Інтернет речей. Система стеження за здоров’ям людини.

# Вступ.

Чи замислювалися ви коли-небудь, наскільки зараз автоматизоване наше повсякденне життя? Ще кілька десятків років тому люди і подумати не могли, що його можна настільки спростити в плані управління побутовими речами. Ми можемо спостерігати за станом свого здоров'я, не виходячи з дому, відстежувати потрібний транспорт, управляти пилососом дистанційно, і ще багато чого. Такі вже звичні нам речі роблять наше життя неймовірно комфортним, чи не так? Але щоб зрозуміти тему інтернету речей, ми повинні для початку зрозуміти, як це працює.

Отже, що таке інтернет речей? Інтернет речей (IoT) - це поєднання транспортних засобів, побутової техніки, медичного обладнання з використанням вбудованої електроніки, мікрочіпів і т. д. Ця технологія дозволяє користувачеві дистанційно керувати пристроями через мережу.

Інтернет речей дозволяє створювати динамічні мережі, що складаються з мільярдів і трильйонів таких речей, у яких є комунікація між собою. Таким чином, забезпечиться поєднання цифрового та фізичного світів, для якого додатки, сервіси, компоненти сполучного ПО і кінцеві пристрої - це речі. Ці цифрові аналоги зможуть сприймати інформацію з навколишнього світу, вступати у взаємодію, обмінюватися даними. В результаті складається зовсім нове середовище, де інтелект, закладений в додатки, дозволить оцінювати те, що відбувається в фізичному світі, враховувати накопичені раніше відомості і досвід для підтримки прийняття рішень. В такому середовищі створюються якісно інші умови для бізнесу, для охорони здоров'я, для забезпечення екологічної безпеки і всього іншого, що нас оточує. Зрозуміло, вся ця автоматизація не виключає людини, і як доказ варто привести невтішний висновок, до якого прийшли творці безпілотного автомобіля Google після серії експериментів, що закінчилися в березні 2014 року, - вони вважають результат негативним, і в доступному для огляду майбутньому без водія обійтися не вдасться, більш того, рівень автоматизації вже сьогодні час обмежити, не доводячи його до тієї межі, коли людина втрачає почуття відповідальності за те, що відбувається.

У майбутньому не передбачається, що IoT повністю автоматизує речі, - по суті, він орієнтований на людину і надає йому можливість доступу до речей, хоча багато речей зможуть вести себе інакше, ніж ми уявляємо собі сьогодні. У IoT кожна річ буде мати свій унікальний ідентифікатор (Unique Identifier) або віртуальний ідентифікатор (Virtual Identifier), які спільно утворюють континуум речей, здатних адресуватися один одному, створюючи тимчасові або постійні мережі. Речі зможуть брати участь в процесі їх переміщення, повідомляючи про себе відомості, вони дозволять повністю автоматизувати процес логістики, а маючи вбудований інтелект, вони зможуть змінювати свої властивості і адаптуватися до навколишнього середовища в тому числі для зменшення енергоспоживання. Володіючи «органами почуттів», вони зможуть виявляти інші, так чи інакше, пов'язані з ними речі, і налагоджувати з ними взаємодію. Типовий приклад такого роду, так званий атакуючий рій, - зграя невеликих безпілотних літаків, здатна виконувати поставлене перед нею завдання. Більш того, IoT дозволяє створювати комбінацію з інтелектуальних пристроїв (наприклад, різного роду засоби дистанційного збору даних і роботи), об'єднаних мультипротокольними мережами зв'язку, і людей-операторів. Спільно вони можуть створювати системи для роботи в середовищах, незручних або недоступних для людини: космос, великі глибини, ядерні установки, трубопроводи і т. п. Синергія різних речей в поєднанні з творчими можливостями може принести якісно нові результати.

# Приклади реалізації IoT

Фантазія в частині застосування розумних речей нічим не обмежена, але це в майбутньому, а вже сьогодні проглядаються додатки, де IoT дасть очевидний ефект.

Авіаційна та аерокосмічна промисловість.

Традиційні методи контролю не виключають ймовірності використання контрафактних вузлів, це хвороба загальна, нею страждають і інші галузі, але тут вона особливо небезпечна і є причиною для третини авіаційних подій. При наявності невіддільною від виробу мітки RFID і розподіленої бази даних випущених різними виробниками запасних частин проблема контролю походження тієї чи іншої деталі знімається. Наступний крок - контроль стану виробу в процесі експлуатації, при цьому відповідальні вузли і механізми можуть бути забезпечені бездротовими системами діагностики та збору даних для аналізу і прийняття рішень з використанням сучасних аналітичних технологій.

Автомобільна промисловість.

У цій сфері можуть бути реалізовані системи моніторингу і також до того механізми взаємодії між транспортними засобами (Vehicle to Vehicle, V2V), взаємодії транспортного засобу з інфраструктурою (Vehicle to Infrastructure, V2I). Постачання автомобілів системами позиціонування в реальному часі (Real-time Locating Systems, RTLS) дозволяє оптимізувати рух, а системами зв'язку на малій відстані (Dedicated Short Range Communication, DSRC) - спростити проходження пунктів оплати, митних терміналів. Системи V2V і V2I дозволяють організувати інтелектуальні транспортні мережі, налагодити ідентифікацію мікроточки, коли в непримітних місцях наклеюється мітка, що містить персональний ідентифікаційний номер автомобіля VIN, що в поєднанні з технологією RFID скоротить можливості викрадення.

Телекомунікації.

IoT відкриває можливості для об'єднання різних телекомунікаційних технологій з метою надання сервісів нового типу. Передбачається інтеграція глобального цифрового мобільного стільникового зв'язку GSM з комунікаціями ближнього радіусу дії (Near Field Communication, NFC), персональними мережами на базі Bluetooth, бездротовими локальними мережами, бездротовими сенсорними мережами стандарту ZigBee в поєднанні з системою глобального позиціонування і технологією ідентифікації абонента (SIM-карти ). Така інтеграція дозволить сервісам долати кордони різних адміністративних доменів і утворювати необхідні користувачу композиції.

Розумні будинки.

Сьогодні уявлення про розумний будинок поширюється на дорогі офіси, а IoT демократизує ці можливості перш за все за рахунок використання масових продуктів (станеться приблизно те ж, що було з переходом від мейнфреймів до ПК).

Близькі за змістом перетворення можливі в медицині, в техніці догляду за хворими, в фармацевтиці, в різних областях виробництва, в страхуванні і т. д.

Навігація всередині будівель. Як відомо, сигнал GPS погано взаємодіє з металевими перекриттями сучасних торгово-розважальних і ділових центрів. ГЛОНАСС до них відноситься не менш чутливо. Загалом, сигнал "не пробиває". У той же час інші заклади (ну, хто так будує ?!) являють собою повноцінні лабіринти, причому, іноді здається, що неевклідової геометрією будівельники зовсім не гребують. Заблукати в таких собі ТРЦ можна легко.

Рішення: розставляємо маячки в різних місцях ТЦ із застосуванням цвяхів і шурупів (щоб не потягли), пишемо додаток-навігатор, який зчитує показання сигналів маячків і намагається методом трилатирації \ полігонометрії визначити ваше положення в просторі. Потрібно тільки зєднання з інтернетом, щоб отримати координати і UUID маячків. Або не потрібен - ввести заздалегідь, а додаток просто періодично оновлювати.

Зрозуміло, великої точності визначення місцезнаходження не одержати, але плюс-мінус десять метрів в приміщенні досить, щоб знайти дорогу до виходу.

Виробничий процес. Це для таких виробництв, де оперують великими складальними одиницями. Або для логістичних центрів з контейнерами, наприклад. У контейнер ставиться маяк, а зчитувати їх можна як стаціонарними постами, так і мобільними пристроями - підійшов зі смартфоном до контейнера і тут же отримуєш дані про нього. І не потрібно нічого сканувати і / або зчитувати. Власне, рішення вже описано.

Хронологгер - а якщо з попереднього варіанту потік даних надсилати не в Фейсбук, а в корпоративну систему, то можна створити систему обліку часу і писати статистику переміщення співробітників з метою оптимізації процесів. Потрібно тільки не акцентувати увагу на заохоченні / покаранні, а зробити процес робочих веселим, але корисним.

Якщо забезпечити маячки будь-яким датчиком, який змінює значення інформації що “cвітиться” (це можна зробити як раз за допомогою змінних major і minor, що входять в UUID), то з'являється можливість організації моніторингу навколишнього середовища "за недорого". Обмеження - радіус дії маяка. Якщо використовувати прості, неенергоємнні датчики типу "контакт", то на терміні служби батарейки маячка це ніяк не відіб'ється. Можливість підключення таких датчиків, наприклад, у Kontakt.io є.

Мобільні платежі можна зробити більш безпечними ввівши третю дозвільну категорію для фіксації угоди - тепер до "мати" (фізичний носій) і "знати" (пароль / пін-код) можна ввести ще і "перебувати". Айбікон може використовуватися в якості тригера місцезнаходження фізичного носія. Сценарій приблизно такий: ви бронюєте місце в кінотеатрі і оплачуєте його. Але гроші з вашого рахунку не спишуться, поки ви зі своїм смартфоном і відповідним додатком не з'явитесь особисто в кінотеатр. Як тільки прийшли, і ваш смартфон зафіксував близькість відповідного маяка - дається сигнал з проведення транзакції. Нам такий сценарій здається більш ніж зручним. А якщо ідею розвинути і прикласти, наприклад, до міського транспорту, то виходить наступна схема - підписався на послугу в місцевому трамвайно-тролейбусному управлінні, які розставили маячки у всіх своїх ТЗ. Далі залишається тільки здійснювати оплату за проїзд при вході в салон.

Ще кілька прикладів IoT речей в реальній реалізації:

• Смарт-годинник, фітнес-трекери - легко синхронізуються з мобільними пристроями, з їх допомогою ви можете відстежувати деякі дані вашого здоров'я (пульс, активність сну і т.п.), а також на них легко відображаються повідомлення з мобільних пристроїв, що є дуже зручним фактором.

• За допомогою програми CitySense, легко отримати дані в режимі реального часу для зовнішнього освітлення, і саме на їх основі включаються або вимикаються вуличні ліхтарі.

• Чи існують також різні додатки, що дозволяють контролювати сигнали руху і доступність паркування в місті.

• Також є безліч додатків для моніторингу стану здоров'я пацієнтів.

Грунтуючись на порівнюваних даних, служби контролюють дозування ліків. Такі програми, як UroSense, можуть контролювати рівень рідини в тілі пацієнта і в залежності від необхідності ініціюють прийом рідини. У той же час дані можуть передаватися бездротовим способом на монітори лікарів.

Нижче наведені деякі з найбільш використовуваних технологій в IoT:

RFID [Радіочастотний код] і EPC [Електронний код продукту]

NFC [Near Field Communication] використовується для включення двосторонніх взаємодій між електронними пристроями і в основному використовується для безконтактних транзакцій.

Bluetooth: використовується там, де досить коротких повідомлень, щоб уникнути проблем.

Z-Wave: це низькочастотний радіозв'язок. Перш за все він використовується для домашньої автоматизації, управління лампами і т. д.

WiFi: найбільш використовувана технологія для Інтернету речей. У локальній мережі це допомагає легко передавати файли, дані та повідомлення.

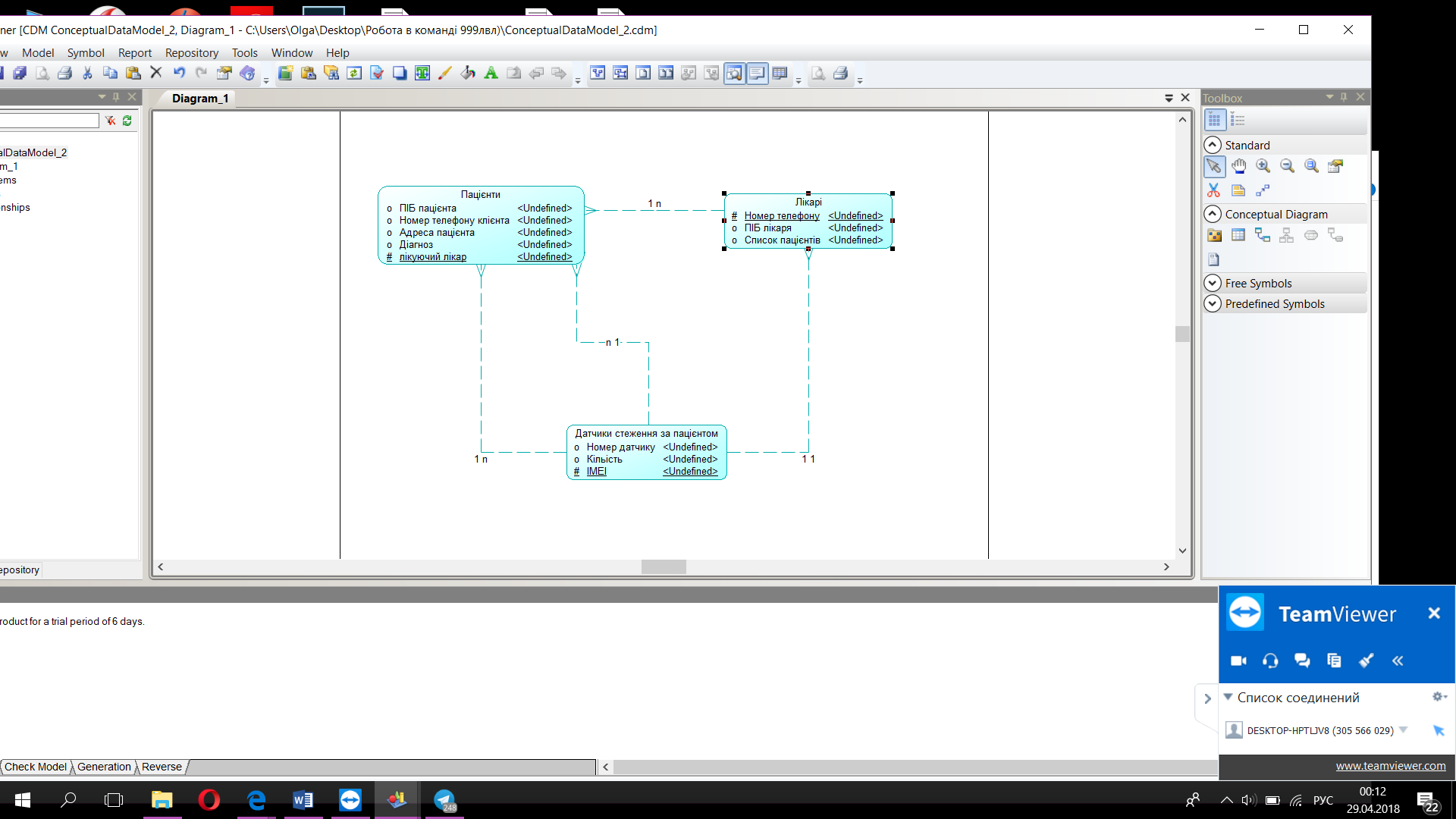
Останній наведений приклад реальної реалізації ми якраз і розглянемо в даному проекті.

Візьмемо систему стеження за здоров'ям, в якій прилад контролює здоров'я пацієнта, частоту серцевих скорочень, дані про споживання рідини і відправляє звіт лікарям. Ці дані записуються в систему і можуть бути переглянуті в міру необхідності.

Її можна запускати віддалено з будь-якого пристрою, до якого підключено медичне обладнання.

Розглянемо реалізацію за допомогою моделей.

# Реалізація за допомогою моделей



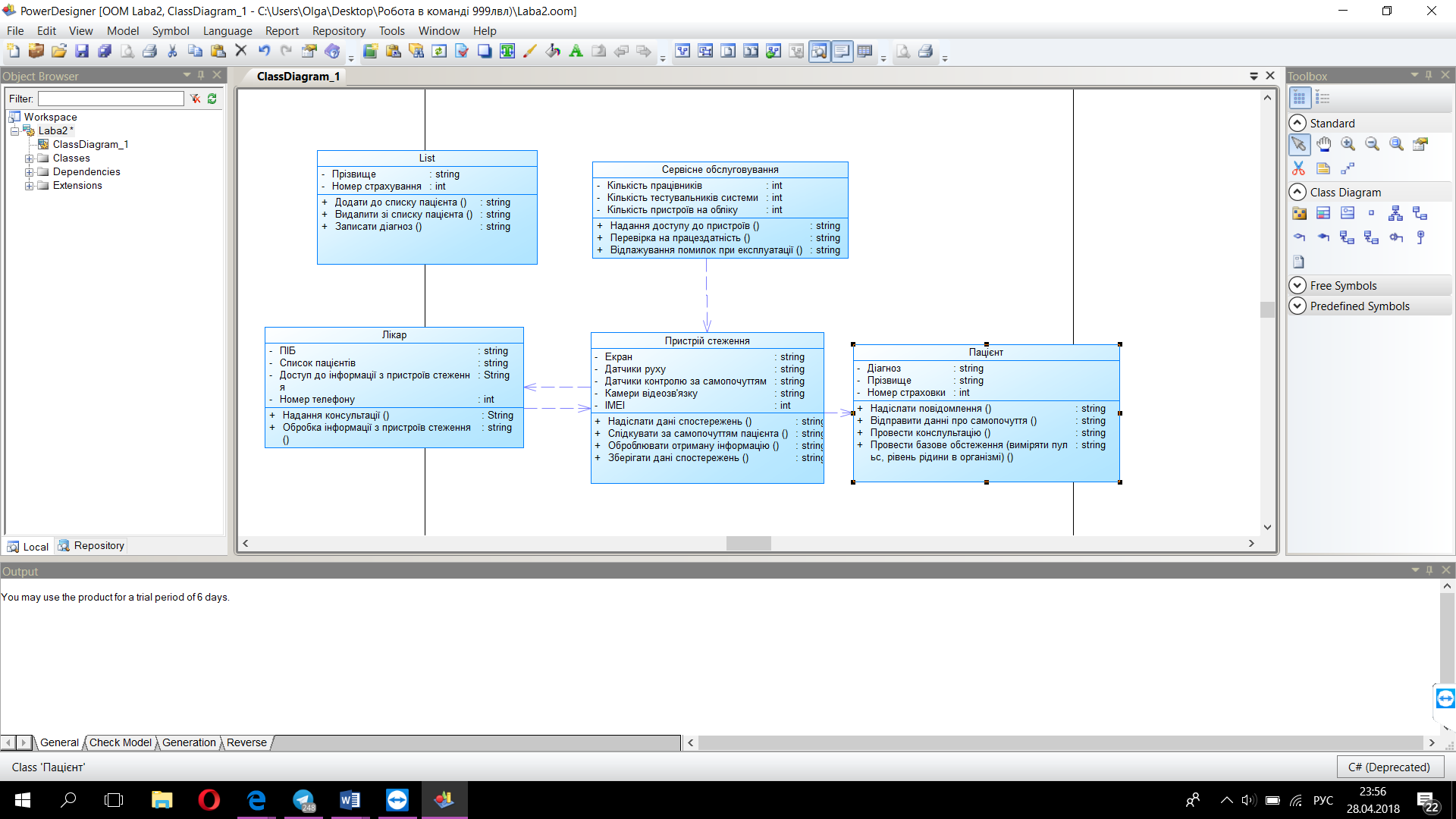
Схема 1. «Концептуальна модель (CDM) системи IoT»

Схема 2. «Діаграма класів (ClassDiagram) системи IoT»

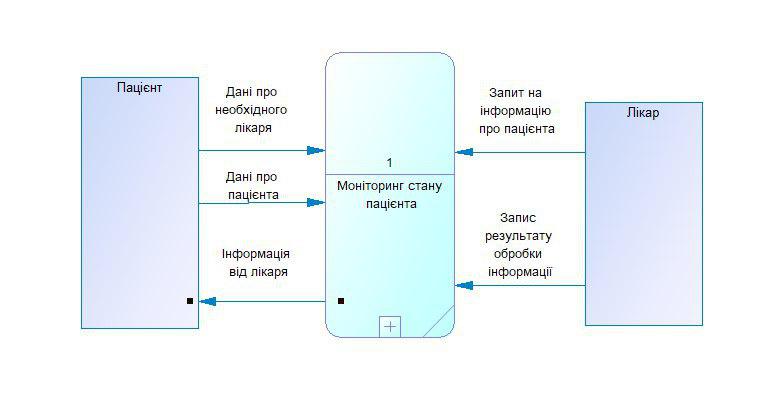
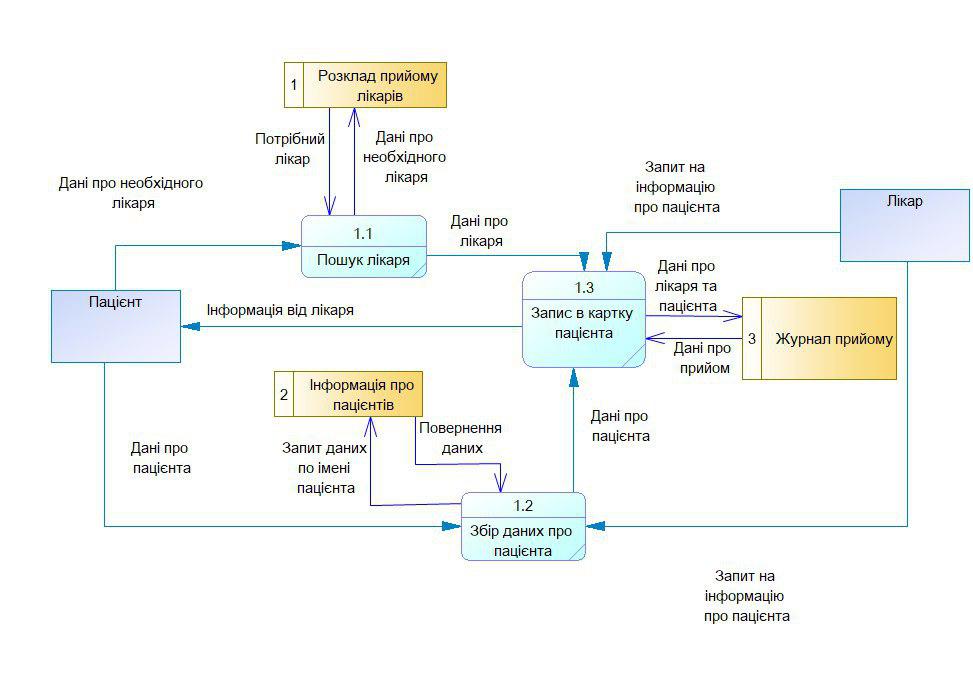


Схема 3. Частина 1. «Діаграма потоків даних (Data Flow Diagram)»

Схема 3. Частина 2. «Діаграма потоків даних (Data Flow Diagram)»

Розглянемо дерево функцій системи:

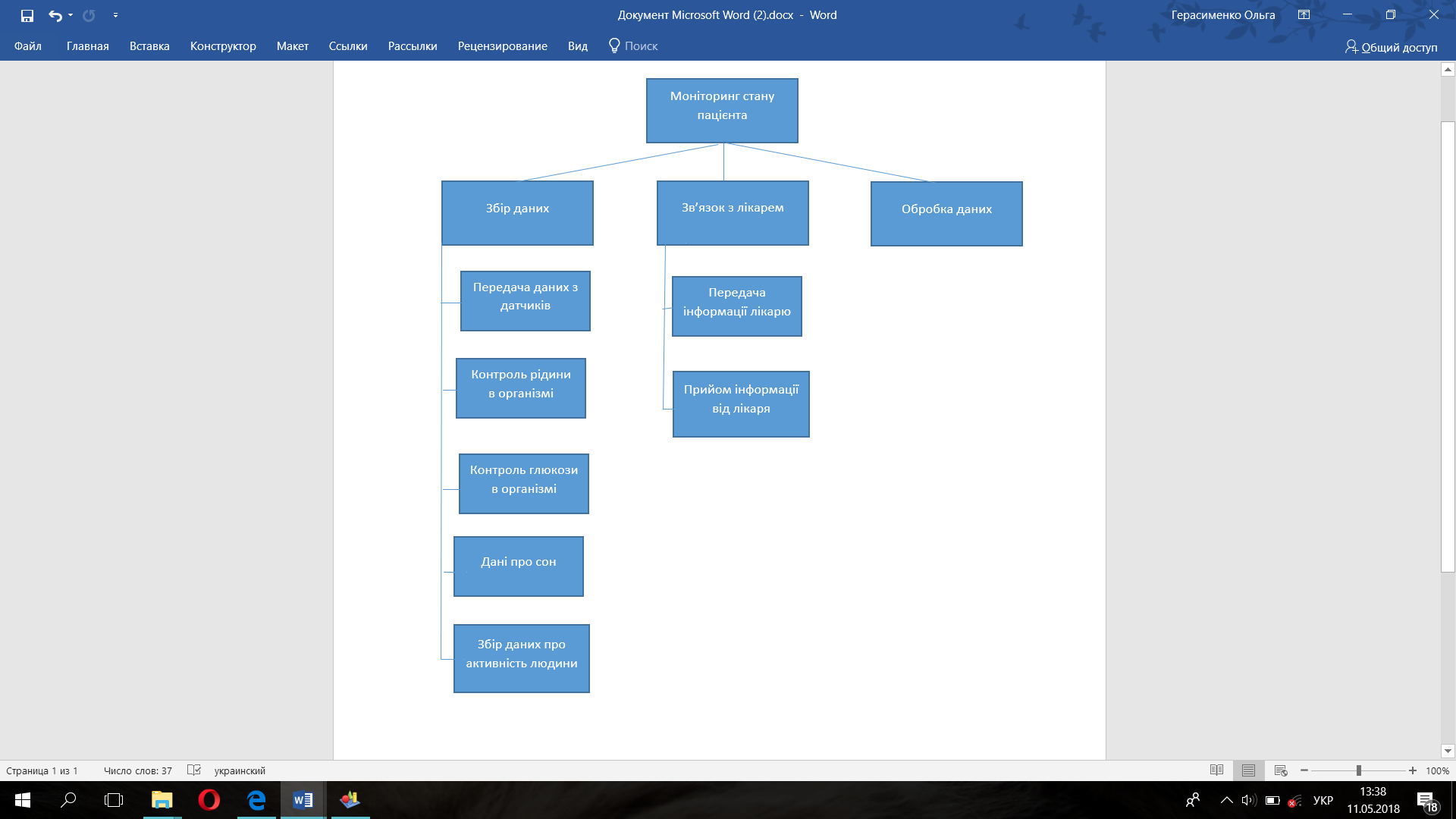


Схема 4. «Дерево функцій»

# Детальний опис системи стеження за здоров’ям

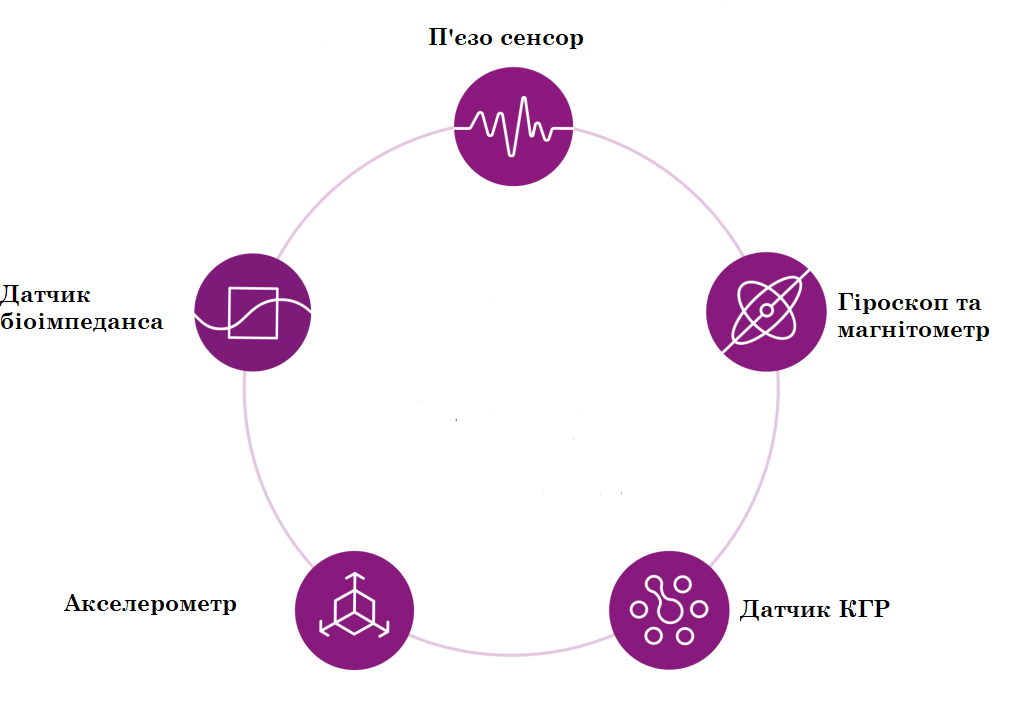
Система не відноситься до розряду «магічних артефактів», а працює за допомогою складної апаратно-програмної технології. Куди більш складною, ніж у фітнес-браслетах. Будучи технічно непростим пристроєм, вона має певні обмеження в роботі і вимагає точного дотримання інструкції по експлуатації. Якщо їх дотримуватися, то і показання приладу будуть досить точними. (див. Рис.1)

Рис. 1

Всі секрети криються в унікальному математичному апараті, за допомогою якого відбувається аналіз біоімпеданса, а також знімаються одночасно з ним показників ще з ряду датчиків. Крім уже згаданого вище датчика біоімпеданса, в систему вбудований датчик КГР (шкірно-гальванічної реакції), пьезодатчик (для вимірювання пульсу), акселерометр, гіроскоп і магнітометр.

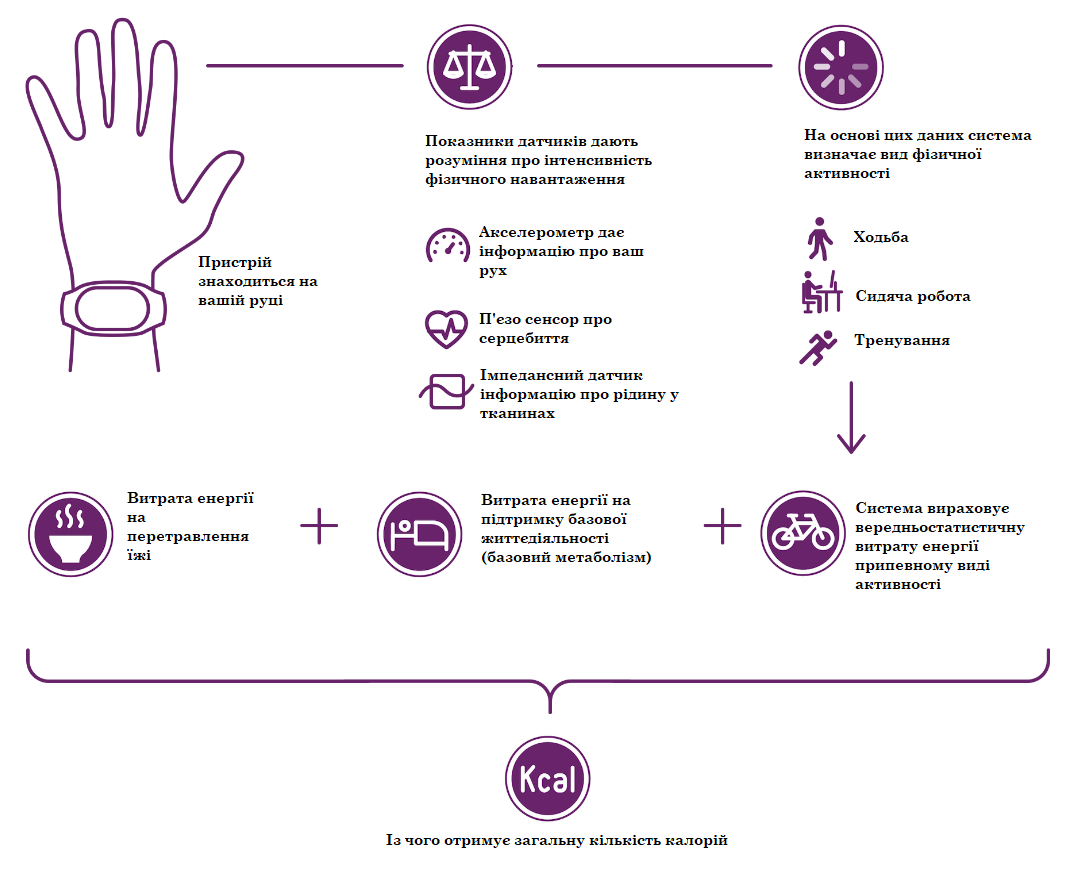


Рис. 2

Технологія відстежує зміни рівня глюкози в організмі, а не точну її кількість. При підвищенні концентрації глюкози клітини починають вбирати глюкозу, вивільняючи воду. Посилаючи високочастотні і низькочастотні сигнали через шкіру, датчик біоімпеданса вимірює об'єм рідини, що вивільняється і вбирається клітинами (див. Рис.2).

В результаті аналізу інформації, що надходить, програмно-апаратний комплекс надає користувачеві дані про засвоєні організмом калорії, склад нутрієнтів (кількості білків, жирів і вуглеводів), а також про рівень води в організмі. Пристрій також вміє не тільки рахувати витрату калорій, але ще і враховувати базальний метаболізм - кількість енергії, необхідну для забезпечення основних функцій організму в спокої. Підсумовуючи ці дані, програма знаходить поточний енергетичний баланс, за яким можна визначити, чи не потрібно вам додати або, навпаки, знизити калорійність вашого раціону їжі (див. Рис.3)

Рис. 3

Крім того, на підставі даних з датчиків інформації, програмний комплекс автоматично визначає, коли ви спите, вираховує фази сну і дає рекомендації по його тривалості. Також браслет проводить аналіз прояву ваших емоцій і вираховує рівень стресу. Ну а вмінням підраховувати кроки вже нікого не здивуєш. Звісно, пристрій робить і це.

А тепер докладно розглянемо роботу окремих елементів нашої системи.

П’єзо сенсор

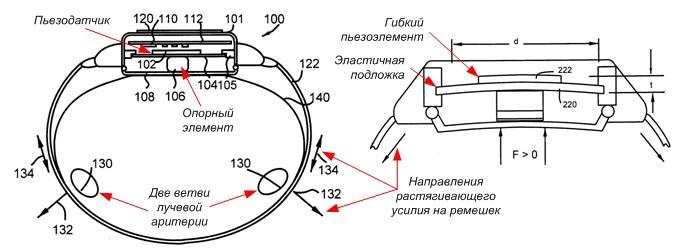
Ідея способу на основі п'єзоелемента добре розкрита в патенті Wrist plethysmograph US 20070287923 A1. На зображенні показана схема пристрою. На датчик працює вся конструкція пристрою - ремінець забезпечує розтяжне зусилля на краях п’єзодатчика і виконує роль своєрідної манжети, корпус надає необхідну жорсткість і опору (див. Рис. 4)

Рис. 4

Обчислення пульсу по сфігмограммі таке ж, як в плетизмографії, так як одержувані пульсові криві практично ідентичні.

При практичній реалізації можуть бути нюанси, пов'язані з індивідуальними особливостями. Але система була досліджена таким чином, що вивчалася залежність амплітуди пульсового сигналу від сили тиску пьезодатчика, індивідуальних параметрів руки пацієнтів і т.п. Датчик до зап'ястя підводився кроковим двигуном зі зворотним зв'язком і, таким чином, нормувалося сила натискання. Розкид індивідуальних тисків досить високий, а також могли бути проблеми з реєстрацією у людей з надмірною вагою зі збільшеною товщиною жирового підшкірного шару, але це неприпустимо в такому пристрої.

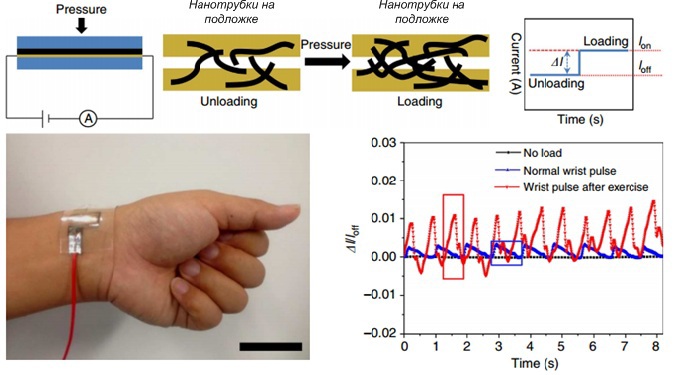
Є концепти і наукові дослідження щодо застосування подібних датчиків. Ось приклад, де описана реалізація ультратонкого гнучкого датчика на основі золотих нанотрубок (див. Рис.5).

Рис. 5

При вигині поверхні датчика виникає дельта струму. Цією дельти досить, щоб фіксувати динамічну складову тиску від 13 Па (для порівняння: 1 Па (Н / м2) дорівнює 7,50062 мкм ртутного стовпа).

Датчик фіксується на шкірі в районі запьястя и реєструє пульсові хвилі. Дослідження датчика показало, що на амплітуду сигналу впливає рівень поточного звукового фону, наприклад голос та музика, що було досить очікувано.

Ось ще приклад датчика на основі 2D-масиву п’єзокомірок (див. Рис.6).

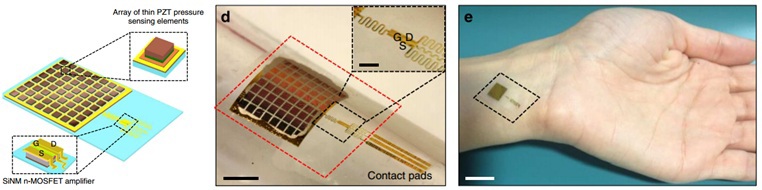


Рис. 6

Цей датчик більш досконалий і функціонально закінчений: містить схему первинного посилення і має контакти для підключення. Ось приклади наклейки датчика на різні частини тіла (див. Рис.7).

Якщо знімати сигнал з зап'ястя і шиї, то можна реалізувати метод вимірювання кров'яного тиску на основі обчислення відносної швидкості пульсової хвилі (pulse wave velocity (PWV)) між артерією на шиї і артерією на зап'ясті (щодо зрушення фаз між сигналами). Власне датчик позиціонується для вирішення саме цього завдання.

Рис. 7

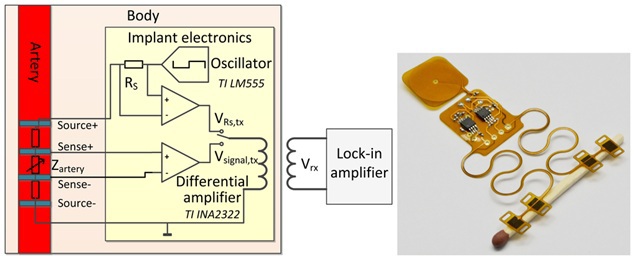
Наступний приклад концепту імплантуємого датчика для контролю кровообігу артерії. Активний датчик поміщається прямо на артерію, з хост-девайсом спілкується по індуктивному зв'язку. Це дуже цікавий і перспективний підхід. Принцип роботи зрозумілий з малюнку. Сірник показаний для розуміння розміру. Використовується 4-х точкова схема реєстрації та гнучка друкована плата (див. Рис. 8).

Рис. 8

*Body-тіло*

*Implant electronics-імплантова електроніка*

*Oscillator-осцилятор*

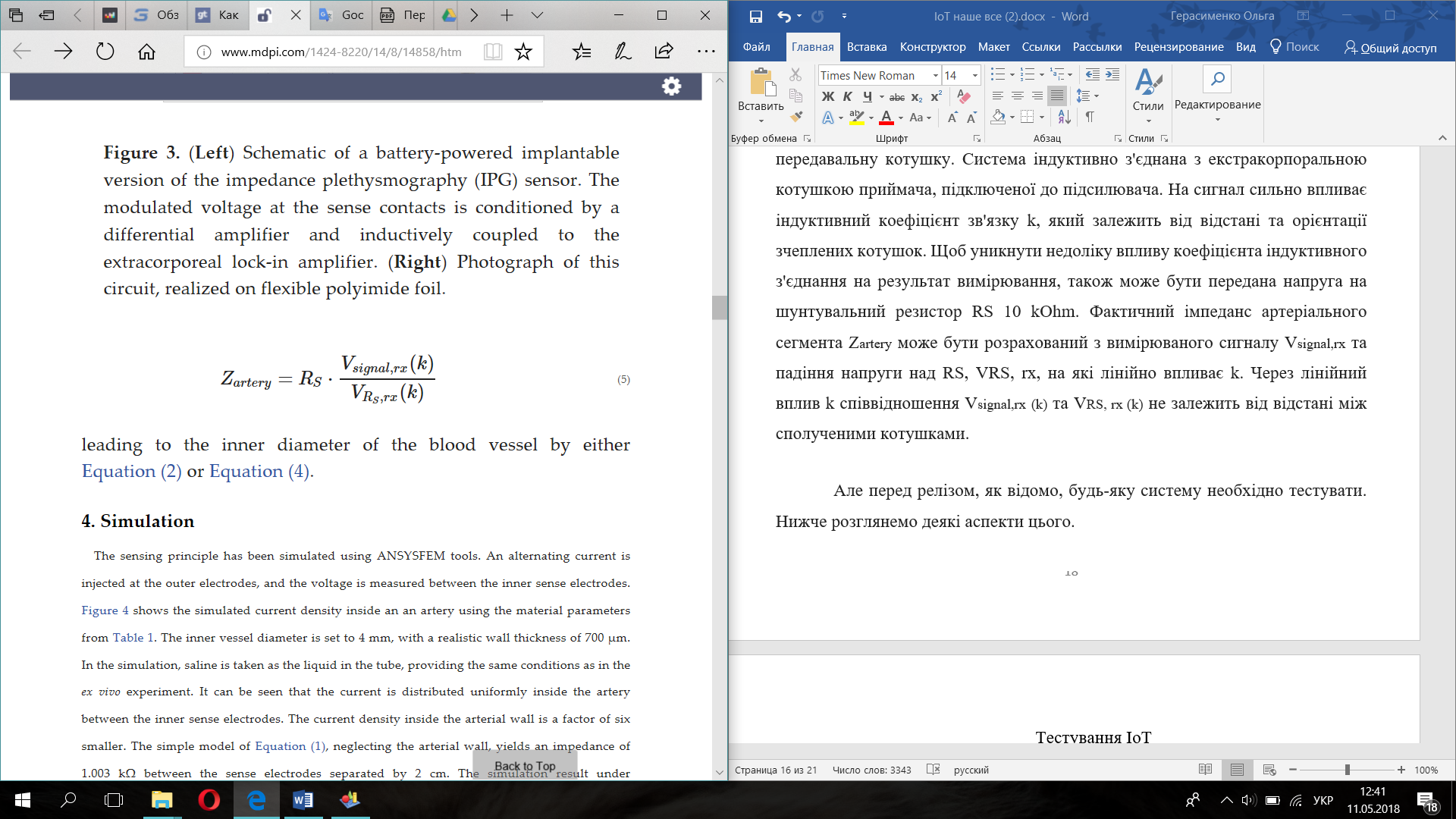
*Differential amplifier-диференціальний підсилювач*

*Source-джерело*

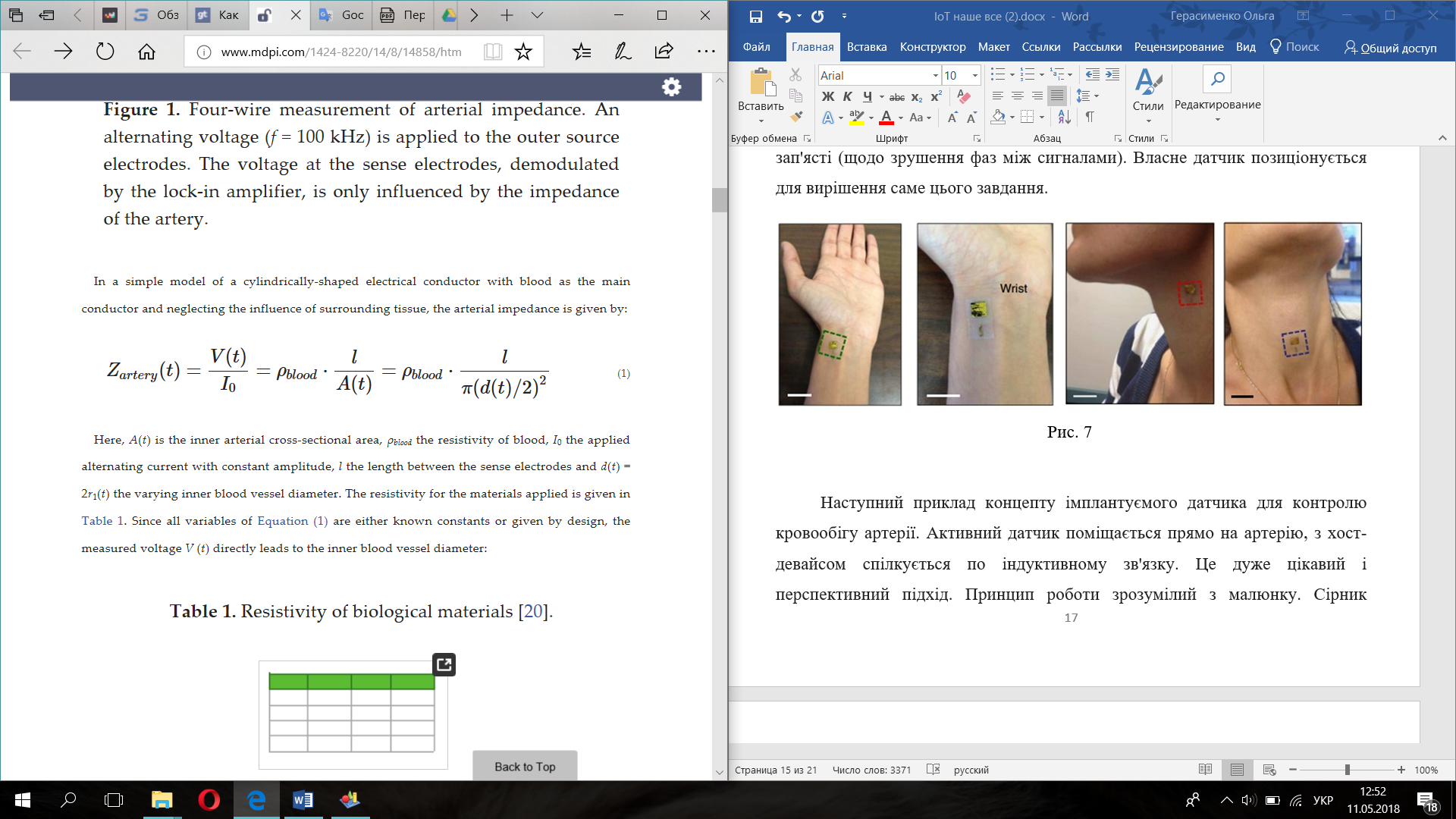
*Sense-сенсор*

*Lock-in-amplifier-фіксований підсилювач*

Ми пропонуємо бездротове передавання модульованих аналогових даних. Імплантована система живиться від акумулятора та генерує сигнал змінного струму для вимірювання, як показано на схемі на рисунку 8. Сигнал з електродів обумовлений диференційним підсилювачем та наноситься на передавальну котушку. Система індуктивно з'єднана з екстракорпоральною котушкою приймача, підключеної до підсилювача. На сигнал сильно впливає індуктивний коефіцієнт зв'язку k, який залежить від відстані та орієнтації зчеплених котушок. Щоб уникнути недоліку впливу коефіцієнта індуктивного з'єднання на результат вимірювання, також може бути передана напруга на шунтувальний резистор RS 10 kOhm. Фактичний імпеданс артеріального сегмента Zartery може бути розрахований з вимірюваного сигналу Vsignal,rx та падіння напруги над RS, VRS, rx, на які лінійно впливає k. Через лінійний вплив k співвідношення Vsignal,rx (k) та VRS, rx (k) не залежить від відстані між сполученими котушками.

Розрахунок відбувається за допомогою наступної формули:

У простій моделі циліндричного електропровідника можна знехтувати впливом зовнішніх тканин тому, що кров являється головним провідником і артеріальний опір вираховується наступним чином:



Де A (t) - внутрішня площа артеріального поперечного перерізу, ρ - коефіцієнт питомого опору крові, I0 - застосовуваний змінний струм з постійною амплітудою, l - довжина між сенсорними електродами та d (t) = 2r1 (t) - змінний внутрішній діаметр судин крові. Високостійкість прикладеного матеріалу наведена на рисунку 9.

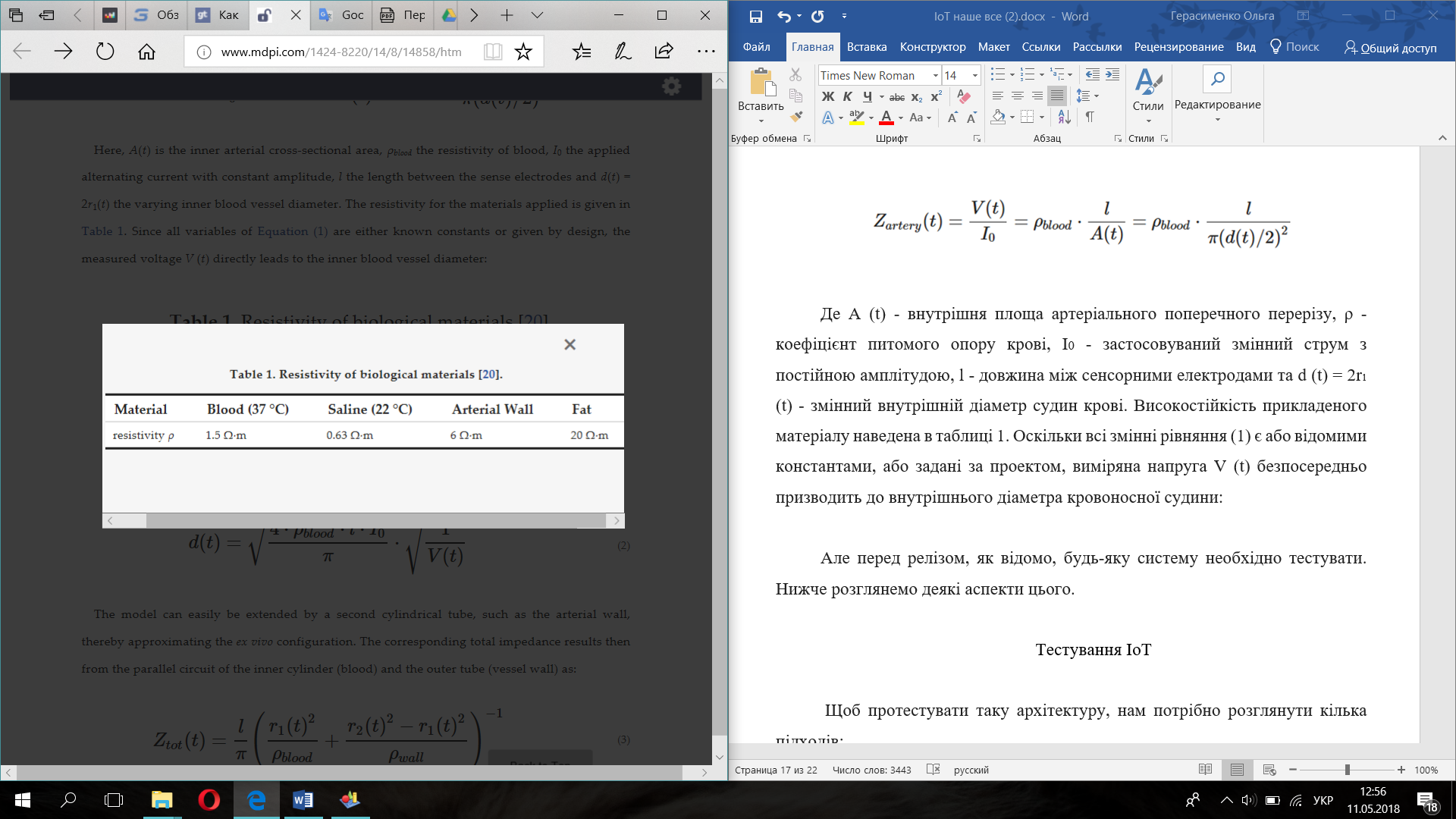
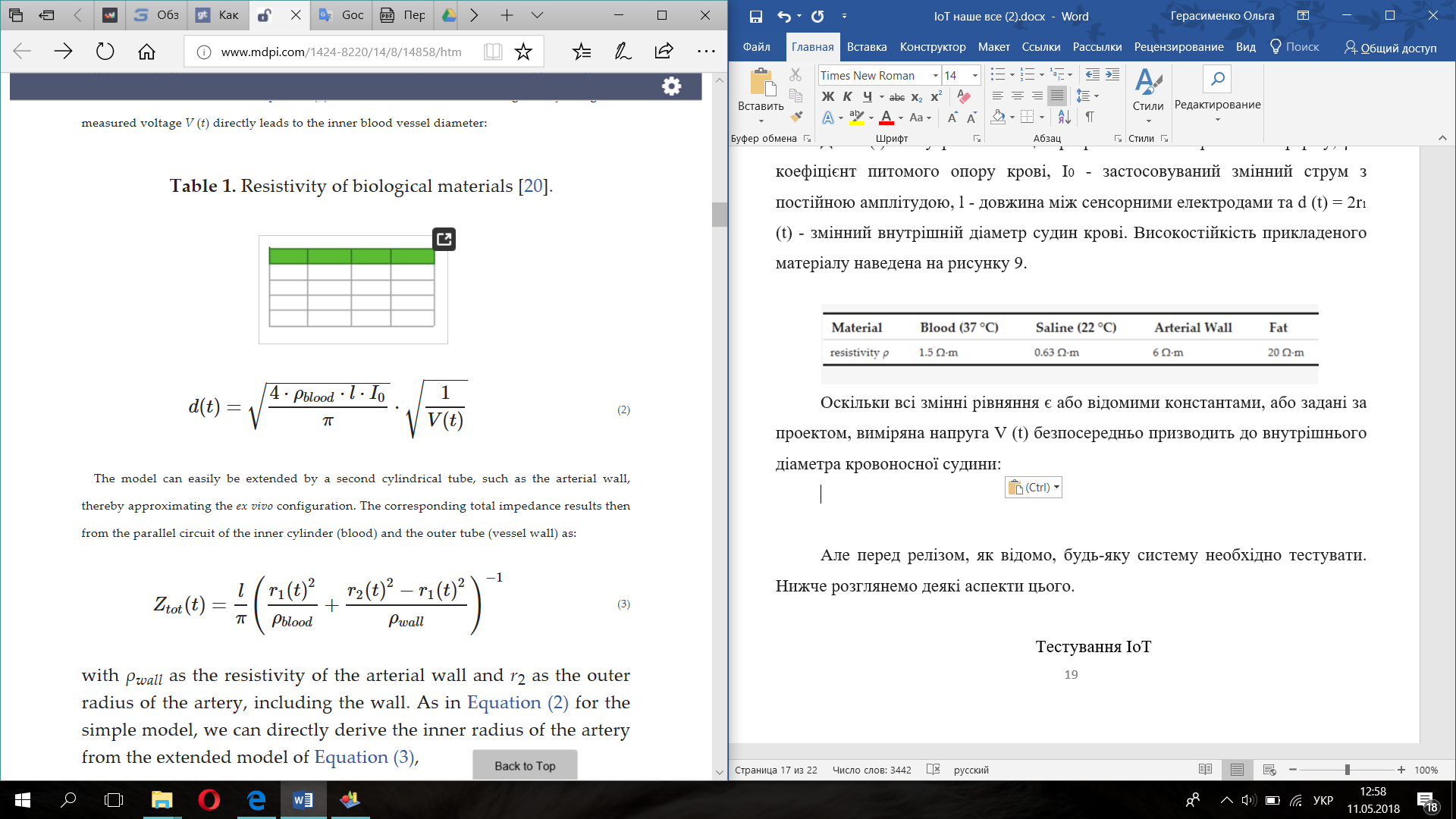
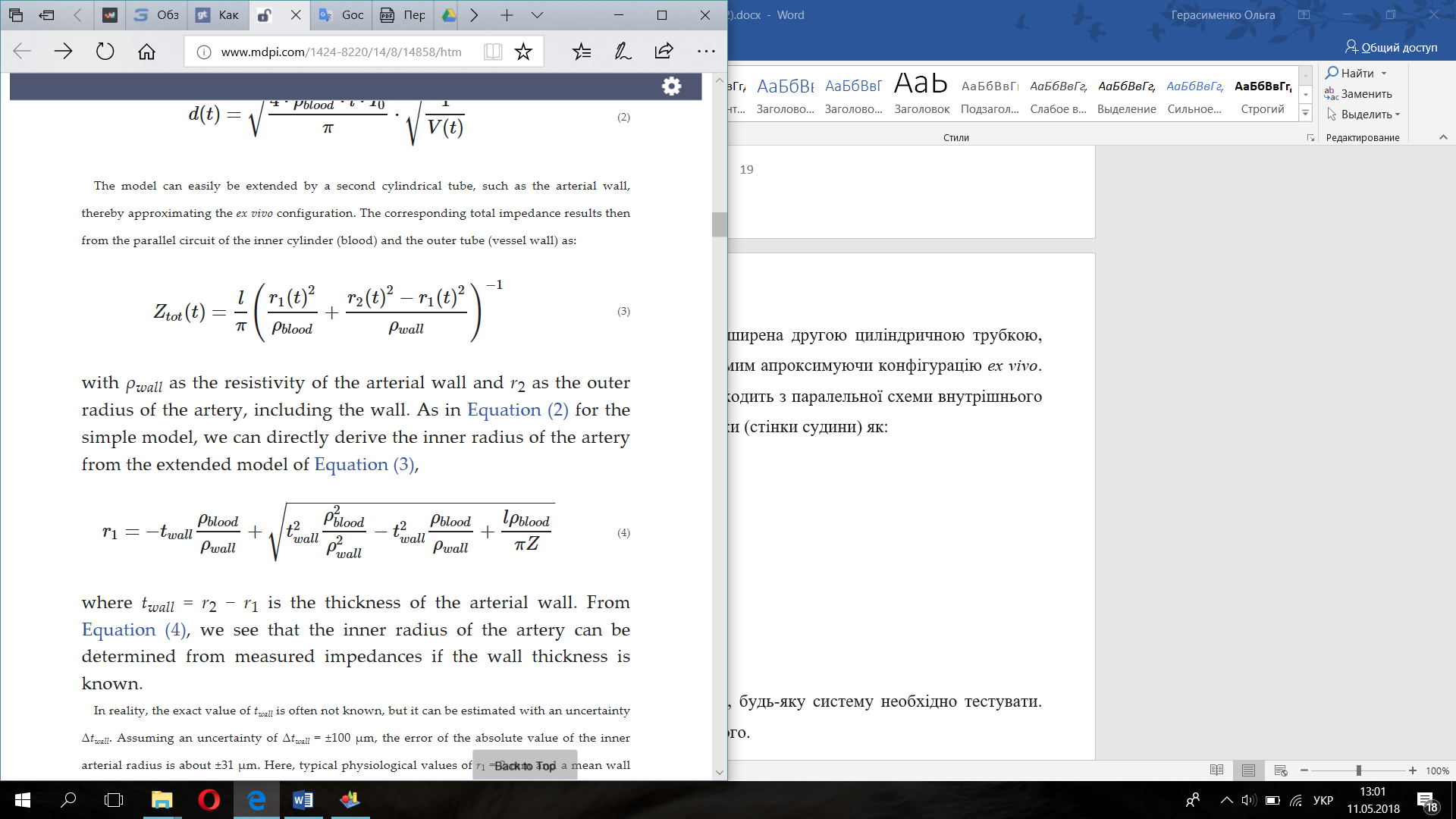


Рис. 9

Оскільки всі змінні рівняння є або відомими константами, або задані за проектом, виміряна напруга V (t) безпосередньо призводить до внутрішнього діаметра кровоносної судини:



Модель легко може бути розширена другою циліндричною трубкою, такою як артеріальна стінка, тим самим апроксимуючи конфігурацію *ex vivo*. Відповідний загальний імпеданс виходить з паралельної схеми внутрішнього циліндра (крові) та зовнішньої трубки (стінки судини) як:



Але перед релізом, як відомо, будь-яку систему необхідно тестувати. Нижче розглянемо деякі аспекти цього.

# Тестування IoT

Щоб протестувати таку архітектуру, нам потрібно розглянути кілька підходів:

1. Зручність використання:

Ми повинні переконатися в можливості коректного використання кожного з даних нам пристроїв.

Апарат повинен бути досить мобільним, щоб користувач легко міг перенести його в будь-яке місце. Обладнання повинно бути досить розумним, щоб виводити не тільки повідомлення, але також повідомлення про помилки, попередження і т. д.

Система повинна мати можливість реєструвати всі події, щоб забезпечити ясність картини в цілому або ж мати доступ до бази даних, також повідомлення повинні відображатися на дисплеї і повинна бути можливість перенесення даних на екрани моніторів / мобільних пристроїв.

Зручність використання в плані відображення даних, обробки даних, введення завдань з різних пристроїв повинно бути ретельно перевірено.

1. Безпека IoT:

Інтернет речей орієнтований на те, що всі підключені пристрої / системи працюють на основі доступних даних.

Коли справа доходить до потоку даних між пристроями, завжди є ймовірність, що дані можуть бути доступні або прочитані при передачі.

З точки зору тестування нам потрібно перевірити, захищені / шифруються дані при переході з одного пристрою на інший.

Там, де є призначений для користувача інтерфейс, ми повинні переконатися, що на ньому є захист паролем.

1. Можливості підключення:

Оскільки це прилад для охорони здоров'я, підключення грає життєво важливу роль. Система повинна бути доступна весь час і повинна мати безшовну зв'язок з користувачами.

Ще один момент, в незалежності від того, наскільки надійна система і мережу, є ймовірність, що система відключиться. Ми повинні перевірити автономні умови роботи. Як тільки система недоступна в мережі, має надходити попередження, яке може пробудити лікарів, щоб вони могли вручну стежити за станом здоров'я, незалежно від системи. Також в системі повинен бути механізм, який дозволить зберігати всі дані в ньому протягом певного періоду. Після того, як система увійде в роботу, всі ці дані повинні поширитися. Втрата даних є неприпустимою.

1. Ефективність:

Система для охорони здоров'я повинна бути досить стійка.

Тестування виконується для 2-10 пацієнтів за раз, і дані поширюються на 10-20 пристроїв.

Коли до неї підключено 180-200 пацієнтів, поширювані дані набагато більше, ніж були в тестовому варіанті. Нам необхідно переконатися, що система працює однаково, навіть якщо поширюються такі великі обсяги даних.

Ми також повинні перевірити утиліту моніторингу для відображення використання системи, енергії, температури і т. д.

Тестування на сумісність:

Виходячи з того, що архітектура системи IoT є досить складною, тестування на сумісність є обов'язковим.

Тестування декількох версій операційної системи, типів браузерів і відповідних версій, генераторів пристроїв, режимів зв'язку [наприклад: Bluetooth 2.0, 3.0] необхідно для повного тестування сумісності IoT.

Експериментальне тестування:

Під час експериментального тестування система піддається впливу обмеженого числа користувачів, але якщо система працює нормально в таких умовах, це все одно не дає 100-відсоткову гарантію на правильну роботу в реальному часі. Але відгуки користувачів важливі, оскільки на основі них система допрацьовується і приймає той вид, в якому її бачитимуть інші користувачі.

Тестування оновлень:

IoT - це комбінація кількох протоколів, пристроїв, операційних систем, прошивки, обладнання, мережевих шарів і т. Д.  
Коли виконується оновлення, будь то для системи або для будь-якого з задіяних елементів, як зазначено вище, слід провести ретельне регресійне тестування.

Проблеми, з якими стикається тестувальник в IoT, полягають в наступному:

1. Апаратно-програмна сітка

IoT - це архітектура, яка тісно пов'язана з різними апаратними та програмними компонентами. Важливу роль відіграють не тільки програмні додатки, але і апаратні - датчики, шлюзи зв'язку і т. Д.

1. Модуль взаємодії з пристроєм

Оскільки ця архітектура пов'язує різні набори апаратного і програмного забезпечення, обов'язкова вимога - їх взаємодія один з одним в режимі реального часу. Але ось такі деталі, як безпека, зворотна сумісність, проблеми з оновленням, стають проблемними для тестувальників.

1. Інтерфейс

IoT поширюється по пристроях, що належить до кожної платформі [iOS, Android, Windows, Linux]. Тестування на деяких пристроях може бути виконано без особливих проблем, але тестування на всіх можливих пристроях практично неможливо.

Ми не можемо не брати до уваги можливість доступу до призначеного для користувача інтерфейсу з пристрою, якого у нас немає. Якраз таки тестування цього стає складним завданням.

1. Доступність мережі

Мережеве з'єднання грає життєво важливу роль, оскільки IoT - це дані, які передаються весь час на швидких швидкостях. Архітектура IoT повинна тестуватися в усіх видах здійснювати підключення до мережі / швидкостей.  
Щоб перевірити це, віртуальні мережеві симулятори в основному використовують зміни мережевого навантаження, підключення, стабільності і т. д. Але в реальному часі дані / мережа завжди є непередбачуваними і тестувальники не завжди можуть передбачити як поведе себе система.

Інструменти тестування IoT

Існують різні інструменти, які використовуються під час тестування систем IoT. Вони можуть бути класифіковані на основі цілей і приклади наведені нижче:

1. Програмне забезпечення:

Wireshark: це додаток з відкритим вихідним кодом, що використовується для відстеження трафіку в інтерфейсі, вихідних / цільових адресах хоста і т. д.

Tcpdump: робить ту ж роботу, що і Wireshark, крім цього, у нього немає графічного інтерфейсу. Це утиліта, заснована на командному рядку, яка допомагає користувачеві відображати TCP / IP і інші пакети, які передаються або приймаються через мережу.

1. Устаткування:

JTAG Dongle: Це схоже на відладчик в додатках для ПК. Це допомагає налагоджувати код цільової платформи і показувати крок за кроком.  
Цифровий запам'ятовує осцилограф: використовується для перевірки різних подій з відмітками часу, збоїв в джерелі живлення, перевірки цілісності сигналу.

Програмне забезпечення Defined Radio: використовується для емуляції приймача і передавача для широкого спектра бездротових шлюзів.

У світі, що розвивається IoT - це зростаючий ринок і має багато можливостей. Гаджет, що підтримує IoT, додаток смарт-пристрої і модуль зв'язку відіграють важливу роль у вивченні і оцінці продуктивності різних служб IoT. Поганий дизайн пристроїв і служб з підтримкою IoT може перешкоджати правильному функціонуванню додатки. А це, в свою чергу, негативно позначається на використанні користувачами.

Методи тестування IoT можуть відрізнятися в залежності від використовуваної системи / архітектури. Тестировщики повинні більше зосередитися на методі Test-As-A-User [TAAS], а не на тестах, заснованих на вимогах.

Тестування IOT може бути складним завданням, але в той же час дуже цікавим, адже команда тестувальників повинна впевнитися в правильній роботі такої складної сітки пристроїв, протоколів, обладнання, операційних систем, прошивки.

# Список використаної літератури

1. <https://3dnews.ru/954710>
2. <https://geektimes.com/company/darta_systems/blog/247100/>
3. <http://www.mdpi.com/1424-8220/14/8/14858/htm>
4. <http://www.mdpi.com/1424-8220/14/8/14858/htm>
5. <https://geektimes.com/company/dataart/blog/300781/>
6. https://3dnews.ru/wearable

Зміст

[Вступ. 3](#_Toc513891226)

[Приклади реалізації IoT 5](#_Toc513891227)

[Реалізація за допомогою моделей 9](#_Toc513891228)

[Детальний опис системи стеження за здоров’ям 13](#_Toc513891229)

[Тестування IoT 21](#_Toc513891230)

[Список використаної літератури 27](#_Toc513891231)