**Зміст**

[Вступ 2](#_Toc396949627)

[Структура медичної системи 3](#_Toc396949628)

[SSL 3](#_Toc396949629)

[HL7 4](#_Toc396949630)

[DICOM 4](#_Toc396949631)

[Висновок 4](#_Toc396949632)

Вступ

Для кращого розуміння функціональних можливостей сучасних медично-інформаційних систем потрібно розглянути та проаналізувати їх загальну структуру та існуючі розробки. Нижче приведений опис таких систем та короткий список їх функціональних можливостей.

За кілька останніх десятиліть рівень застосування комп'ютерів в медицині надзвичайно підвищився. Практична медицина стає все більш і більш автоматизованою. Почало з’являтися багато програм та пристроїв з якими вони взаємодіють для забезпечення функціонування медичних установ.

Виділяють два види комп'ютерного забезпечення: програмне та апаратне. Програмне забезпечення включає в себе системне й прикладне.

Системне програмне забезпечення призначене для функціонування самого комп'ютера як єдиного цілого. Це, в першу чергу, операційна система, а також сервісні програми різного призначення - драйвери, утиліти і т. п. У системне програмне забезпечення входить мережевий інтерфейс, який забезпечує доступ до даних на сервері. Дані, введені в комп'ютер, організовані, як правило, в базу даних, яка, в свою чергу, управляється прикладною програмою системою керування базами даних (СКБД) і може містити, зокрема, історії хвороби, рентгенівські знімки, статистичну звітність зі стаціонару, бухгалтерський облік та іншу інформацію.

Нові вимоги в політиці охорони здоров'я, а також бурхливий розвиток комп'ютерних технологій ставлять перед розробниками програмного забезпечення завдання створення комплексних систем автоматизації діяльності медичних установ. Розробка та впровадження таких систем дозволяє ефективно вирішувати завдання інтеграції всіх наявних джерел інформації як медичної, так і господарської орієнтації, полегшити роботу медичного персоналу. Це виражається в збільшенні швидкості обробки інформації різного типу, підвищення оперативності прийняття рішень.

Структура медичної системи

Розписати структуру ситеми БД, Клієн, Сервер, Принтер

SSL

SSL (англ. Secure Sockets Layer — рівень захищених сокетів) — криптографічний протокол, який забезпечує встановлення безпечного з'єднання між клієнтом і сервером. SSL спочатку розроблений компанією Netscape Communications. Згодом на підставі протоколу SSL 3.0 був розроблений і прийнятий стандарт RFC, що отримав ім'я TLS. Перед обміном повідомленнями необхідно провести обмін сертифікатами, які містять відкриті ключі клієнта і сервера. Протокол забезпечує конфіденційність обміну даними між клієнтом і сервером, що використовують TCP/IP, причому для шифрування використовується асиметричний алгоритм з відкритим ключем. При шифруванні з відкритим ключем використовується два ключі, причому будь-який з них може використовуватися для шифрування повідомлення. Тим самим, якщо використовується один ключ для шифрування, то відповідно для розшифровки потрібно використовувати інший ключ. У такій ситуації можна отримувати захищені повідомлення, публікуючи відкритий ключ, і зберігаючи в таємниці секретний ключ.



Протокол широко використовується для обміну миттєвими повідомленнями, передачі голосу через IP (VoIP), а також в програмах електронної пошти. На основі протоколу SSL функціонує протокол HTTPS. Протокол є надійним способом захисту даних в мережі Інтернет. Недоліками протоколу можуть бути можливість атак, проте він не буде вразливий до них при використанні довірених серверів для обробки інформації. Також до недоліків можна віднести можливість перехоплення даних спецслужбами за допомогою спеціальних систем «сніферів» в дата центрах в обхід SSL, тому SSL не може стовідсотково захищати з’єднання з зовнішнім веб-сайтом.

HL7

Розписати структуру системи БД, Клієнт, Сервер, Принтер

DICOM

Розписати структуру системи БД, Клієнт, Сервер, Принтер

Висновок

Розписати для чого система