерфейсу, пропонуючи розробнику уточняти компоненти користувальницького інтерфейсу з використанням мов специфікацій. Можна виділити кілька основних способів специфікації інтерфейсу:

1. Мовний, коли застосовуються спеціальні мови для завдання синтаксису інтерфейсу (декларативні, об'єктно-орієнтовані, мови подій і ін.).

2. Графічна специфікація пов'язана з визначенням інтерфейсу, як правило, засобами візуального програмування, програмуванням демонстрацій і за прикладами. Подібний спосіб підтримує обмежений клас інтерфейсів.

3. Специфікація інтерфейсу, заснована на об'єктно-орієнтованому підході, пов'язана з принципом, званім безпосереднє маніпулювання. Основна його властивість - взаємодія користувача з індивідуальними об'єктами, а не з усією системою як єдиним цілим. Типовими компонентами, використовуваними для маніпуляцій з об'єктами і керуючими функціями, є обробники, меню, зони діалогу, кнопки різного виду.

4. Специфікація інтерфейсу за специфікацією прикладної задачі. Тут інтерфейс створюється автоматично за специфікацією семантики прикладної задачі. Однак складність опису інтерфейсу ускладнює можливості швидкої появи систем, що реалізують даний підхід.

Інтерфейс повинен відповідати наступним правилам:

- Врожайність.
- коротка.
- Ідентифікується.
- Сприйнятливість.
- Послідовність.
- Атракція.
- ефективність.

Сторінки веб-сайту динамічно генеруються на основі використовуваного шаблону сторінки, даних, що відображаються компонентами, та статичної інформації, опублікованої на сторінці.

3.8 Опис контрольного прикладу реалізації проекту

Перш ніж публікувати розроблений проект в Інтернеті, немає необхідності перевіряти його на наявність помилок, лазівок та неправильних умов. Домашня сторінка цього веб-сайту багата на зміст. Користувачі можуть отримати інформацію про діяльність медичних закладів тут. У верхній частині сторінки знаходиться меню, за допомогою якого користувачі можуть зареєструватися або увійти в систему.

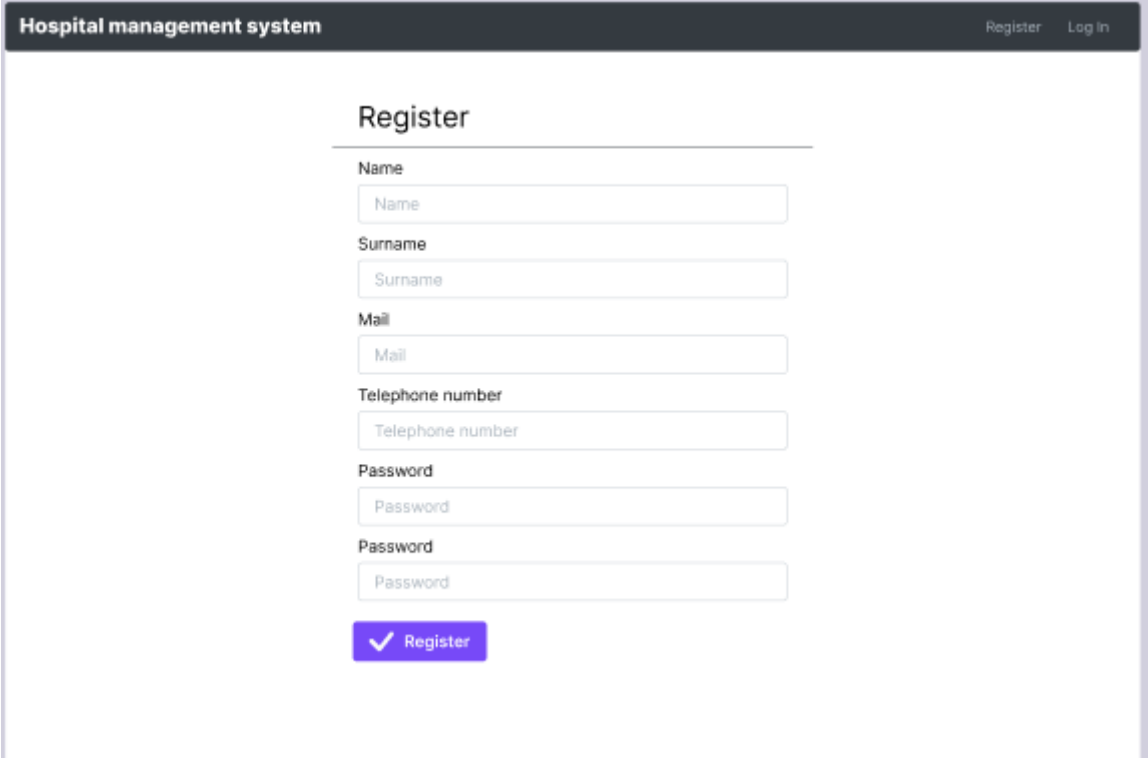
Цей фрагмент домашньої сторінки показаний на малюнку 3.2.



Мал. 3.2 Головна сторінка

Щоб використовувати інформацію про сайт, потрібно завершити процес реєстрації, як показано на малюнку 3.3. Користувач повинен ввести прізвище, ім'я, номер телефону, ім'я для входу, пароль, який містить щонайменше 6 символів, і пароль підтверджено. Після реєстрації на веб-сайті особистий кабінет користувача доступний, і він може отримувати інформацію про обраний медичний заклад та домовлятися про зустрічі з лікарями.

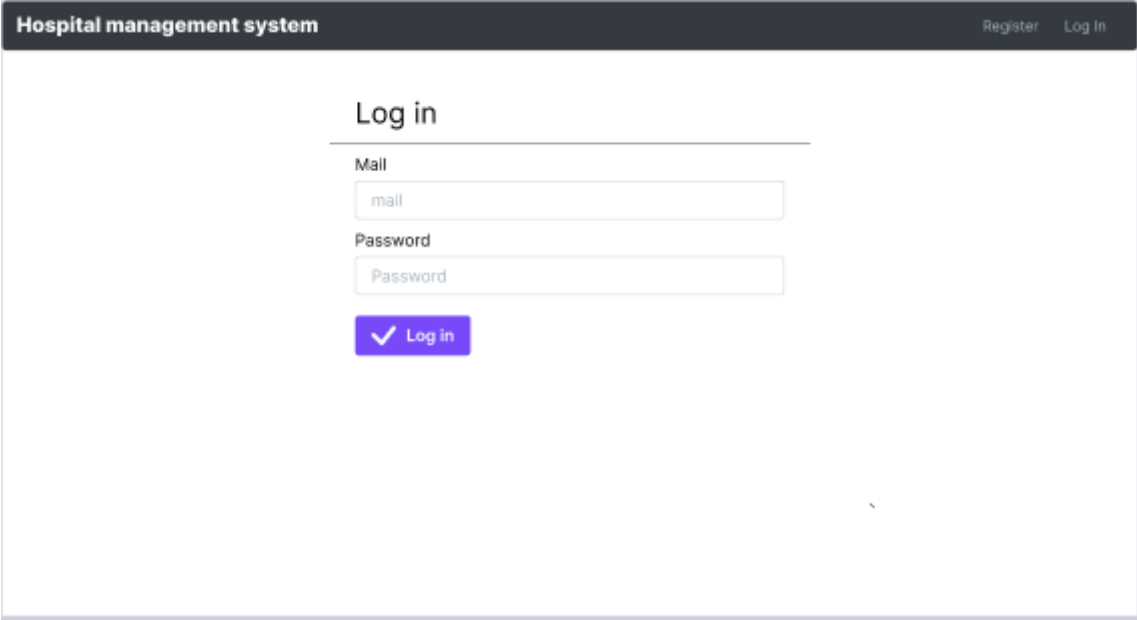
Реєстраційна форма представлена на рисунку 3.3.



The image shows a web interface for a 'Hospital management system'. At the top, there is a dark header with the text 'Hospital management system' on the left and 'Register Log in' on the right. Below the header, the main content area is titled 'Register'. The form consists of several input fields, each with a label above it: 'Name', 'Surname', 'Mail', 'Telephone number', 'Password', and another 'Password' field. At the bottom of the form, there is a blue button with a white checkmark and the text 'Register'.

Мал. 3.3 Форма реєстрації

Якщо користувач вже зареєстрований, він повинен виконати процес авторизації, в якому повинні бути введені ім'я для входу та пароль. Форма дозволу наведена на рисунку 3.4..



The image shows a web interface for a "Hospital management system". At the top left, the title "Hospital management system" is displayed. At the top right, there are links for "Register" and "Log In". The main content area is titled "Log in" and contains a form with two input fields: "Mail" (containing the text "mail") and "Password" (containing the text "Password"). Below the fields is a purple button with a white checkmark and the text "Log in".

Мал. 3.4 Форма авторизації

РОЗДІЛ 4. ПРОГРАМНА РЕАЛІЗАЦІЯ

4.1. Програмна реалізація проекту

Розроблена система програмного забезпечення орієнтована на Інтернет, а потім використовує інтегроване середовище розробки Visual Studio 2019 як основу для розробки.

Microsoft Visual Studio - це серія продуктів Microsoft, яка включає інтегроване середовище розробки програмного забезпечення та багато інших інструментів. Ці продукти дозволяють розробляти консольні та графічні додатки, включаючи підтримку технології Windows Forms та підтримку веб-сайтів, веб-програм та веб-служб для всього власного коду та керованого коду. Платформи, що підтримуються Microsoft Windows, Windows Mobile, Windows Phone, Windows CE, .NET Framework, .NET Compact Framework та Microsoft Silverlight.

C # - це об'єктно-орієнтована мова програмування з безпечною системою набору тексту для платформи .NET. Розроблений Андерсом Галесбергом, Скоттом Вільтамутом та Пітером Голде під егідою Microsoft Research (належить Microsoft).

Синтаксис C # близький до C ++ та Java. Мова має сувору статичну типізацію, підтримує поліморфізм, перевантаження оператора, вказівники на функції члена класу, атрибути, події, атрибути, винятки, коментарі у форматі XML. Відповідно до своїх звичок використання, він використовує багато своїх попередників - C ++, Object Pascal, Module та Smalltalk-C #, і виключає деякі моделі, які виявились проблематичними при розробці програмних систем, таких як C #, із-за C ++, не забезпечує багаторазове успадкування класів.

4.2. Модуль роботи з інтерфейсом Razor Pages

Починаючи з версії 2.0 в ASP.NET Core була додана така функціональність, як Razor Pages. Razor Pages надають технологію, альтернативну систе-

му Model-View-Controller. Razor Pages дозволяють створювати сторінки з кодом Razor, які можуть обробляти запити. В деякій мірі ця функціональність нагадує роботу веб-форм, які представляли сторінку з розширенням `aspx` і мали файл логіки на `C #`, пов'язаний з даною сторінкою. В цьому плані Razor Pages представляють альтернативу стандартній моделі MVC для побудови програми.

Головною відмінністю цього проекту від інших типів проектів є наявність папки Pages. Ця папка містить усі сторінки Razor у проекті за замовчуванням. Кожна сторінка Razor представляє файл із розширенням `.cshtml` і містить суміш HTML-коду та конструкцій `C #`. Це, по суті, однакові уявлення, що використовуються в MVC. Але на відміну від MVC, кожна сторінка Razor пов'язана з окремим файлом логічного коду в `C #`. Наприклад, файл `Index.cshtml.cs` асоціюється з файлом `Index.cshtml`, останній використовує синтаксис Razor + HTML / CSS для визначення візуальної частини, а останній використовує код `C #` для визначення логіки сторінки або її поведінки. Певним чином, ця модель схожа на модель у формах WPF або Xamarin, де файл визначає візуальну частину, а пов'язаний файл коду визначає поведінку.

4.3. ASP.NET Core MVC

Використання режиму MVC є головним моментом платформи ASP.NET Core. Крім того, номер останньої версії платформи MVC, що використовується в ASP.NET Core, становить 3.0 / 3.1. Тому важливо не плутати ASP.NET MVC 5 (для ASP.NET 4.5-4.8) та MVC (для ASP.NET Core). Хоча багато в чому ці рамки однакові.

Також невірно прирівнювати ASP.NET Core до середовища ASP.NET Core MVC. Фреймворк ASP.NET Core MVC працює на платформі ASP.NET Core і має на меті спростити створення програм. Але ми не можемо використовувати MVC, а можемо використовувати лише чистий ASP.NET Core і будувати логіку програми поверх нього.

Шаблон MVC сам по собі не є новою ідеєю в архітектурі додатків, він з'явився на Xerox наприкінці 1970-х років як спосіб організації компонентів у графічному додатку в Smalltalk.

Концепція шаблону MVC передбачає поділ програми на три частини:

Модель: Опишіть дані, що використовуються в додатку, та логіку, безпосередньо пов'язану з даними, наприклад, логіку перевірки даних. Зазвичай об'єкти моделі зберігаються в базі даних.

У MVC модель представлена двома основними типами: модель презентації (що відображає відображення та передачу даних) та модель домену (використовується для опису логіки управління даними).

Модель може містити дані, зберігаючи логіку управління даними. У той же час модель не повинна містити логіку взаємодії з користувачем, а також не повинна визначати механізм обробки запитів. Крім того, модель не повинна містити логіки для відображення даних у поданні.

-View: відповідає за візуальну частину або користувальницький інтерфейс, як правило, HTML-сторінку, через яку користувач взаємодіє з додатком. Презентація також може містити логіку, пов'язану з відображенням даних. У той же час подання не повинно містити обробки запитів користувача або логіки управління даними.

-Контролер: представляє центральний компонент MVC, який забезпечує зв'язок між користувачами та програмами, поданнями та сховищами даних. Він містить логіку для обробки запитів користувачів. Контролер отримує вхідні дані користувача та обробляє їх. І на основі результатів обробки надіслати конкретний висновок користувачеві, наприклад, у формі заповнення моделі даних.

Однак неправильно повністю асоціювати всю платформу ASP.NET Core з MVC. MVC - це просто режим, реалізований на платформі. Ми можемо створити проект на основі шаблону Empty, де немає контролера, моделі чи представлення, а лише клас запуску. І побудувати всю обробку запитів

через цей клас. Але природно, що використання MVC може сприяти роботі додатків.

3.6 Вимоги до апаратного забезпечення

Основним завданням клієнтської програми є веб-сторінка, тому програма повинна відповідати таким мінімальним вимогам: 1 ГГц процесор, щонайменше 512 МБ оперативної пам'яті та 4,5 ГБ вільного місця. Для його використання потрібен швидкий Інтернет та браузер.

3.7 Опис функціональних можливостей

Оскільки основною метою кваліфікаційної роботи є вивчення захисту даних у веб-додатках (тобто базах даних), а не загальний розвиток кінцевого продукту, фокус функції зосереджений на зручності досліджень.

Впроваджено тестовий додаток для роботи медичної системи. Дані системи захищаються трьома способами. Перший раз для перевірки особи за роллю, другий раз для доступу до будь-якої інформації мають лише зареєстровані користувачі, кожна квитанція заповнюється та підписується ЕЦП, а всі прийоми здійснюються через ІСРС2.

Ролі адміністратор, доктор та пацієнт, які реалізовані з використанням класу **IdentityRole**. Представлений у виді:

```
public virtual TKey Id { get; set; }
public virtual string Name { get; set; }
public virtual string NormalizedName { get; set; }
public virtual string ConcurrencyStamp { get; set; }
```

Для кожної ролі відведений свій контролер.

Контролер адміна:

```
[Authorize(Roles = "admin")]
public class AdminController : Controller
```

Основна задача Адміністратора це додавання та видалення докторів, призначення лікарів в департаменти.

```

public async Task<IActionResult> EditDeclaration(string userID)
{
    var currentUserId = _userManager.GetUserId(this.User);
    if (userID == currentUserId)
    {
        ViewBag.message = "Doctor cannot be declarant to yourself";
        return View(null);
    }
    ViewBag.message = "Already has declaration with other doctor";
    var declarations = _db.Declarations.Include(p => p.Patient).Include(d =>
    d.Doctor).FirstOrDefault(p => p.PatientID == userID && p.DoctorID !=
    currentUserId);
    if (declarations != null)
    {
        return View(null);
    }
    else
    {
        Declaration declaration = new Declaration()
        {
            Data = DateTime.Now,
            Patient = _db.Users.First(p => p.Id == userID),
            PatientID = userID,
            Doctor = _db.Doctors.Include(d => d.User).First(d => d.UserId ==
            currentUserId),
            DoctorID = currentUserId,
            Status = 1
        };
        if (_db.Declarations.Include(p => p.Patient).Include(d =>
        d.Doctor).FirstOrDefault(d => d.DoctorID == currentUserId && d.PatientID ==
        userID) == null){
            _db.Declarations.Add(declaration);
            await _db.SaveChangesAsync();
        }
        return View(declaration);
    }
}

```

Контролер лікаря:

```
[Authorize(Roles = "doctor")]
```

```
public class DoctorController : Controller
```

Основна задача підписання декларацій з пацієнтами, заповнення прийому и підписання прийому з використанням ЕЦП. При прийомі пацієнта и для збереження використовуються коди симптомів з таблиці ІСРС2. В БД зберігаються тільки перші 4 символи ЕЦП лікаря, для перевірки чи належить

лікар власником ключа. Підпис даних та перевірка здійснюється за допомогою бібліотеки `System.Security.Cryptography`.

```

        if (_db.Doctors.FirstOrDefault(u => u.User.Id == userID) != null)
        {
            var doctor = _db.Doctors.First(d => d.User.Id == userID);
            doctor.DepartmentId = Convert.ToInt32(departmentID);
            _db.Doctors.Update(doctor);
        }
        else {

            var doctor = new Doctor()
            {
                UserId = userID,
                User = _db.Users.First(u => u.Id == userID),
                DepartmentId = 1,
                Department = _db.Departments.First(d => d.DepartmentId ==
                    Convert.ToInt32(departmentID))
            };

            _db.Doctors.Add(doctor);
            await _userManager.AddToRoleAsync(doctor.User, "DOCTOR");
        }
    }
}

```

Контролер пацієнта:

```

[Authorize(Roles = "patient")]

public class DoctorController : Controller

```

Підтвердження підписання декларації з лікарем, огляд минулих прийомів.

МІВ.

```

[Authorize(Roles = "patient")]
public class PatientController : Controller
{
    readonly ApplicationDbContext _db;

    private readonly UserManager<ApplicationUser> _userManager;
    public PatientController(ApplicationDbContext db,
        UserManager<ApplicationUser> userManager)
    {
        _userManager = userManager;
        _db = db;
    }
    public IActionResult Index()
    {
        return View();
    }
    public IActionResult DeclarationList()

```

```

{
var currentUserId = _userManager.GetUserId(this.User);
List<Declaration> declarations = _db.Declarations.Include(p =>
p.Doctor).Where(d => d.PatientID == currentUserId).ToList();

PatientsViewModel patients = new PatientsViewModel()
{
Declarations = _db.Declarations.Include(p => p.Patient).Where(d => d.DoctorID
== currentUserId).ToList()
};
return View(patients);
}

```

Кожний прийом лікар підписує власним ЕЦП.

```

public void CryptSignature(string key, string examinationID) {

List<ICPC> codes = _db.Examinations.Include(ex => ex.LExDetail).Where(ex =>
ex.ExaminationID == examinationID).toList();
byte[] hashValue = ICPCToByte(codes);
byte[] signedHashValue;
RSA rsa = CreateKeyBySign(key);
RSAPKCS1SignatureFormatter rsaFormatter = new
RSAPKCS1SignatureFormatter(rsa);
rsaFormatter.SetHashAlgorithm("SHA1");
signedHashValue = rsaFormatter.CreateSignature(hashValue);
ExSinature exSinature = new ExSinature()
{
ExaminationID = examinationID,
SignedHashValue = signedHashValue
};
_db.ExSinatures.Add(exSinature);
await _db.SaveChangesAsync();
}

```

Метод який обмежує кількість для підбору паролю.

```

services.Configure<IdentityOptions>(options =>
{
options.Lockout.MaxFailedAccessAttempts = 10;
options.Lockout.DefaultLockoutTimeSpan = TimeSpan.FromMinutes(10);
});

```

Під час реєстрації користувачі проходять двофакторну авторизацію.

Після заповнення форми на електронну адресу надходить лист з кодом підтвердження.

```

public static void CreateTestMessage2(string emailto, string emailfor, string

```

```

code, string server)
{

    MailMessage message = new MailMessage(emailfor, emailto);
    message.Subject = "Hospital auth";
    message.Body = @"Code"+code;
    SmtplibClient client = new SmtplibClient(server);
    client.UseDefaultCredentials = true;
    try
    {
        client.Send(message);
    }
    catch (Exception ex)
    {
        Console.WriteLine("Error while sending email", ex.ToString());
    }
}

```

Додається в базу даних дослідження в таблицю якого входить ІСРС декларації та Дата

Окремо створюється і виводиться список симптомів, який містить айди на це обстеження і ID коду ІСРС

Окрема таблиця, тому що в БД списки не містити

```

public async Task<IActionResult> EditExamination(string userID, string
searchICPC)
{
    var currentUserID = _userManager.GetUserId(this.User);
    Declaration declaration = _db.Declarations.Include(p => p.Patient).Include(d
=> d.Doctor).FirstOrDefault(d => d.DoctorID == currentUserID && d.PatientID
== userID);
    Examination examination;
    if (_db.Examinations.Include(d => d.Declaration).FirstOrDefault(d =>
d.DeclarationId == declaration.DeclarationId && d.Date == DateTime.Today) ==
null)
    {
        examination = new Examination()
        {
            DeclarationId = declaration.DeclarationId,
            Date = DateTime.Today
        };
        _db.Examinations.Add(examination);
    }
}

```



```
await _db.SaveChangesAsync();

}
else
{
    examination = _db.Examinations.Include(d => d.Declaration).FirstOrDefault(d
=> d.DeclarationId == declaration.DeclarationId && d.Date == DateTime.Today);
}

ExaminationViewModel examinationViewModel = new ExaminationViewModel()
{
    SearchResult = searchICPC == null ? null : _db.ICPCs.Where(i=>i.id ==
searchICPC || i.Title.Contains(searchICPC)).ToList(),
    Examination = examination,
    Symptoms = _db.ListSymptoms.Include(e => e.Examination).Where(ex =>
ex.ExaminationID == examination.ExaminationID).ToList()
};
return View(examinationViewModel);
}
```

ВИСНОВКИ

Україна має величезний науково-гуманістичний потенціал у галузі комп'ютерних технологій. Водночас інформатизація медичних закладів є хаотичною, відсутність галузевих стандартів та ліцензій на програмне забезпечення, уніфіковані вимоги до зберігання та форматування інформації та єдиних форм статистичних звітів. Інформатизація галузі. У свою чергу, запланований перехід на загальнообов'язкове медичне страхування призведе до необхідності надання страховим компаніям ключової медичної інформації про хвороби пацієнтів та вживання наркотиків, що відпускаються за рецептом, стимулюючи тим самим ріст інформаційних звітів та ефективно унеможливаючи роботу. Будь-яка організація, яка перебуває в "ручному режимі". Інформатизація охорони здоров'я - це лише питання часу, і, звичайно, це великі капітальні вкладення.

Загалом, розвиток медичних інформаційних технологій може бути одним із важливих факторів для прискорення реальних реформ та розвитку української медицини, і він розвивається у напрямку вдосконалення медичної допомоги та надання якісних медичних послуг людям.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Коваленко Ю. О. Забезпечення інформаційної безпеки на підприємстві / Ю. О. Коваленко // Економіка промисловості. - 2010. - № 3. - С. 123-129. - Режим доступу: http://nbuv.gov.ua/UJRN/econpr_2010_3_20
2. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Нормативний документ системи технічного захисту інформації.
3. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007—2015 роки» від 09.01.2007 № 537-V
4. Теория информационной безопасности и методология защиты информации: учебное пособие. / И.В. Аникин, В.И. Глова, Л.И. Нейман, А.Н. Нигматуллина - Казань: Изд-во Казан. гос. техн. ун-та, 2008. – с. 358.
5. Обрати медичну інформаційну систему. Офіційний сайт електронної системи охорони здоров'я eHealth. [Електронний ресурс]. — URL: <https://ehealth.gov.ua> (дата звернення: 24.05.2020).
6. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України № 2-рп/2012 від 20.01.2012 р. / [Електронний ресурс]. – Режим доступу: <http://www.ccu.gov.ua/uk/doccatalog/list?currDir=167724>.
7. Кавун С.В. Інформаційна безпека. Навчальний посібник. Ч.1/ С.В. Кавун, В.В. Носов, О.В. Мажай. – Харків: Вид. ХНЕУ, 2008. – 352 с.
8. Гафнер, В.В. Информационная безопасность: учебное пособие [Текст] / В.В. Гафнер. — Екатеринбург : Феникс плюс, 2010. — 324 с. — ISBN: 9785222173893.
9. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Нормативний документ системи технічно-

- го захисту інформації. [Електронний ресурс]. — URL: <https://web.archive.org/web/20121202025850/http://am-soft.ua/files/KSZI/2.5-004-99.pdf> (дата звернення: 09.05.2019).
10. Про Основні засади розвитку інформаційного суспільства [Електронний ресурс]. — URL: <http://zakon4.rada.gov.ua/laws/show/537-16> (дата звернення: 09.05.2019).
11. Теория информационной безопасности и методология защиты информации: учебное пособие. / И.В. Аникин, В.И. Глова, Л.И. Нейман, А.Н. Нигматуллина - Казань: Изд-во Казан. гос. техн. ун-та, 2008. – с. 358.
12. Фещенко, А.В. Основи сайтобудування: Електронний навчальний посібник [Електронний ресурс] / А.В. Фещенко-Томськ, 2013 Режим доступу: http://ido.tsu.ru/other_res/ep/sait_umk/
13. Тіторенко, Г.А. Інформаційні технології управління [Текст] / Г.А. Тіторенко-М.: ЮНИТИ-ДАНА, 2014
14. Міжнародний класифікатор хвороб [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%9C%D1%96%D0%B6%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D0%B8%D0%B9_%D0%BA%D0%BB%D0%B0%D1%81%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%82%D0%BE%D1%80_%D1%85%D0%B2%D0%BE%D1%80%D0%BE%D0%B1.
15. Медичні інформаційні технології в Україні [Електронний ресурс] – Режим доступу до ресурсу: <https://www.medsprava.com.ua/article/855-medichn-nformatsyn-tehnolog-v-ukran>.
16. Громадське здоров'я та охорона здоров'я. Под ред. В.А. Міняєва, Н.І. Вишнякова М. «Вища школа», 2002. - С. 173-194
17. Обрати медичну інформаційну систему. Офіційний сайт електронної системи охорони здоров'я eHealth. [Електронний ресурс]. — URL: <https://ehealth.gov.ua> (дата звернення: 14.05.2019).

- 18.Є.М. Кривенко. ВИКОРИСТАННЯ МЕДИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМ УКОМУНІКАЦІЙНІЙ ДІЯЛЬНОСТІ [Електронний ресурс] / Є.М. Кривенко, О.Р. Ситенко, М.А.Знаменська // ІНФОРМАТИЗАЦІЯ ОХОРОНИ ЗДОРОВ'Я – Режим доступу до ресурсу: file:///C:/Users/User/AppData/Local/Temp/Uzn_2015_3_17.pdf.):
- 19.Microsoft Visual Studio [Електронний ресурс] // Вікіпедія – Режим доступу до ресурсу: [https://uk.wikipedia.org/wiki/Microsoft_Visual_Studio].
- 20.C Sharp [Електронний ресурс] // Вікіпедія – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/C_Sharp.
- 21.Т.Б. Большаков, Д.В. Іртегов. Операційні системи. Матеріали сайту http://www.citforum.ru/operating_systems/ois/introd.shtml.
- 22.Методи і засоби розробки користувальницького інтерфейсу: сучасний стан, Клещев А.С. , Грибова В.В. , 2001. Матеріали сайту <http://www.swsys.ru/index.php?page=article&id=765>.
- 23.Дейтел Г. Введення в операційні системи. У двох томах / Пер, з англ. Л.А. Теп-Ліцкая, А.Б. Ходулева, В.С. Штаркмана під ред.В.С. Штаркмана. - М .: Мир, 1987.
- 24.Програмна інженерія. Стандартизація призначеного для користувача інтерфейсу. Євген Волченков. М, 2002. Матеріали сайту <http://tizer.adv.vz.ru>.
- 25.Microsoft Access 2000: довідник / під ред. Ю. Колесникова. - СПб .: Питер, 2001.
- 26.Інформатика. Базовий курс. / Симонович С.В. та ін. - СПб .: Питер, 2006. - 640
- 27.с.Хомоненко А.Д., Циганков В.М., Мальцев М.Г. Бази даних / під ред. проф. А.Д. Хомоненко. - СПб .: КОРОНА, 2000. - 416с.
- 28.Економічна інформатика та обчислювальна техніка. / Под ред. В.П. Косарева. М .: Фінанси і статистика, 2005. -592с
- 29.К. Дж. Дейт Введення в системи баз даних-8-е изд. - М .: «Вільямс», 2006. - С. 1 328.


- 30.Голіцина О.Л., Максимов Н.В., Попов І.І. Бази даних: Навчальний посібник. - М .: ФОРУМ: ИНФРА-М, 2003. - С.352
- 31.
- 32.Карпова Т.С. Бази даних: моделі, розробка, реалізація. - СПб .: Пітер, 2002. - С.304
- 33.Гурська Г. В., магістрантка, Скрипник І.А., доц., канд. техн. наук. — науковий керівник. Система захисту інформації в медичній інформаційних системах. Молода наука-2020 : зб. наук. праць студентів, аспірантів і молодих вчених. Запоріжжя : ЗНУ, 2020. Т. 5.
- 34.Вуколова А. І., магістрантка, Полякова Н.П., доц., канд. техн. наук — науковий керівник. Інформаційна система закладу охорони здоров'я. Матеріали XXV науково-технічної конференції студентів, магістрантів, аспірантів, молодих вчених та викладачів. Запоріжжя : ЗНУ, 2020.

**Декларація
академічної доброчесності
здобувача ступеня вищої освіти ЗНУ**

Я, Гурська Ганна Вікторівна, студент _2_ курсу, форми навчання денної, Інженерного навчально-наукового інституту, спеціальність 121 Інженерія програмного забезпечення, адреса електронної пошти sp115-11@stu.zsea.edu.ua, — підтверджую, що написана мною кваліфікаційна робота на тему «**Інформаційна система закладу охорони здоров'я**» відповідає вимогам академічної доброчесності та не містить порушень, що визначені у ст.42 Закону України «Про освіту», зі змістом яких ознайомлений.

- заявляю, що надана мною для перевірки електронна версія роботи є ідентичною її друкованій версії;

згоден/згодна на перевірку моєї роботи на відповідність критеріям академічної доброчесності у будь-який спосіб, у тому числі за допомогою інтернет-систем, а також на архівування моєї роботи в базі даних цієї системи.

Дата 30.11.2020 Підпис _____  Г.В. Гурська (студентка)

Дата 30.11.2020 Підпис _____  І.А. Скрипник (науковий керівник)