В роботі проаналізовано три представлення слабоструктурованої інформації:
1) OEM (Object Exchange Model, модель обміну об’єктами);
2) XML (Extensible Markup Language, розширювана мова розмітки);
3) RDF (Resource Description Framework, фреймворк опису ресурсів).

АНАЛІЗ АПАРАТНИХ ПЛАТФОРМ ДЛЯ РЕАЛІЗАЦІЇ СИСТЕМИ БРОНЮВАННЯ ЗАПИСИ ДО ЛІКАРЯ

Бабак О.В.
Науковий керівник – ***Булаєнко М.В., канд. техн. наук, доцент***

Влітку 2017 року МОЗ України повідомив про початок роботи електронної медичної системи для лікарів і пацієнтів - eHealth. Однією з її можливостей став запис до лікаря і виклик лікаря додому за допомогою електронного запису. Перехід на електронний запис для медустанов не обов'язковий, але передбачається, що в подальшому без електронної бази працювати буде все складніше. Записатися на прийом до лікаря можна на різних сайтах. Медустанова сама обирає, до якої з розроблених інформаційних систем підключитися.

Зараз державні установи ведуть запис через інформаційні системи: Helsi, Medics, Поліклініка без Черги, Мій Мед Кабінет, Доктор Елекс, MedCard, Emsimed, medstar, eLife та інші. Всі сайти влаштовані досить просто і розраховані навіть на мало просунутих користувачів комп'ютера. Деякі установи уможливили запис на прийом через свій сайт (рис.1).

Рисунок 1- *On-line* запис

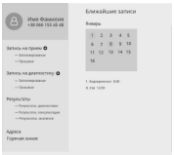

Рисунок 2 - *Widget* модуль

У роботі пропонується система (рис. 2) ві́джет - бронювання записи до лікаря, яка може бути реалізована на різних операційних системах Linux, Android, iOS. Веб-ві́джет — контент-модуль, що вбудовується у веб-сторінку або у браузер. Цей тип заснований на веб-технологіях, що працюють через браузер: HTML, Flash тощо. Модуль є адаптивним і ідеально сумісним з WordPress и Joomla. Модуль можна встановити як Pop up, так і в форматі IFrame. Система віджет-бронювання допоможе швидко та без зайвих зусиль записатися до лі-

каря, на діагностику, оплатити консультацію чи діагностику. У системі є можливість відстежувати аналізи та заключення лікаря, що не потребує наявність пацієнта у лікарні та очікування своєї черги.

В роботи проводиться аналіз особливостей реалізації внутрішніх алгоритмів керування основними ресурсами комп'ютера (процесорами, пам'яттю, пристроями), розглядається відмінність відповідних апаратних платформ.

ЗАХИСТ НАШОГО ЖИТТЯ В ІНТЕРНЕТІ

Воронов Д.М.
Науковий керівник – ***Булаєнко М.В., канд. техн. наук, доцент***

Комп'ютерні пристрої зберігають наші дані та є порталом до нашого життя. Що ми маємо зробити, щоб захистити наші пристрої?

Використовувати антивірусні та антишпигунські програми – зловмисне програмне забезпечення (ПЗ), таке як віруси, троянські коні, хробаки, програми-здирники та шпигунські програми, встановлюються на комп'ютерних пристроях без нашого дозволу, щоб отримати доступ до комп'ютера та даних. Віруси можуть знищити дані, уповільнити роботу комп'ютера або взяти його під контроль. Шпигунське програмне забезпечення може контролювати наші дії в Інтернеті, збирати нашу особисту інформацію або відкривати небажані спливаючі вікна з рекламою у нашому веб-браузері під час роботи в Інтернеті. Антивірусне програмне забезпечення призначене для сканування комп'ютера та вхідної електронної пошти на наявність вірусів та їх видалення. Іноді антивірусне програмне забезпечення також містить антишпигунське ПЗ.

Комп'ютерні пристрої, зокрема ПК, ноутбуки, планшети або смартфони, повинні бути захищені паролем для запобігання несанкціонованому доступу. Збережена на них інформація, а особливо важливі або конфіденційні дані, повинна бути зашифрована. На мобільних пристроях потрібно зберігати лише необхідну інформацію, з урахуванням того, що ці пристрої можуть бути вкрадені або втрачені, коли ви перебуваєте далеко від дому, таким чином злочинці можуть отримати доступ до всіх наших даних через постачальника послуг хмарного сховища, наприклад iCloud або Google Drive.

Напевно, ви маєте більше ніж один обліковий запис в Інтернеті, і для кожного з них слід використовувати унікальний пароль. Використання однакового пароля для усіх облікових записів в Інтернеті - це те саме, що й використання одного ключа для замикання усіх дверей. Таким чином, доводиться пам'ятати багато паролів. Одним із способів уникнення повторного використання паролів або вибору слабких па-