

Є. Б. Радзішевська, О. В. Висоцька

Інформаційні технології в медицині

E-health

За редакцією В. Г. Кнігавка



МІНІСТЕРСТВО ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ
Харківський національний медичний університет

Є. Б. Радзішевська, О. В. Висоцька

Інформаційні технології в медицині. E-health

*Підручник
для студентів медичних закладів вищої освіти*

За редакцією В. Г. Кнігавка

**Харків
ХНМУ
2019**

УДК: 004.9:614.2(075.8)

Р 15

Затверджено вченою радою ХНМУ.

Протокол № 9 від 17.10.19.

Рецензенти

Бих А. І. – д-р фіз.-мат. наук, проф. (ХНУРЕ).

Малєєва О. В. – д-р техн. наук, проф. (НАУ ім. М. С. Жуковського "ХАІ").

Радзішевська Є. Б., Висоцька О. В.

Р 15 Інформаційні технології в медицині. E-health / за ред. В. Г. Кнігавка. – Харків : ХНМУ, 2019. – 72 с.

Підручник наслідує та розвиває питання, викладені в підручнику для студентів медичних ВНЗ "Медична інформатика" за редакцією В. Г. Кнігавка (2015). Складається з 5 розділів, які об'єднано загальною ідеєю розвитку електронної системи охорони здоров'я (E-health). У цьому контексті розглянуто питання стандартизації в медицині, ідеологію E-health та електронної медичної карти, проблеми захисту інформації з огляду на три основні вектори інформаційної безпеки: конфіденційність, цілісність та доступність даних. Інтелектуальні системи підтримки прийняття лікарських рішень як невід'ємна складова E-health представлено у двох розділах підручника, присвячених теорії прийняття рішень у медицині та створенню баз медичних знань. На підставі викладеного матеріалу розкривається основна теза сучасної медичної інформатики: успішне впровадження сучасних інформаційних технологій у медицину та охорону здоров'я для рішення проблем і підтримки прийняття лікарських рішень забезпечить надання високоякісної допомоги пацієнтам та є головною метою охорони здоров'я.

УДК: 004.9:614.2(075.8)

© Харківський національний
медичний університет, 2019

© Радзішевська Є.Б.,
Висоцька О.В., 2019

ВСТУП

У червні 2019 р. Міністерство охорони здоров'я України оприлюднило для громадського обговорення проект Концепції інформатизації охорони здоров'я. Основою стратегії визнано тактику орієнтованості на пацієнта, що означає безперервне накопичення та зберігання даних з прив'язкою до облікового запису пацієнта в його електронній медичній картці, надання пацієнту, як суб'єкту персональних даних, можливості керувати власними медичними даними й доступом до них. Реалізація цього принципу веде до того, що "медичні дані ходять за пацієнтом" при зміні ним лікаря або закладу, що надає пацієнту медичні послуги.

Технологія передбачає пріоритетність електронної форми, тобто при створенні, обміні та зберіганні даних перевага надається електронній формі даних, що обробляються із застосуванням інформаційно-комп'ютерних технологій. Для реалізації цього принципу необхідні інші підходи до аналізу процесів у системі охорони здоров'я та вимоги до структурованості інформації, що матиме наслідком перегляд більшості первинних та облікових форм медичної документації, форм статистичної та іншої звітності. При розгляді будь-яких процесів політики та законодавства у сфері охорони здоров'я в основу має покладатись обмін даними в електронній формі.

Електронна охорона здоров'я (E-health) передбачає використання інформаційно-комунікаційних технологій для поліпшення рівня охорони здоров'я, включаючи спосіб мислення та організації процесів у системі охорони здоров'я та пов'язаних сферах (науці, освіті, дослідницькій діяльності). E-health є галуззю, яка включає в себе не лише інформаційно-телекомунікаційні системи, але й такі компоненти, як органи управління, нормативно-правова база, стандарти і контроль відповідності, кадрові ресурси, інфраструктура, стратегія та модель залучення інвестицій.

У підручнику розглянуто низку питань, що безпосередньо стосуються згаданих вище: значення стандартів у створенні та забезпеченні взаємодії медичних інформаційних систем; електронна система охорони здоров'я як нова галузь розвитку суспільства; права доступу до інформації та захист медичних даних; процеси прийняття рішень у медичній індустрії; підходи до оцінки ефективності діагностичного тесту; автоматизовані системи підтримки прийняття лікарських рішень, основи інтелектуального підходу.

Метою підручника є ознайомлення студентів медичних ЗВО із сучасними тенденціями в системі інформатизації охорони здоров'я та формування необхідних компетенцій у майбутніх спеціалістів.

Розділ 1

ЗНАЧЕННЯ СТАНДАРТІВ У СТВОРЕННІ ТА ЗАБЕЗПЕЧЕННІ ВЗАЄМОДІЇ МЕДИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

1.1. Поняття стандартизації та стандарту

Інформатизація як частина процесу технологічного оновлення медицини стимулює процеси її стандартизації. Це відбувається внаслідок необхідності використання однакової системи кодування і класифікації, упорядкування термінології, а також регламентації основних процесів у медичних інформаційних системах (МІС).

Стандартизація – це діяльність, спрямована на розробку і встановлення вимог, норм, правил, характеристик, як обов'язкових для виконання, так і рекомендованих, яка призначена забезпечити право споживача на придбання товарів і послуг належної якості, а також право на безпеку і комфортність праці. Мета стандартизації – досягнення оптимального ступеня впорядкування в тій чи іншій галузі за допомогою широкого і багаторазового використання встановлених положень, вимог і норм для вирішення реально існуючих, планованих або потенційних завдань.

Стандарт (перше значення) – зразок, еталон, модель, які прийняті за вихідні, для зіставлення з ними інших подібних об'єктів. Стандарт може бути розроблений як на матеріальні предмети (продукцію, зразки речовин), так і на норми, правила і вимоги в різних галузях.

Стандарт (друге значення) – нормативний документ, розроблений на основі консенсусу та затверджений визнаним органом, який спрямований на досягнення оптимального ступеня упорядкування в певній галузі. У стандарті встановлено для загального та багаторазового використання загальні принципи, правила і характеристики різних видів діяльності і/або їх результатів. Стандарт повинен бути заснований на узагальнених результатах наукових досліджень, технічних досягнень і практичного досвіду. В цьому випадку його використання принесе максимальну вигоду для суспільства. Стандарти займають все більш значуще місце в розвитку індустрії інформаційних технологій. На теперішній момент більше 250 підкомітетів в офіційних організаціях по стандартизації працюють над стандартами в галузі інформаційних технологій.

Стандартизація здійснюється на різних рівнях. Рівень стандартизації залежить від того, учасники якого географічного, економічного, політичного регіону світу приймають стандарт. Якщо участь у стандартизації відкрито для відповідних органів будь-якої країни, то це міжнародна стандартизація. Регіональна стандартизація – це діяльність, відкрита тільки для відповідних органів держав одного географічного, політичного або економічного регіону. Регіональна і міжнародна стандартизація здійснюється фахівцями країн, представлених у регіональних і міжнародних організаціях.

Державні стандарти розробляються на продукцію, роботи і послуги, потреби в яких носять міжгалузевий характер. Галузеві стандарти розробляються відповідно до продукції певної галузі. Їх вимоги не повинні суперечити обов'язковим вимогам державних стандартів, а також правилам і нормам безпеки, встановленим для галузі. Приймають такі стандарти державні органи управління (наприклад, міністерства), які несуть відповідальність за відповідність вимог галузевих стандартів обов'язковим вимогам державних стандартів.

Об'єктами галузевої стандартизації можуть бути:

- продукція, процеси та послуги, що застосовуються в галузі;
- правила, що стосуються організації робіт з галузевої стандартизації;
- типові конструкції виробів галузевого застосування, інструменти, деталі кріплення тощо);
- правила метрологічного забезпечення в галузі.

1.2. Провідні міжнародні організації з розробки стандартів

На цей момент провідними міжнародними організаціями з розробки стандартів є такі:

1. Міжнародна організація зі стандартизації ISO (ICO, International Organization for Standardization). Сфера діяльності ICO стосується стандартизації у всіх галузях, крім електротехніки та електроніки, які відносяться до компетенції Міжнародної електротехнічної комісії (МЕК). Деякі види робіт виконуються спільними зусиллями цих організацій. Крім стандартизації, ICO також займається проблемами сертифікації. Своїми завданнями ICO вважає сприяння світовій стандартизації для забезпечення міжнародного обміну товарами і послугами, а також розвиток світового співробітництва в інтелектуальній, науково-технічній та економічній галузях. Основними об'єктами стандартизації ICO є:

- машинобудування;
- хімія;
- руди і метали;
- інформаційна техніка;
- будівництво;
- медицина і охорона здоров'я;
- навколишнє середовище;
- системи забезпечення якості.

До складу ICO входять близько 120 країн зі своїми національними організаціями зі стандартизації. Крім того, з ICO підтримують зв'язок близько 500 міжнародних організацій, зокрема, всі спеціалізовані агенції ООН, що працюють у суміжних напрямках. Практично всі члени регіональних організацій зі стандартизації одночасно є членами ICO, тому при розробці регіональних стандартів за основу береться стандарт ICO. Найбільш тісна співпраця підтримується між ICO і Європейським комітетом зі стандартизації CEN (фр. Comité Européen de Normalisation) – міжнародною некомер-

ційною організацією, основною метою якої є сприяння розвитку торгівлі товарами і послугами шляхом розробки європейських стандартів (євро-норм, EN). У цілому, три організації (ICO, CEN, MEK) охоплюють міжнародною стандартизацією всі сфери техніки і стабільно взаємодіють у галузях інформаційних технологій і зв'язку. Міжнародні стандарти ICO не мають статусу обов'язкових для всіх країн-учасниць. Будь-яка країна світу може їх застосовувати чи не застосовувати. Вирішення даного питання пов'язане переважно зі ступенем участі країни в міжнародному поділі праці і станом зовнішньої торгівлі.

2. Міжнародна електротехнічна комісія (МЕК, англ. International Electrotechnical Commission, IEC) займається стандартизацією у галузі електротехніки, електроніки, радіозв'язку, приладобудування. Ці галузі не входять до сфери діяльності ICO. Основними об'єктами стандартизації МЕК є:

- матеріали для електротехнічної промисловості;
- електротехнічне обладнання виробничого призначення (зварювальні апарати, двигуни, світлотехнічне обладнання та ін.);
- електроенергетичне обладнання (турбіни, лінії електропередач, генератори, трансформатори);
- вироби електронної промисловості (інтегральні схеми, мікропроцесори, друковані плати і т. д.);
- електронне обладнання побутового та виробничого призначення;
- електроінструменти;
- обладнання для супутникового зв'язку;
- термінологія.

3. Об'єднаний технічний комітет (JTC1).

У 1987р. ICO та МЕК об'єднали свою діяльність у галузі стандартизації інформаційних технологій і створили єдиний орган – комітет JTC1 (Joint Technical Committee). Комітет призначений для формування всеохоплюючої системи базових стандартів у галузі інформаційних технологій від техніки програмного забезпечення до мов програмування комп'ютерної графіки та обробки зображень, сполучення устаткування, методів захисту та ін.

1.3. Процеси стандартизації в медичній галузі

Процеси стандартизації міцно увійшли і в медичну індустрію, розвиваючись у міру розвитку медичної інформатики.

Під медичними інформаційними стандартами розуміється набір регламентуючих документів з формування, передачі й обробки медичної інформації, у тому числі в медичних інформаційних системах (МІС).

Ефективний обмін інформацією як усередині медичних установ, так і з іншими організаціями, у тому числі за допомогою МІС, неможливий без однозначного тлумачення понять, які використовуються в численних підрозділах органів охорони здоров'я. Однією з умов вирішення цього завдання є застосування єдиної мови, каталогу і тезаурусу метаданих, що також є предметом стандартизації.

Метадані буквально перекладається як «дані про дані», тобто інформація про інші набори даних. Метадані – це структуровані, кодовані дані, які описують характеристики об'єктів – носіїв інформації і сприяють ідентифікації, виявленню, оцінці та управлінню цими об'єктами. Метадані необхідні для опису значень і властивостей інформації з метою кращого її розуміння, управління і використання. Класичним прикладом є бібліотеки: книги (дані) можна класифікувати, управляти ними і знаходити тільки за допомогою відповідних метаданих (тобто заголовка, автора, ключових слів і змісту).

Зберігання і доставка інформації в електронному вигляді породжує багато проблем. Користувачі повинні мати можливість знайти потрібну інформацію, отримати доступ до неї в прийнятній для них формі. Творці інформації повинні бути впевнені, що їх права на інтелектуальну власність будуть захищені, а адміністратори й інші фахівці повинні мати можливість із супроводу електронної інформації, наприклад, забезпечення її збереження протягом тривалого часу. Метадані є ключовим компонентом для вирішення цих проблем. З огляду на те, що значна частина службових завдань може вирішуватися і реально вирішується без участі людини, метадані поділяють на призначені для використання додатками і для використання людиною. В англійській мові цьому підрозділу відповідають терміни *machine-readable* і *human-readable*.

На практиці метадані зазвичай представляють згідно з певним форматом. Формати метаданих – це стандарти, призначені для формального опису деякої категорії ресурсів, які розробляються міжнародними організаціями або консорціумами, що включають у себе зацікавлені в появі стандарту державні організації та приватні компанії (наприклад, W3C, ICO, ANSI і т. п.)

Інтерес до метаданих істотно зріс у зв'язку з інтенсивним розвитком мережових технологій, які передбачають формування і існування численних спільнот, де взаємодіють люди з різними рівнями знань та інтересів, а межі між традиційними ролями (наприклад, лікар, програміст, інженер, медсестра) розмиті. У зв'язку з цим одним з найбільш перспективних стандартів метаданих є так звана технологія семантичної мережі, розроблена консорціумом W3C (World Wide Web Consortium). Цей стандарт передбачає розширення можливостей Інтернету завдяки наданим механізмам чіткого визначення поняття «інформація», яке дозволяє ефективно використовувати її в спільній роботі як комп'ютерів, так і людей. Технологія семантичної мережі містить середовище опису ресурсів (Resource Description Framework, RDF), механізми для опису загальної архітектури метаданих і забезпечує їх сумісність завдяки використанню спільної семантики, структури та синтаксису.

Так зване Дублінське ядро (Dublin Core) являє собою набір елементів метаданих, який призначений полегшити пошук електронних ресурсів. Спочатку цей стандарт був задуманий як засіб для авторського опису ресурсів у глобальній мережі, проте досить швидко набув міждисциплінарного і міжнародного характеру. Основний набір метаданих дублінської групи є одним з найбільш часто використовуваних стандартів, призначених для підтримки процесу пошуку інформації в ресурсах загального призначення, зокрема для медичних ресурсів.

Тезаурус є засобом, який може гарантувати, що «наскрізна» інформація, яка використовується в медичній установі (а також передається між різними органами охорони здоров'я і між медичними та іншими організаціями) є уніфікованою, тобто однаковою метаданим завжди відповідають однакові поняття.

Тезаурус в загальному сенсі – спеціальна термінологія, більш строго і предметно – словник, набір відомостей, який повномірно охоплює поняття, визначення і терміни спеціальної галузі знань або сфери діяльності, що має сприяти правильній лексичній корпоративній комунікації (розуміння у спілкуванні і взаємодії осіб, пов'язаних однією дисципліною чи професійними обов'язками). На відміну від тлумачного словника, тезаурус дозволяє виявити сенс не тільки за допомогою визначення, але і за допомогою співвіднесення слова з іншими поняттями та їх групами, завдяки чому може використовуватися для наповнення баз знань систем штучного інтелекту.

1.4. Сучасні світові медичні інформаційні стандарти

Умовно їх можна розділити на дві групи: термінологічні стандарти і стандарти обміну інформацією.

Найбільш поширеними термінологічними стандартами є LOINC, MeSH, SNOMED та ін. Медичні предметні рубрики (Medical Subject Headings, MeSH) – всеосяжний контрольований словник, що індексує журнальні статті та книги з природничих наук. Він може також служити тезаурусом, що полегшує пошук інформації. MeSH створений і оновлюється Національною медичною бібліотекою США і використовується в базах статей доказової медицини Medline і PubMed.

Приклад. Згідно з MeSH під вторинної метакхронною пухлиною (Second Primary Neoplasm, Metachronous Second Primary Neoplasms, Neoplasms Metachronous, Second Malignancy, Second Malignancies, Second Neoplasm) розуміють розростання тканини, який йде за попереднім новоутворенням, але не є його метастазом. Друге новоутворення, можливо, має такий самий або інший гістологічний тип і може відбуватися з того ж органа, що і попереднє новоутворення або з іншого органа, але у всіх випадках є результатом незалежного онкогенезу. Виникнення другого новоутворення може бути пов'язано з попереднім лікуванням, а може і не мати до нього відношення, а провокуватися генетичним або іншим фактором.

До числа значущих міжнародних стандартів увійшла номенклатура SNOMED. Комітет зі стандартизації передачі медичних зображень (DICOM) обрав цю номенклатуру для доповнення до своїх стандартів завдяки її гнучкості та інтернаціональному характеру. DICOM рекомендує SNOMED як систему кодування текстових даних, що передаються разом із зображеннями.

SNOMED (Systematized Nomenclature of Human and Veterinary Medicine – Міжнародна систематизована номенклатура людської і ветеринарної медицини) дозволяє кодування декількох аспектів хвороби та є багатоаспектовою системою кодування. Вона складається з 11 пов'язаних взаємними посиланнями класифікацій, званих модулями (табл. 1.1). Структура кожного модуля схожа на структуру класифікації МКХ-9. Крім того, для багатьох термінів є посилання на інші модулі та класифікацію МКБ. Наприклад, діагностичний термін DE-14810 "Легеневий туберкульоз" містить посилання на терміни T-28000 – "Легеня" (топографія), L-21801 – "Бацила туберкульозу людини" (живі організми), а також посилання на код МКХ-9 011.9. Ця додаткова довідкова структура забезпечує зручні можливості пошуку інформації.

Таблиця 1.1.

Розділи Міжнародної класифікації SNOMED

Вісь	Визначення	Опис
T	Топографія	Анатомічні умови
M	Життя організмів	Зміни в клітинах, тканинах і органах
L	Життя організмів	*Бактерії і віруси
C	Хімічні	Ліки
F	Функція	Знаки і симптоми
J	Заняття	Умови, які описують заняття
D	Діагноз	Діагностичні умови
P	Процедура	Адміністративні, діагностичні та терапевтичні процедури
A	Фізичні представники, дії	Пристрої, дії, пов'язані з хворобою
S	Громадський контекст	Суспільні умови і взаємодії в медицині
G	Загальний	Синтаксичні об'єднання і визначення

* Живі організми – розширена класифікація представників тваринного і рослинного світу. Включає практично всі викликані ними патогенні чинники.

Розглядаючи можливості застосування номенклатури SNOMED, слід мати на увазі, що вона насамперед призначена для формалізації опису результатів клінічних спостережень. За її логічну модель автори пропонують наступну формулу:

Для пацієнта з соціального середовища S з професією J [процедура P, застосована до місця T, показала/виявила морфологію M, живий організм L,

хімічний, лікарський і біологічний продукт C, функцію F, фізичний вплив A, захворювання або діагноз D] [з модифікатором G].

Кожна група з розробки стандартів має деяку спеціалізацію. Так, ASC займається зовнішніми стандартами обміну електронними документами, ASTM – стандартами обміну даними лабораторних тестів, IEEE (або "MEDIX") – стандартами обміну медичними даними, DICOM – стандартами, пов'язаними з обміном зображень тощо. Найбільш серйозні стандарти знаходять програмно-апаратну підтримку у таких потужних виробників медичної техніки, як Philips, Siemens, Acuson та ін. У ряді країн питання стандартизації обміну медичними даними вирішуються досить глобально. Так, наприклад, в США, в 1996 р. Американським національним інститутом стандартів ANSI був затверджений національний стандарт обміну медичними даними в електронному вигляді HL7 (Health Level 7).

Health Level 7 (HL7) є стандартом обміну, управління та інтеграції електронної медичної інформації. Він надає ряд гнучких стандартів, директив та методологій, за допомогою яких медичні комп'ютерні програми можуть обмінюватися інформацією між собою. Такі директиви або стандарти є набором правил, які дозволяють поширювати і обробляти інформацію одноманітно, а також сприяють обміну клінічною інформацією між медичними організаціями. HL7 включає в себе концептуальні стандарти (HL7 RIM), документальні стандарти (HL7 CDA), стандарти додатків (HL7 CCOW) і стандарти обміну повідомленнями (HL7 v2.x і v3.0). Останні особливо важливі, оскільки саме вони визначають шлях передачі інформацією між учасниками.

Іншим стандартом, що постійно та інтенсивно розвивається, є DICOM (Digital Imaging and Communications in Medicine – цифрові зображення та обмін між ними в медицині), про який вже згадувалося вище. DICOM – це індустріальний стандарт для передачі радіологічних зображень та іншої медичної інформації. Стандарт DICOM описує "паспортні" дані пацієнта, умови проведення дослідження, положення пацієнта в момент отримання зображення і т. п., для того щоб надалі було можливо провести медичну інтерпретацію цього зображення.

Стандарт дозволяє організувати цифровий зв'язок між різним діагностичним і терапевтичним обладнанням, що використовується в системах різних виробників. Робочі станції, комп'ютерні та магнітно-резонансні томографи, мікроскопи, УЗ-сканери, загальні архіви та ін., що створені різними виробниками, можуть "спілкуватися" один з одним на основі DICOM на базі відкритих мереж за стандартними протоколами. З використанням DICOM'а можна проводити різні медичні дослідження в територіально-розподілених діагностичних центрах з можливістю збору і обробки інформації в потрібному місці.

Серед розробників медичних стандартів можна виділити також європейський комітет CEN / TC 251 (Comite Europeen de Normalisation / Comite 251) з розробки та впровадження стандартів обміну даними між незалежними комп'ютерними системами, який працює за такими напрямками: інформаційні моделі і формати даних в охороні здоров'я; термінологія, семантика і бази знань в охороні здоров'я; комунікації і передача повідомлень в охороні здоров'я; медичні зображення і мультимедіа; передача даних між медичними пристроями; захист, забезпечення конфіденційності та збереження інформації в охороні здоров'я; обмін даними зі змінними пристроями (включаючи магнітні картки).

1.5. Адаптація законодавства України до законодавства ЄС.

На сьогодні адаптація законодавства України до законодавства ЄС відбувається відповідно до положень Закону України про Загальнодержавну програму адаптації законодавства України до законодавства Європейського Союзу від 18 березня 2004 року № 1629-IV. До пріоритетних сфер адаптації належать, зокрема, "охорона здоров'я та життя людей" й "технічні правила і стандарти". Поеднання цих складових на тлі безперервно зростаючого рівня активності у царині біомедичної та медичної інформатики (електронний пропис ліків, електронна медична документація, особисті медичні записи тощо) виводять на принципово новий рівень значущості питання кодування, класифікації та стандартизації в медицині. Системою кодування та класифікації в Україні традиційно є система МКХ, проте у 2017 р. Міністерство охорони здоров'я України уклало угоду з WONCA – Всесвітньою організацією сімейних лікарів – про застосування на ліцензійних засадах системи кодування ICD-2. Цю систему було розроблено WONCA для лікарів загальної практики й натепер однією з її офіційних мов є українська мова.

Ще одним із напрямків інтеграції в європейське співтовариство є розробка і впровадження в повсякденну медичну практику клінічних настанов (рекомендацій), клінічних протоколів та стандартів медичної допомоги.

Практично всі стандарти медичної інформатики, так чи інакше, пов'язані з веденням електронної історії хвороби. Одні стандарти описують термінологію, що повинна бути в ній використана, інші – передачу медичних документів і зображень в електронну історію хвороби, треті – способи організації даних в електронній історії хвороби, четверті – забезпечення доступу медичних працівників і самих пацієнтів до електронної історії хвороби і т. д. Детально питання, що стосуються електронної історії хвороби, будуть розглянуті у наступному розділі.

Питання для самоконтролю

1. Мета стандартизації. Рівні стандартизації з огляду на її відкритість для певної геополітичної одиниці (міжнародна, регіональна). Державні стандарти, об'єкти державної стандартизації. Галузеві стандарти, об'єкти галузевої стандартизації.
2. Міжнародна організація зі стандартизації (ISO). Сфера діяльності ISO. Основні об'єкти стандартизації ISO. Склад ISO, партнери ISO, співпраця ISO з регіональними організаціями зі стандартизації.
3. Міжнародна електротехнічна комісія (МЕК). Сфера діяльності МЕК. Основні об'єкти стандартизації МЕК.
4. Об'єднаний технічний комітет (JTC1). Сфера діяльності JTC1.
5. Медичні інформаційні стандарти. Стандартизація в медичних інформаційних системах (MIC).
6. Поняття метаданих. Роль метаданих у супроводі електронної інформації. Типи метаданих (machine-readable і human-readable). Формати метаданих. Технологія семантичної мережі W3C (World Wide Web) як один з найбільш перспективних стандартів метаданих.
7. Дублінське ядро. Призначення стандартів метаданих дублінської групи.
8. Поняття тезауруса. Семантичні властивості тезауруса.
9. Основні групи медичних інформаційних стандартів (термінологічні стандарти, стандарти обміну інформацією). Найбільш поширені термінологічні стандарти. Медичні предметні рубрики (MeSH). Номенклатура SNOMED.
10. Стандарт обміну, управління та інтеграції електронної медичної інформації HL7.
11. Індустріальний стандарт для передачі радіологічних зображень та іншої медичної інформації DICOM.
12. Європейський комітет CEN / TC 251 (Comite Europeen de Normalisation / Comite 251) з розробки та впровадження стандартів обміну даними між незалежними комп'ютерними системами. Напрямки роботи.
13. Угода про застосування в Україні системи кодування ICD-2. Впровадження в повсякденну медичну практику клінічних настанов, клінічних протоколів та стандартів медичної допомоги.

Розділ 2

ЕЛЕКТРОННА СИСТЕМА ОХОРОНИ ЗДОРОВ'Я

2.1. Медичні інформаційні системи.

Інформатизація діяльності закладів охорони здоров'я давно вже є не просто даниною сучасним віянням, а безумовним трендом розвитку цифрових технологій. Обробка безперервно зростаючого об'єму фінансової, медичної та статистичної інформації стала можливою лише за умови використання сучасних інформаційних комп'ютерних технологій. Провідне місце в цих процесах займають медичні інформаційні системи (МІС), створені на підставі діючих стандартів та призначені для автоматизації різних процесів, що відбуваються в закладах системи охорони здоров'я.

Існують різні підходи до класифікації МІС. Найбільш природним для вітчизняної системи охорони здоров'я (СОЗ) є підхід, заснований на ієрархічному принципі, який відповідає багаторівневій структурі СОЗ та складається з МІС базового рівня, рівня лікувально-профілактичних установ та рівня територій. При такому підході до класифікації назва МІС фактично є відповіддю на запитання «для кого призначено це програмне забезпечення та що воно робить?».

2.1.1. Медичні інформаційні системи базового рівня.

Основною метою МІС базового рівня є комп'ютерна підтримка роботи *лікаря* – клініциста, гігієніста, лаборанта та ін. До них відносяться:

1. Медичні інформаційно-довідкові системи, призначені для пошуку і видачі медичної інформації за запитом користувача. Інформаційні масиви таких систем (бази і банки даних) містять медичну довідкову інформацію різного характеру. Системи цього класу не здійснюють обробку інформації, але забезпечують швидкий доступ до необхідних відомостей. Прикладами таких систем є довідники лікарських препаратів, електронні атласи, класифікатори тощо.

2. Медичні консультативно-діагностичні системи (КДС, або Системи підтримки прийняття лікарських рішень (СППЛР), від англ. "Clinical decision support system" [CDSS]) призначені для діагностики патологічних станів. У самому загальному випадку КДС може містити такі складові частини:

- база даних, призначена для зберігання конкретних даних про об'єкти сфери діяльності КДС;

- база знань, що містить знання, які відносяться до конкретної прикладної галузі, у тому числі окремі факти, правила, а також, можливо, евристики для вирішення завдань у цій прикладній галузі;

- механізм логічного висновку (МЛВ), який на підставі правил та методів бази знань перетворює конкретну інформацію про об'єкт на вид, що відповідає призначенню КДС (діагноз, план дій та ін.);

– інтерфейс з користувачем, що забезпечує безперебійний обмін інформацією між користувачем і системою та надає користувачеві можливість спостерігати за процесом рішення задач, що протікають у МЛВ.

За способом реалізації МЛВ розрізняють експертні та ймовірнісні КДС. В основі МЛВ ймовірнісних КДС лежать методи теорії ймовірностей (ці КДС відносять до класу систем, заснованих на даних), в основі експертних КДС – методи штучного інтелекту. В останніх реалізується логіка прийняття рішення досвідченим лікарем-клініцистом й ці системи відносять до систем, заснованих на *знаннях*.

3. Медичні апаратно-програмні комплекси (МАПК) призначені для інформаційної підтримки та/або автоматизації діагностичного та лікувального процесу, що здійснюється при безпосередньому контакті з організмом хворого або об'єктом дослідження. Використання комп'ютера в поєднанні з вимірювальною і керуючою технікою в медичній практиці дозволило створити нові ефективні засоби для забезпечення автоматизованого збору інформації про стан хворого, її обробки в реальному масштабі часу і управління його станом.

За призначенням МАПК можуть бути розділені на ряд класів:

– системи для проведення функціональних і морфологічних досліджень (дослідження системи кровообігу, органів дихання, головного мозку і нервової системи, органів чуття (зір, слух), рентгенологічні дослідження, УЗД – діагностика та ін.);

– моніторні системи (контроль стану хворого в палатах інтенсивної терапії та операційних);

– системи управління лікувальним процесом (інтенсивна терапія, біологічний зворотний зв'язок, протези і штучні органи, що створені на базі мікропроцесорної техніки);

– системи лабораторної діагностики;

– системи для медично-біологічних досліджень.

4. Автоматизоване робоче місце (АРМ) лікаря. Ці МІС призначені для автоматизації всього технологічного процесу лікаря відповідної спеціальності та забезпечують інформаційну підтримку при прийнятті діагностичних і тактичних лікарських рішень. Всі розглянуті вище інформаційні системи клінічного рівня можуть і повинні входити в структуру АРМ.

Останнім часом бурхливого розвитку набувають також системи для пацієнтів (електронні кабінети пацієнтів, веб-портали, мобільні додатки, системи, що передають медичні дані з носимих пристроїв (wearables) тощо, які також можна віднести до МІС базового рівня.

2.1.2. Медичні інформаційні системи рівня лікувально-профілактичних установ.

Інформаційні системи цього рівня представлені такими групами:

1. МІС консультативних центрів. Призначені для забезпечення функціонування відповідних підрозділів та інформаційної підтримки лікарів

при консультуванні, діагностиці та прийнятті рішень при невідкладних станах.

2. Банки інформації медичних установ і служб. Містять зведені дані про якісний і кількісний стан працівників установи, прикріпленого населення, основні статистичні відомості, характеристики районів обслуговування та інші необхідні відомості.

3. Персоніфіковані реєстри (бази і банки даних). Це різновид інформаційно-довідкових систем, що містять інформацію на прикріпленій або спостережуваний контингент на основі формалізованої історії хвороби або амбулаторної карти. До цієї категорії МІС належать, зокрема, електронні медичні картки.

4. Скринінгові системи. Призначені для проведення долікарського профілактичного огляду населення, а також для лікарського скринінгу (формування груп ризику і виявлення хворих, які потребують допомоги фахівця).

5. Інформаційні системи лікувально-профілактичних закладів. Це інформаційні системи, засновані на об'єднанні всіх інформаційних потоків в єдину систему, які забезпечують автоматизацію різних видів діяльності установи. Зазвичай розрізняють програмні комплекси інформаційних систем: "Стационар", "Поліклініка", "Швидка допомога".

Різновидом МІС цієї категорії є госпітальні інформаційні системи (ГІС), які призначені для інформатизації діяльності медичного стаціонару. Повний комплекс ГІС фактографічного типу може включати в себе: автоматизовані робочі місця головного лікаря та його заступників, підсистеми "Стационар", "Поліклініка", "Параклінічні служби", "Лабораторні дослідження", "Облік лікарських засобів", "Довідкове бюро", "Архів", "Лікувальне харчування", "Бухгалтерські розрахунки", "Економічні розрахунки", "Кадровий облік", "Контроль виконавської діяльності", "Медстатистика", "Облік медобладнання" тощо. Управління та взаємозв'язок між усіма підсистемами здійснюється службовою підсистемою, що являє собою складний програмний комплекс.

6. МІС для науково-дослідних інститутів (НДІ) і ЗВО вирішують три основні завдання: інформатизацію технологічного процесу навчання, науково-дослідної роботи та управлінської діяльності НДІ і ЗВО.

2.1.3. Медичні інформаційні системи територіального рівня.

МІС територіального рівня забезпечують управління спеціалізованими і профільними медичними службами, поліклінікою, стаціонарною й швидкою допомогою населенню на рівні територій (міста, області та ін.).

На цьому рівні МІС представлені такими групами:

1. Адміністративно-управлінські МІС для керівників територіальних медичних служб.

2. Статистичні МІС для роботи зі зведеною по території інформацією.
3. МІС спеціалізованих служб і напрямів: швидкої допомоги, лікарського забезпечення, реєстри (фтизіатрія, психіатрія, інфекційні хвороби та ін.).
4. Комп'ютерні телекомунікаційні мережі, що створюють єдиний інформаційний простір у сфері охорони здоров'я.

2.2. Електронна охорона здоров'я як нова галузь розвитку суспільства.

Протягом останнього десятиліття прогресуюче впровадження нових технологій призвело до революційних змін у поглядах на охорону здоров'я та надання медичних послуг, а також на механізми і канали взаємодій між пацієнтами та постачальниками медичних послуг. В основі цього перетворення лежить зміна шляхів, за якими відбуваються збір, обробка, обмін, зберігання та аналіз медико-санітарної інформації.

Використання електронних процесів у СОЗ сприяє ефективному застосуванню ресурсів, включаючи скорочення витрат, підвищення темпів надання послуг, економію часу, запобігання надмірному використанню або небезпечним взаємодіям лікарських препаратів, скорочення вимушених поїздок і усунення необхідності в наявності фізичної інфраструктури для лікування кожного пацієнта.

Термін «електронна охорона здоров'я» виник давно (деякі пов'язують його появу з дослідженнями академіків Н. М. Амосова та В. М. Глушкова), однак на практиці він став активно застосовуватися на початку нинішнього століття. Сьогодні відомо понад 50 схожих визначень, в яких акцент робиться на різні риси явища, званого електронною охороною здоров'я.

Електронна охорона здоров'я (E-health) розуміє під собою використання інформаційно-комунікаційних технологій для поліпшення рівня охорони здоров'я, включаючи спосіб мислення та організації процесів у системі охорони здоров'я та пов'язаних сферах (науці, освіті, дослідницькій діяльності). E-health є галуззю, яка включає в себе не лише інформаційно-телекомунікаційні системи, але й такі компоненти, як органи управління, нормативно-правова база, стандарти і контроль відповідності, кадрові ресурси, інфраструктура, стратегія та модель залучення інвестицій.

Апаратно-програмною реалізацією електронної охорони здоров'я є електронна система охорони здоров'я (ЕСОЗ).

2.2.1. Основні функції, задачі та можливості ЕСОЗ.

ЕСОЗ забезпечує автоматизацію ведення обліку медичних послуг та управління медичною інформацією шляхом створення, розміщення, оприлюднення та обміну інформацією, даними і документами в електронному вигляді. До складу ЕСОЗ входять центральна база даних та МІС, між якими забезпечено автоматичний обмін інформацією, даними та документами через відкритий програмний інтерфейс (рис. 2.1).

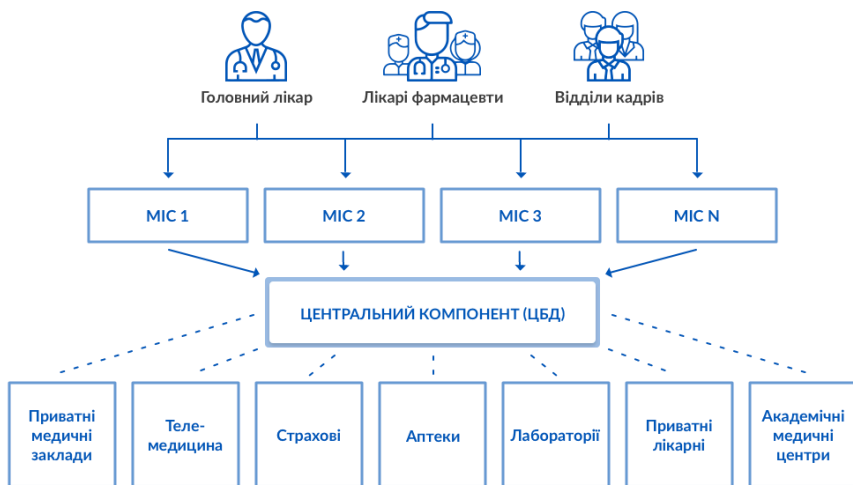


Рис. 2.1. Умовна структура ЕСОЗ

ЕСОЗ дозволяє призначати лікування пацієнтам без необхідності їхньої присутності в кабінеті лікаря, проводити підвищення кваліфікації медичних працівників через систему онлайн-навчання, відслідковувати випадки захворювань і епідемічних спалахів; здійснювати ініціативи щодо зміцнення здоров'я, надавати підтримку в прийнятті медичних рішень тощо.

Впровадження ЕСОЗ дозволяє подолати неефективність системи охорони здоров'я, що пов'язана з недостатністю у лікаря інформації про пацієнта, обмеженістю доступу до медичних послуг, непрозорістю системи охорони здоров'я, недостовірністю даних та з корупцією.

Задачами електронної охорони здоров'я шляхом залучення ЕСОЗ є:

- забезпечення наявності своєчасної та достовірної інформації для державних інституцій, що беруть участь в управлінні системою охорони здоров'я;

- використання переваг обробки так званих "великих даних" (Big Data) та інтелектуальних систем для прогнозування потреб охорони здоров'я;

- планування ресурсів у галузі;

- надання достовірної інформації в необхідному обсязі, у потрібному місці, у потрібний час для учасників системи охорони здоров'я – пацієнтам, лікарям, фармацевтам, науковцям;

- підвищення ефективності праці лікарів, якості медичних послуг шляхом вдосконалення робочих процесів за допомогою інформаційно-комп'ютерних технологій, впровадження систем підтримки клінічних рішень;

– залучення пацієнта до піклування про власне здоров'я та отримання медичних послуг завдяки наданню доступу до власних медичних даних та розпорядження ними.

2.2.2. Базові засади розвитку E-health в Україні.

Основною стратегією проекту Концепції інформатизації охорони здоров'я, що була оприлюднена для громадського обговорення у червні 2019 р. Міністерством охорони здоров'я, визнано тактику орієнтованості на пацієнта, що означає безперервне накопичення та зберігання даних з прив'язкою до облікового запису пацієнта в системі його електронної медичної картки (ЕМК, англ. *electronic health records* або *EHR*), надання пацієнту, як суб'єкту персональних даних, можливості керувати власними медичними даними й доступом до них. Реалізація цього принципу призводить до того, що «медичні дані ходять за пацієнтом» при зміні пацієнтом лікаря або закладу, що надає пацієнту медичні послуги.

При розробленні будь-яких процесів політики та законодавства у сфері охорони здоров'я в основу має покладатись обмін даними в електронній формі.

На перше місце ставиться принцип одноразового введення та багаторазового використання даних в інформаційних системах, завдяки чому персонал у сфері охорони здоров'я отримує вигоду від більш ефективних процесів та відмови від зберігання і обробки даних на паперових носіях.

Комп'ютерні технології з обробки "великих даних" (Big Data) дозволять державі, науковцям та бізнес-середовищу приймати ефективні, економічно обґрунтовані рішення, розробляти інноваційні рішення та підвищувати рівень охорони здоров'я в країні.

Примітка. "Великі дані" (big data) – це широкий термін, що позначає масиви даних, які є настільки великими або мають настільки комплексну природу, що не піддаються обробці традиційними аналітичними методами. Великі і комплексні масиви даних зазвичай вимагають використання розподілених баз даних і складних методів аналізу. Ці масиви описуються як "великі дані", коли їх обсяг значно перевищує звичайні розміри, тип змісту варіюється та необхідна швидкість генерування і обробки даних значно перевищує аналогічні показники типової системи.

Для забезпечення розвитку E-health у країні необхідними є постійні кроки у формуванні Єдиного медичного інформаційного простору з метою створення умов сумісності/інтеграції та можливості передавати дані між системами як в рамках E-health, так й із суміжними галузями та сферами як на рівні України, так і на міждержавному, для подальшої інтеграції з відповідними системами в ЄС. Формування єдиного інформаційного середовища має відбуватися на підставі міжнародних технічних стандартів обміну інформацією, термінологічних словників, класифікаторів у сфері медицини та охорони здоров'я, технічних рішень, гармонізації

законодавства України з законодавством ЄС, зокрема, з вимогами Генерального регламенту ЄС із захисту персональних даних (General Data Protection Regulation (EU) 2016/679, GDPR).

У 2018 р. в Україні почала працювати центральна база даних електронної системи охорони здоров'я (ЦБД ЕСОЗ) (див. рис. 2.1), у рамках якої було створено ряд ключових реєстрів (пацієнтів, медичних спеціалістів, надавачів медичних послуг та ін.), які є критичними для функціонування єдиного інформаційного простору E-health, та сервісів, необхідних для адміністрування програми державних гарантій медичного обслуговування населення (реєстр декларацій про вибір лікаря, який надає первинну медичну допомогу, реєстр договорів про медичне обслуговування населення, звітність тощо).

У 2019 р. на базі ЦБД ЕСОЗ був запущений сервіс електронного рецепту для цілей Урядової програми «Доступні ліки».

Подальший розвиток ЦБД ЕСОЗ вбачається у її розширенні до загальнонаціональної інформаційної платформи (центрального компонента ЕСОЗ), метою якої є, по-перше, сприяння створенню єдиного інформаційного простору шляхом побудови платформи/шини для обміну даними між іншими інформаційними системами у сфері охорони здоров'я та надання доступу до централізованих ключових реєстрів (пацієнти, медичні спеціалісти, надавачі медичних послуг), єдиних класифікаторів й словників. По-друге, створення загальнонаціональної інформаційної платформи має забезпечити зберігання та оброблення даних в обсязі, що є необхідним для управління системою охорони здоров'я та керування програмою медичних гарантій, а також для ефективного використання бюджетних коштів і забезпечення гарантованого доступу до найбільш важливих медичних даних пацієнтів.

Політика держави полягає в інтеграції різних МІС, що призначені для різних категорій користувачів та різних форм власності, з централізованою або децентралізованою архітектурою у єдиний інформаційний простір в рамках ЕСОЗ.

Прикладом таких інформаційних систем є:

- інформаційні системи в закладах охорони здоров'я (амбулаторіях, лікарнях, діагностичних центрах, аптечних закладах тощо), до яких відносяться медичні, госпітальні інформаційні системи, лабораторні інформаційні системи, радіологічні, аптечні інформаційні системи, системи телеконференцій, телемоніторингу, системи планування та управління ресурсами організацій охорони здоров'я;

- системи для пацієнтів, що надають доступ та можливість керування медичними даними (електронні кабінети пацієнтів, веб-портали, мобільні додатки, системи що передають медичні дані з носимих пристроїв (wearables) тощо);

- інформаційні системи у сфері екстреної допомоги;

- інформаційні системи для управління логістикою, обліком складських запасів лікарських засобів та медичних виробів;
 - інформаційні системи у сфері громадського здоров'я та санітарно-епідеміологічного нагляду;
 - реєстри та інформаційні системи у сфері трансплантології;
 - реєстри та системи, пов'язані з випуском електронних листків непрацездатності та довідок;
 - клінічні реєстри та популяційні реєстри, що містять відомості щодо окремих нозологій (наприклад, Національний канцер-реєстр, реєстр пацієнтів, що потребують інсулінотерапії тощо).
- Для повноцінного функціонування ЕСОЗ та всього середовища E-health вдосконалення потребують такі питання:
- оброблення персональних даних, які становлять особливий ризик для прав і свобод суб'єктів персональних даних, їх використання для цілей статистичних, наукових досліджень та з іншими цілями поза метою надання медичної допомоги;
 - порядок ідентифікації, аутентифікації пацієнтів та інших осіб у сфері ЕСОЗ, надання унікального ідентифікатора пацієнта;
 - електронний документообіг;
 - вимоги до технічного захисту інформації в середовищі E-health;
 - вимоги до електронних медичних інформаційних систем та порядков перевірки їх дотримання;
 - порядок ведення форм медичної документації, порядок функціонування медичної статистики.

2.3. Електронна медична карта.

Важливою частиною центрального компонента E-health є інтегрована електронна медична карта, що становить систематизований та стандартизований перелік медичних записів пацієнта в електронному вигляді, які можуть бути створені в різних закладах охорони здоров'я, або посилання на записи, що можуть зберігатись в інших інформаційних системах.

Згідно із класифікацією, запропонованою американським Інститутом медичних записів (Medical Records Institute, USA), фактично можна виділити 5 різних рівнів комп'ютеризації історії хвороби (KIX).

На першому рівні KIX з'являються автоматизовані медичні записи. На цьому рівні в комп'ютерну систему вноситься тільки близько 50 % інформації про пацієнта, яка потім подається у вигляді звітів. Таким чином, така комп'ютерна система являє собою електронний прошарок між користувачем та «паперовою» технологією ведення історії хвороби. Функціями таких систем є реєстрація та виписка пацієнтів, зберігання у словесному вигляді результатів діагностичних процедур та лікарських призначень, протоколи оперативних втручань тощо, які йдуть паралельно паперовій технології.

Другий рівень КІХ є рівнем комп'ютеризованого медичного запису (Computerized Medical Record System). На цьому рівні розвитку "стартує" технологія збереження образів, при якій інформація з діагностичних приладів (роздруківки, сканограми, топограм тощо) скануються, індексуються та фіксуються в системах електронного зберігання зображень (як правило, на магнітооптичних накопичувачах).

Третій рівень розвитку КІХ має назву рівня "електронних медичних записів" (Electronic Medical Records). Для цього рівня необхідним є наявність в медичному закладі такої інфраструктури, яка дозволяє опрацьовувати електронну інформацію з робочих місць. На цьому рівні користувачі вже мають бути ідентифіковані системою, мати права доступу, що відповідає їх статусу. На цьому електронний медичний запис як одиниця КІХ вже може використовуватися у процесах прийняття рішень та інтегруватися з експертними системами в задачах постановки діагнозу та вибору тактики лікування.

Четвертий рівень розвитку КІХ – системи електронних медичних записів (Electronic Patient Record Systems) – є рівнем розвинутих електронних записів, що формуються на підставі численних інформаційних джерел, які можуть надаватися різними медичними установами. Цей рівень розвитку потребує загальнодержавної або інтернаціональної системи ідентифікації пацієнтів, єдиної системи термінології, структури інформації, кодування та ін.

П'ятий рівень розвитку КІХ – "електронний запис про здоров'я" (Electronic Health Record), має практично необмежену кількість інформаційних джерел про здоров'я пацієнта, зокрема, відомості з галузей нетрадиційної медицини, поведінкової діяльності (куріння, заняття спортом, використання дієт та ін.).

З класифікації, наведеної вище, виходить, що наявність електронної медичної картки зокрема та технології E-health у цілому потребують наявності у країні як мінімум четвертого рівня розвитку КІХ. Переваги використання електронної медичної картки наведено на *рис. 2.2*.

2.3.1. Основні поняття та визначення

Електронна історія хвороби (EIX) – це інформаційна система, яка призначена для ведення, зберігання на електронних носіях, пошуку та видачі за інформаційними запитами (у тому числі і за електронними каналами зв'язку) персональних медичних записів.

Іноді використовують терміни електронна медична карта, персональна електронна медична картка та система ведення електронних медичних карт. При цьому традиційний термін «електронна історія хвороби» є аналогом системи ведення електронних медичних карток.

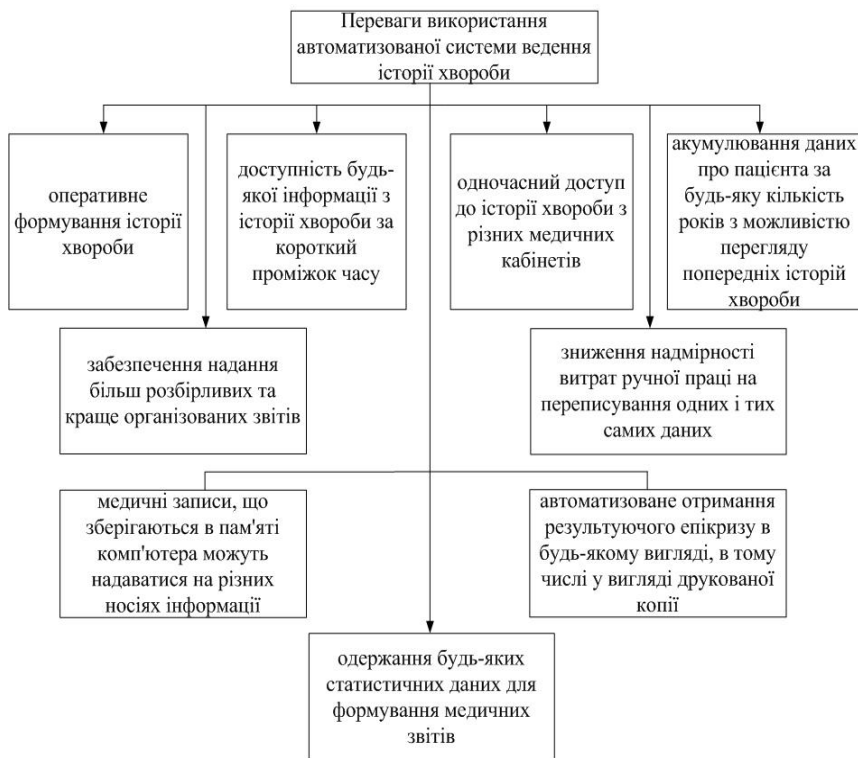


Рис. 2.2. *Переваги використання автоматизованої системи ведення історії хвороби*

Електронна медична картка (друге значення) – сукупність електронних персональних медичних записів (ЕПМЗ), які відносяться до однієї людини, що збираються, зберігаються та використовуються в рамках однієї медичної організації. Яке із наведених значень мається на увазі, зазвичай є зрозумілим із контексту.

Електронний персональний медичний запис (ЕПМЗ) – будь-який персональний медичний запис, зроблений конкретним медичним працівником відносно конкретного пацієнта та збережений на електронному носії.

Електронний медичний документ (ЕМД) – електронний медичний персональний запис, що пройшов стадію підписання уповноваженою особою, яка повністю відповідає за його зміст, і який є юридично значимим медичним документом, що володіє властивостями постійності та цілісності.

ЕМК є індивідуальною і містить таку інформацію: паспортні дані, дату та рік народження, місце проживання, ідентифікаційний код, належ-

ність до груп населення (пенсіонери, діти, службовці, робітники і т. д.), зайнятість (працюючий або непрацюючий), група інвалідності (якщо встановлена), право на пільги, наявність хронічних захворювань, інформацію про перенесені захворювання, операції, лікування.

Поряд з цим ЕМК містить інформацію фінансового характеру, зокрема щодо накопичених страхових внесків, вартості наданої медичної допомоги.

ЕМК створюється один раз при першому зверненні пацієнта в медичний заклад при його реєстрації. Усередині ЕМК фіксуються епізоди по кожному випадку звернення пацієнта до лікувального закладу. У разі знаходження пацієнта на стаціонарному лікуванні формується електронна історія хвороби. У разі поліклінічного лікування – амбулаторна карта пацієнта.

При закритті епізоду, документи, що сформовані в ЕМК, змінюють чи доповненням не підлягають. Інформація до ЕМК збирається протягом всього життя людини.

ЕМК включає в себе:

– електронні медичні записи (рис. 2.3) – лікарські огляди, результати консультацій фахівців, записи медсестер, результати аналізів, результати досліджень (рис. 2.4);

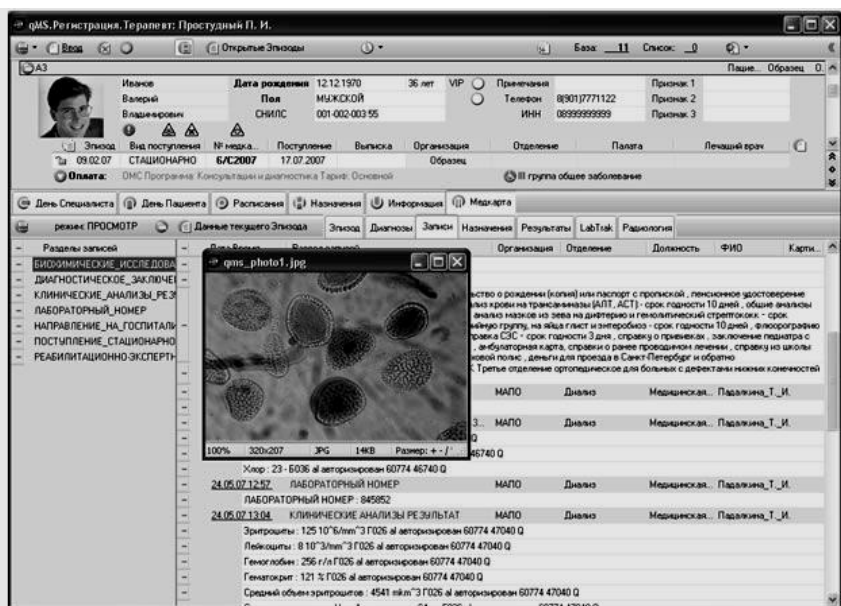


Рис. 2.3. Диалогове вікно "Медкарта" (MIC "qMS"»)

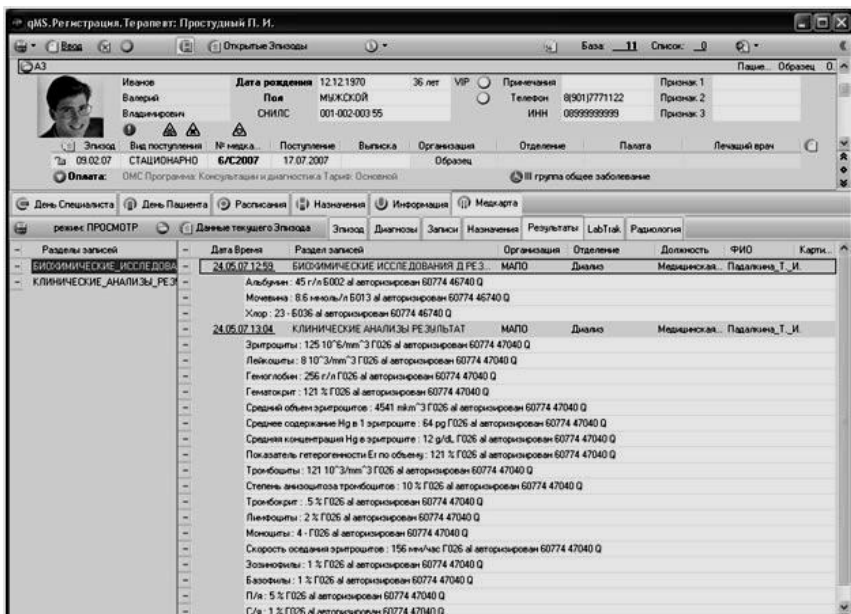


Рис. 2.4. Диалогове вікно "Результаты" (MIC "qMS")

– призначення – всі види призначень пацієнтові за випадками лікування (лабораторні дослідження, діагностичні маніпуляції, медикаменти – у тому числі пільгові рецепти, консультації фахівців тощо);

– результати лабораторних та інструментальних досліджень, що зберігаються в ЕМК у вигляді як сканованих, так і цифрових зображень завдяки інтеграції системи з лабораторними системами та системами зберігання медичних зображень;

– графічні файли, скановані зображення, цифрові фотографії, що дозволяють оцінити тяжкість перебігу захворювання та динаміку стану процесу в ході лікування пацієнта.

Кількість необхідних розділів медичних записів в ЕМК пацієнта не обмежена, для кожного фахівця можуть бути створені свої шаблони і свої розділи, необхідні для введення медичних записів, у тому числі з використанням загальноприйнятих класифікаторів, які дозволяють максимально швидко та повно відображати стан пацієнта.

У будь-якій частині ЕМК лікарю надана можливість введення вільного тексту, що відповідає вимогам системи стандартів ведення електронних медичних записів.

ЕМК містить всі необхідні розділи для ведення лікарями амбулаторної карти пацієнта і його історії хвороби (для стаціонарів) в електронному вигляді, а саме:

- скарги;
- анамнез захворювання та анамнез життя;
- огляди пацієнта лікарями-спеціалістами;
- попередній клінічний і заключний клінічний діагнози;
- план обстеження;
- план лікування;
- лист лікарських призначень;
- температурний лист;
- дані лабораторних та інструментальних досліджень;
- етапний, перекладний і виписаний епікриз.

Інтегрована електронна медична карта (ІЕМК) – сукупність електронних персональних медичних записів (ЕПМЗ), які відносяться до однієї людини, що збираються і використовуються декількома медичними організаціями. Інтегрована електронна медична карта може бути створена групою медичних організацій, органом управління охороною здоров'я регіону або навіть на національному рівні. Спосіб управління ІЕМК, зберігання інформації в ній, права доступу та стандарти інформаційного обміну й інтероперабельності повинні бути визначені організаціями, що використовують ІЕМК, або органами управління охорони здоров'я, що створюють ІЕМК. Загальні вимоги до ІЕМК повинні бути сформульовані в окремому національному стандарті.

Персональна електронна медична карта (ПЕМК) – сукупність ЕПМЗ, що надійшли з різних джерел та відносяться до однієї людини, яка і здійснює їх збір, управління ними, а також визначає права доступу до них. Зберігання ПЕМК може здійснюватися її власником на власних електронних носіях (особистому комп'ютері, флеш-пам'яті та ін.) або у спеціалізованих сховищах, доступних через мережу Інтернет або інші канали зв'язку. В останньому випадку зберігання, а також надання сервісу ведення та управління ПЕМК здійснює спеціалізований провайдер на підставі угоди, укладеної з власником ПЕМК. Загальні вимоги до провайдерів ПЕМК і наданому ними сервісу, а також до систем ведення ПЕМК на особистих електронних носіях повинні бути сформульовані в окремому національному стандарті.

Електронний медичний архів (ЕМА) – електронне сховище даних, що містить ЕМК пацієнтів однієї медичної організації та інші набори даних і програм (класифікатори та довідники, списки пацієнтів і співробітників, засоби навігації, пошуку, візуалізації, інтерпретації, перевірки цілісності та електронно-цифрового підпису тощо), необхідні для повноцінного функціонування систем ведення електронних медичних карт у цій медичній організації..

ЕМА є єдиним інформаційним об'єктом, що дозволяє виконати всі необхідні процедури щодо ЕМК, які зберігаються в ньому. Поняття "електронний медичний архів" еквівалентно поняттю "база даних". Слово "архів" тут використовується в значенні "сховище".

Інтегрований електронний медичний архів (ІЕМА) – електронне сховище даних, що містить ІЕМК, які збираються і використовуються декількома медичними організаціями, а також інші набори даних та програм, необхідні для спільного використання збережених ІЕМК. ІЕМА створюється групою медичних організацій для спільного використання або органом управління охороною здоров'я для підвідомчих йому організацій. Зберігання інформації в рамках ІЕМА може бути централізованим або розподіленим. В останньому випадку доступ до інформації ІЕМК пацієнтів здійснюється через централізований індекс, що є частиною ІЕМА. Вимоги та правила функціонування ІЕМА, права доступу і стандарти інформаційного обміну встановлюються медичними організаціями, які спільно використовують ІЕМА, або органом управління охороною здоров'я, який його створив. Загальні вимоги до ІЕМА повинні бути сформульовані в окремому національному стандарті.

Персональний електронний медичний архів (ПЕМА) – електронне сховище даних, що містить ПЕМК, а також інші набори даних, програм і сервісів, необхідні для збору, ведення та управління ПЕМК з боку їх власників. ПЕМА створюється конкретним провайдером для надання приватним особам послуг з ведення, безпечного зберігання та управління їх особистими ПЕМК. Засоби управління, що входять до складу ПЕМА, повинні передбачати можливість надання прав доступу до ПЕМК або її частини медичним працівникам, організаціям або іншим особам, за розсудом власника ПЕМК. Взаємовідносини між власником ПЕМК і провайдером ПЕМА встановлюються на підставі договору (угоди). Правила функціонування ПЕМА, права та обов'язки користувачів, стандарти електронного обміну, вимоги безпеки встановлюються провайдером відповідно до чинного законодавства. Загальні вимоги до ПЕМА повинні бути сформульовані в окремому національному стандарті.

Система ведення електронних медичних карт (СВЕМК) – набір комп'ютерних програм, організаційної та технічної документації, а також служб супроводу та підтримки, призначених для збору і використання інформації, що входить до складу електронних медичних карт (у тому числі інтегрованих та персональних). Традиційний термін "електронна історія хвороби" є аналогом СВЕМК. Поняття СВЕМК включає засоби, що дозволяють користувачам взаємодіяти з інформацією, яка міститься в електронних медичних архівах (ЕМА, ІЕМА, ПЕМА).

2.3.2. Структура електронного персонального медичного запису.

ЕПМЗ включає в себе такі обов'язкові елементи:

1. Ідентифікатор пацієнта – елемент, який однозначно визначає, якому пацієнту належить ця ЕПМЗ.

Ідентифікатор, як правило, є посиланням до списку пацієнтів цієї установи, міститься в електронному медичному архіві. Однак ідентифікатором може бути і набір реквізитів пацієнта, що дозволяє однозначно знайти його серед пацієнтів цієї медичної організації.

2. Ідентифікатор даної ЕПМЗ – елемент, що дозволяє однозначно знайти цю ЕПМЗ в електронному архіві відповідної медичної організації.

3. Дата та час події, що описується цією ЕПМЗ (огляд пацієнта, проведення маніпуляції, забір біоматеріалу для аналізу та ін.). Дата є обов'язковим елементом, час вказують там, де він має значення.

4. Ідентифікатор особи, що створила запис – елемент, який дозволяє однозначно визначити, хто створив цей запис. Ідентифікатором може бути посилання на довідник співробітників або набір реквізитів, що дозволяє однозначно визначити автора ЕПМЗ серед співробітників цієї медичної організації. Особа, яка створила запис, і автор запису можуть не збігатися.

5. Ідентифікатор автора ЕПМЗ – обов'язковий елемент, що дозволяє однозначно визначити, хто є автором цього медичного запису і несе відповідальність за її зміст. Автором ЕПМЗ вважається саме особа, яка несе відповідальність за її зміст, а не особи, що брали участь у її підготовці. Наприклад, автором аналізу є лікар-лаборант, який затвердив його, а не лаборанти, які виконували окремі тести (їх ідентифікатори можуть міститися в інших, необов'язкових елементах ЕПМЗ). Ідентифікатором може бути посилання на довідник співробітників або набір реквізитів, що дозволяє однозначно визначити автора ЕПМЗ серед співробітників цієї медичної організації. При використанні електронного цифрового підпису (ЕЦП) ідентифікатор автора повинен дозволити знайти сертифікат ЕЦП та перевірити його.

6. Дата та час підписання ЕПМЗ. Обов'язковий елемент, що вказує, з якого моменту ЕПМЗ вважається закінченим, підписаним і набуває статусу офіційного медичного документа. Цей елемент також є ознакою статусу запису: якщо дата та час вказані, то ЕПМЗ закінчена і доступна іншим медичним працівникам як офіційний медичний документ; якщо дата та час не вказані, то ЕПМЗ не закінчена і є робочим документом автора або групи співробітників.

7. Дайджест – елемент, отриманий методом хешування* вмісту ЕПМЗ і зашифрований особистим ключем сертифіката ЕЦП особи, яка підписала ЕПМЗ. Дайджест повинен бути отриманий хешуванням всього

вмісту ЕПМЗ, включаючи всі прикріплені файли і всі елементи формалізованих даних, з тим щоб жоден із цих елементів не можна було змінити, не порушивши цілісності ЕЦП. Даний елемент обов'язковий при використанні ЕЦП.

Примітка. *Хешування (англ. Hashing) – перетворення вхідного масиву даних довільної довжини на вихідний бітовий рядок фіксованої довжини. Такі перетворення також називаються хеш-функціями або функціями згортки, а їх результати називають хешем, хеш-кодом або дайджестом повідомлення (англ. message digest). Хешування застосовується для порівняння даних: якщо у двох масивів хеш-коди різні, масиви гарантовано розрізняються, якщо однакові – масиви, швидше за все, однакові. У загальному випадку однозначної відповідності між вихідними даними і хеш-кодом немає через те, що кількість значень хеш-функцій менша, ніж варіантів вхідного масиву; існує безліч масивів, що дають однакові хеш-коди – так звані колізії. Імовірність виникнення колізій відіграє важливу роль в оцінці якості хеш-функцій. Існує безліч алгоритмів хешування з різними характеристиками (розрядність, обчислювальна складність, криптостійкість і т. п.). Вибір тієї чи іншої хеш-функції визначається специфікою розв'язуваної задачі. Найпростішими прикладами хеш-функцій можуть служити контрольна сума).

ЕПМЗ може включати в себе наступні необов'язкові елементи:

1. Ідентифікатор типу ЕПМЗ – елемент, який визначається згідно з класифікатором типу записів, що використовуються в цьому електронному архіві відповідної медичної організації. Може бути опущений, якщо в цьому електронному архіві використовують всього один тип ЕПМЗ (наприклад, в ізольованому електронному архіві лабораторії, де проводять один тип аналізів і, відповідно, ведуть один тип ЕПМЗ).

2. Номер історії хвороби або амбулаторної карти – необов'язковий елемент, що дозволяє визначити, у рамках якої історії хвороби або амбулаторної карти складений цей ЕПМЗ.

3. Текст ЕПМЗ – необов'язковий елемент, що являє собою медичний зміст цього ЕПМЗ (результат аналізу або обстеження, статус, епікриз, призначення ліків і т. д.). Текст може бути відсутнім, якщо він міститься у файлах, прикріплених до ЕПМЗ, або будується на підставі формалізованих даних, прикріплених до ЕПМЗ.

4. Прикріплені файли – необов'язкові елементи, що містять додаткову інформацію про цю ЕПМЗ (медичні зображення, графічні матеріали, тексти в різних форматах і т. д.). Прикріплені файли повинні мати стандартні формати. У систему повинні бути включені засоби (програми), що забезпечують перегляд файлів використовуваних форматів.

5. Формалізовані дані, прикріплені до ЕПМЗ – необов'язкові елементи, що містять набір кодів, формалізовані значення і реквізити, які дозволяють за допомогою спеціальних програмних модулів представити медичний зміст ЕПМЗ у вигляді, що легко читається, а також проводити

електронну обробку ЕПМЗ. Формалізація даних дозволяє індексувати ЕПМЗ, виробляти їх пошук, відбір та фільтрацію за певними ознаками, будувати динамічні криві, проводити статистичну обробку, формувати звіти і т.д. Формалізація даних може також служити для контролю та регламентації введеної інформації (вибір з певної безлічі відповідей) і скорочення довжини тексту, що вводиться (кодування стандартних фраз, фрагментів та термінів).

ЕПМЗ може включати в себе й інші структурні елементи, визначені правилами роботи конкретної медичної організації.

2.3.2. Життєвий цикл електронних персональних медичних записів.

Життєвий цикл ЕПМЗ включає в себе такі етапи:

- створення;
- ведення;
- підписання;
- зберігання з наданням доступу до нього зацікавлених осіб;
- знищення.

Створення ЕПМЗ може бути виконане медичним співробітником, який має право на створення цього типу ЕПМЗ. У момент створення вказують перші п'ять обов'язкових структурних елементів ЕПМЗ і номер історії хвороби або амбулаторної карти. Задані структурні елементи повинні залишатися незмінними протягом усього життєвого циклу ЕПМЗ.

Ведення ЕПМЗ включає в себе створення та перетворення на електронну форму змістовної медичної частини цього медичного запису.

Термін зберігання ЕПМЗ визначається нормативними документами, що регламентують терміни зберігання звичайних (паперових) медичних документів даного типу. Протягом всього терміну зберігання для ЕПМЗ повинні бути забезпечені збереження, незмінність і достовірність.

Для забезпечення збереження зазвичай використовують методи дублювання електронного устаткування та резервного копіювання.

Для забезпечення незмінності та достовірності зазвичай використовують комплекс технологічних і адміністративних процедур, що перешкоджають випадковій або навмисній зміні збережених записів. Найкращим рішенням є використання електронного цифрового підпису, що дозволяє в будь-який момент перевірити незмінність збереженого запису порівняно з моментом його підписання.

Інформаційна система не повинна нав'язувати процедуру підписання ЕПМЗ (може тільки нагадувати про не підписані документи).

Медичний працівник повинен ініціювати процедуру підписання самостійно. Згода на процедуру підписання повинна супроводжуватися діями, що дозволяють провести персоніфікацію і аутентифікацію медичного працівника:

- введення пароля;
- підключення електронного пристрою, що ідентифікує (SMART-карти або ключа);
- зчитування коду з індивідуальної карти (магнітної, штрихкової або оснащеної чіпом);
- введення PIN-коду для SMART-карти або ключа, постійно підключеного до комп'ютера.

Питання для самоконтролю

1. Медичні інформаційні системи (МІС). Класифікація МІС.
2. МІС базового рівня, їх призначення. Інформаційно-довідкові МІС, призначення, приклади. Медичні консультативно-діагностичні системи (КДС). Призначення, типовий склад. База даних, база знань, механізм логічного висновку (МЛВ), інтерфейс з користувачем. Класифікація КДС за ознакою реалізації МЛВ. Системи, засновані на даних. Системи, засновані на знаннях. Медичні апаратно-програмні комплекси (МАПК), призначення, класифікація. Автоматизоване робоче місце (АРМ) лікаря. Системи базового рівня для пацієнтів.
3. МІС консультативних центрів, їх призначення. Банки інформації медичних установ і служб. Їх призначення, характер інформації, що зберігається. Персоніфіковані реєстри (бази і банки даних). Їх призначення, характер інформації, що зберігається. Електронні медичні картки як представники персоніфіковані реєстрів. Скринінгові системи, їх призначення. Інформаційні системи лікувально-профілактичних закладів, їх основні представники. Госпітальні інформаційні системи (ГІС) як різновид систем цієї категорії. Основні компоненти ГІС. МІС для науково-дослідних інститутів (НДІ) і ЗВО.
4. Адміністративно-управлінські МІС. Статистичні МІС для роботи зі зведеною по території інформацією. МІС спеціалізованих служб і напрямів. Комп'ютерні телекомунікаційні мережі.
5. Використання електронних процесів в охороні здоров'я. Електронна охорона здоров'я (E-health). Електронна система охорони здоров'я (ЕСОЗ) як апаратно-програмна реалізація електронної охорони здоров'я.
6. Призначення ЕСОЗ. Склад ЕСОЗ. Умовна структура ЕСОЗ. Задачі E-health, що вирішуються шляхом залучення ЕСОЗ (наявність достовірної інформації, можливість прогнозування потреб охорони здоров'я, планування ресурсів, надання достовірної інформації в необхідному обсязі всім суб'єктам E-health, впровадження систем підтримки клінічних рішень, залучення пацієнта до піклування про власне здоров'я).
7. Концепції інформатизації охорони здоров'я, тактика орієнтованості на пацієнта. Пріоритетність електронної форми роботи з даними. Принцип одноразового введення та багаторазового використання даних

в інформаційних системах. Комп'ютерні технології з обробки "великих даних" (Big Data). Роль Єдиного медичного інформаційного простору в інтеграційних процесах між системами в рамках E-health, із суміжними галузями та сферами на рівні України та на міждержавному рівні, для подальшої інтеграції з відповідними системами в ЄС. Роль міжнародних технічних стандартів обміну інформацією у формуванні єдиного інформаційного середовища.

8. Сучасні надбання в процесах створення E-health в Україні. Найближчі перспективи процесів створення E-health в Україні (розвиток МІС лікувально-профілактичних закладів, МІС для пацієнтів, інформаційних МІС та реєстрів).

9. Інтегрована електронна медична карта як важлива частина центрального компоненту E-health. П'ять рівнів комп'ютеризації історії хвороби. Переваги використання електронної медичної карти.

10. Електронна медична картка. Електронний персональний медичний запис. Електронний медичний документ. Вміст електронної медичної карти. Інтегрована електронна медична карта. Персональна електронна медична карта. Електронний медичний архів. Інтегрований електронний медичний архів. Персональний електронний медичний архів. Система ведення електронних медичних карт. Структура електронного персонального медичного запису. Життєвий цикл електронних персональних медичних записів.

Розділ 3

ПРАВА ДОСТУПУ ДО ІНФОРМАЦІЇ ТА ЗАХИСТ МЕДИЧНИХ ДАНИХ

3.1. Законодавча база процесів захисту медичної інформації.

Особливістю медичної інформації є її конфіденційність. Права громадян на конфіденційність інформації про факт звернення по медичну допомогу та будь-які відомості, які передаються ними при зверненні по допомогу, регулюються на законодавчому рівні держави, зокрема, Законом України "Про захист персональних даних" (№ 2297-VI від 01.06.2010). Перша стаття Закону в останній чинній редакції від 1 січня 2014 року під назвою "Сфера дії Закону" декларує: "Цей Закон регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних. Цей Закон поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів".

3.2. Захист інформації МІС.

Стратегія впровадження E-health в Україні розуміє під собою, зокрема, повномасштабне використання в системі охорони здоров'я МІС різного призначення. Відомості, якими оперує медична інформаційна система, є персональними даними та можуть становити лікарську таємницю. Крім того, бази даних МІС всіх рівнів містять критично важливу інформацію, від якої, зокрема, може залежати життя людини, тому ключовим фактором при створенні МІС має стати забезпечення цілісності бази даних і можливість стеження за станом системи та її безпекою.

Суттєва складність і специфіка інтегрованих медичних систем обумовлює відповідну складність питань безпеки. Крім того, в медичних системах багато проблем безпеки виглядають специфічно, оскільки при безумовній необхідності дотримання приватності даних, вони мають бути відкритими для статистики, аналізу та проведення різних досліджень. Навіть для строго анонімних даних, їх знеособлене використання третіми особами, взагалі кажучи, не завдає шкоди конкретному пацієнту, а таємницю, у тому числі державну, можуть представляти дані статистики і аналізу лише популяційно значущої вибірки. Водночас обробка та аналіз масивів записів можуть бути надзвичайно корисні як в науковому плані, так і для отримання різного роду прогнозів, оцінок, важливої статистичної інформації, бути вельми продуктивними в плані підвищення кваліфікації лікарів, медичних працівників, а також використовуватися для розробки і тестування нових методик, ліків, обладнання та ін.

3.3. Поняття "інформаційної безпеки" як термін інформаційно-комп'ютерних технологій.

Під інформаційною безпекою (ІБ) зазвичай розуміють захист інтересів суб'єктів інформаційних відносин. ІБ можна визначити як стан захищеності інформаційного середовища суспільства, який забезпечує його (інформаційного середовища) формування, використання та розвиток в інтересах громадян, організацій і держави. Більш конкретно під безпекою інформації розуміється:

1) стан захищеності інформації, яка обробляється засобами обчислювальної техніки або автоматизованої системи, від внутрішніх або зовнішніх загроз;

2) стан інформації, інформаційних ресурсів та інформаційних систем, при якому в рамках деяких несуперечливих правил забезпечується захист інформації (даних) від витоку, розкрадання, втрати, несанкціонованого знищення, викривлення, модифікації (підробки), копіювання та блокування інформації.

Відповідно, захист інформації (інформаційна безпека) – це:

1) діяльність, спрямована на запобігання витоку інформації та її захист від несанкціонованих і ненавмисних дій;

2) комплекс заходів для запобігання витоку, розкраданню, втраті, несанкціонованому знищенню, викривленню, модифікації (підробки), несанкціонованому копіюванню та блокуванню інформації.

Під гарантовано захищеною системою розуміється система, яка доказово задовольняє критеріям прийнятої в організації політики безпеки. ІБ контролюється стандартом ISO / IEC 15408 "Загальні критерії оцінки безпеки інформаційних технологій".

Отже, захист інформації – це забезпечення її безпеки від будь-яких (у тому числі санкціонованих) дій, що тягнуть за собою її несанкціоновану втрату, модифікацію або розкрадання.

Загрози, статистика та характер порушень ІБ, взагалі кажучи, дещо змінюються в часі. Натепер основними факторами порушення ІБ є: витік інформації по технічним каналам – 20 % порушень, людський фактор – 80 % порушень.

Основні типи порушень ІБ:

- розкрадання, модифікація і псування інформації;
- DOS атаки "відмова в обслуговуванні"*;
- інциденти з вірусами, іншими шкідливими програмами, у тому числі через електронну пошту ;
- критичні апаратні відмови, у тому числі "наведені";
- прояви недбалості з боку власних співробітників;
- атаки з боку власних співробітників;

– інші причини (помилки конфігурації, розбіжність стандартів, недотримання життєвого циклу систем та ін.).

Примітка. *Атака на відмову в обслуговуванні, розподілена атака на відмову в обслуговуванні (англ. DoS attack, DDoS attack, (Distributed) Denial-of-service attack) — напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена. Одним із найпоширеніших методів нападу є насичення атакованого комп'ютера або мережевого устаткування великою кількістю зовнішніх запитів (часто безглузвих або неправильно сформульованих). Як наслідок, атаковане устаткування не може відповісти користувачам або відповідає настільки повільно, що стає фактично недоступним.)

Загальний річний збиток від порушень ІБ у світі складає понад 100 млрд \$ (за деякими оцінками до 1 трлн \$ на рік).

3.4. Основні проблеми та напрямки забезпечення інформаційної безпеки.

Інформаційна безпека при функціонуванні МІС забезпечується завдяки взаємопов'язаному комплексному використанню організаційних, програмних і технічних засобів захисту. Основними напрямками можливих порушень інформаційної безпеки (ІБ) є:

- витік даних (порушення конфіденційності);
- втрата даних;
- несанкціонована модифікація даних.

Нарощування вимог з ІБ неминуче накладає обмеження на доступність даних для користувачів МІС. Існує три основних вектори інформаційної безпеки: конфіденційність, цілісність, доступність даних. Забезпечення ІБ має будуватися на компромісі між ними, гарантуючи прийнятний рівень безпеки поряд з прийнятними для роботи користувачів обмеженнями в частині санкціонування використання ресурсів і сервісів МІС.

До будь-якої інформаційної системи, зокрема медичної, ставляться три основні вимоги: система повинна забезпечувати – функціональність, інформаційну безпеку, сумісність. При вирішенні ряду питань ці вимоги повинні розглядатися спільно. На початку свого становлення інформаційно-обчислювальні системи, мережі і технології будувалися значною мірою для забезпечення великих наукових проєктів (функціональність) і, як правило, на основі «відкритої» архітектури. При прийнятті основних рішень мало зверталось уваги на проблеми безпеки. У той же час комп'ютерні системи та мережі увійшли в ділове життя настільки органічно, що порушення в їх роботі впливають на функціонування систем на принциповому рівні. У зв'язку з цим питання забезпечення ІБ в інформаційно-телекомунікаційних і обчислювальних системах набувають першорядного значення. При цьому питання безпеки інформації, пов'язані з тривалим і надійним зберіганням великих масивів даних на машинних носіях і створенням архівів тривалого зберігання, поступово вирішуються з впровадженням нових технологій.

ІБ, якщо розглядати в найзагальнішому сенсі, можна трактувати як термін, що складається з підмножин, або аспектів:

- організаційного;
- політико-правового;
- економічного;
- промислового;
- кримінологічного;
- інформаційного.

3.5. Можливі шляхи захисту інформації в МІС на сучасному етапі розвитку.

Для забезпечення конфіденційності інформації, яка використовується та контролюється МІС, на сучасному етапі розвитку ІБ застосовують такі дії:

- за допомогою комп'ютерного алгоритму присвоюються букви і цифри пароллю; користувач може в будь-який час отримати новий пароль;
- кожен пароль змінюється один раз на шість місяців;
- завідувачі відділеннями видають паролі і визначають рівень поважень;
- всім користувачам повідомляють про те, що пароль прирівнюється до офіційного підпису і що ні за жодних обставин і нікому він не може бути розкритий;
- група обслуговування інформаційної системи видає паролі завідувачам відділень і контролює їх використання;
- доступ до даних може обмежуватися як паролем, так і місцем знаходження терміналу;
- користувачі автоматично відключаються від системи при зупинці роботи терміналу більш ніж на 5 хв;
- комп'ютерна система зберігає в пам'яті кожен випадок доступу до інформації про пацієнтів з фіксацією особистості, професійної належності, місця, типу отриманої інформації, дати і часу;
- кожен співробітник, який використовує МІС, має можливість побачити на дисплеї імена всіх осіб, які переглядали певну персональну електронну медичну картку;
- пацієнт може запитати список осіб, які переглядали його медичну картку;
- термінали блокуються в разі введення нелегального пароля кілька разів;
- термінали автоматично виводять на екран попередження, якщо користувач переглядає картку знаменитостей, співробітників лікарні та їхніх родичів;
- термінали за випадковим принципом виводять на дисплей попередження про конфіденційність відомостей приблизно на кожен 500-й запит відомостей про пацієнта;

– для доступу з домашнього телефону потрібен другий пароль на базі вбудованого в систему, специфічний по відношенню до пацієнта, наприклад, дівоче прізвище матері.

Впізнання користувача на основі пароля – приклад так званої однокфакторної ідентифікації.

3.5.1. Апаратні методи ідентифікації.

Сучасні методи ідентифікації ґрунтуються на множинних факторах (існує і широко застосовується двофакторна і навіть трифакторна ідентифікації). Наприклад, двофакторна ідентифікація користувача проводиться не тільки на основі того, що користувач знає пароль (password), але і того, що він має персональний ідентифікатор (login). Як такий ідентифікатор може використовуватися апаратний токен (від англ. *Token* – розпізнавальний знак), смарт-карта та ін.

Апаратні токени для ідентифікації користувачів можуть бути автономними або такими, що підключаються, або USB-токенами.

Автономні токени – це мобільні персональні пристрої, що не під'єднуються до комп'ютера і мають власне джерело живлення. Вони дозволяють користувачеві ідентифікувати себе на серверах, використовуючи або одноразовий пароль (токени з використанням OTP – англ. One-Time Password), або метод запит–відповідь. Суть методу запит–відповідь полягає в наступному:

- користувач вводить свій ідентифікатор на робочій станції, яка передає його по мережі сервера;

- сервер аутентифікації генерує випадковий запит, який по мережі передається користувачеві;

- користувач вводить запит в ідентифікаційний токен;

- токен користувача за допомогою якогось алгоритму і секретного ключа користувача зашифровує цей запит і результат відображає на своєму екрані;

- користувач вводить результат на робочій станції, яка повертає його серверу;

- сервер зашифровує те саме випадкове число (запит);

- при збігу результатів процес запит/відповідь в існуючій системі аутентифікації успішно завершується.

USB-токени – пристрої, оформлені у вигляді флеш-карти, які підключаються до стандартних портів USB і містять мікроконтролер і/або мікросхему – електронний чіп. Вони дозволяють здійснювати сувору двофакторну ідентифікацію користувача, а також забезпечують функції шифрування і формування електронного цифрового підпису користувача. На відміну від OTP-токенів вони не потребують додаткового програмного забезпечення, що встановлюється на сервері.

Смарт-карти (англ. *SmartCard* – інтелектуальна карта) являють собою пластикові картки розміром з кредитку (рис. 3.1), що містять чіп

(мікропроцесор) для криптографічних обчислень (електронно-цифровий підпис, шифрування) і вбудовану захищену пам'ять для зберігання інформації (дані про користувача, криптографічні ключі, сертифікати та ін.). Для використання смарт-карт необхідний зчитувач (карт-рідер).



Рис. 3.1. Смарт-карти лікаря і пацієнта, що використовуються в системі охорони здоров'я Німеччини

За методом зчитування інформації смарт-карти діляться на такі:

- контактні;
- безконтактні;
- зі здвоєним інтерфейсом.

Контактні карти взаємодіють із зчитувальним пристроєм (зчитувачем) (рис. 3.2) за допомогою безпосереднього зіткнення металеві контактною площадки карти і контактів зчитувача. Цей метод зчитування є простим у реалізації, але підвищує знос карти при частому використанні.



Рис. 3.2. Контактні зчитувальні пристрої для смарт-карт, що підключаються через порт USB (зліва) або у відповідний слот ноутбука (праворуч)

Безконтактні картки мають вбудовану котушку індуктивності, яка в електромагнітному полі зчитувача забезпечує живленням мікросхему, яка видає інформаційні радіосигнали. Такий метод зчитування дозволяє часто використовувати карту без зносу карти пам'яті та зчитувача.

Карти зі здвоєним інтерфейсом мають одночасно і контактну площадку, і вбудовану котушку індуктивності. Такі карти дозволяють здійснювати роботу з різними типами зчитувачів. Смарт-карти можуть бути альтернативою захисту паролем, проте частіше доповнюють його, забезпечуючи більш повну (дво- або тривірневу) ідентифікацію користувача.

Іншим, досить простим способом ідентифікації користувача, є штрих-код. Ця досить ефективна, але одночасно дешева технологія. Використовується, наприклад, в бібліотечних інформаційних системах (штрих-код є одним з реквізитів читацького квитка) та в касових терміналах (штрих-код нанесений на бейджик касира і виконує роль його додаткового ідентифікатора). У медичних інформаційних системах штрих-код може наноситися на амбулаторну карту пацієнта і бути аналогом її номеру.

Для ідентифікації користувачів широкого розповсюдження набули пристрої iButton. Кожен пристрій укладено в сталевий герметичний циліндричний корпус MicroCap, має унікальний номер (ID) і витримує серйозні механічні та температурні навантаження.

Обмін даними з iButton проводиться через однопровідний інтерфейс 1-Wire. Інформація в цьому інтерфейсі передається по єдиному провіднику. Живлення iButton отримує з цього ж провідника, заряджаючи внутрішній конденсатор в моменти, коли на шині немає обміну даними. Швидкість обміну достатня для забезпечення передачі даних в момент торкання контактного пристрою.

Для підключення iButton до комп'ютера випускаються зчитувачі (адаптери), що перетворюють сигнали стандартних портів комп'ютера на сигнали 1-Wire (рис. 3.3). Брелок для ключів дозволяє надійно закріпити "таблетку" iButton.



Рис. 3.3. iButton – сімейство мікроелектронних пристроїв, розроблених фірмою Dallas Semiconductor (USA)

Разом з тим ідентифікаційні процедури не дозволяють однозначно визначити, що логін, пароль і/або будь-який додатковий пристрій пред'являються саме їх власником. Як теоретично, так і практично вони можуть

бути передані іншій людині або викрадені нею. З огляду на це значно більш надійною є ідентифікація за біологічними параметрами, що є незмінними характеристиками людини протягом усього життя.

Біометричні системи ідентифікації, доступні в цей час або такі, що знаходяться в стадії розробки, включають системи доступу за відбитком пальця, формою вуха, геометрією обличчя, температурою шкіри обличчя, клавіатурним почерком, відбитком долоні, малюнком вен долоні, структурою сітківки ока, малюнком райдужної оболонки ока, підписом і голосом.

Використання ідентифікації за відбитками пальців у майбутньому буде використовуватися найбільш широко. Її перевагою є швидкість і простота використання, зручність і надійність. Імовірність помилки при ідентифікації користувача набагато менше порівняно з іншими біометричними методами. Крім того, сам пристрій ідентифікації є досить компактним (рис. 3.4).

Ідентифікація за геометрією руки застосовується сьогодні в США в більш ніж 8 000 організацій, включаючи Колумбійський законодавчий орган, Міжнародний аеропорт Сан-Франциско, лікарні та імміграційні служби. Її переваги можна порівняти з ідентифікацією за відбитком пальця, хоча пристрій займає більше місця. Найбільш вдалий пристрій, Handkey, сканує як внутрішню, так і бічну сторони руки.



Рис. 3.4. *Сканери BioLink, які дозволяють виробляти біометричну аутентифікацію за відбитком пальця (зліва) і комбіновану, що доповнює використання смарт-карт (праворуч)*

Для зчитування інформації користувач (рис. 3.5) кладе долоню на панель пристрою, де спеціальні фіксатори допомагають скоригувати її розташування. Тривимірне зображення кисті руки фіксується спеціальною телекамерою з інфрачервоним підсвічуванням. Інформацію про товщину

кисті пристрій отримує за допомогою бічних дзеркал, які потрапляють в огляд телекамери. Відскановане зображення порівнюється з шаблоном, що зберігається в пам'яті зчитувача. За результатами порівняння зчитувач ідентифікує користувача.

Процедура ідентифікації особистості за допомогою біометричного зчитувача HandKey II проводиться у два етапи. Спочатку на клавіатурі співробітник набирає свій унікальний ідентифікаційний номер, а потім зчитувач сканує кисті руки і порівнює отриману інформацію з шаблоном. Крім того, замість набору PIN-коду в HandKey II передбачено підключення зчитувача електронних карт доступу, що використовують протоколи Proximity, Wiegand та ін.

Двоетапна процедура ідентифікації користувача, з одного боку, істотно підвищує рівень безпеки, а з іншого – дозволяє практично миттєво здійснити зіставлення з шаблоном з бази даних. Набираючи свій PIN-код (або використовуючи карту доступу), людина заздалегідь "повідомляє" зчитувача, з яким саме шаблоном необхідно порівняти отримані дані. Час верифікації не перевищує 1 с, а загальний час ідентифікації в системі становить 1–5 с.



Рис. 3.5. Ідентифікація особистості за допомогою біометричного зчитувача HandKey II

Перевага сканування райдужної оболонки полягає в тому, що зразок плям на райдужній оболонці знаходиться на поверхні ока, і від користувача не потрібно спеціальних зусиль – фактично відеозображення ока може бути відскановано на відстані метра, що робить можливим використання таких сканерів у банкоматах (рис. 3.6). Катаракта – помутніння кришталика ока – жодним чином не впливає на процес сканування райдужної оболонки.



Рис. 3.6. Ручний (зліва) і стаціонарний (праворуч) сканери райдужної оболонки ока

Результати досліджень розробника технології – компанії Iridian Technologies показали, що при надзвичайно великій базі реєстрацій (близько мільярда) ймовірність помилкового розпізнавання людини була нижче 0,000001, а ймовірність помилкової відмови в розпізнаванні – нижче 0,003.

Процес ідентифікації особистості відбувається наступним чином. У системі формується знімок райдужної оболонки в інфрачервоному світлі (700–900 нм), який потім перетворюється на 512-байтний код (IrisCode), що описує структуру оболонки. Отриманий IrisCode перевіряється на відповідність усім IrisCode, що знаходяться в базі даних, і за результатами порівняння відбувається або ідентифікація особистості, або відмова в доступі користувачеві.

Сканування сітківки відбувається з використанням інфрачервоного світла низької інтенсивності, спрямованого через зіницю до кровоносних судин на задній стінці ока. Сканери для сітківки ока набули значного поширення в надсекретних системах контролю доступу, оскільки ці коди ідентифікації характеризуються одним з найнижчих відсотків відмови в доступі зареєстрованим користувачам і майже нульовим відсотком помилкового доступу. Однак сканування сітківки є потенційно більш небезпечним, оскільки проводиться спеціальним лазерним променем. Крім того, при скануванні сітківки очі мають знаходитися на відстані не більше 1,5 см від пристрою, що зчитує, а погляд необхідно фіксувати на певній точці та зберігати нерухомим під час сканування.

Ідентифікація за рисами обличчя (за геометрією обличчя) – один з напрямків у біометричній індустрії, що розвиваються найбільш активно. На сьогодні існує дві таких біометричних технології. В основі першої лежить спеціальне програмне забезпечення, яке отримує зображення зі звичайної веб-камери та обробляє його. На обличчі виділяються окремі об'єкти

(брови, очі, ніс, губи), для кожного з яких обчислюються параметри, які повністю його визначають. При цьому багато сучасних систем будують тривимірний образ обличчя людини. Це потрібно для того, щоб уможливити ідентифікацію, наприклад, при нахилі і повороті голови, зміні виразу обличчя або макіяжі у жінок.

Інша технологія заснована на ідентифікації людини за її обличчям із використанням термограми. Фотографія користувача, зроблена за допомогою спеціальної інфрачервоної камери, дозволяє отримати "карту" розташування артерій, яка у кожної людини різна. Навіть у однайцевих близнюків артерії розташовані по-різному. Завдяки цьому надійність методу досить висока. Проте цей метод з'явився недавно і поки не набув широкого використання.

3.5.2. Криптографічний метод захисту.

Серед базових технологій безпеки, можна виділити криптографію (від грец. *Κρυπτός* – прихований і *γράφω* – пишу) – наука про методи забезпечення конфіденційності і автентичності інформації.

Багато служб інформаційної безпеки, такі як контроль входу в систему, розмежування доступу до ресурсів, гарантування безпечного зберігання даних і ряд інших, спираються на використання криптографічних алгоритмів.

Шифрування – процес перетворення повідомлення з відкритого тексту на шифротекст таким чином, щоб:

- його могли прочитати лише ті сторони, для яких він призначений;
- була можливість перевірити справжність відправника (ідентифікація);

- були гарантії, що відправник дійсно надіслав дане повідомлення.

В алгоритмах шифрування передбачається наявність ключа. Ключ – це певний параметр, що не залежить від відкритого тексту.

Існують два види криптографічних систем:

- системи з секретним ключем (симетричні);
- системи з відкритим ключем (асиметричні).

Як випливає з назви, симетричні системи використовують один і той же ключ для проведення операцій шифрування і розшифровки, а несиметричні системи – різні. У симетричних систем обидві сторони, що обмінюються інформацією, повинні мати цей загальний для них ключ, але ніхто інший цим ключем володіти не повинен. Тим самим забезпечується таємність переданої інформації.

Асиметричне шифрування з відкритим ключем базується на наступних принципах (рис. 3.7):

- Можна згенерувати пару дуже великих чисел (відкритий ключ і закритий ключ) так, щоб, знаючи відкритий ключ, не можна було вирахувати закритий ключ за розумний термін. При цьому механізм генерації є загальновідомим.

➤ Є надійні методи шифрування, що дозволяють зашифрувати повідомлення відкритим ключем так, щоб розшифрувати його можна було тільки закритим ключем. Механізм шифрування є загальновідомим.

➤ Власник двох ключів нікому не повідомляє закритий ключ, але передає відкритий ключ контрагентам або робить його загальновідомим.

➤ Якщо необхідно передати зашифроване повідомлення власнику ключів, то відправник повинен отримати відкритий ключ. Відправник шифрує своє повідомлення відкритим ключем одержувача і передає його одержувачу (власнику ключів) по відкритих каналах. При цьому розшифрувати повідомлення не може ніхто, крім власника закритого ключа.

У результаті можна забезпечити надійне шифрування повідомлень, зберігаючи ключ розшифровки секретним для всіх – навіть для відправників повідомлень.



Рис. 3.7. *Схема асиметричного шифрування з відкритим ключем*

Користувач повинен тримати свій закритий ключ у секреті від сторонніх. Закритий ключ зазвичай зберігається на будь-якому знімному носії (флеш-карті, смарт-карті) в зашифрованому вигляді і розшифровується тільки на час якихось дій. Криптографічні операції часто виконуються всередині такого пристрою, видаючи на вихід тільки результат, але не розкриваючи вмісту закритого ключа. Закритий ключ, що зберігається на смарт-карті, може бути захищений паролем.

Найбільш популярними алгоритмами шифрування з секретним ключем є DES, TripleDES і ряд інших.

Несиметричні системи дозволяють створювати цифровий підпис, який будучи поставленим на цифровому документі, є гарантією того, що саме власник цього ключа, а не хтось інший дійсно підписав цей доку-

мент. Для цього користувач-відправник, використовуючи свій закритий ключ, виробляє над даними, які він має намір підписати, деяку операцію і передає її результат разом з вихідними даними будь-якого іншого суб'єкта – одержувача підписаного електронного документа. Цей суб'єкт, використовуючи тільки відкритий ключ відправника, парний закритому, може перевірити, що цифровий підпис є вірним, тобто відповідає відправникові. Під час такої перевірки встановлюється відповідність електронного документа його відкритому ключу, тобто справжність електронного підпису (належність підпису його власнику), а також встановлюється наявність або відсутність спотворень електронного документа після його електронного підписання (умисне або викликане помилками при його передачі по каналах зв'язку).

Перевірка виконується за допомогою хешування – обчислення контрольної суми біт електронного документа. Побутовим аналогом хешування може служити прийом, коли при переїздах у пам'яті тримають кількість місць багажу. Тоді для перевірки не потрібно згадувати про кожну валізу, а досить їх порахувати. Збіг буде означати, що жодну валізу не втрачено. Тобто, кількість місць багажу є його хеш-кодом. Будь-яка зміна підписаних даних (навіть зміна всього одного біта у великому файлі) веде до зміни їх хеш-коду і робить електронний цифровий підпис недійсним.

Гарантією відповідності відкритого ключа його власнику є сертифікат, що формується і видається членам системи захищеного документообігу, котрі засвідчуються Центром системи. Цей цифровий сертифікат є певним конгломератом з відкритого ключа користувача, інформації про нього, імені сертифіката і цифрового підпису Центру, який скріплює всі ці дані один з одним. При цьому сертифікат має термін дії, який обмежує термін відповідності відкритого ключа його власникові.

Електронно-цифровий підпис в електронному документі стає рівнозначним власноручного підпису за таких умов (одночасно):

- 1) сертифікат ключа електронно-цифрового підпису не втратив силу;
- 2) підтверджена автентичність електронно-цифрового підпису в електронному документі;
- 3) електронно-цифровий підпис використовується у відносинах, що мають юридичне значення.

Електронне повідомлення, підписане електронним цифровим підписом, визнається електронним документом, рівнозначним документам, які підписані власноручним підписом, у випадках, коли законодавчими актами держави не встановлено вимогу про складання такого документа на паперовому носії.

Використання електронних документів набуло широкого розповсюдження в багатьох сферах діяльності, причому вони застосовуються не тільки поряд з традиційними паперовими документами, а й замість них.

У сучасних медичних інформаційних системах електронний цифровий підпис може застосовуватися з кількома цілями:

- Персоніфікація даних, що накопичуються в інформаційній системі, що дозволяє однозначно визначити автора запису.
- Зберігання в інформаційній системі закінчених документів, коли після підписання документа за допомогою електронного цифрового підпису неможливим є подальше редагування документа. Це надає документу юридичний статус і обґрунтовано дозволяє відмовитися від еквівалентного паперового документа.

Питання для самоконтролю

1. Закон України "Про захист персональних даних". Сфера дії Закону.

2. МІС як складова E-health. Проблеми лікарської таємниці при розробці МІС. Проблеми цілісності бази даних при розробці МІС. Специфічність проблем безпеки медичних інформаційних систем: відкритість даних для статистики, аналізу та проведення різних досліджень на тлі дотримання приватності даних.

3. Основні напрямки порушень інформаційної безпеки (ІБ) в МІС (витік, втрата, несанкціонована модифікація даних). Основні вектори інформаційної безпеки (конфіденційність, цілісність, доступність даних). Загальні вимоги до МІС (функціональність, інформаційна безпека, сумісність та суперечливість між ними).

4. Визначення інформаційної безпеки. Основні категорії безпеки інформації. Визначення захисту інформації (інформаційної безпеки). Стандарти інформаційної безпеки. Загрози, статистика та характер порушень ІБ. Основні типи порушень ІБ.

5. Дії для забезпечення конфіденційності інформації на сучасному етапі розвитку ІБ (цифрові паролі та їх підтримка і таємниця; обмеження доступу до даних паролем та місцем знаходженням терміналу; автоматичне відключення від системи; фіксація всіх епізодів доступу до персональних даних; можливість блокування терміналів; інформаційні повідомлення тощо).

6. Двофакторна ідентифікація. Апаратні токени. Метод запит-відповідь. USB-токени. Смарт-карти. Типи смарт-карт. Штрих-код як засіб ідентифікації. Пристрої iButton. Біометричні системи ідентифікації (за відбитком пальця, формою вуха, геометрією обличчя, температурою шкіри обличчя, клавіатурним почерком, відбитком долоні, малюнком вен долоні, структурою сітківки ока, малюнком райдужної оболонки ока, підписом і голосом).

7. Криптографія як наука. Шифрування. Види криптографічних систем (симетричні та асиметричні). Електронно-цифровий підпис. Використання цифрового підпису в МІС.

Розділ 4

ПРОЦЕСИ ПРИЙНЯТТЯ РІШЕНЬ В МЕДИЦИНІ.

ОЦІНКА ЕФЕКТИВНОСТІ ДІАГНОСТИЧНОГО ТЕСТУ

4.1. Теорія прийняття рішень як наука. Прийняття рішень в медицині.

Теорія прийняття рішень – міждисциплінарна галузь дослідження, що становить інтерес для практиків і пов'язана з математикою, статистикою, економікою, філософією, менеджментом і психологією; вивчає, як реальні особи, які приймають рішення, вибирають рішення і наскільки оптимальні рішення можуть бути прийняті.

Протягом усього життя (приватного, соціального, професійного) перед людиною постає вибір найкращого варіанту поведінки серед усіх можливостей з урахуванням ситуації. Чим менш структурованою є проблема, тим більш проблемним є пошук оптимального вибору серед множини обставин.

Прийняття медичних рішень належить до одного з найбільш складних напрямків людської діяльності з огляду на проблему прийняття професійних рішень.

Лікар стикається із проблемою прийняття рішень на кожному етапі своєї діяльності: збір інформації про хворого, діагностика, вибір тактики лікування. Математика як наука є основним інструментом у процесі пошуку істини і, отже, в процесі прийняття рішень.

Медицина являє собою слабоструктуровану галузь знання, що створює серйозні труднощі для процесу прийняття рішень. В одних випадках, що характеризуються класичними проявами хвороби, гіпотеза або навіть остаточне рішення виникає вже в процесі огляду, в інших – тільки після спеціального обстеження. При цьому послідовність діагностичних досліджень може піддаватися корекції, а іноді й докорінній трансформації, залежно від одержуваних у процесі обстеження результатів. Швидкість прийняття рішення залежить як від кваліфікації та діагностичного "чуття" лікаря, так і від особливостей прояву захворювання у конкретного хворого.

4.2. Елементи теорії прийняття рішень.

Прийняти рішення означає здійснити вибір із деякого набору альтернатив. Основними етапами цього процесу є:

- 1) визначення мети;
- 2) формування множини альтернатив (визначення безлічі допустимих рішень);
- 3) формування оцінки, що дозволяє порівнювати альтернативи (задача оцінювання);
- 4) вибір найкращого рішення з безлічі допустимих рішень (завдання оптимізації).

Прийняття рішень, по суті, є ні що інше, як вибір. Варіанти вибору прийнято називати альтернативами.

Наслідком прийняття рішення є подія (результат), можливість появи якої продиктована цим рішенням.

Система переваг – правила, критерії, за допомогою яких порівнюються альтернативи і приймаються рішення.

Рішення – це сукупність тих альтернатив, що задовольняють правилам, які містяться в системі переваг.

Загальну задачу прийняття рішень (завдання вибору), можна сформулювати наступним чином.

Нехай X – множина альтернатив (рішення), Y – множина наслідків (фіналів, результатів). Передбачається існування причинного зв'язку між вибором деякої альтернативи і настанням відповідного результату. Крім того, передбачається наявність механізму оцінки якості вибору – зазвичай шляхом оцінювання якості результату. Потрібно вибрати найкращу альтернативу, для якої відповідний результат має найкращу оцінку якості.

Виходячи зі зв'язків між рішеннями і результатами прийнята наступна класифікація задач прийняття рішень.

Детермінована задача прийняття рішень. Їй відповідає найбільш простий вид зв'язку – детермінований, коли кожна альтернатива приводить до єдиного результату. У цьому випадку існує функціональна залежність між альтернативою x_i і результатом y_i .

У разі, коли кожній альтернативі відповідає не єдиний результат, тобто зв'язок є *недетермінованим*, то задачі прийняття рішень розпадаються на два підкласи:

а) задача прийняття рішень в умовах ризику;

б) задача прийняття рішень в умовах стохастичної (імовірнісної) невизначеності.

У випадку (а), на відміну від випадку (б), для кожної альтернативи x_i відповідає функція щільності ймовірностей на множині результатів Y (кажуть, що з кожним x_i пов'язана деяка лотерея).

В умовах стохастичної невизначеності (випадок б) недетермінованого зв'язку альтернативи та результату виникають два типи задач:

1) прийняття рішень в умовах пасивної взаємодії особи, що приймає рішення (ОПР), та зовнішнього середовища, тобто зовнішнє середовище веде себе пасивно щодо ОПР;

2) прийняття рішень в умовах конфлікту (гри); у цій ситуації зовнішнє середовище поводить себе активно щодо ОПР, що проявляється діями іншої особи.

Під ОПР (особою, що приймає рішення) розуміється людина, яка задає пріоритети та в інтересах якої приймаються рішення. Як правило, ОПР (наприклад, лікар) прагне прийняти найкраще (оптимальне) з його точки зору рішення. Вибір рішення залежить від інформації, якою володіє

ОПР в цій предметній галузі, а також від того, як він встановлює пріоритети, тобто стилу мислення і стратегії поведінки. Наприклад, один людина ризикувати, інший – надмірно обережний, третій віддає перевагу «золотій середині» тощо. Таким чином, ОПР має деяку свободу вибору, однак, якщо вона не буде враховувати особливостей рішень проблеми, то прийняте рішення може значно розходитися з реальністю і привести до негативних наслідків.

4.4. Прийняття діагностичних рішень у медицині. Ефективність діагностичного дослідження.

Одним з найбільш типових для лікаря напрямком прийняття рішень є діагностика. Для її проведення використовуються різні діагностичні дослідження (тести). Під ефективністю діагностичного дослідження розуміють насамперед можливість тесту розділяти обстежених на осіб із хворобою і здорових. Мова йде, звичайно, не тільки про діагностику, а також про диференційну діагностику та виявлення непатологічних станів, тому ефективність тесту слід визначати як можливість з його допомогою провести розподіл за певними групами людей, які перебувають у різному стані.

Для порівняльної оцінки ефективності діагностичного тесту з референтним (еталонним) застосовано ряд показників. Останнім часом все більше дослідників віддають перевагу альтернативним оцінкам, які розподіляють групу, що вивчається, на дві частини: хворі, у яких наявна ця ознака, та ті, у кого її немає. Найпростішим прикладом є поділ людей на хворих та здорових.

У подальшому викладенні використовується ця класифікація, хоч зрозуміло, що її мета може бути різною та часто значно складнішою.

Як числові характеристики тесту при альтернативному методі дослідження використовують операційні характеристики: чутливість та специфічність.

Чутливість (sensitivity, Se) – це частка людей в обстеженій популяції, які дійсно хворіють та які за результатами тесту виявляються як хворі. Чутливість – це міра ймовірності того, що будь-який випадок хвороби (стану) буде ідентифікований за допомогою тесту. У клініці тест з високою чутливістю корисний для виключення діагнозу, якщо результат негативний.

Специфічність (specificity, Sp) – це частка тих, у кого тест негативний, серед всіх людей, які не мають хвороби (стану). Це міра ймовірності правильної ідентифікації людей, які не мають хвороби, за допомогою тесту. У клініці тест з високою специфічністю корисний для включення діагнозу в число можливих у разі позитивного результату (табл. 4.1).

Таблиця 4.1

Операційні характеристики діагностичного тесту

Дані тесту, що вивчається	Референтні дані	
	Істинно хворі (+) P	Істинно здорові (-) N
Визнані хворими за даними тесту (+)	A Істиннопозитивні (хворий референтно і згідно з тестом)	B Хибнопозитивні (здоровий референтно, але згідно з тестом хворий)
Визнані здоровими за даними тесту (-)	C Хибнонегативні (хворий референтно, але згідно з тестом здоровий)	D Істиннонегативні (здоровий референтно і згідно з тестом)
Характеристика тесту	Чутливість $Se = A/(A+C)$	Специфічність $Sp = D/(B+D)$

Як правило, діагностичному висновкові не властива абсолютна діагностична ефективність, тобто він безпомилково поділяє здорових та хворих. Помилки діагностичних досліджень можна віднести до двох типів:

I – хибнопозитивне рішення (людину визнають здоровою, але за результатами тесту вона виявляється хворою);

II – хибнонегативне (хворий за результатами тесту визнається здоровим).

Чутливість та специфічність методу залежать від суб'єктивного фактора, тобто від підходу конкретного лікаря до оцінки результату. При суворому підході до встановлення діагнозу, або певній "оптимістичності", лікар виявляє захворювання не у всіх хворих, тобто у його руках з таким підходом до вибору точки поділу на інтервалі "норма–патологія" метод має низьку чутливість (помилка II роду).

Проте при цьому не виключено, що здорові будуть помилково класифіковані, як хворі, тобто високими є специфічність та ймовірність помилки I роду. Теоретично неможливо віддати перевагу помилкам I або II роду.

Звичайно вважається, що хибнопозитивний результат не такий небезпечний, як хибнонегативний.

4.5. Апарат характеристичних кривих як інструмент, для оцінки якості медичних діагностичних технологій.

Як встановити межу розподілу, враховуючи «шкоду» від можливих хибних рішень? Для цього використовують апарат характеристичних кривих (ROC-curve receiver operating characteristic curve), тобто кривих взаємної залежності хибнопозитивних та позитивних результатів, у термінах їхньої ймовірності при зміні точки розподілу.

Відомо, що ідеальний діагностичний тест має цілком безпомилково відрізнити людей з хворобою, яка вивчається, та без неї. Реальні ж тести дають помилки як I та II роду.

Для прикладу оцінимо якість деякого тесту, спираючись на відомі дані референтного методу діагностики.

Припустимо, що за такими даними, отриманими для групи G з 73 чоловік, визнані здоровими 36 осіб, а хворими на дане захворювання А – 37. Запропоновано оцінити інший тест для діагностики цього ж захворювання А на підставі вивчення деякої ознаки S (симптому, результату вимірювання, рентгенівської ознаки та ін.). Припустимо, що дана ознака має кількісне вираження і воно може бути 1, 2 ... 20. Після застосування тесту S у групі G отримано результати, наведені гістограмами розподілу результатів у здорових та хворих людей (рис. 4.1).

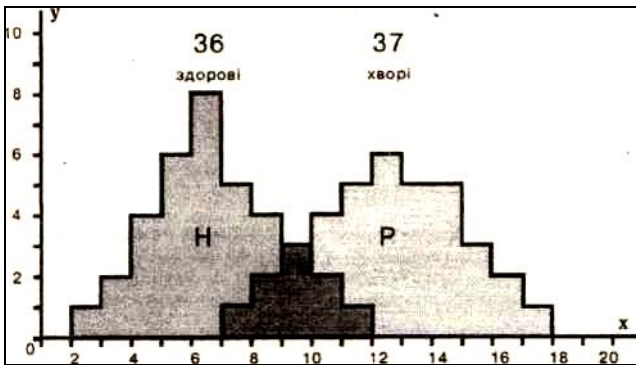


Рис. 4.1. Гістограми розподілу результатів застосування тесту F у групі G:
H – здорові обстежені, P – хворі.

По осі x – значення ознаки, по осі y – кількість людей

З гістограм видно, що значення ознаки S, яке дорівнює 2, виявлено у особи, референтно здорової, значення ознаки S, що дорівнює 2 – у 2 пацієнтів, і вони здорові і т. п. – до значення ознаки, що дорівнює 7 і яке мають 5 істинно здорових та 1 істинно хворий.

Віднесемо себе до групи перестраховальників, які віддають перевагу помилці I роду, і оберемо за точку розподілу значення ознаки, що дорівнює 7, тобто вважатимемо хворими усіх, у кого ознака S перевищує або дорівнює 7. При цьому частину здорових пацієнтів буде свідомо віднесено до хворих.

Як зміниться картина, якщо за точку розподілу взяти значення ознаки, наприклад, 8? Яку з точок розподілу слід вважати найбільш оптимальною?

Щоб відповісти на ці питання, побудуємо відповідну ROC-криву як залежність хибнопозитивних (абсциса) та істиннопозитивних (ордината) результатів. Для цього розглянемо ділянку перехрещення гістограм (H) та (P), тобто значення ознаки, які мають як істинно хворі, так і істинно здорові (див. рис. 4.1).

Для значення ознаки, що дорівнює 7 (рис. 4.2), отримуюмо першу точку ROC-кривої P7 (X_1, Y_1), де $X_1=15/36$ (15 чоловік з числа здорових (36) помилково віднесені до хворих (хибнопозитивний результат), а $Y_1=37/37$ (усі 37 хворих визнані хворими).

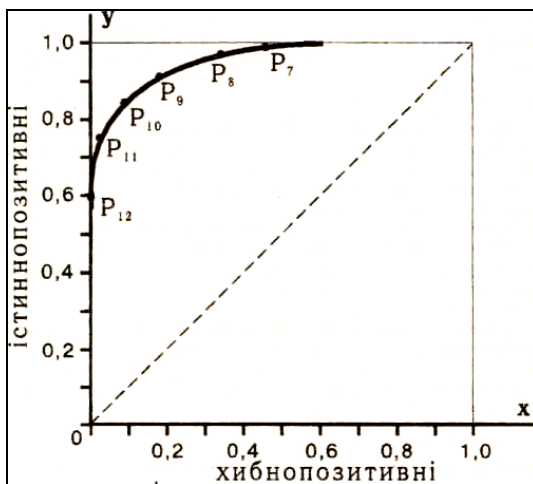


Рис. 4.2. Графік ROC-кривої

Другу точку ROC-кривої P8 (X_2, Y_2) отримаємо для значення ознаки, що дорівнює 8:

$X_2 = 10/36$ (значення більше або що дорівнює 8 зафіксовано у 10 здорових осіб),

$Y_2 = 36/37$ та ін.

Для значення ознаки, що знаходиться в діапазоні значень від 7 до 12 отримуюмо (табл. 4.2) дані для побудови ROC-кривої, яку наведено на рис. 4.2.

Таблиця 4.2.

Таблиця даних для побудови ROC-кривої

Значення ознаки	7	8	9	10	11	12
Точка	P7	P8	P9	P10	P11	P12
X	0,417	0,278	0,167	0,083	0,028	0
Y	1	0,973	0,919	0,838	0,729	0,595

Залежно від форми розподілу H та P і ступеня їх накладання ця крива має різні форми та положення. Чим менший її вигин і чим ближче вона розташована до бісектриси 1-го квадранта координатної площини, тим менша ефективність діагностичного дослідження. Точки на бісектрисі відповідають відсутності діагностичної значущості тесту (при переміщен-

ні точки поділу не відбувається змін пропорцій між хибно- та істинно-позитивними результатами).

Головною позитивною якістю ROC-кривої є спільний опис "показань" та "похибок" у процедурі встановлення діагнозу. Оскільки існує можливість зважити з певним наближенням "користь" та "шкоду" вірних і хибних рішень, у певних випадках виникає можливість обрати на кривій точку, котра відповідає максимуму «користі» та мінімуму «шкоди».

Зазначимо, що в літературі поряд з показниками чутливості та специфічності (%) використовуються протилежні їм – нечутливості і неспецифічності, що обчислюються як доданок до одиниці:

– нечутливість = $1 - Se$;

– неспецифічність = $1 - Sp$.

Звернемо увагу на те, що в наукових статтях поряд з термінами "чутливість" і "специфічність" використовуються їх прямі смислові аналоги:

– істиннопозитивна частка (True Positive Fraction) = чутливість (sensitivity);

– істиннонегативна частка (True Negative Fraction) = специфічність (specificity).

ROC-аналіз виявився достатньо дієвим і у випадку інтерпретації результатів не на якісному, а на кількісному рівні, коли використовується градація результатів типу: "безперечно патологія", "майже напевно патологія", "певно патологія", "суміжний випадок", "певно норма", "майже певно норма", "безперечно норма". На графіку ROC-кривої в термінах "не специфічність" (абсциса), "чутливість" (ордината) позиціонування подібних проміжків виглядає, наприклад, як на *рис. 4.3*.

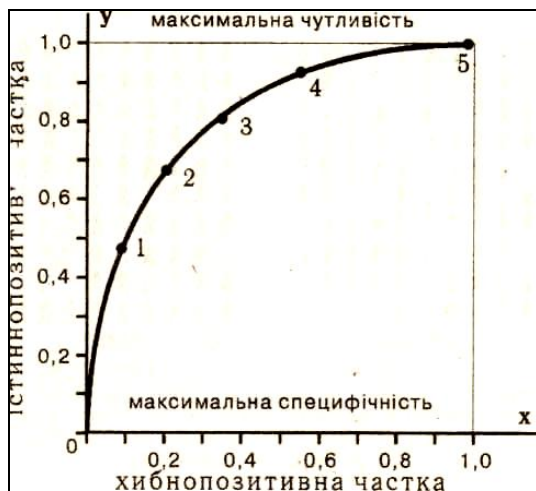


Рис. 4.5.3. Будова ROC-кривої. Рух вправо відповідає зростанню чутливості і зниженню специфічності, вліво – навпаки

Тут рух ROC-кривою вправо відповідає використанню найсуворішого діагностичного критерію. Верхній правий кут, що відповідає 100 % чутливості і 0 % специфічності, позначає ситуацію, коли згідно з тестом всі результати оголошуються патологією, а нижній лівий кут (чутливість – 0 %, специфічність – 100 %) – нормою.

Таким чином, ROC-крива абсолютно досконалого тесту виглядає як крива А, результат випадкових угадувань – крива С, а найбільш типова – як крива В (рис. 4.4).

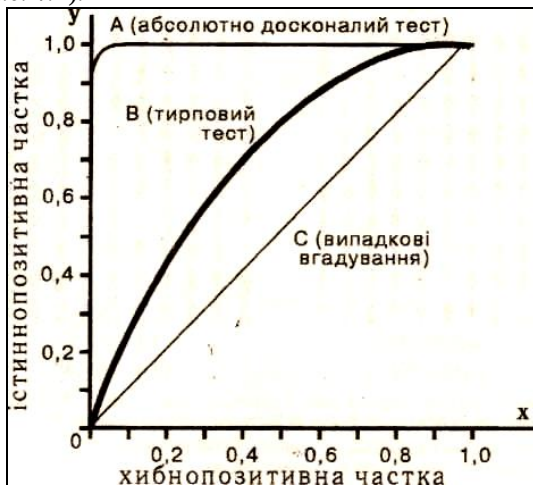


Рис. 4.4. Вигляд ROC-кривої залежно від якості тесту:

А – абсолютно досконалий тест; В – типовий тест; С – випадкові вгадування

Ілюстрацією до викладеного вище може бути праця David I. Vining, Gregory W. Cladish, у якій аналізується питання вибору інтервалів градації для оцінки результатів талійного стрес-тесту (Thallium stress Test), застосовуваного для діагностики захворювань серця. Зокрема, при використанні простого критерію типу "якщо дефект міжшлуночкової перегородки більше 50 %, то результат – патологія, якщо менше – норма", після тестування отримаємо чутливість 84 % та специфічність 94 %. Це означає, що 84 % хворих будуть визнані за результатами тесту хворими та у 94 % здорових підтвердиться відсутність хвороби. Тобто при такому підході до оцінки результатів тест виявляється недостатньо адекватним.

Ситуація змінюється докорінно, якщо в тесті, що розглядається, застосувати таку градацію: "безперечно патологія" – якщо дефект більше 50 %; "певно патологія" – дефект перегородки – 30–50 %; "пограничний стан" – дефект 10–30 %; "певно норма" – 1–10 %; "безперечно норма" – 0 %.

Оцінити придатність тесту допомагає апарат ROC-кривих. Для цього досліджується група пацієнтів із уже встановленим діагнозом. Аналогічно

технології, описаній вище, проводиться серія іспитів зі зміщенням точки поділу. Першим етапом є точка "безперечно патологія" (ті пацієнти, котрі не належать до цієї групи, вважаються здоровими). Потім точка поділу переноситься на інтервал "певно патологія", хворими вважаються пацієнти, віднесені до груп "патологія" та "певно патологія", а решта – здоровими. Для кожного з проведених іспитів розраховується неспецифічність і чутливість. Отримані точки з'єднуються кривою. На *рис. 4.5* схематично наведено відповідну ROC- криву.

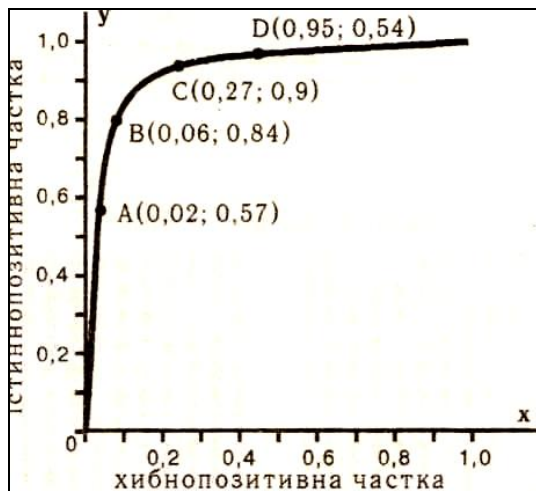


Рис. 4.5. ROC-крива талійного стрес-тесту

Апарат ROC-кривих успішно використовується для обґрунтування надійності роботи автоматизованих діагностичних систем. Так, наприклад, лабораторія дослідження радіологічних образів Kurt Rossman департаменту радіології Чиказького університету запропонувала комп'ютерні технології для аналізу груп мікрокальцинатів з метою диференціації доброякісних та злоякісних новоутворень на мамограмах.

Система не тільки аналізує групи мікрокальцинатів, але й сама виділяє зони інтересу. При дослідженні 100 мамограм від 53 пацієнтів з відомими результатами біопсії комп'ютерний аналіз дозволив ідентифікувати злоякісні новоутворення у 100 % випадків та доброякісні – у 82 %. Цей надзвичайно високий показник значно перевищує результати діагностики, проведеної спеціалістами-мамологами. У результаті комп'ютерної обробки із 100 образів відібрано 107 зон інтересу для подальшого аналізу. Для автоматичного формування таких зон для кожного мікрокальцинату обчислюють: а) його площу; б) ефективну товщину (фізичну товщину по лінії проєкціювання оцінюють, виходячи з контрасту з використанням

математичної моделі); в) ефективний об'єм (добуток площі на ефективну товщину).

Потім для кожної групи мікрокальцинатів розраховують 5 характеристик: кількість утворень у групі; середню площу; середній ефективний об'єм; відносне стандартне відхилення ефективної товщини; відносне стандартне відхилення ефективного об'єму. Як шоста ознака розглядається іррегулярність форм мікрокальцинатів.

Результати роботи системи підсумовували шляхом побудови ROC-кривої. Діагноз злоякісного новоутворення встановлювався, якщо хоча б одна з груп мікрокальцинатів підходила під цей діагноз; доброякісного – якщо всі групи кваліфікувалися як доброякісні.

Для порівняльної характеристики методу використовували результати аналізу тих самих мамограм, що були проведені групою з 5 радіологів. Що до того, куди віднести більше половини зображень, радіологи вагалися і при встановленні діагнозу обмежувалися градацією «можливо злоякісне новоутворення» або «певно злоякісне».

Були побудовані ROC-криві для мамограм, виконаних кожним з 5 фахівців, та загальна крива як наслідок їх спільного аналізу. Порівняння характеристик відповідних ROC-кривих свідчить про те, що запропонований метод придатний для виконання завдання класифікації.

Діаграму ROC-кривих для комп'ютеризованого методу та спільної діагностичної роботи 5 радіологів при аналізі мамограм наведено на *рис. 4.6*.

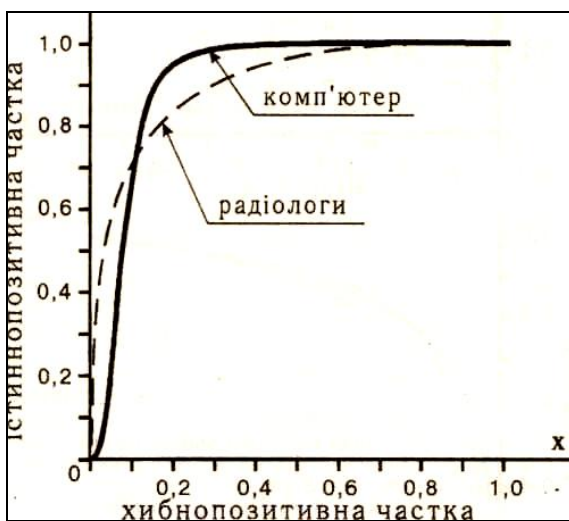


Рис. 4.6. Діаграма ROC-кривих, отриманих комп'ютеризованим методом та в результаті спільної діагностичної роботи 5 радіологів при аналізі мамограм

З наведеного можна бачити, що ROC-криві являють собою ефективний інструмент, для оцінки якості медичних діагностичних технологій, зокрема, комп'ютерних.

Питання для самоконтролю

1. Сфери використання теорії прийняття рішень як міждисциплінарної галузі дослідження. Напрямки застосування підходів прийняття рішень в медицині.

2. Прийняття рішень як процес вибору деякого набору альтернатив. Основні етапи процесу прийняття рішень (визначення мети, формування множини альтернатив, формування оцінки для порівняння альтернатив, вибір найкращого рішення з безлічі допустимих рішень). Наслідок прийняття рішення. Система переваг. Рішення як сукупність альтернатив, що задовольняють правилам системи переваг.

3. Класифікація задач прийняття рішень виходячи зі зв'язків між альтернативою та результатом. Детерміновані задачі прийняття рішень. Недетерміновані задачі прийняття рішень. Задача прийняття рішень в умовах ризику. Задача прийняття рішень в умовах стохастичної (імовірнісної) невизначеності. Задачі прийняття рішень в умовах пасивної взаємодії особи, що приймає рішення, та зовнішнього середовища. Задачі прийняття рішень в умовах конфлікту (гри). Особа, що приймає рішення (ОПР).

4. Діагностика як один з найбільш типових для лікаря напрямків прийняття рішень. Використання альтернативних оцінок для порівняльної оцінки ефективності діагностичних тестів. Чутливість та специфічність як числові характеристики тесту при альтернативному методі дослідження. Помилки діагностичних досліджень (хибнопозитивні, хибнонегативні).

5. Технологія побудови характеристичних кривих як залежності хибнопозитивних (абсциса) та істиннопозитивних (ордината) результатів. Поняття нечутливості та неспецифічності. Вид ROC-кривої залежно від якості тесту. Використання апарату ROC- кривих для обґрунтування надійності роботи автоматизованих діагностичних систем.

Розділ 5

АВТОМАТИЗОВАНІ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ ЛІКАРСЬКИХ РІШЕНЬ. ОСНОВИ ІНТЕЛЕКТУАЛЬНОГО ПІДХОДУ

5.1. Роль автоматизованих систем прийняття рішень у розвитку електронної охорони здоров'я.

Медичні консультативно-діагностичні системи (КДС, або Системи підтримки прийняття лікарських рішень (СППЛР), від англ. "Clinical decision support system" [CDSS]) призначені для діагностики патологічних станів.

Визначення цього типу систем було запропоновано Р. Хейвордом, співробітником Центру доказової медицини (Centre for Health Evidence): "Системи підтримки прийняття лікарських рішень пов'язують результати клінічних досліджень з даними, наявними у відношенні конкретного пацієнта, впливаючи на вибір лікарського рішення для більш ефективного надання медичної допомоги". Розробка і впровадження СППЛР в практику належать до найголовніших напрямків розвитку штучного інтелекту в медицині.

Зазначимо, що вибір того чи іншого рішення спирається на знання, накопичені раніше – банки даних систем, тобто у спрощеному вигляді алгоритм роботи є приблизно таким: шукаю аналогічну ситуацію у своєму довіднику, дивлюся, який висновок при цьому зробив лікар, і в моєму випадку пропоную його ж. Якість запропонованого висновку безпосередньо залежить від того, наскільки добре було навчено систему, тобто який об'єм даних накопичено для її бази знань.

Електронні медичні карти (ЕМК) являють собою майбутнє індустрії охорони здоров'я (*див. Розділ 2*). Вони є способом реєстрації даних і їх застосування в реальному часі для забезпечення надання пацієнтам високоякісної допомоги при ефективному використанні часу і ресурсів. Спільна інтеграція ЕМК і СППЛР в клінічний процес потенційно може привести до принципової зміни методів навчання та медичної практики. Було висловлено думку, що найвищим рівнем розвитку ЕМК є СППЛР.

Успішна інтеграція СППЛР з ЕМК має забезпечити надання високоякісної допомоги пацієнтам, що і є головною метою охорони здоров'я.

Помилки в галузі надання медичних послуг виникали завжди, тому спроби зведення їх до мінімуму є важливою складовою цього процесу. Завдяки впровадженню СППЛР і ЕМК можна вирішити проблеми в трьох напрямках:

- помилки при призначенні лікарських препаратів;
- небажані явища, пов'язані з лікарськими препаратами;
- інші медичні помилки.

СППЛР будуть надзвичайно корисними в майбутньому, коли заклади охорони здоров'я стануть "на 100 % електронними" щодо отримання інформації про пацієнтів у реальному часі, що значно знизить кількість змін, необхідних для адаптації всіх систем одна до одної.

Існує два основні різновиди СППЛР:

- засновані на наукових знаннях;
- засновані на даних, наприклад, на результатах обробки зібраних статистичних даних математичними методами.

Системи, засновані на наукових знаннях, є наразі одними з найбільш динамічних напрямків розробки систем СППЛР. Ядром систем цього рівня є бази знань систем штучного інтелекту і проблема вилучення (здобуття) знань не втрачає своєї актуальності.

5.2. Моделі представлення знань. Методи представлення знань у медичних експертних системах.

Представлення знань у комп'ютері тією чи іншою мірою відображає всі ознаки, що характеризують знання. В основі комп'ютерної бази знань завжди лежить певна модель представлення знань, від вибору якої залежить спосіб прийняття рішень. Моделі подання знань – це один з найважливіших напрямків досліджень в галузі штучного інтелекту. Без знань штучний інтелект існувати не може.

Для представлення знань у СППЛР використовуються логічні, продукційні семантичні та моделі, засновані на апараті фреймів.

Продукційна модель – це модель, заснована на правилах, що дозволяє представити знання у вигляді пропозицій типу: "ЯКЩО умова, ТО дія".

Основним недоліком продукційної моделі є той факт, що при накопиченні досить великої кількості (порядку декількох сотень) продукцій вони починають суперечити одна одній. Крім того, до недоліків таких систем можна віднести:

- відмінність від структур знань, що властиві людині;
- неясність взаємних відносин правил;
- складність оцінки цілісного образу знань;
- низька ефективність обробки знань.

До основних переваг систем, заснованих на продукційних моделях, належить простота подання знань і організації логічного висновку. При розробці невеликих систем (десятки правил) проявляються, в основному, позитивні сторони продукційних моделей знань, проте при збільшенні обсягу знань більш помітними стають слабкі сторони.

Основна ідея при побудові *логічних моделей* знань полягає в наступному. Вся інформація, необхідна для вирішення прикладних завдань, розглядається як сукупність фактів і тверджень, які представляються як формули в деякій логіці. Знання відображаються сукупністю таких формул, а отримання нових знань зводиться до реалізації процедур логічного висновку.

Основні переваги логічних моделей знань:

- "фундаментом" моделей є класичний апарат математичної логіки, методи якої досить добре вивчені і формально обґрунтовані;
- існують досить ефективні процедури виведення, у тому числі реалізовані в мовах логічного програмування;

- у базах знань можна зберігати лише безліч аксіом, а всі інші знання отримувати з них за правилами виведення.

У логічних моделях знань слова, що описують сутність предметної галузі, називаються термами (константи, змінні, функції), а слова, що описують відносини сутностей – предикатами. Предикат – логічна n -мірна пропозиційна функція, що окреслена предметної галуззю та набуває значення істинності або хибності. Пропозиційною називається функція, яка ставить у відповідність до об'єктів з галузі визначення одне зі значень – "істина" або "хиба". Предикат набуває значення "істина" або "хиба" залежно від значень термів, які є його складовою.

Спосіб опису предметної галузі, який використовується в логічних моделях знань, призводить до втрати деяких нюансів, властивих природному сприйняттю людини, і тому знижує описову можливість таких моделей.

Однозначне визначення *семантичної мережі* (мережевої моделі знань) на поточний час відсутнє. В інженерії знань під нею мається на увазі граф, що відображає зміст цілісного образу. Вузли графа відповідають поняттям та об'єктам, а дуги – відносинам між об'єктами.

Фреймова модель являє собою систематизовану психологічну модель пам'яті людини і її свідомості. Фрейм – це мінімально можливий опис сутності будь-якої події, ситуації, процесу або об'єкта. Поняття "мінімально можливе" означає, що при подальшому спрощенні опису втрачається його повнота, і воно перестає визначати ту одиницю знань, для якої було призначене. Подання знань за допомогою фреймів розуміється як один із способів представлення знань про ситуації. Фрейм має ім'я (назву) та складається зі слотів. Слоти – це незаповнені (нульові) позиції фрейму. Якщо у фрейму всі слоти заповнені – це опис конкретної ситуації. У перекладі з англійської слово "фрейм" означає "рамка", а слово "слот" – "щілина". На відміну від моделей інших типів у фреймових моделях фіксується жорстка структура інформаційних одиниць, яка називається протофреймом. У загальному вигляді структура інформаційних одиниць виглядає наступним чином:

(Ім'я фрейму:

ім'я слота 1 (значення слота 1);

ім'я слота 2 (значення слота 2);

.....

ім'я слота n (значення слота n)).

Значенням слота може бути практично що завгодно (числа, математичні співвідношення, тексти природною мовою або мовою програм, посилання на інші слоти даного фрейму). Значенням слота може виступати й окремий фрейм, що є дуже зручним для упорядкування знань за ступенем спільності.

При конкретизації фрейму йому і слотам приписуються конкретні імена і відбувається заповнення слотів. Таким чином, з протофрейму виходять фрейми – екземпляри.

Центральними фігурами для формування бази знань є експерт – носій знань у певній галузі (наприклад, у певному напрямку медицини) та інженер зі знань (англ. Knowledge engineer) – фахівець зі штучного інтелекту, який проектує та створює експертну систему. Зазвичай інженер зі знань виступає в ролі посередника між експертом і базою знань. Інженер зі знань:

- допомагає експерту виявити і структурувати знання, необхідні для роботи експертної системи, можна навіть сказати, що інженер зі знань витягує з експерта неформалізовані знання останнього;

- здійснює вибір тієї інтелектуальної системи (ІС), яка найбільше підходить для цієї проблемної галузі, і визначає спосіб представлення знань у цій ІС;

- виділяє і програмує (традиційними засобами) стандартні функції (типів для цієї проблемної галузі), які будуть використовуватися в програмах, що вводяться експертом.

Інженер зі знань (аналітик) є головною фігурою при здобутті знань з джерела знань (експерта, документації і т. д.). Результат його роботи відображає структуру уявлень і міркувань фахівців.

Об'єктивні труднощі вилучення знань полягають в наступному:

- знання експерта багатопланові, часто з ланцюжка міркувань згодом випадають ланки, які непросто відновити;

- частина знань і умінь зберігається в пам'яті в невербальній формі і пов'язана складною логіко-асоціативною мережею;

- більшості експертів не властива аналітичність і здатність до ясного викладу.

Інженер зі знань повинен володіти спеціальними знаннями із системного аналізу, формальної логіки, когнітивного моделювання, а головне – методології здобування знань. Якість вилучення знань може бути значно підвищена, якщо експерт у предметній галузі володіє певними знаннями щодо технології одержання. Базові засади технології викладено нижче.

5.3. Стратегії здобуття знань.

Здобуттям знань називається процес виявлення знань із джерел та перетворення їх на потрібну форму, а також перенесення в базу знань ІС. Знання, які отримані з літературних джерел, інших баз знань і т. п. та приведені до форми, яка робить їх доступними для споживача, є об'єктивними знаннями. Іншим типом знань є експертні знання, які є у спеціалістів, але не зафіксовані у зовнішніх по відношенню до нього сховищах. Експертні знання є суб'єктивними. Ще одним видом суб'єктивних знань є емпіричні знання. Такі знання можуть здобуватися ІС шляхом спостереження за навколишнім середовищем (якщо у ІС є засоби спостереження).

Слід зауважити, що всі аспекти теорії, яку викладено нижче, є справедливими для будь-яких інтелектуальних систем, у тому числі для людини.

5.3.1. Класифікація методів вилучення знань.

Класифікацію методів вилучення знань наведено на *рис. 5.1*. З представленої схеми класифікації видно, що основний принцип поділу пов'язаний із джерелом знань.



Рис.5.1. Класифікація методів вилучення знань

Комунікативні методи охоплюють всі види контактів з живим джерелом знань – експертом, а *текстологічні* стосуються методів вилучення знань з документів (методик, посібників, керівництв) і спеціальної літератури (статей, монографій, підручників).

Поділ цих груп методів на верхньому рівні класифікації не означає їх антагоністичності, зазвичай інженер зі знань комбінує різні методи, наприклад, спочатку вивчає літературу, потім розмовляє з експертами, або навпаки.

5.3.2. Комунікативні методи вилучення знань.

Комунікативні методи можна розділити на дві групи: активні і пасивні. *Пасивні методи* передбачають, що провідна роль у процедурі вилучення знань ніби передається експерту, а інженер зі знань тільки протоколює міркування експерта під час його реальної роботи щодо прийняття рішень

або записує те, що експерт вважає за потрібне самостійно розповісти у формі лекції. В *активних методах*, навпаки, ініціатива повністю в руках інженера зі знань, який активно контактує з експертом різними способами – в іграх, діалогах, бесідах за «круглим столом» і т. д.

Пасивні методи на перший погляд досить прості, але насправді вимагають від інженера зі знань уміння чітко аналізувати "потік свідомості" експерта і виявляти в ньому значущі фрагменти знань. Відсутність зворотного зв'язку (пасивність інженера зі знань) значно послаблює ефективність цих методів, чим і пояснюється їх зазвичай допоміжна роль при активних методах.

Активні методи можна розділити на дві групи залежно від кількості експертів, які віддають свої знання. Якщо їх кількість більше одного, то доцільно крім серії індивідуальних контактів з кожним застосовувати і методи групових обговорень предметної галузі. Такі групові методи зазвичай активізують мислення учасників дискусій та дозволяють виявляти досить нетривіальні аспекти їх знань. У свою чергу, індивідуальні методи на сьогодні залишаються провідними, оскільки "передача знань" часто не терпить зайвих свідків.

Говорячи про активні методи, окремо слід сказати про ігри. Ігрові методи зараз широко використовуються в різних галузях для підготовки керівників, вчителів, лікарів та інших фахівців. *Гра* – це особлива форма діяльності і творчості, де людина розкріпачується та відчуває себе набагато вільніше, ніж у звичайній трудовій діяльності.

5.3.2.1. Пасивні методи вилучення знань.

До пасивних методів належить:

- спостереження;
- аналіз протоколів «думок вголос»;
- лекції.

У процесі *спостережень* інженер зі знань знаходиться безпосередньо поряд з експертом під час його професійної діяльності або імітації цієї діяльності; при підготовці до сеансу вилучення експерту необхідно пояснити мету спостережень та попросити максимально коментувати свої дії.

Під час сеансу аналітик записує всі дії експерта, його репліки і пояснення. Може бути зроблений і відеозапис в реальному масштабі часу. Неодмінна умова цього методу – невтручання аналітика в роботу експерта хоча б на перших порах.

Існують два різновиди проведення спостережень:

- спостереження за реальним процесом;
- спостереження за імітацією процесу.

Протоколи спостережень ретельно розшифровуються, а потім обговорюються з експертом. Таким чином, спостереження – один з найбільш поширених методів вилучення знань на початкових етапах розробки. Зазвичай воно застосовується не самостійно, а в сукупності з іншими методами.

Протоколювання «думок вголос» відрізняється від спостережень тим, що експерта просять не просто прокоментувати свої дії та рішення, але і пояснити, як це рішення було знайдено, тобто продемонструвати весь ланцюжок своїх міркувань. Під час міркування експерта всі його слова протоколюються інженером зі знань.

Основною трудностю при протоколюванні "думок вголос" є принципова складність для будь-якої людини пояснити, як вона думає. При цьому існують експериментальні психологічні докази, що люди не завжди в змозі достовірно описати розумові процеси. Крім того, частина знань, що зберігаються в невербальній формі (наприклад, різні процедурні знання типу "як зав'язувати шнурки"), взагалі слабо корелюють з їх словесним описом. Автор теорії фреймів М. Мінський вважає, що "лише як виняток, а не як правило людина може пояснити те, що вона думає".

Розшифровка отриманих протоколів проводиться інженером зі знань самостійно з корекціями на наступних сеансах вилучення знань. Вдало проведене протоколювання "думок вголос" є одним з найбільш ефективних методів вилучення, оскільки в ньому експерт може проявити себе максимально яскраво, він нічим не скутий та може бути максимально вільним у своїх умовиводах та міркуваннях. Для великої кількості експертів це найприємніший спосіб вилучення знань.

Лекція – найстаріший спосіб передачі знань. Лекторське мистецтво здавна високо цінувалося у всіх галузях науки та культури. Якщо у експерта є досвід викладача (наприклад, професора клініки), то його лекція може стати концентрованим фрагментом знань.

В лекції експерту надається багато ступенів свободи для самовираження, тому досвідчений лектор може заздалегідь структурувати свої знання, хід міркування. Від інженера зі знань у цій ситуації потрібно лише грамотно законспектувати лекцію і в кінці поставити необхідні питання. Тривалість лекції стандартна – від 40 до 50 хв і через 5–10 хв – ще стільки ж. Курс – від двох до п'яти лекцій.

5.3.2.2. Активні методи вилучення знань.

Діляться на індивідуальні і групові.

Активні індивідуальні методи вилучення знань на сьогодні найбільш розповсюджені. Тією чи іншою мірою до них вдаються при розробці практично будь-якої експертної системи.

До основних *активних індивідуальних* методів можна віднести:

- анкетування;
- інтерв'ю;
- вільний діалог;
- ігри з експертом.

У цих методах активну функцію виконує інженер зі знань, який пише сценарій та керує сеансами вилучення знань. Ігри з експертом істотно відрізняються від інших методів. Три метода, що залишилися, дуже схожі

між собою і відрізняються лише за ступенем свободи, яку може собі дозволити інженер зі знань при проведенні сеансів вилучення знань.

Анкетування – найбільш жорсткий метод, тобто найбільш стандартизований. Інженер зі знань заздалегідь складає опитувальник або анкету, розмножує її і використовує для опитування декількох експертів. Це основна перевага анкетування.

Сама процедура може проводитися двома способами:

- аналітик вголос ставить питання і сам заповнює анкету з відповідей експерта;

- експерт самостійно заповнює анкету після попереднього інструктування.

Існує кілька загальних правил при складанні анкет. По-перше, анкета не повинна бути монотонною і одноманітною, тобто викликати нудьгу або втому. Це досягається варіаціями питань, зміною тематики, вставкою питань-жартів та ігрових запитань. По-друге, анкета повинна бути пристосована до мови експертів. По-третє, оскільки питання впливають одне на одного, послідовність їх повинна бути строго продумана. По-четверте, бажано прагнути до оптимальної надмірності. Відомо, що в анкеті завжди багато зайвих питань, частина з них необхідна – це так звані контрольні питання, а іншу частину потрібно мінімізувати. І, нарешті, по-п'яте, в анкеті мають бути «хороші манери», тобто її мова ясна, зрозуміла, гранично ввічлива. Методичною майстерністю складання анкети оволодівають лише на практиці.

Під *інтерв'ю* розуміється специфічна форма спілкування інженера зі знань та експерта, в якій інженер зі знань ставить експерту серію заздалегідь підготовлених питань з метою вилучення знань про предметну галузі.

Інтерв'ю дуже близько до анкетування, коли аналітик сам заповнює анкету, заносючи туди відповіді експерта. Основна відмінність у тому, що інтерв'ю дозволяє аналітику опускати ряд питань залежно від ситуації, вставляти нові питання в анкету, змінювати темп, урізноманітнювати ситуацію спілкування.

Інженери зі знань рідко замислюються: чи вміють вони ставити питання? У філософії та математиці ця проблема обговорюється з давніх пір. Існує навіть спеціальна гілка математичної логіки – логіка запитань.

Вкажемо три основні характеристики питань, які впливають на якість інтерв'ю:

- стиль (зрозумілість, лаконічність, термінологія);
- порядок (логічна послідовність і немонотонність);
- доречність (етика, ввічливість).

Очевидно, що будь-яке питання має сенс тільки в контексті. Тому питання може готувати інженер зі знань, який вже опанував ключовий набір знань. Питання для експерта мають діагностичне значення – кілька

відвертих "дурних" питань можуть повністю розчарувати експерта і відбити у нього бажання до подальшої співпраці.

Питання поділяються на відкриті та закриті. *Відкрите питання* позначає тему чи предмет, надаючи експерту свободу за формою і змістом відповіді. При *закритому питанні* експерту пропонується набір відповідей, серед яких він повинен зробити вибір. Закриті питання легше обробляються, але вони певною мірою «програмують» відповідь експерта та "закривають" хід його міркувань. Тому при складанні сценарію інтерв'ю зазвичай чергують відкриті і закриті питання та особливо ретельно продумують зміст закритих питань.

Крім того, питання поділяються на особисті та безособові. *Особисте питання* апелює до індивідуального досвіду експерта. Особисті питання зазвичай активізують мислення експерта, "грають" на його самолюбстві, прикрашають інтерв'ю. *Безособове питання* націлене на виявлення найбільш поширених і загальноприйнятих закономірностей предметної галузі.

При підготовці питань враховують, що мовні можливості експерта, як правило, обмежені. Через замкнутість, скутість та боязкість окремі експерти не можуть відразу висловити свою думку і надати потрібні знання. Тому часто використовують не прямі питання, які безпосередньо вказують на предмет або тему, а непрямі, опосередковано направляючи увагу на актуальну проблему. Іноді в інтересах справи доводиться ставити декілька непрямих питань замість одного прямого. *Вербальні питання* – це традиційні усні запитання. *Питання з використанням наочного матеріалу* урізноманітнюють інтерв'ю і знижують стомлюваність експерта. Як наочний матеріал використовують фотографії, рисунки та картки.

Поділ питань за функцією на основні, зондувальні і контрольні пов'язано з тим, що нерідко експерт з якихось причин йде в бік від питання та основні питання інтерв'ю виявляються непродуктивними. Тоді аналітик застосовує *зондувальні питання*, що концентрують увагу експерта в потрібному напрямку. *Контрольні питання* використовують для перевірки достовірності та об'єктивності отриманої інформації.

Вільний діалог – це метод вилучення знань у формі бесіди інженера зі знань та експерта, у якій немає жорстко регламентованого плану та опитувальника.

Кваліфікована підготовка до діалогу допомагає аналітику запланувати гладкий перебіг процедури вилучення, пробудивши інтерес і завоювавши довіру експерта.

До *активних групових методів вилучення знань* відносяться:

- рольові ігри;
- дискусії за круглим столом за участю декількох експертів;
- мозковий штурм.

Активні групові методи самі по собі не можуть служити джерелом більш-менш повного знання. Вони виступають як додаткові і служать хорошою «приправою» до індивідуальних методів вилучення знань, активізують мислення і поведінку експертів.

Основна перевага групових методів – це можливість одночасного поглинання знань від декількох експертів, взаємодія яких вносить елемент принципової новизни від накладення різних поглядів і позицій.

Метод круглого столу (термін запозичений з журналістики) передбачає обговорення будь-якої проблеми з обраної предметної галузі, у якому беруть участь з рівними правами кілька експертів. Зазвичай спочатку учасники висловлюються в певному порядку, а потім переходять до живої вільної дискусії. Кількість учасників дискусії коливається від трьох до п'яти-семи.

Задача дискусії – колективно, з різних точок зору, під різними кутами досліджувати спірні гіпотези предметної галузі. Зазвичай емпіричні галузі багаті на такий дискусійний матеріал. Для гостроти на круглий стіл запрошують представників різних наукових напрямків та різних поколінь, це також зменшує небезпеку отримання односторонніх знань.

Наукова плідність дискусій робить їх привабливими не тільки для інженера зі знань, але й для самих експертів, особливо для тих, хто знає менше.

Мозковий штурм, або *мозкова атака*, – один з найбільш поширених методів розкріпачення та активізації творчого мислення. Вперше цей метод був використаний у США як спосіб отримання нових ідей в умовах заборони критики. Помічено, що боязнь критики заважає творчому мисленню, тому основна ідея штурму – це відокремлення процедури генерування ідей у замкнутій групі спеціалістів від процесу аналізу та оцінки висловлених ідей.

Як правило, штурм триває близько 40 хв. Учасникам (до 10 осіб) пропонується висловлювати будь-які ідеї (жартівливі, фантастичні, помилкові) на задану тему (критика заборонена). Зазвичай висловлюється більше 50 ідей. Регламент до двох хвилин на виступ. Найцікавіший момент штурму – це момент піку (ажіотажу), коли ідеї починають «фонтанувати», тобто відбувається мимовільна (несвідома) генерація гіпотез учасниками. При подальшому аналізі всього лише 10–15 % ідей виявляються розумними, але серед них бувають досить оригінальні. Оцінює результати зазвичай група експертів, яка не брала участь у генерації.

Ведучий мозкового штурму – інженер зі знань – повинен вільно володіти аудиторією, підбирати активну групу експертів – "генераторів", не затискати погані ідеї – вони можуть служити каталізатором хороших. Мистецтво ведучого – це мистецтво ставити запитання аудиторії, "підігрі-

ваючи" генерацію. Питання служать «гачком», яким витягуються ідеї. Питання також можуть зупиняти багатослівних експертів і служити способом розвитку ідей інших.

Грою називають такий вид діяльності, який відображає (відтворює) інші її види. Поняття експертної гри, або гри з експертами, в цілях вилучення знань зводиться до трьох понять – ділової гри, яка широко використовується при підготовці фахівців і моделюванні, діагностичної гри, а також комп'ютерні ігри, які все частіше застосовуються в навчанні.

Під *діловою грою* найчастіше розуміють експеримент, де учасникам пропонується виробнича ситуація, а вони на основі свого життєвого досвіду, загальних і спеціальних знань та уявлень приймають рішення. Рішення аналізуються, і розкриваються закономірності мислення учасників експерименту. Саме ця, аналізуюча, частина ділової гри корисна для отримання знань. Якщо учасниками такої гри стають експерти, то гра з ділової перетворюється на експертну. З трьох основних типів ділових ігор (навчальних, планово-виробничих і дослідницьких) до експертних ближче всього дослідні, які використовуються для аналізу систем, перевірки правил прийняття рішень.

Діагностична гра – це та ж ділова гра, але вживана конкретно для діагностики методів прийняття рішення в медицині (діагностика методів діагностики). Ці ігри виникли при дослідженні способів передачі досвіду від кваліфікованих лікарів новачкам. Діагностична гра є експертною грою з жорстко закріпленою предметною галуззю – медициною.

Додатково до наведеної класифікації експертні ігри можна розділити на *індивідуальні та групові*, а також ігри *із використанням спеціального обладнання та комп'ютерної техніки*.

Плідність моделювання реальних ситуацій в іграх підтверджується сьогодні практично у всіх галузях науки і техніки. Вони розвивають логічне мислення, здібності швидко приймати рішення, викликають інтерес в експертів.

У разі *індивідуальних ігор* з експертом інженер зі знань бере на себе якусь роль у ситуації, що моделюється. Наприклад, гра "Вчитель і учень", в якій інженер зі знань бере на себе роль учня та на очах експерта виконує його роботу, а експерт виправляє помилки "учня".

В іншій грі інженер зі знань бере на себе роль лікаря, який добре знає хворого, а експерт – роль консультанта. Консультант ставить питання, робить прогноз про доцільність застосування того чи іншого виду лікування. Така гра "двох лікарів" дозволила, наприклад, виявити, що експерту знадобилося всього 30 питань для успішного прогнозу, у той час як первісний опитувальник, складений медиками з цією ж метою, містив 170.

Рольові *ігри в групі* передбачають участь декількох експертів (від трьох до шести). До такої гри зазвичай заздалегідь складається сценарій,

розподіляються ролі, до кожної ролі готується портрет-опис та розробляється система оцінювання гравців. У разі більшої кількості експертів вони розбиваються на групи, між якими організовуються змагання: чий діагноз виявиться ближче до істинного, чий план раціональніше використовує ресурси, хто може швидше визначити несправність у технічному блоці та ін.

Ігри з тренажерами значною мірою ближче не до ігор, а до імітаційних вправ у ситуації, наближеної до дійсності.

Наявність тренажера дозволяє відтворити майже виробничу ситуацію і поспостерігати за експертом. Тренажери широко застосовують для навчання (наприклад, льотчиків або операторів атомних станцій). Очевидно, що застосування тренажерів для вилучення знань дозволяє зафіксувати фрагменти «летючих» знань, що виникають під час та на місці реальних ситуацій і випадають з пам'яті при виході за межі ситуації.

5.3.3. Текстологічні методи вилучення знань.

Група текстологічних методів об'єднує методи вилучення знань, засновані на вивченні спеціальних текстів з підручників, монографій, статей, методик та інших носіїв професійних знань.

Задачу вилучення знань з текстів можна сформулювати як задачу розуміння та виділення змісту тексту. Сам текст природною мовою є лише провідником сенсу, а задум та знання автора лежать у вторинній структурі (смісловій або макроструктурі тексту), що настроюється над природним текстом.

При цьому можна виділити дві такі смислові структури: *M1* сенс, який намагався закласти автор, це його модель світу, і *M2* сенс, який осягає читач, у даному випадку інженер зі знань (рис. 5.2) у процесі інтерпретації *I*. При цьому *T* – це словесне одіяння *M1*, тобто результат вербалізації *V*. У широкому сенсі вербалізація означає вербальний (словесний) опис переживань, почуттів, думок, поведінки.



Рис. 5.2. Вилучення знань з текстів

Складність процесу полягає у принциповій неможливості збігу знань, що утворюють *M1* і *M2*, через те, що *M1* утворюється завдяки сукупності уявлень, потреб, інтересів та досвіду автора, лише мала частина

яких знаходить відображення в тексті *T*. Відповідно і *M2* утворюється у процесі інтерпретації тексту *T* завдяки залучення всієї сукупності наукового та людського багажу читача.

Постає задача з'ясувати, завдяки чому можна досягти максимальної адекватності *M1* і *M2*, пам'ятаючи про те, що розуміння завжди відносно. Розглянемо докладніше, які джерела живлять модель *M1* і створюють текст *T*. Це первинний матеріал спостережень та система наукових понять у момент створення тексту. Крім того, додатково до об'єктивних даних експериментів і спостережень в тексті обов'язково наявні суб'єктивні погляди автора, результат його особистого досвіду, а також деякі "загальні місця", або "вода". Крім того, будь-який науковий текст містить запозичення з інших джерел (статей, монографій) і т. п.

При вилученні знань аналітику, який інтерпретує текст, доводиться вирішувати задачу декомпозиції цього тексту на перераховані вище компоненти для виділення істинно значимих для реалізації бази знань фрагментів. Складність інтерпретації наукових і спеціальних текстів полягає ще й у тому, що будь-який текст набуває сенсу тільки в контексті, де під контекстом розуміється оточення, в яке «занурений» текст.

Основними моментами розуміння тексту є:

- висування попередньої гіпотези про сенс всього тексту (передбачення);
- визначення значення незрозумілих слів (тобто спеціальної термінології);
- виникнення загальної гіпотези про зміст тексту (про знання);
- уточнення значення термінів та інтерпретація окремих фрагментів тексту під впливом загальної гіпотези (від цілого до частин);
- формування деякої смислової структури тексту за рахунок встановлення внутрішніх зв'язків між окремими важливими (ключовими) словами і фрагментами, а також за рахунок утворення абстрактних понять, узагальнюючих конкретні фрагменти знань;
- коригування загальної гіпотези щодо фрагментів знань, які містяться у тексті (від частин до цілого);
- прийняття основної гіпотези, тобто формування *M2*.

Найбільш простим методом є аналіз підручників, у яких логіка викладу зазвичай відповідає логіці предмету, і тому макроструктура такого тексту буде, напевно, більш значуща, ніж структура тексту будь-якої спеціальної статті. Аналіз методик утруднений якраз стислістю викладу та практичною відсутністю коментарів, тобто фонових знань, що полегшують розуміння для неспеціалістів.

Питання для самоконтролю

1. Системи підтримки прийняття лікарських рішень (СППЛР) як складова система штучного інтелекту. Перспективи інтеграції СППЛР та електронної медичної карти (ЕМК). СППЛР, засновані на наукових знаннях. СППЛР засновані на даних. Бази знань як ядро СППЛР.

2. Моделі подання знань як один з найважливіших напрямків досліджень в галузі штучного інтелекту. Логічні, продукційні семантичні моделі та моделі, засновані на апараті фреймів. Експерт та інженер зі знань як центральні фігури для формування бази знань. Функції інженера зі знань. Об'єктивні труднощі вилучення знань.

3. Процес здобуття знань. Об'єктивні, суб'єктивні та емпіричні знання.

4. Комунікативні та текстологічні методи вилучення знань. Структурна схема вилучення знань.

5. Активні та пасивні комунікативні методи. Загальна структура активних методів. Загальна структура пасивних методів вилучення знань. Ігрові методи.

6. Спостереження, аналіз протоколів "думок вголос" та лекції – основні типи пасивних методів вилучення знань. Два різновиди проведення спостережень – спостереження за реальним процесом, спостереження за імітацією процесу. Труднощі методу протоколюванні "думок вголос". Лекція як найстаріший спосіб передачі знань.

7. Основні активні індивідуальні методи вилучення знань – анкетування, інтерв'ю, вільний діалог, ігри з експертом. Анкетування. Два способи проведення анкетування. Загальні правила складання анкет. Інтерв'ю, його відмінність від анкетування. Логіка запитань. Основні характеристики питань, які впливають на якість інтерв'ю. Відкриті та закриті питання для експерта. Поділ питань на особисті та безособові. Вербальні питання та питання з використанням наочного матеріалу. Вільний діалог.

8. Основні активні групові методи вилучення знань (рольові ігри; дискусії за круглим столом за участю декількох експертів; мозковий штурм). Ділова гра. Діагностична гра для діагностики методів прийняття рішення в медицині (діагностика методів діагностики). Індивідуальні та групові ігри. Ігри із використанням спеціального обладнання. Ігри із застосуванням комп'ютерної техніки.

9. Задачі вилучення знань з текстів. Смислова структура (макро-структура) тексту.

ЛІТЕРАТУРА

1. Медична інформатика : підруч. для студентів мед. ВНЗ /за ред. В. Г. Книгавка. – Харків : ХНМУ, 2015. – 288 с.
2. Медицинская информатика : учеб. для студентов 2-го курса мед. ВУЗов : в 2 ч. / под ред. В. Г. Книгавко. – Харьков : ХНМУ, 2017.
3. Висоцька О. В. Медичні інформаційні системи : навч. посібник / О. В. Висоцька. – Харків : ХНУРЕ, 2014. – 472 с.
4. Дабагов А. Р. Информатизация здравоохранения и некоторые проблемы построения интегрированных медицинских информационных систем [Электронный ресурс] / А. Р. Дабагов // Журнал радиоэлектроники. – 2011. – № 9. – Режим доступа : <http://jre.cplire.ru/jre/sep11/2/text.html>
5. Міністерство охорони здоров'я України. Концепція інформатизації охорони здоров'я. – Режим доступу : <http://moz.gov.ua/article/reform-plan/jak-bude-rozvivatisja-enealth-v-ukraini-prezentuvali-proekt-koncepcii-informatizacii-ohoroni-zdorovja>
6. Про необхідність ознайомлення студентів вищих медичних навчальних закладів з системою кодування ІСРС-2 / Є. Б. Радзішевська, О. В. Висоцька, С. С. Гранкіна та ін. // Актуальні питання вищої медичної освіти в Україні (з дистанційним під'єднанням ВМ(Ф)НЗ України за допомогою відеоконференц-зв'язку) : матеріали XV Всеукр. наук.-практ. конф. з міжнар. участю (Тернопіль, 17–18 трав. 2018 р.) / Терноп. держ. мед. ун-т ім. І. Я. Горбачевського. – Тернопіль : ТДМУ, 2018. – С. 254
7. Застосування апарату характеристичних кривих (ROC-кривих) у діагностичній радіології та комп'ютерних медичних системах / М. І. Пилипенко, Є. Б. Радзішевська, В. Г. Книгавко, В. Г. Нестеров // УРЖ. – 1997. – № 4. – С. 411–417
8. Высоцкая Е. В. Многомерный статистический анализ в прикладных медицинских исследованиях : монография / Е. В. Высоцкая. – Харьков, 2013. – 140 с.

ЗМІСТ

Вступ	3
Розділ 1. Значення стандартів у створенні та забезпеченні взаємодії медичних інформаційних систем	4
Розділ 2. Електронна система охорони здоров'я	13
Розділ 3. Права доступу до інформації та захист медичних даних	32
Розділ 4. Процеси прийняття рішень у медицині.	
Оцінка ефективності діагностичного тесту	46
Розділ 5. Автоматизовані системи підтримки прийняття лікарських рішень. Основи інтелектуального підходу	57
Література	71

Навчальне видання

Радзішевська Євгенія Борисівна
Висоцька Олена Володимирівна

Інформаційні технології в медицині. E-health

***Підручник
для студентів медичних закладів вищої освіти***

За редакцією В. Г. Книгавка

Відповідальний за випуск Є. Б. Радзішевська



Редактор М. В. Тарасенко
Комп'ютерна верстка О. Ю. Лавриненко

Формат А5. Ум.-друк. арк. 4,5. Зам. № 19-33845.

**Редакційно-видавничий відділ
ХНМУ, пр. Науки, 4, м. Харків, 61022
izdatknmurio@gmail.com**

Свідectво про внесення суб'єкта видавничої справи до Державного реєстру видавництв, виготівників і розповсюджувачів видавничої продукції серії ДК № 3242 від 18.07.2008 р.