УДК 616.12

Нацевич М.В., студ., гр. БІ-20
Нікітчук Т.М., к.т.н., доц., зав. кафедри БІтаТ
Державний університет «Житомирська політехніка»

ФОНОКАРДІОГРАФІЧНА СИСТЕМА

У зв’язку з щорічним зростанням в Україні кількості серцево-судинних захворювань, і як наслідок − смертей від хвороб, пов’язаних з ними, актуальною задачею є удосконалення методів, що вже добре зарекомендували себе на практиці, в основному за рахунок вдосконалення електронної схемотехніки, алгоритмів обробки сигналів та методичних прийомів використання результатів, передачі їх на відстань (до лікарень з віддалених населених пунктів). Дистанційний моніторинг можна представити узагальненою схемою, що показаний на рисунку 1.

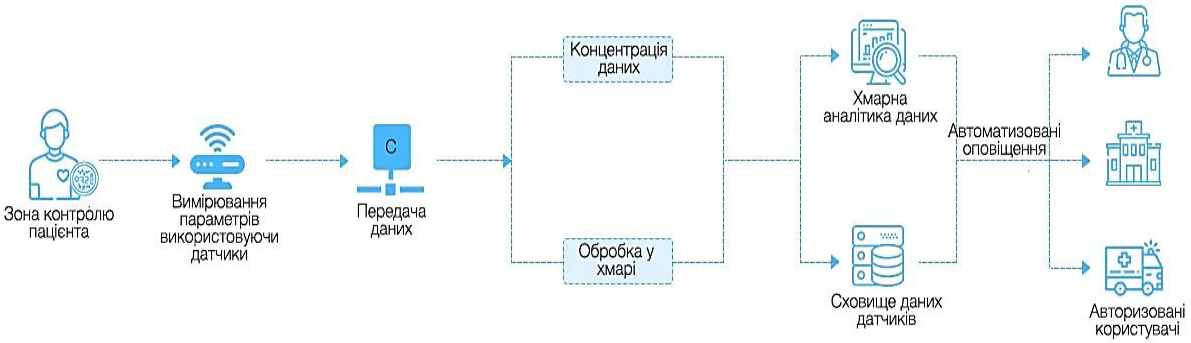


Рис. 1. Узагальнена схема передачі медичних даних на відстань

Сьогодні лікарями активно використовуються апаратурні методи реєстрації акустичних коливань, що характеризують якість роботи серцевого м'яза, клапанів серця, великих судин.

Фонокардіографія (ФКГ) – метод дослідження серця, заснований на реєстрації та аналізі звуків, які виникають при його роботі, та реєструються за допомогою відповідного приладу – фонокардіографа. В наш час, не дивлячись на все більші розповсюдження ультразвукових методів дослідження серця, ФКГ продовжує досить широко використовуватись, що пояснюється наступними його перевагами:

- ФКГ – неінвазивний, безпечний метод, який не має ніяких протипоказань;
- нові інформаційні технології дозволяють розширити діагностичні можливості ФКГ;
- для ФКГ потребується відносно недороге обладнання.

Принцип роботи апарату для ФКГ полягає в тому, що мікрофон, встановлений в точках аускультації серця на грудній клітині, перетворює механічні коливання в електричні. Спектр звуків серця у вигляді електричних сигналів надходить до підсилювача та фільтрів фонокардіографа. Після цього електричні сигнали переходять на відповідний канал реєструючого пристрою і записуються у вигляді фонокардіограми. В системі, що пропонується, буде реалізовано блок порівняння з базою фонокардіографічних сигналів та подальша передача отриманого результату на відстань, наприклад на сервер лікарні та/чи телефон пацієнта. Дана система дозволяє пацієнту проходити фонокардіографічне дослідження і одразу отримувати її результат в зручному вигляді у відповідному мобільному додатку. Структура фонокардіографічної системи складається з шести основних частин, які виконують такі функції:

1. Датчик: в його якості виступає мікрофон, що щільно прилягає до поверхні грудної клітини, він приймає та перетворює шуми серця в електричні сигнали.
2. Підсилювач: отриманий з мікрофону сигнал надходить до підсилювача, який допомагає покращити подальшу фільтрацію.
3. Фільтр: «очищає» підсилений сигнал від шумів та виділяє потрібні в подальшому складові.
4. Аналого-цифровий перетворювач: перетворює вже відфільтрований аналоговий сигнал в цифровий. Процес відбувається в три розділених в часі етапи: 1) вибірка; 2) квантування; 3) кодування.
5. Блок порівняння та прийняття рішення: за допомогою попередньо встановленої, шляхом програмування, бази еталонів відбувається порівняння отриманого результату з тими, що знаходяться в базі та виводить його на монітор або надсилає користувачу.
6. Блок передачі даних: за допомогою бездротових технологій здійснюється передача отриманих даних на сервер, телефон лікаря або пацієнта.

Система, що пропонується, має на меті полегшити проведення фонокардіографічних досліджень, як для лікарів так і для пацієнтів, шляхом покращення обробки результатів та їх передачі на відстань.

УДК 533.9.07+615.847

Якімчук О.М., студ., гр. БІ-19
Науковий керівник: Коломієць Р.О., к.т.н., доц. кафедри БІтаТ
Державний університет «Житомирська політехніка»

РОЗРОБКА ГЕНЕРАТОРА ХОЛОДНОЇ ПЛАЗМИ ДЛЯ ВИКОРИСТАННЯ У МЕДИЦИНІ

В організмі людини оксид азоту (NO) має багато важливих біологічних функцій, які призводять до його регулятивної ролі в серцево-судинній, дихальній, травній та нервовій системах, грає ключову роль в лікуванні інфекцій, запалень та бореться з ростом ракових пухлин. Основним джерелом екзогенного оксиду азоту є технологія холодної плазми. У технології плазмотерапії використовується потік екзогенного оксиду азоту (плазмо-хімічний генезис), який нормалізує мікроциркуляцію, активує антиоксидантний захист та має антибактеріальний ефект. Все це разом не тільки значно зменшує розповсюдження інфекцій та запалень, а і стимулює регенерацію тканин. Холодна плазма вбиває бактерії краще ніж антибіотики. Під час обробки ран холодною плазмою створюється широкий спектр екологічно чистих частинок (NO, озон, УФ-випромінювання і т. д.), що знищують біологічно небезпечні забруднювачі – патогени і токсини.

До переваг використання холодної плазми в медицині відносять:

- можливість зупинити кровотечу, включаючи великі поверхні ;
- бактерицидна дія;
- можливість лікування у важкодоступних місцях;
- відсутність будь-якого жорсткого іонізуючого випромінювання;
- обладнання є цілком безпечним, за умови дотримання загальновизнаних заходів безпеки та правильного методичного використання.

При всьому різноманітті приладів для терапії холодною плазмою існує порівняно мало типів генераторів холодної плазми. За типом газу, який використовується у даних приладах, найбільш широко використовувались джерела холодної атмосферної, гелієвої та аргонової плазми. Найбільший інтерес представляють саме джерела атмосферної плазми, як найбільш універсальних. Їх головна перевага - відсутність потреби в газовому балоні (аеростаті) і здатність виробляти плазму безпосередньо з повітря.

Залежно від конструкції «запалювальної» частини генераторів холодної плазми можна виділити шість основних типів структур:

- діелектричний бар'єрний розряд (тип DBD) –розряд на між вкритою діелектриком поверхнею активного електрода та тілом людини;
- розряд «pin-to-hole» (тип PTH) – розряд між електродом у формі стрижня та у формі кільця з системою видування газу (plasma jet);
- гібридна конструкція (містить елементи як DBD, так і PTH типів);
- розряд між двома довгими паралельними електродами (plasma blanket);
- п'єзоелектричний генератор;
- ковзний дуговий плазмотрон.

Найбільш поширеними є типи генераторів PTH та DBD.

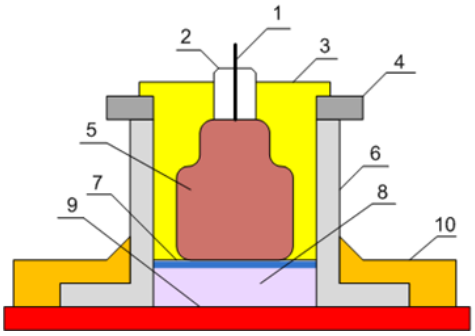
Для своєї бакалаврської роботи я обрав тип DBD.

Апарат для генерування холодної плазми складається з п'яти основних частин:

1. Блок живлення;
2. Генератор високочастотного сигналу;
3. Підсилювач потужності;
4. Високовольтний блок;
5. Система формування газового розряду.

Dielectric barrier discharge (DBD)

Система формування газового розряду генератора холодної плазми типу DBD (рис. 1) складається з надійно ізольованого масивного мідного електрода, який знизу має пласку форму і вкритий тонким діелектриком. Площа електрода дорівнює площі оброблення плазмою. Електрод поміщений у міцний полікарбонатний корпус, верхня частина якого конструктивно зроблена так, щоб за неї було зручно братися рукою, а нижня формує надійну опору для того, щоб весь електрод повністю накрив рану і відстань від діелектрика до рани становила 0,7…1,5 мм (висота розрядного проміжку 8 на рис. 1). Таким чином, другим електродом виступає тіло пацієнта. Для захисту від ураження електричним струмом служить діелектрик (позн. 7 на рис. 1) і висока частота робочої напруги генератора плазми. Для отримання розряду, необхідного для створення плазми, потрібні високі напруги (до 10…15 кВ). Споживання енергії становить від 10 до 100 Вт.



1 – вхід високої напруги;
2 – перший шар ізоляції (м'який пористий діелектрик);
3 – другий шар ізоляції (поліетилен або поліпропілен);
4 – верхня частина корпусу;
5 – мідний електрод;
6 – полікарбонатний корпус;
7 – ізоляція електроду (діелектрик, на якому формується плазмовий розряд);
8 – область плазмового розряду;
9 – область обробки плазмою;
10 – нижня частина корпусу

Рис. 1. Структура електроду генератора холодної плазми DBD-типу

Формування робочого сигналу відбувається за допомогою класичної схеми генератора синусоїдального сигналу на операційному підсилювачі із ланцюжками зсуву фази (рис. 2). Така схема дозволяє задати майже будь-яку частоту сигналу та відзначається хорошою стабільністю при відсутності кварцевого резонатора.

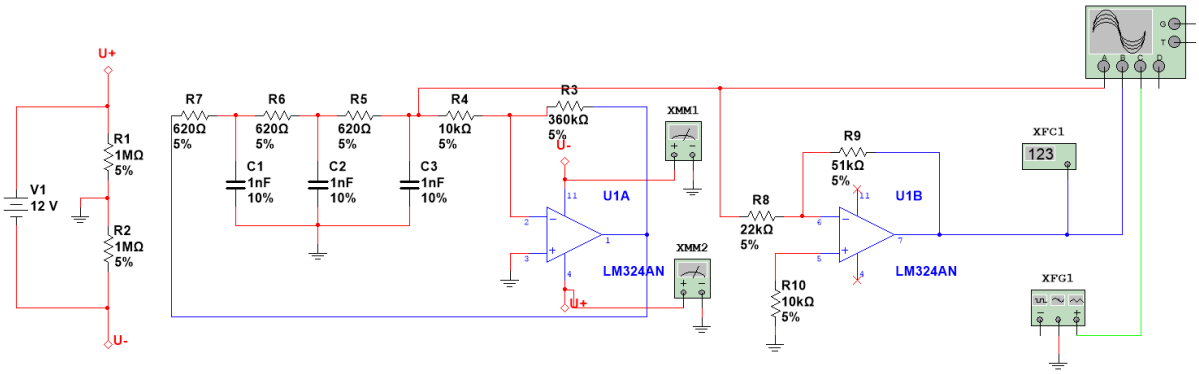


Рис. 2. Схема генератора робочого сигналу для джерела холодної плазми

Високовольтний блок може бути просто об'єднаний із підсилювачем потужності, який найпростіше виконати по класичній схемі підсилювача класу В (рис. 3). У цій схемі резистор R7 з опором 20 МОм не є реальною деталлю, а імітує опір діелектрика на вихідному електроді. Підвищення вихідної напруги до рівня 15 кВ виконується трансформатором Т2.

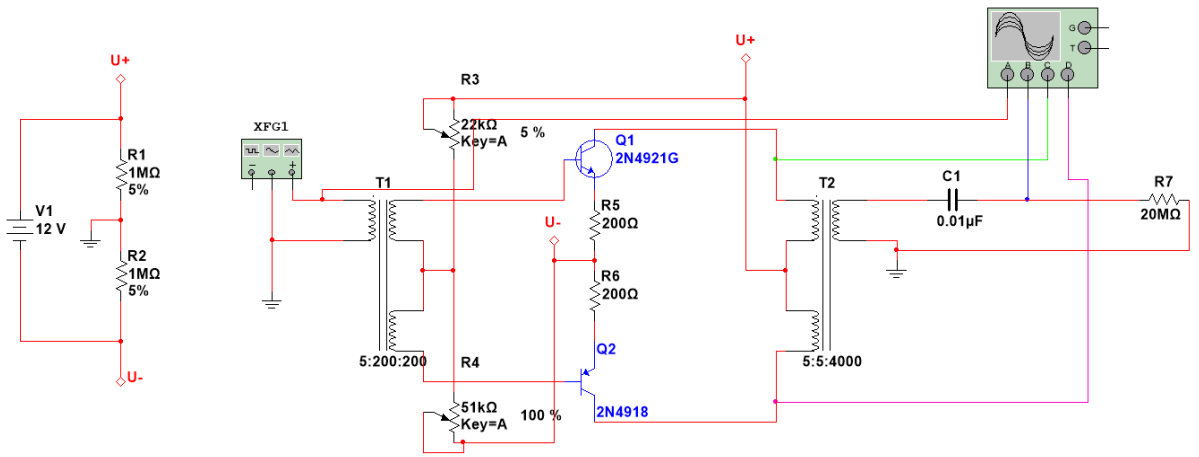


Рис. 3. Схема високовольтного блоку джерела холодної плазми

УДК 612.014.464:612.233

Бенедицький В.Б., ст. викл.
Коренівська О.Л., к.т.н, доц.
Терех К.С., студ.
Державний університет «Житомирська політехніка»

СИСТЕМА МОНІТОРИНГУ МІКРОКЛІМАТУ ПРИМІЩЕННЯ

Сьогодні галузі промисловості та наукових досліджень, навчальні заклади потребують моніторингу таких факторів як температура, відносна вологість повітря, рівень вуглекислого газу в повітрі, концентрація легких аероіонів. Від цих параметрів залежить працездатність людини та її самопочуття. Під час навчання та праці людина перебуває під дією ряду факторів, які можуть викликати надмірне підвищення або зниження температури тіла, підвищення тиску, зміну частоти серцевих скорочень. В більшості на стан людини впливає повітря, яке окрім хімічного складу характеризується електропровідність, яка визначається співвідношенням іонів повітря різних знаків заряду. Надмірний рівень вуглекислого газу, недостатній рівень легких аероіонів в повітрі може стати причиною головних болів, запаморочень, сонливості, втрати працездатності тощо. Особливу увагу слід приділяти навчальним закладам – школам, дитячим садочкам, вищим навчальним закладам, іншим закладам освіти, де скупчення людей протягом тривалого часу призводить до збільшення рівня вуглекислого газу, зміни аероіонного стану повітря та призводить до негативних наслідків у фізіологічному стані здобувачів освіти. Тривале перебування в таких умовах призводить до швидкої втомлюваності студентів, втрати уваги та виникненню дискомфортних станів, головного болю. Тому насичення повітря аероіонами дозволяє підтримувати нормативні показники в межах норми та робить перебування студентів в умовах аудиторій під час навчання більш комфортним.

Для вирішення проблеми моніторингу мікроклімату приміщення в роботі пропонується розробка системи вимірювання кліматичних параметрів, таких як температура, відносна вологість повітря, рівень вуглекислого газу в повітрі та концентрація легких аероіонів з записом даних на смартфон та збереженням на віддаленому сервері. Також розроблена система може використовуватися для моніторингу мікроклімату в герметизамкнутих військових об’єктах – ракети, літальні апарати, танки, тощо.

На рисунку 1 наведено структурну схему розробленої системи моніторингу якості повітря.

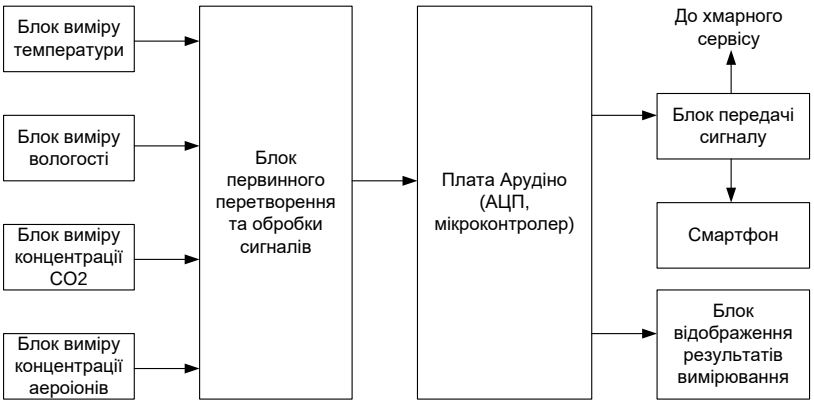


Рис. 1. Структурна схема системи моніторингу якості повітря

Система містить набір датчиків для зняття основних параметрів мікроклімату – це сенсор температури, вологості, концентрації CO_2. Для вимірювання температури та вологості було обрано цифровий датчик підвищеної точності DHT 22, який містить чутливий до вологості ємнісний елемент та терморезистор, виконаний за технологією NTC, який зменшує свій опір зі збільшенням температури. Чутливі елементи вимірювального перетворювача з’єднанні з високопродуктивним 8-бітним мікроконтролером, що забезпечує високу якість, швидку відповідь, захист від завад та низьку ціну. Для визначення рівня вуглекислого газу обраний модуль датчика якості повітря MQ7.

Для реєстрації концентрації аероіонів розроблено власний первинний вимірювальний перетворювач, конструкція якого є складеною і містить вимірювальний (накопичуючий) електрод, виконаний у формі куба та вхідний інтегруючий конденсатор, призначений для накопичення кількості зарядів в конкретній точці повітряного простору навколишнього середовища та представляє собою конструкцію об’ємного ємнісного сенсора заряду.

Далі зняті сигнали надходять на блок попередньої обробки та комутації, потім на блок АЦП – для перетворення сигналу з аналогової форми у цифрову. Після цього сигнал поступає на мікроконтролер, де обробляється та передається за допомогою блоку бездротової передачі даних на смартфон (може бути ПК) та через середовище Інтернет надходить на хмарний сервіс.

Для реалізації основної частини розробленої системи моніторингу мікроклімату обрали платформу Arduino на базі мікроконтролера ATmega2560, яка суміщає одночасно АЦП та мікроконтролер на одному модулю. Плати Arduino дешеві, багатофункціональні, мають розвинуту підключаєму інфраструктуру, гарну вбудовану систему програмування через ПК. Платформа відповідає за управління роботою системи, а саме зчитує через модуль інтерфейсів показники сенсорів та згідно із внутрішньою програмою проводить необхідну обробку, передачу та відображення результатів моніторингу.

Для обміну інформацією між пристроями використаємо технології бездротових мереж (Wi-Fi, Bluetooth, ZigBee, 6LoWPAN). В даній розробці передачу інформації на ПК або смартфон проводимо за допомогою бездротових технологій – WiFi та Bluetooth. Для цього використали спеціалізований WiFi Bluetooth модуль ESP-32. В даній схемі оператор, використовуючи веб-інтерфейс (сайт або додаток), через комп'ютер може віддалено проводити моніторинг параметрів мікроклімату приміщення, в якому встановлено розроблюваний пристрій.

За допомогою розробленої системи було виконано серію вимірювань стану мікроклімату в навчальних приміщеннях. В таблицях 1, 2 наведено результати вимірювань параметрів мікроклімату в аудиторіях під час проведення занять за наявності та відсутності примусової аероіонізації.

Таблиця 1

Результати вимірювання параметрів мікроклімату в аудиторії в звичних умовах

Час вимірювання, год.	8,50	9,00	9,10	9,20	9,30	9,40	9,50	10,00
Температура t, ºС	23,29	23,25	23,23	24,03	24,08	24,10	24,12	24,33
Вологість, φ, %	20,33	20,38	20,39	20,47	20,70	20,53	20,32	20,63
Концентрація аероіонів, іон/см^3	436	452	420	373	415	320	250	282
Концентрація CO_2, ppm	180	185	232	250	256	280	284	312

Таблиця 2

Виміряні параметри мікроклімату в аудиторії при додатковій аероіонізації

Час вимірювання, год.	Початок вимірювань	30 хв. впливу	60 хв. впливу	80 хв. впливу
Температура t, ºС	22,02	22,53	23,23	24,03
Вологість, φ, %	21,36	21,38	21,39	20,47
Концентрація аероіонів, іон/см^3	436	1506	2763	4324
Концентрація CO_2 ppm	180	185	200	241

Також проведені дослідження впливу параметрів мікроклімату на їх фізіологічні показники. Під час занять спостерігається незначна зміна вологості, яка не сильно вплине на людину, зростання температури приблизно на 1 градус, зниження концентрації аероіонів та підвищення рівня вуглекислого газу, що може негативно впливати на стан студентів. Дані зняті протягом однієї пари. Нажаль, зміну показників протягом більш тривалого часу не реєстрували, бо на перерві за рахунок відкриття дверей, вікон порушувався мікроклімат у приміщенні, а групи, у якої були всі заняття в одній аудиторії протягом дня не було.

Але отримані показники підтвердили гіпотезу, що мікроклімат в закритих приміщеннях під час великого скупчення людей значно погіршується у короткий час. Тому необхідно вживати заходи по оздоровленню мікроклімату. Одним з варіантів покращення параметрів мікроклімату під час занять є аероіонізація. Тому також були проведені дослідження по впливу аероіонів на зміну фізіологічних показників студентів.

УДК 621.396.663

Ципоренко В.В., к.т.н., доц.
Молдамурат К.М., магістрант, гр. ТРм-19-2
Есмухаммед Е., магістрант, гр. ТРм-19-2
Державний університет «Житомирська політехніка»

РОЗРОБКА КРИТЕРІЯ ЕФЕКТИВНОСТІ КОРЕЛЯЦІЙНО-ІНТЕРФЕРОМЕТРИЧНИХ РАДІОПЕЛЕНГАТОРІВ

На сьогодні пеленгування радіоелектронних засобів повинно здійснюватись в умовах складної електромагнітної обстановки, великої апріорної невизначеності щодо параметрів радіовипромінювань, а також в умовах реального масштабу часу реалізації. Перспективним напрямком реалізації пеленгування для вказаних умов є використання широкосмугових цифрових кореляційно-інтерферометричних радіопеленгаторів. Для порівняльної оцінки різних методів пеленгування доцільно розробити критерій ефективності роботи пеленгатора, який буде враховувати необхідні вимоги за точністю та швидкодією пеленгування. Невирішеною раніше частиною загальної проблеми розробки ефективних швидкодіючих кореляційно-інтерферометричних радіопеленгаторів є розробка критерія ефективності кореляційно-інтерферометричних радіопеленгаторів.

Нехай здійснюється прийом впродовж обмеженого часу аналіз часового радіовипромінювання $S(t)$ з рівномірно розподіленою спектральною густиною потужності $S^2(\omega) = const$ в межах відомої смуги $\Delta\omega_S$ частот рознесення у просторі на базу d двома ідентичними пеленгаційними радіоканалами. Будемо вважати, що пеленгаційні радіоканали мають власні адитивні стаціонарні часові шуми n_1 і n_2 з однаковою спектральною густиною потужності, що рівноцінно розподілена в межах смуги $\Delta\omega_k$ їх просування. Напрямок θ_S на джерело радіовипромінювання (ДРВ) $S(t)$ апріорі невідомий і є випадковою величиною з рівномірним розподілом густини імовірності в секції $(0-180)^0$. Просторово ДРВ знаходиться відносно апертури антенної бази пеленгатора в дальній зоні, а саме випромінювання $S(t)$ і власні адитивні шуми n_1 і n_2 пеленгаційних радіоканалів можуть мати кругову $F(\theta)=1$ або гостроспрямовану $F(\theta)=1$, де $\theta \in \{\theta_{H.}, \theta_B\}$ діаграми спрямованості. Для вказаних умов необхідно визначити напрямок на ДРВ $S(t)$ відносно антенної бази d, початкові умови пеленгування можуть бути представлені наступним чином:

$$\begin{aligned} U_1(t) &= S(t) + n_1(t); \\ U_2(t) &= S(t-\tau_S) + n_2(t), \end{aligned} \qquad (1)$$

де $U_1(t), U_2(t)$ – реалізації адитивної суміші сигналу $S(t)$, що прийняли першим і другим пеленгаційним каналом відповідно, τ_S – відповідна затримка прийому сигналу $S(t)$ між пеленгаційними радіоканалами.

Для вказаних умов оптимальну оцінку напрямку $\hat{\theta}$ на ДРВ за критерієм максимуму правдоподібності забезпечує кореляційний метод пеленгування. Інформаційним параметром, за яким оцінюється напрямок $\hat{\theta}$ на ДРВ, є відносна затримка τ_S прийому випромінювання $S(t)$ між рознесеними у просторі пеленгаційними радіоканалами пеленгатора. Правдоподібна оцінка $\hat{\tau}_S$ відносної затримки визначається по максимальному значенню взаємно кореляційної функції $K_{12}(\tau)$ прийнятих реалізацій $U_1(t)$ і $U_2(t)$ пеленгаційними радіоканалами:

$$\hat{\tau}_S = \arg\{\max(K_{12}(\tau))\}, \qquad (2)$$

де $K_{12}(\tau) = \int U_1(t) U_2(t-\tau) dt$ – взаємно кореляційна функція прийнятих сумішей $U_1(t)$ і $U_2(t)$.

Безпосередньо рівняння правдоподібності (2) оцінки $\hat{\tau}_S$ відносного часу затримки прямого розв'язку не має. Тому положення максимуму $\max(K_{12}(\tau))$ взаємно-кореляційної функції визначають зазвичай одним із двох основних методів пошуку і паралельним (багатоканальним) і послідовним (одноканальним). При паралельному методі використовують багатоканальний корелятор, який містить M одночасно

(паралельно) працюючих каналів кореляційного оброблення (прийому). В результаті сукупністю M каналів корелятора визначається відповідно M дискретних значень $K_{12}(\tau_m) \mid m \in \{0, M-1\}$ взаємно-кореляційної функції $K_{12}(\tau)$ для масиву $\{\tau_m\}$ з M можливих значень $\tau_m \in \{-\tau_{\max}, \tau_{\max}\}$ відносної затримки прийому, де максимальне значення $\tau_{\max} = d/c$ визначається величиною бази d. Перевагою паралельного кореляційного алгоритму є відповідно мінімальна тривалість пеленгування, висока швидкодія пеленгування з можливістю працювати в реальному масштабі часу, коли тривалість пеленгування і часу та оцінки напрямку $\hat{\theta}$ на ДРВ дорівнює тривалості одного циклу $T_{кор}$ кореляцій оброблення:

$$\min(T_{\text{пел}}) = T_{\text{а}} = T_{\text{кор}}. \tag{3}$$

Основним недоліком паралельного алгоритму кореляційного методу пеленгування є великі (максимальні) апаратурні витрати.

Для умов використання в радіоканалах кореляційного пеленгатора гостроспрямованих антен, що реалізуються зазвичай на основі багатоелементних АР, в процесі пеленгування використовується попередня просторова селекція випромінювань. Якість попередньої просторової селекції також доцільно оцінювати відповідним коефіцієнтом фільтрації $K_{f\theta}$, кількістю сигналів $M_{s\theta}$, роздільною просторовою здатністю $\Delta\theta_p$ і шириною просторового сектора D_θ пеленгування. Для вказаних умов рівняння ефективності (12) пеленгування прийме вигляд:

$$\eta_{\theta,\omega,t} = \frac{N_{on.k} + \alpha \cdot Z}{(D_\theta / \Delta\theta_p) \cdot K_{f\theta} \cdot M_{s\theta} \cdot (D_\omega / \Delta\omega_p) \cdot K_{f\omega} \cdot M_{s\omega} (D_r / \sigma_r) \cdot K_{fr} \cdot M_{sr}}. \tag{4}$$

Необхідно відмітити, що при пеленгування ДВР здійснюється добування (отримування) певної кількості інформації з урахуванням значень діапазону невизначеності можливих значень випромінювань за напрямком θ, частотою ω і затримкою τ, а також відповідних значень коефіцієнтів фільтрації $(K_{f\theta}, K_{f\omega}, K_{f\tau})$ і кількості сигналів $(M_{s\theta}, M_{s\omega}, M_{s\tau})$. З урахуванням цього рівняння ефективності пеленгування можуть бути представлені у співвідношенні (кількості операцій і каналів) на один біт інформації:

$$\eta = \frac{N_{on.k} + \alpha \cdot Z}{\log_2[(D_r/\sigma_r) \cdot K_{fr} \cdot M_{sr}]};$$

$$\eta_{\omega,\tau} = \frac{N_{on.k} + \alpha \cdot Z}{\log_2[1 + (D_\omega/\Delta\omega_p) \cdot K_{f\omega} \cdot M_{s\omega}] + \log_2[1 + (D_\tau/\sigma_\tau) \cdot K_{f\tau} \cdot M_{s\tau}]}; \tag{5}$$

$$\eta_{\theta,\omega,\tau} = \frac{N_{on.k} + \alpha \cdot Z}{\log_2[1 + \frac{D_\theta}{\Delta\theta_p} \cdot K_{f\theta} \cdot M_{s\theta}] + \log_2[1 + \frac{D_\omega}{\Delta\omega_p} \cdot K_{f\omega} \cdot M_{s\omega}] + \log_2[1 + \frac{D_\tau}{\sigma_\tau} \cdot K_{f\tau} \cdot M_{sr}]}.$$

Аналіз рівнянь (5) ефективності алгоритмів пеленгування показує, що запропоновані оцінки ефективності за відношенням (точність/швидкодія) не залежить від апріорі невизначених і різних абсолютних значень параметрів точності, швидкодії і апаратурних витрат. Це дозволяє оцінити ефективність різних варіантів алгоритму пеленгування, які відповідають різним умовам застосування і різним параметрам пеленгатора, а також можливість їх практичної реалізації на основі оптимального оброблення.

Отримані рівняння ефективності пеленгування за відношенням точність/(швидкодія, апаратурні витрати), а також у співвідношенні кількості операцій і каналів на один біт інформації. При цифровій реалізації алгоритмів кореляційного пеленгування їх відповідні часові витрати оцінено більш уніфікованим і узагальненим показником, таким як кількість операцій кореляційного оброблення. Виконано аналіз запропонованих рівнянь критерія ефективності алгоритмів пеленгування. Запропоновані оцінки ефективності за відношенням (точність/швидкодія), що не залежать від апріорі невизначених і різних абсолютних значень параметрів точності, швидкодії і апаратурних витрат. Це дозволяє оцінити ефективність різних варіантів алгоритму пеленгування, які відповідають різним умовам застосування і різним параметрам пеленгатора, а також можливість їх практичної реалізації на основі оптимального оброблення.

УДК 621.396.663

Сабиболда А.М., магистрант, гр.ТРм-19-2
Ципоренко В.Г., к.т.н., доц.
Государственный университет «Житомирская политехника»

ИССЛЕДОВАНИЕ ЦИФРОВОГО МЕТОДА ОЦЕНКИ ЗАДЕРЖКИ РАДИОСИГНАЛОВ

Актуальной задачей современных радиолокационных систем (РЛС) является оперативный и достоверный контроль воздушной обстановки. Особенностью современной воздушной обстановки является её динамичность, насыщенность воздушными объектами. Перспективным направлением развития современных РЛС является использование полуактивных и пассивных методов локации (мониторинга), которые обладают значительным преимуществом, состоящим, главным образом, в скрытности их работы и живучести лишь при незначительном ухудшении точностных характеристик.

Исследования показали, что в современных РЛС целесообразно применение позиционных методов определения положения цели в пространстве. Суть этих методов заключается в использовании в качестве радионавигационного параметра суммы или разности расстояний до цели, угла направления на неё и скорости цели. Наибольшее распространение получил разностно-дальномерный метод, основанный на измерении разности хода сигналов до пространственно-разнесённых приёмных позиций. Особенно эффективен он в случаях, когда для вычисления разности хода применяется цифровая корреляционная обработка, при которой вид принимаемых сигналов не имеет значения. Корреляционная функция позволяет определить временное запаздывание сигнала, что является наиболее трудоёмкой операцией. При временном цифровом алгоритме корреляционной оценки времени запаздывания частота дискретизации сигналов существенно зависит от требуемой точности измерений. Поэтому массивы измеренных данных становятся очень объёмными, что значительно снижает быстродействие вычислений итерационным методом. С точки зрения реализации это требует значительных временных и аппаратурных затрат, что снижает эффективность системы.

Спектральное разложение сигнала обеспечивает как быстродействие, так и минимальные ресурсные затраты. Для данных условий предложена модель взаимного спектра сигналов в виде эквивалентного узкополосного спектрально-пространственного сигнала с неизвестной частотой, однозначно соответствующей относительной задержке принятых сигналов. Для оценки частоты такого эквивалентного сигнала предложено использовать спектральный анализ на основе алгоритма БПФ. На рис. 1 представлена зависимость СКО погрешности измерения задержки от отношения сигнал/шум при различных типах окон. Тип окон: 1 – прямоугольное, 2 – Блэкмана, 3 – Ханна, 4 – Кайзера, 5 – Хэмминга. Доказана целесообразность применения окна Ханна.

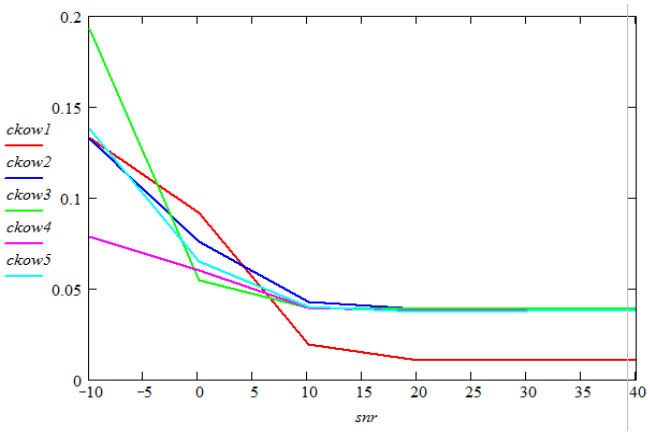


Рис. 1. Зависимость СКО погрешности измерения задержки от отношения сигнал/шум

Для повышения эффективности определения времени запаздывания сигналов предложен быстродействующий цифровой спектральный метод, позволяющий определить задержку сигналов в разностно-дальномерных системах за одну итерацию. При этом целесообразно корреляционную обработку реализовать путём формирования и анализа взаимного комплексного спектра принятых сигналов с пунктов наблюдения. В этом случае информационным параметром взаимного спектра является его разностный фазовый спектр и скорость его изменения от частоты. Проведенные экспериментальные исследования и полученные точностные характеристики подтвердили эффективность предложенного метода измерения задержки радиосигналов.

УДК 621.396.24

Корольова Є.С., студентка, ФІКТ
Державний університет «Житомирська політехніка»

РОЗРОБКА МОДЕМУ БАГАТОКАНАЛЬНОЇ АВТОНОМНОЇ СИСТЕМИ СИГНАЛІЗАЦІЇ

На сьогоднішній день набули широкого використання системи охорони та сигналізації з віддаленим доступом. При цьому більшість систем для передачі даних використовує канали частот ISM діапазону з обмеженою потужністю передавача радіолінії, або канали систем мобільного зв'язку. Бездротовий стандарт GPRS передбачає використання пакетної передачі даних при доступі в інтернет. У сучасних телекомунікаційних системах, при передачі даних по радіоканалу ISM діапазону, набули використання різноманітні технології розширення спектру сигналу. Використання широкосмугових сигналів забезпечує потрібну швидкість передачі цифрових даних по радіоканалах ISM діапазону з необхідною якістю. При цьому, зменшення спектральної щільності широкосмугових сигналів дозволяє організувати багатоканальну передачу даних з кодовим розділенням каналів, що підвищує ефективність використання частотного ресурсу і забезпечує достатньо низьку ймовірність виявлення сигналу, що відповідає потребам кібербезпеки і конфіденційності передачі даних. Наприклад, система мобільного зв'язку CDMA для організації багатоканальної передачі на одній несучій використовує набір взаємно-ортогональних функцій Уолша-Адамара, що забезпечує розширення спектру сигналу у 64 рази. Технологія «Nanotron» передбачає використання широкосмугового сигналу із середньою частотою 2,4 ГГц та лінійно-частотною модуляцією, що дозволяє забезпечити необхідне відношення сигнал/шум, при потужності передавача до 20дБм. Необхідна дальність радіолінії, при обмеженій потужності передавача, забезпечується у технології «LoRa» шляхом адаптивної зміни як швидкості передавання, так і параметрів сигналу із лінійно-частотною модуляцією, ширина спектру якого перевищує смугу частот, що необхідна для передачі даних із визначеною швидкістю. При цьому, завдяки оптимальній обробці у приймачі широкосмугового сигналу можливо отримати збільшення потужності корисного сигналу у базу разів. При смузі радіоканалу 125кГц, для отримання значення бази сигналу 4096, тривалість передачі одного байта інформації у технології «LoRa» складає близько 32 мс.

Однак, використання IoT технології можливо лише при наявності доступу до інтернет- мережі. На сьогоднішній день існують віддалені об'єкти, що не мають доступу до інтернету. Тому розробка радіоканалу передачі даних в автономній системі охорони повинна бути організована без використання IoT технології та систем мобільного зв'язку.

У роботі запропоновано створити радіолінію обміну цифровими даними з використанням мікросхем серії TX5000 і RX5000 фірми RFM з амплітудною маніпуляцією несучої частоти 433,92 МГц. Радіомодулі ISM діапазону прості в експлуатації і, на відміну від радіопристроїв не ISM-діапазону, не вимагають реєстрації та плати за використання частотного ресурсу. Мікросхема TX5000 - передавач. Вона містить задаючий генератор з резонатором на поверхневих акустичних хвилях, який і визначає робочу частоту. Підсилювач потужності в мікросхемі має фільтр на поверхневих акустичних хвилях, що придушує позасмугові випромінювання передавача. Максимальна вихідна потужність передавача 1,2 мВт, що забезпечує максимальну дальність передачі сигналу 250 м. Для збільшення потужності передавача до 10 мВт можливо використати вихідний підсилювач на транзисторі АТ-32011, спеціально призначений для роботи при низькій напрузі живлення та малому струмі колектору. Швидкість передачі даних в режимі амплітудної маніпуляції – 10кбіт/с. Значно підвищити перешкодостійкість передачі даних можна використанням цифрового кодування. У передавачі можна використовувати кодер MC145026 (виробництва Motorola), а в приймачі - декодер MC145027. Активний сигнал на виході декодера з'явиться тільки при збігу кодової комбінації на виводах 1-5 кодеру і декодеру. Таким чином, реалізуючи кодове розділення каналів, можна отримати дуже велику кількість комбінацій, що дозволить використовувати один частотний канал багатьма користувачами. По радіоканалу будуть передаватися закодовані сигнали від датчиків руху, пожежної сигналізації та контролю доступу. З виходу декодеру сигнали подаються до пристрою контролю стану системи охорони, який передбачається реалізувати на мікроконтролері.

Реалізація дуплексного режиму роботи радіолінії дозволить передавати тестові сигнали по зворотному каналу зв'язку і проводити перевірку працездатності системи охорони. Для живлення прикінцевих пристроїв з малим споживанням струму можуть бути використані дві пальчикові батарейки, або мініатюрні елементи CR2032. Збільшення дальності дії радіолінії може бути здійснено шляхом застосування додаткового каскаду підсилення з вихідною потужністю до 10Вт з використанням мікросхеми M57716 фірми MITSUBISHI.

УДК 621.396.24

Андреєв О.В., к.т.н., доц.
Державний університет «Житомирська політехніка»
Полещук І.І.
Національний центр управління та випробувань космічних засобів

ВИКОРИСТАННЯ ФУНКЦІЙ УОЛША ДЛЯ ПІДВИЩЕННЯ ЕНЕРГЕТИЧНОЇ СКРИТНОСТІ ЦИФРОВОЇ РАДІОЛІНІЇ

Організація радіозв'язку завжди пов'язана з вибором частотного діапазону. Відомо, що для радіозв'язку у районах зі складним рельєфом місцевості широко використовується діапазон частот від 20 МГц до 76 МГц. При цьому більшість засобів радіозв'язку використовують частотну модуляцію при вузькій смузі радіоканалу, що не перевищує 25 кГц та потужністю передавача до 20 Вт. Це дає змогу виявляти і перехоплювати повідомлення, що передаються цими засобами, які у подальшому будемо називати вузькосмуговими, на відстанях, що перевищують дальність їх зв'язку.

У сучасних телекомунікаційних системах, при передачі даних по радіоканалу НВЧ діапазону, набули використання різноманітні технології розширення спектру сигналу. Використання широкосмугових сигналів (ШС) забезпечує потрібну швидкість передачі цифрових даних по радіоканалах НВЧ діапазону з необхідною якістю. При цьому, у НВЧ діапазоні можливо забезпечити достатньо низьку ймовірність виявлення ШС, що відповідає потребам кібербезпеки і конфіденційності передачі даних. Наприклад, система мобільного зв'язку CDMA для організації багатоканальної передачі на одній несучій використовує набір взаємно-ортогональних функцій Уолша-Адамара, що забезпечує розширення спектру сигналу у 64 рази. Технологія "Nanotron" передбачає використання ШС із середньою частотою 2,4 ГГц та лінійно-частотною модуляцією, що дозволяє забезпечити необхідне відношення сигнал/шум, при потужності передавача до 20дБм. Необхідна дальність радіолінії, при обмеженій потужності передавача, забезпечується у технології "LoRa" шляхом адаптивної зміни як швидкості передавання, так і параметрів сигналу із лінійно-частотною модуляцією, ширина спектру якого перевищує смугу частот, що необхідна для передачі даних із визначеною швидкістю. При смузі радіоканалу 125кГц, для отримання значення бази сигналу 4096, тривалість передачі одного байта інформації складає близько 32 мс.

Однак, при передаванні сигналу мови із верхньою частотою спектру 3,9 кГц, період дискретизації не може перевищувати 128мкс. Тому раніше розглядалась можливість створення аналогової радіолінії передачі мови з використанням ШС із лінійно-частотною модуляцією несучої 30МГц із базою сигналу, що дорівнює 54. Завдяки оптимальній обробці у приймачі ШС можливо отримати збільшення потужності корисного сигналу у базу разів. Зменшення спектральної щільності ШС суттєво зменшує дальність, на якій можливо виявити випромінення широкосмугового засобу радіозв'язку (ШЗР), порівняно із звичайними вузькосмуговими засобами із тією ж самою потужністю передавача. Подальше покращення енергетичної прихованості радіолінії можливо при збільшенні бази сигналу з одночасним зменшенням потужності передавача. Однак такий підхід до розв'язання задачі прихованості радіосигналу у діапазоні від 20 МГц до 76 МГц з використанням ШС у літературі достатньої уваги не знайшов.

Запропоновано для передачі по цифровій радіолінії використовувати для розширення спектру сигналу функції Уолша розмірністю 256. Передаванню підлягає сигнал мови із верхньою частотою спектру 3,9 кГц, а при аналого - цифровому перетворенні сигналу використовується 256 рівнів квантування з періодом дискретизації 128мкс. На кожному інтервалі дискретизації на вхід кодеру надходить 8 біт, які відповідають певній функції Уолша. При тривалості елементарного символу функції 0,5мкс, відбувається розширення спектру сигналу до 2 МГц, а база сигналу дорівнює 256. Для організації багатоканальної передачі передбачається використовувати частотне розділення з фазовою маніпуляцією несучої частоти, що дозволить не враховувати взаємну кореляція сигналів різних ШЗР, які використовують ідентичні функції Уолша. Проведені розрахунки показали, що для потужності передавача ШЗР 5 Вт на частоті 30 МГц, при використанні неспрямованих антен, дальність дії радіолінії трохи перевищує 6 км. При цьому на відстані 1 км можливо виявлення сигналу з умовною ймовірністю правильного виявлення не менше 0,8. При зменшенні потужності передавача ШЗР до 0,1 Вт, передача інформації із заданими показниками якості забезпечується на відстані до 2км, а умовна ймовірність правильного виявлення сигналу набуває значення меншого ніж 0,5 вже на відстані 0,4км.

Таким чином, застосування ШС із великою базою в запропонованому цифровому засобі радіозв'язку погіршує умови виявлення факту випромінювання передавача порівняно із вузькосмуговими засобами. Зменшення ймовірності виявлення факту випромінювання передавача цифрової радіолінії, що використовує ШС із великою базою, можливо при одночасному зменшенні потужності випромінення передавача. Відсутність апріорних даних про параметри кодування сигналу ШЗР суттєво ускладнює перехоплення інформації засобами частотного моніторингу.

УДК 004.77

Андрущенко Ю.А., к.г.н., нач. відділу науково-дослідного, випробувального
Лящук О.І., к.ф-м.н., заст. нач. центру
Іващенко О.Є., нач. відділу інформаційно-обчислювального
Головний центр спеціального контрою ДКА України

ВИКОРИСТАННЯ ХМАРНОГО СЕРЕДОВИЩА ПРИ ОБРОБЦІ ДАНИХ ГЕОФІЗИЧНОГО МОНІТОРИНГУ

Головний центр спеціального контролю (ГЦСК) Національного центру управління та випробувань космічних засобів Державного космічного агентства України виконує задачі забезпечення міжнародних зобов'язань України щодо контролю за дотриманням вимог про обмеження і заборону випробувань ядерної зброї, випробувань ядерної зброї на іноземних випробувальних полігонах і здійсненням ядерних вибухів у мирних цілях. Цілодобовий геофізичний моніторинг здійснюється шляхом використання територіально розподіленої вимірювальної системи. Обробка даних здійснюється з використанням сучасного спеціалізованого програмного забезпечення, що встановлене на окремому сервері та вимагає високих технічних характеристик.

Протягом останніх десяти років спостерігається стрімкий розвиток спеціалізованого програмного забезпечення, пов'язаного з виконанням завдань геофізичного моніторингу. Спеціалісти здійснюють розробку широкого спектру програмних продуктів від модулів збору геофізичних даних до повнофункціонального програмного забезпечення для моніторингу землетрусів у реальному часі. З'явилась можливість автоматичного виявлення подій, можливості визначення місцезнаходження джерела та його енергетичних параметрів.

Підчас несення оперативного чергування майже весь персонал ГЦСК використовує ті чи інші інструменти одночасно, що призводить до уповільнення роботи сервера, або його зависання. Такі проблеми призвели до необхідності пошуку новітніх технологій та способів організації комп'ютерної інфраструктури, які дозволяють гнучко розподіляти обчислювальну потужність і обсяги сховища даних та сприятимуть збільшенню ефективності оперативної обробки геофізичної інформації.

На сьогоднішній день найбільш перспективними та потужними сервісами, що забезпечують виконання вищезазначених задач, є – хмарні сервіси, Впровадження хмарної технології надає змогу уніфікувати підхід до організації, розміщення та конфігурування спеціального програмного забезпечення для роботи з геофізичними даними, що підвищує оперативність їх обробки та аналізу.

Провівши аналіз найпопулярніших хмарних сервісів була обрана платформа Unigeocloud (Jelastic).

Платформа має дуже простий, але в те й же час гнучкий інтерфейс, який ідеально підходить для виконання цілей, поставлених перед ГЦСК. Платформа працює набагато стабільніше за рахунок невисоких технічних вимог до серверу. Платформа дає можливість розгортання ПМЗ не тільки для виконання поставлених цілей, а й для проведення експериментів та тестування нового ПМЗ. Платформа дає можливість не прив'язуватись до робочого місця, а працювати з будь якого пристрою, але за умови що пристрій повинен бути підключений до мережі Internet.

Основними перевагами такої платформи є:

- інтеграція геофізичних мереж в рамках хмари;
- уніфікація форматів даних та автоматизація їх конвертації;
- широкий вибір програмного забезпечення, яке підтримується платформою (з відкритим та закритим кодом, готові до використання дані в хмарі);
- можливість використовувати приватну або гібридну платформу, надаючи необхідний рівень захисту даних;
- віддалений доступ до внутрішніх робочих місць хмари для обробки даних; легка технологія розширення платформи з додатковим програмним забезпеченням;
- можливість працювати з платформою з будь-якого пристрою, без досвіду встановлення та конфігурації програмного забезпечення.

В тестуванні хмарної платформи активну участь приймають курсанти військових навчальних закладів. Застосування в навчальному процесі інформаційних технологій, що реалізують концепцію «хмарних технологій» забезпечує суттєве виділення необхідних ресурсів в залежності від потреб, визначених програмою навчання, В процесі навчання курсанти мають доступ до баз даних зареєстрованих сигналів та можливість використовувати весь спектр програмних засобів, що застосовується в ГЦСК при оперативній обробці геофізичної інформації.

УДК 004.056

Байлюк Є.М., ст. викл. кафедри КІ та КБ
Покотило О.А., ст. викл. кафедри КІ та КБ
Державний університет «Житомирська політехніка»

АНАЛІЗ ТЕХНОЛОГІЇ КОНТРОЛЮ ДОСТУПУ НА ОСНОВІ КОНТЕКСТУ CONTEXT-BASED ACCESS CONTROL

Безпека мережі важлива як для домашніх, так і для корпоративних мереж. У більшості будинків із високошвидкісним підключенням до Інтернету є один або кілька бездротових маршрутизаторів, які можуть бути використані зловмисниками, якщо вони незахищені. Надійна система мережевої безпеки допомагає зменшити ризик втрати конфіденційних даних.

Технологія управління доступом на основі контексту CBAC(Context-Based Access Control) – це особливість програмного забезпечення брандмауера, яка інтелектуально фільтрує пакети TCP та UDP на основі інформації про сеанс протоколу прикладного рівня. Його можна використовувати для інтрамереж, екстрамереж та інтернету. CBAC є набором функцій брандмауера Cisco IOS, які активно перевіряє передачу трафіка із зовнішньої мережі у внутрішню. Технологія CBAC визначає, який трафік потрібно дозволяти, а який - забороняти, використовуючи списки доступу (так само, як в Cisco IOS). Однак списки доступу CBAC включають оператори ip inspect, які дозволяють перевірити конкретні протоколи, щоб переконатися, що дані не підроблені до того, як повідомлення цих протоколів перейдуть до внутрішньої мережі. CBAC можна налаштувати для того, щоб дозволяти вказаний TCP та UDP-трафік через брандмауер лише тоді, коли з'єднання ініціюється всередині мережі, яку необхідно захистити[1].

CBAC забезпечує наступні переваги: блокування Java, попередження та виявлення відмови в обслуговуванні, попередження в реальному часі та аудит, виявлення та запобігання більшості популярних атак. Дана технологія також має недоліки. CBAC не забезпечує інтелектуальну фільтрацію для всіх протоколів, а лише для протоколів, які були вказані при налаштуванні. CBAC не захищає від атак, що походять із захищеної мережі.

Технологію CBAC можна налаштувати для перевірки таких типів сеансів: усі сеанси TCP, незалежно від протоколу прикладного рівня (іноді їх називають «одноканальним» або «загальним» інспектуванням TCP); усі сеанси UDP, незалежно від протоколу прикладного рівня (іноді їх називають «одноканальними» або «загальними» інспекціями UDP).

CBAC також можна налаштувати для наступних протоколів прикладного рівня: CU-SeeMe (лише версія White Pine), FTP, H.323 (наприклад, NetMeeting, ProShare), Java, R-команди UNIX (такі як r-login, r-exec та r-sh), RealAudio, RPC (Sun RPC, не DCE RPC або Microsoft RPC), SMTP, SQL * Net, StreamWorks, FTP, VDOLive.

CBAC має деякі обмеження. Він доступний лише для трафіку протоколу IP. Перевіряються лише пакети TCP та UDP. Інший IP-трафік, такий як ICMP, не можна відфільтрувати за допомогою CBAC, а натомість його слід відфільтрувати за допомогою основних списків доступу. CBAC працює з швидким перемиканням та перемиканням процесів. Якщо списки доступу переналаштовуються під час налаштування CBAC і ці списки доступу блокують трафік TFTP у внутрішній інтерфес, то завантажитися через цей інтерфейс буде неможливо. Це не є специфічним обмеженням CBAC, але є частиною існуючої функціональності списку доступу. CBAC ігнорує недосяжні повідомлення ICMP.

Якщо між двома маршрутизаторами передається зашифрований трафік, а брандмауер знаходиться між двома маршрутизаторами, CBAC може не працювати належним чином. Це тому, що корисні навантаження пакетів зашифровані, тому CBAC не зможе їх точно перевірити. Крім того, якщо і шифрування, і CBAC налаштовані на одному брандмауері, CBAC не працюватиме для певних протоколів. У цьому випадку CBAC буде працювати з одноканальними TCP та UDP, за винятком Java та SMTP[2].

Таким чином, технологія управління доступом на основі контексту CBAC відіграє важливу роль в захисті комп'ютерних мереж. Вона дає змогу адміністратору мережі налаштувати брандмауер таким чином, щоб попередити реалізацію атак зловмисників із зовнішньої мережі. Крім того, реалізація технології CBAC не потребує великих матеріальних затрат, оскільки підтримується ОС маршрутизаторів.

Список використаної літератури:

1. Context-Based Access Control (CBAC): Introduction and Configuration. URL: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/13814-32.html#intro (дата звернення 05.05.2021).
2. Cisco IOS Firewall Feature Set and Context-Based Access Control. URL: http://www.blacksheepnetworks.com/security/info/fw/cisco/firewall.htm#xtocid155310 (дата звернення 05.05.2021).

УДК 004.087.5

Коровaєва Б.М., студ. ЗКБ-17
Науковий керівник: Пірог О.В., к.т.н., доц.
Державний університет «Житомирська політехніка»

ОБОВ'ЯЗКОВІСТЬ І ОБҐРУНТОВАНІСТЬ ТОКЕНІЗАЦІЇ В УКРАЇНІ

Токенізація - новий етап кіберзахисту XXI століття. Токени призначені для електронного посвідчення особи. Вони можуть використовуватися замість або разом з паролем. Деякі призначені для зберігання криптографічних ключів (електронний підпис або біометричні дані). Держава змушує купувати токени, бо Україна готується до підписання з угоди Євросоюзом про взаємне визнання системи електронних довірчих послуг. Щоб підписати цю угоду, необхідно адаптувати компоненти української системи електронної довіри відповідно до вимог ЄС. Для цього розроблено новий Закон України "Про електронні довірчі послуги", у якому йдеться про захист особистого ключа КЕП. Підписання угоди зробить можливим взаємне визнання електронних довірчих служб. І документи, які видані в Україні та підписані КЕП, будуть визнаватися в ЄС. Це дасть можливість здійснювати транскордонні транзакції з використанням КЕП. З метою покращення надання послуг у сфері дистанційного обслуговування клієнтів Казначейство України продовжує проводити заходи щодо впровадження нових систем криптографічного захисту інформації, які відповідають вимогам вітчизняного законодавства.

Чи потрібні токени тільки бюджетникам, а для всіх інших вони не обов'язкові? За відповіддю необхідно звернутися до Закону України "Про електронні довірчі послуги". В ньому йдеться про те, що кваліфікований електронний підпис (КЕП) пройшов перевірку та отримав підтвердження, якщо особистий ключ зберігається в засобі КЕП. Відповідно до цього ж закону, засіб КЕП – це апаратно-програмний, апаратний пристрій чи програмне забезпечення, що відповідає вимогам цього закону. Тобто, не зважаючи на те, хто використовує КЕП, для того, щоб він вважався дійсним, його необхідно зберігати у засобах КЕП, які мають експертний висновок Державної служби спеціального зв'язку і захисту інформації.

Тема токенізації та застосування токенів цікава мені тому, що я пишу дипломну роботу бакалавра з оцінки білінгових систем та розробки авторської білінгової системи, в якій враховуються сучасні вимоги стосовно кібербезпеки.

Для захисту платіжних реквізитів клієнта їх краще винести за межі білінгу. Для цих цілей, як правило, використовуються провайдери платіжних послуг (Payment Service Provider, PSP). Наприклад: PayPal, CyberSource. Таким чином ще й підвищується ступінь довіри клієнта до білінгу. Білінг не зберігатиме у своїй базі даних (БД) платіжні реквізити клієнта, а буде зберігати тільки отриманий від PSP токен. Токен дозволяє здійснювати виключно тільки певні транзакції, що робить безглуздим його крадіжку. Шахрай не зможе за допомогою токена зробити платіж в свою користь. Крім того, клієнт отримує можливість відстежувати свої транзакції як на білінгу, так і на PSP.

Але токен, як матеріальний предмет, можуть вкрасти. Яка ж користь від захисту токеном? При використанні для зберігання свого КЕП звичайного накопичувача або будь-якого не захищеного носія інформації, секретний ключ можуть скопіювати, і користувач про це навіть не дізнається. Під час роботи з токенами скопіювати секретний ключ неможливо, а втрату самого захищеного носія користувач виявить відразу. Так, це дасть змогу миттєво заблокувати КЕП і не дати зловмиснику скористатися ним.

Токени кращі, ніж звичайні накопичувачі, тим, що, по-перше — токен захищений паролем, кількість спроб введення невірного пароля – обмежена! По-друге — ключ ніколи не залишає сховище, а тому скопіювати його з токену не можливо. По-третє — зберігання ключа на захищеному носії відповідає вимогам чинного законодавства та стандартам Європейського Союзу.

УДК 004.056

Пірог О.В., к.т.н., доц.
Державний університет «Житомирська політехніка»

МОДЕЛЮВАННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

З розвитком мережі Інтернет, особливо в період всесвітньої пандемії, все більше бізнесів виводить свою діяльність в он-лайн. Зростають ризики кібербезпеки. Це все актуалізує побудову комплексної системи захисту інформації (КСЗІ) не тільки на підприємствах, де циркулює інформація, що є державною таємницею, але й на дрібних підприємствах, таких як: інтернет-магазин, кафе, аптека, клініка, лабораторія аналізів, навчальний заклад, РЕП, служба таксі, служба доставки, СТО, колл-центр, мала банківсько-кредитна установа і т.ін. Всі вони оперують як конфіденційною інформацією (працівників, клієнтів), так й комерційною таємницею самої компанії та її партнерів (наприклад база клієнтів, база закупок, ціни закупок й т. ін.). Побудову КСЗІ унормовує ряд документів. В першу чергу це закон України Про захист інформації в інформаційно-телекомунікаційних системах [1], ряд інших нормативних актів [2], [3], а також нормативні документи, що видано Державною службою спеціального зв'язку та захисту інформації України (ДССЗЗІ). Зокрема Типове положення про службу захисту інформації в автоматизованій системі [4]. В додатку до цього документу описано процес побудови моделі автоматизованої системи, класифікації інформації, що циркулює в автоматизованій системі, моделі порушника, моделі загроз, оцінки ризиків безпеки та політик безпеки.

Як правило таке моделювання відбувалося на аркуші паперу, або в кращому випадку за допомогою електронних таблиць. Але наразі є різні програмні продукти для полегшення та автоматизації цих процесів. Це в першу чергу Microsoft Threat Modeling Tool та OWASP Threat Dragon [5], що з'явився зовсім нещодавно. Інструмент від компанії Microsoft має масу можливостей, але для зручного використання в тій чи іншій області потребує розробки додаткових бібліотек. В той же час утиліта від OWASP більш гнучка для застосування. Таким чином пропонується її використання для моделювання КСЗІ у перелічених вище випадках та за нормами вказаного документу.

Які ж можливості є у запропонованого інструменту?

В одному проекті є можливість розробки декількох моделей КСЗІ різних ділянок, наприклад декількох аптек з мережі аптек. Також на верхньому рівні проекту в полі «High level system description» окрім опису організації можна описати загальні завдання захисту інформації та основні напрями політики безпеки організації. Є поля, що визначають власника, розробника та перевіряючу особу.

Додаток надає можливість детально та наочно описати всі компоненти автоматизованої системи (АС) та об'єкти інформаційної діяльності (ОІД). Є декілька типів елементів: «Process», «Store», «Actor» та «Data Flow». Пропонується за допомогою елементів «Process» описувати активні елементи АС, що не є суб'єктами та модифікують дані за програмою, наприклад ПЕОМ, «Store» – елементи, що зберігають або передають дані у незмінному вигляді, «Actor» – це суб'єкти АС, наприклад користувачі та/або працівники, «Data Flow» – це канали передачі даних. На схемі потрібно вказати всі важливі с точки зору захисту інформації елементи, а в полі «Description» кожного елементу – склад його технічних (ТЗ) та програмних (ПЗ) засобів. Також потрібно описати ролі користувачів та працівників в системі, їх можливості доступу. З точки зору саме комплексного захисту інформації в даному пункті цікавим є канал передачі даних від ПЕОМ до працівників – це як незахищені відкриті порти для зчитування інформації, так й методи візуальної, звукової передачі даних, що можуть бути каналами витоку інформації з обмеженим доступом. Також важливою є не тільки технічні характеристики та можливості ТЗ та ПЗ, а й ідентифікуюча інформація щодо них. Заміна обладнання може відбутися не тільки з метою крадіжки самого обладнання або інформації, що на ньому зберігається, а й з метою впровадження закладних пристроїв.

Є можливість вивести деякі вказані на схемі елементи з розгляду з допомогою чекбоксу «Out of scope». У випадках коли розгляд цих елементів не є предметом розробки вказаної КСЗІ (наприклад: елементи, що взаємодіють з системою, але є зовнішніми до неї, та організація не має впливу на них, або коли зняття інформації відбувається на законних підставах та протидія йому не є функцією КСЗІ). Такі елементи показуються на схемі пунктиром.

У відповідності з нормативним документом інформацію, що циркулює в АС, потрібно класифікувати на відкриту (яка потребує захисту / не потребує захисту) та з обмеженим доступом (таємну, службову, конфіденційну, комерційну) та вказати на схемі в яких елементах буде зберігатися, циркулювати той або інший від інформації.

Наступним завданням є визначення груп можливих порушників та їх класифікація. Потрібно виділити основні групи порушників. Це можуть бути наприклад: хакери, кримінал, конкуренти, спецслужби. Також потрібно не забути про таку групу порушників як інсайдері. Потім визначити для кожної групи їх: мету, можливості надані їм системою, кваліфікацію, використовувані методи, місце здійснення. Додаток дозволяє використати для елементи типу «Process» та здійснити їх опис в полі «Description».

Також потрібно визначити групи об'єктів загроз, що не є суб'єктами порушниками, наприклад «Природні явища», «Техногенні явища», їх можливо додати на схему за допомогою елементів «Actor». В полі «Description» потрібно описати виділені групи об'єктів загроз, наприклад: пожежа, повінь, землетрус, ураган, вибух, вологість, запилення, зміни температури, аварія, відмова/збій (електроживлення, охолодження, ПЗ, ТЗ). Також є можливість вказати канали здійснення загроз (наприклад: ПЕМВН, акустичні, оптичні, радіо, матеріально-речові, руйнування комплексу засобів захисту (КЗЗ), спецвплив на інформацію для порушення її цілісності, несанкціонований доступ (НСД), підключення до штатних терміналів, роз'ємів, перехоплення паролів, «маскарад», підвищення привілеїв, шкідливе програмне забезпечення (ШПЗ), закладні ПЗ та ТЗ, розголошення і т.ін.). Це можуть бути різнонаправлені канали: як від порушника к об'єкту загроз (наприклад здійснення руйнівного впливу або шантаж), так й назворот (наприклад той або інший канал витоку інформації). В полі «Description» вказаних каналів потрібно визначити склад можливого ТЗ (наприклад: технічні засоби розвідки, апаратні закладні пристрої, апаратні пристрої навмисного силового впливу) та ПЗ (наприклад: програмні закладні пристрої, шкідливе ПЗ, ПЗ для DDoS атак, ПЗ для сканування, ПЗ для brute force атак).

Згідно НД ТЗІ 1.4-001-2000 на наступному етапі потрібно визначити можливі групи загроз та провести їх опис за наведеною класифікацією. А саме визначити для кожної виділеної групи загроз:

- Канали здійснення загроз (технічні, спецвпливу, НСД);
- Результат здійснення загроз (порушення конфіденційності, цілісності або доступності);
- Суб'єктивна / об'єктивна природа загроз;
- Випадковість / навмисність загроз;
- Джерела виникнення загроз (суб'єкти АС або зовнішні);
- Суб'єкти загроз (природні явища, порушники);
- Суттєвість загроз;
- Конкретні назви загроз (зараження вірусами, ШПЗ, фізичне руйнування, пошкодження, крадіжки (носіїв, інформації, паролів, ОІД), відмови, збої (ПЗ, ТЗ, електроживлення, мереж), невиконання організаційних заходів, помилки, розголошення, вивідування, перехоплення, копіювання, читання (сміття, інформації, з монітора, з інших ТЗ), атаки (DDoS, brute force), «маскарад», використання вразливостей, закладні засоби (програмні, апаратні), засоби розвідки, ПЕМВН, відеоспостереження, підслуховування і т. ін.).

Додаток, що розглядається, надає таку можливість. Канали здійснення загроз розміщуються на схемі як окремі елементи та їх розташування на схемі вказує на джерела виникнення загроз та суб'єкти загроз. До кожного такого каналу можна додавати загрози, вказавши їх назву. Система надає можливість класифікації загроз за різними системами: STRIDE, LINDDUN та CIA (тобто – загрози конфіденційності, цілісності або доступності – Confidentiality, Integrity, Availability). В полі «threat type» можна вибрати результат здійснення загрози за обраною системою. За допомогою перемикача «Severity» встановлюється суттєвість загрози («High», «Medium», «Low»), що підсвічується різним кольором.

Таким чином в полі «Description» залишається описати:

- Суб'єктивна (штучні) / об'єктивна (природні) природа загрози;
- Випадковість / навмисність загрози.

Перемикач «Threat status» залишатися у положенні «Open» до обробки загрози за рахунок використання конкретних політик безпеки, та вказаний канал залишається на схемі червоним до обробки всіх виявлених щодо нього загроз. Після обробки та перемикання канал буде чорного кольору.

Далі потрібно для кожної виявленої та описаної загрози вказати методи її обробки, визначити вимоги, заходи, методи та засоби захисту (попередження, пом'якшення наслідків) від виявлених загроз. Також на основі аналізу методів, заходів та засобів можливо на схемі показати захисні лінії з відповідними назвами, що будуть перетинати всі канали здійснення загроз та вказувати на механізми захисту. Додаток має зручну можливість формування звітів, що включають в себе схему та опис всіх елементів схеми.

Таким чином розглянутий додаток OWASP Threat Dragon має достатню функціональність для використання його для моделювання КСЗІ, є безкоштовним гнучким та зручним для процесу моделювання та формування звітів, суттєво підвищує ефективність та наочність моделювання КСЗІ.

Список використаної літератури:

1. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. – URL: https://zakon.rada.gov.ua/laws/show/80/94-вр
2. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Постанова КМ України від 29 березня 2006 р. № 373. – URL: https://zakon.rada.gov.ua/laws/show/373-2006-п
3. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV. – URL: https://zakon.rada.gov.ua/laws/show/3475-15
4. Типове положення про службу захисту інформації в автоматизованій системі : НД ТЗІ 1.4-001-2000.
5. OWASP Threat Dragon Docs. – URL: https://threatdragon.github.io/

УДК 004.056

Пулеко К.І., студ., гр. ЗКБ-18
Пулеко І.В., к.т.н., доц.
Державний університет «Житомирська політехніка»

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ СЕРТИФІКАЦІЇ X.509 ДЛЯ ГАРАНТУВАННЯ БЕЗПЕКИ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ У ХМАРНОМУ СЕРЕДОВИЩІ AZURE

Проблемам безпеки Інтернету речей (англ.: Internet of Things, IoT) приділяється велика увага. Відповідно до загальноприйнятої концепції відповідальність за забезпечення безпеки пристроїв, що підключаються до систем IoT, лежить на розробниках пристроїв і архітекторах систем Інтернету речей. Кожен пристрій, що підключається до системи IoT, повинен проходити перевірку. Для перевірки пристроїв IoT, доцільно використовувати сертифікати X.509, щоб вони могли взаємодіяти з центром Інтернету речей.

В основі сертифікатів X.509 лежить концепція асиметричного шифрування з відкритим і закритим ключами. При використанні ключів для шифрування текст повідомлення спотворюється і замінюється незрозумілими символами. Відкритий ключ не може бути використаний для отримання закритого ключа. Якщо для шифрування повідомлення використовується відкритий ключ, то для його розшифрування можна використовувати тільки закритий. Якщо ж для шифрування використовується закритий ключ, то допустимо використовувати тільки відкритий для розшифрування повідомлення. Використовувані в них математичні функції називаються односторонніми функціями. Асиметричне шифрування більш безпечно, ніж симетричне, де для шифрування і розшифрування повідомлень використовується один і той же ключ.

Для збереження закритих ключів в таємниці потрібна інфраструктура для зберігання (PKI), що дозволяє запобігти їх втраті або крадіжці. Ця інфраструктура може бути недоліком системи з відкритого і закритого ключів. Однак при використанні сертифікатів X.509 зі Службою підготовки пристроїв Azure (DPS) інфраструктура зберігання ключів вбудована в службу. Користувачам служби навіть не потрібно знати свої власні закриті ключі. Закриті ключі створюються загальнодоступними допоміжними інструментами. Ключі зберігаються в сертифікатах X.509, і користувачеві досить відправити їх в службу DPS в Azure. Пароль захищає вміст закритого ключа.

Для перевірки справжності сертифікатів X.509, необхідно здійснювати їх підпис. Це можна зробити двома способами. Можна скористатися послугами організації, відомої як центр сертифікації (ЦС), що спеціалізується на наданні підписаних сертифікатів. Такий підхід варто застосовувати в робочому середовищі, хоча це може бути пов'язано з витратами. Інший підхід – самозавіряємі сертифікати, коли користувач сам перевіряє свої сертифікати. Цей варіант не вимагає плати, хоча ви покладаєтеся на загальнодоступні засоби і ця система не рекомендується для робочого середовища.

При використанні сертифікатів X.509 і PKI немає необхідності поширювати відкриті ключі при створенні пар ключів. Інша перевага полягає в тому, що PKI може підтримувати список недійсних сертифікатів, тому перевіркою достовірності можна управляти централізовано.

При підключенні пристроїв застосовують кореневі, проміжні та кінцеві сертифікати. Це означає, що сертифікат можна використовувати для перевірки іншого сертифіката. Основний сертифікат відомий як кореневий сертифікат або інколи його називають «якір довіри». Цей сертифікат не використовується, для перевірки пристроїв, він служить тільки для перевірки діапазону підлеглих сертифікатів. Ці підлеглі сертифікати можуть бути проміжними сертифікатами. Проміжний сертифікат знову-таки не використовується для перевірки пристроїв, але служить тільки для перевірки інших проміжних або кінцевих сертифікатів.

Кінцевий сертифікат, як і випливає з назви, є сертифікатом кінцевого суб'єкта, який використовується для перевірки пристрою. Кінцеві сертифікати не можуть використовуватися для перевірки інших сертифікатів. Кореневий сертифікат можна використовувати для перевірки будь-якого числа проміжних або кінцевих сертифікатів.

Як правило для групи пристроїв IoT створюється один кореневий сертифікат. На його основі створюються кінцеві сертифікати для кожного пристрою, який буде підключатися до центру Інтернету речей. Всі ці сертифікати будуть самозавіряємі.

Таким чином, технологія відкритого і закритого ключів – це сучасний рівень безпеки. Правильно використовуючи сертифікати X.509, можна бути впевненим в безпеці свого центру Інтернету речей. Це надає захист від неприпустимого пристрою, який надає неприпустимі дані, і атаки типу «відмова в обслуговуванні». Проте безпека не є ідеальною, тому рекомендується проводити подальші дослідження технологій сертифікації.

УДК 004.921

Соін Е.Е., студ.т, гр. КН-20-2, ФІКТ
Лисенко М.С., асист. кафедри КН
Державний університет «Житомирська політехніка»

СТРУКТУРА ВІЗУАЛІЗАЦІЇ ВІРТУАЛЬНИХ ОБ'ЄКТІВ В ТЕХНОЛОГІЇ ДОПОВНЕНОЇ РЕАЛЬНОСТІ

Доповнена реальність - одна з багатьох технологій взаємодії людини і комп'ютера. Її специфіка полягає в тому, що вона програмним чином візуально поєднує два незалежних простора: світ реальних об'єктів навколо нас і віртуальний світ, відтворений на комп'ютері. Нове віртуальне середовище утворюється шляхом накладення запрограмованих віртуальних об'єктів поверх відеосигналу з камери і стає інтерактивним шляхом використання спеціальних маркерів.

Найважливішим компонентом доповненої реальності поряд з трекінгом є візуалізація об'єктів, яка зазвичай здійснюється засобами тривимірної комп'ютерної графіки. Структура системи візуалізації засобами доповненої реальності має на увазі наявність наступних базових компонентів (рис. 1):

1. Підсистема трекінгу, що забезпечує коректну інтеграцію віртуального об'єкта в реальне оточення.
2. Сховище тривимірних моделей та іншої інформації про об'єкти.
3. Підсистема візуалізації, що забезпечує прорисовку об'єктів засобами комп'ютерної графіки.
4. Графічний інтерфейс, що забезпечує взаємодію з користувачем.

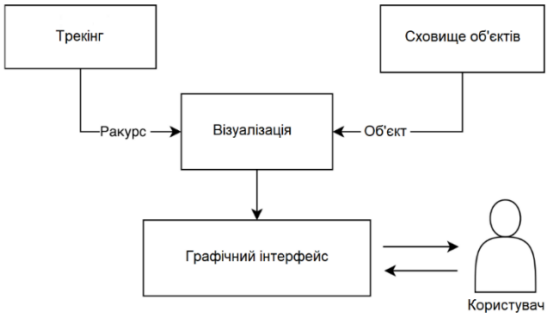


Рис. 1. Основні елементи системи візуалізації доповненої реальності

При оптичному трекінгу маркерів, відеопотік з камери надходить в підсистему трекінгу, де проводиться обробка та аналіз кожного кадру відеопотоку на предмет наявності заданого маркера. Якщо маркер опізнано, обчислюється матриця перетворень моделі за допомогою розтягування, повороту і перенесення. Вона дозволяє однозначно задати положення об'єкта в просторі. За нульову точку в тривимірному середовищі може бути взята як позиція віртуальної камери, так і центр маркера. Тривимірний об'єкт витягується зі сховища і його положення і масштаб встановлюються на задані заздалегідь значення щодо маркера. Потім відбувається візуалізація фінального двомірного зображення. Воно утворюється шляхом накладання віртуального об'єкта на зображення реального оточення з відеопотоку. Після цього на верхньому шарі проводиться рендеринг графічного інтерфейсу користувача.

Ключем до теоретичного обгрунтування візуалізації служить так зване рівняння рендерингу - інтегральне рівняння, яке визначає кількість світлового випромінювання в певному напрямку як суму власного і відбитого випромінювання. Нехай L - це кількість випромінювання по заданому напрямку в заданій точці простору. Тоді кількість вихідного випромінювання (L_o) - це сума випроміненого світла (L_e) і відбитого світла. Відбите світло може бути представлено як сума зовнішнього випромінювання (L_i) з усіх напрямків помноженого на коефіцієнт відбиття з даного кута. Тоді рівняння рендерингу може бути представлено як:

$$L_o(x, \omega, \lambda, t) = L_e(x, \omega, \lambda, t) + \int_\Omega f_r(x, \omega', \omega, \lambda, t)\, L_i(x, \omega', \lambda, t)(-\omega' \cdot n)d\omega',$$

де λ – довжина хвилі світла; t – час; $L_o(x, \omega, \lambda, t)$ – кількість випромінювання даної довжини хвилі λ, що виходить вздовж напрямку ω, за час t, з даної точки x; $L_e(x, \omega, \lambda, t)$ – світло, яке було випромінено; $f_r(x, \omega', \omega, \lambda, t)$ – двунаправленна функція розподілу відображення, кількість випромінювання відбитого від ω' до ω в точці x, під час t, на довжині хвилі λ; $L_i(x, \omega', \lambda, t)$ - кількість випромінювання даної довжини хвилі λ, що виходить вздовж напрямку ω', за час t, до точки x; $(-\omega' \cdot n)$ – поглинання вхідного випромінювання під заданим кутом.

У ході аналізу засобів тривимірної візуалізації були проаналізовані сучасні методи комп'ютерної графіки. Дані методичні та алгоритмічні засоби є основою для розробки інформаційної системи з технологією інтерактивної візуалізації засобами доповненої реальності.

УДК 004.65

Мєдвєдєв В.В., бакалавр, гр. ПІ-61, ФІКТ
Райковський В.А., бакалавр, гр. ІСТ-20-1, ФІКТ
Коротун О.В., к.пед.н, доц. кафедри КН
Державний університет «Житомирська політехніка»

РОЗРОБКА ДОКУМЕНТО ОРІЄНТОВАНОЇ СИСТЕМИ КЕРУВАННЯ БАЗАМИ ДАНИХ

З розвитком мережевих технологій, а також з розвитком технологій збору інформації системи для організації та управління цією інформацією стають основними й найважливішими компонентами усіх організацій. Навіть маленькі організації наразі вимушені працювати з величезними потоками інформації. Розвиток вимог до надійності та, разом з тим, вимог до швидкодії призвів до виділення окремого типу програмного забезпечення, яке може задовольнити ці вимоги й здійснювати контроль над великими потоками даних. Метою є розробка документоорієнтованої системи керування базами даних (СКБД).

В якості засобів реалізації обрано мову програмування C# та платформу .NET з використанням необхідних пакетів здебільшого визначених в просторі імен System.IO. Основним середовищем для розробки програмного продукту – інтегроване середовище розробки (IDE) Microsoft VisualStudio 2019. В якості середовища для модульного тестування коду обрано фреймоворк MSTest через зручну інтеграцію в середовище Micrisoft Visual Studio та платформу .NET. Для роботи з файловою системою було вирішено використовувати системи серіалізації у формат Json. Подібне рішення обумовлене потенційною необхідність використовувати отримані дані в мережі Інтернет. Під час розробки додатку застосовано механізм DataBinding який дозволяє зв'язувати багато різних представлень (View) з однією моделлю представлення (Model-View), що дозволяє розробляти їх відносно незалежно один від одного, та який підтримується платформою. NET по замовченню (рис.1).

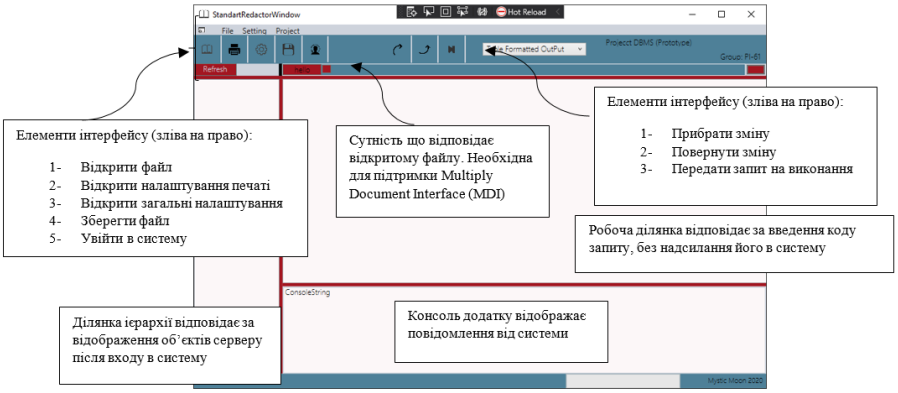


Рис.1. Інтерфейс розробленої СКБД

Проведено аналіз основних алгоритмів у системі та здійснена їх реалізація, створена модель системи, яку потрібно реалізувати, та сформуванні основні вимоги до компонентів цієї системи, проведено визначення основних компонентів необхідних для функціонування СКБД. В розробленій СКБД реалізована: множина команд DDL, що відповідає за створення об'єктів бази даних; множина команд DML, що пов'язана із взаємодією користувача з даними; множина команд DCL, що відповідає за визначення прав користувачів. В системі передбачена можливість виводити дані у файл з форматами PDF та Excel. Для написання складних запитів, які використовують поєднання багатьох таблиць реалізована команда Union, що поєднує дві колекції в одну та команда CrossJoin, що поєднує декілька колекцій в усіх комбінаціях між собою. Для покращення можливостей до автоматизації в систему введені можливості створення представлень, процедур, що зберігаються, та тригерів на команди. В системі є можливість використовувати запити з агрегатними функціями Avg, Count, Sum, Max, Min. Для отримання інформації про колекцію передбачені команди GetDomain та GetConstrain.

Отже, розроблена система керування базами даних здатна виконувати поставлені цілі. Призначена для проектів, які мають працювати з невеликими наборами даних. Має такі переваги: невеликі розміри системи (займає меньше100мб), що поліпшує мобільність; простий інтерфейс користувача; невеликі розміри початкового коду; утворене абстрактне ядро; обробка регламентних правил через спеціальні об'єкти; віддання переваг чистим функціям, що значно полегшує можливості до супроводження системи й зменшує вартість системи для потенційного користувача, що в свою чергу важливо для маленьких підприємств та організацій.

УДК 004.5, 004.75

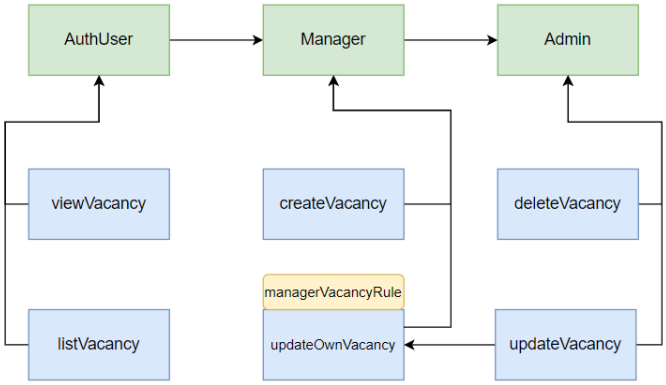
Мартинюк В.М., магістрант, гр. ІСТм-19-1, ФІКТ
Кузьменко О.В., ст. викл. кафедри КН
Державний університет «Житомирська політехніка»

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ ВЕБ-ОРІЄНТОВАНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ВЕДЕННЯ РЕСТОРАННОГО БІЗНЕСУ

Для реалізації можливості бути конкурентоспроможним на ринку сучасний ресторанний бізнес вимагає постійної автоматизації та оптимізації інформаційних процесів. До загальних задач таких процесів віднесемо створення, зберігання, обробку, пошук даних про працівників, вакансій, заявок на роботу, контроль якості виконання обов'язків. До специфічних задач можна віднести сервіси, орієнтовані на комунікаційний аспект виробництва, – взаємодія з персоналом та клієнтами, відслідковування замовлень, керування системою знижок та акцій. На відміну від компаній, що виробляють продукцію, інформаційні елементи яких зосереджуються на своїх внутрішніх потребах, інформаційні системи компаній сфери послуг повинні зосереджуватись насамперед на вдосконаленні послуг, що надаються замовникам та клієнтам. В якості реалізації таких задач запропоновано розробити веб-орієнтовану інформаційну багатокористувацьку систему із можливостями роботи з працівниками, вакансіями, обробки заявок на роботу, а також управління взаємовідносинами з клієнтами. При розробці такої системи слід звернути увагу на ряд факторів: швидкість обробки даних, набір базових та розширених функціональних можливостей системи, постійний технічний супровід, захист системи, дистанційна робота, масштабованість.

Виходячи з вимог до сучасних веб-орієнтованих інформаційних систем з врахуванням особливостей роботи ресторанного бізнесу, було здійснено аналіз бізнес-процесів ресторану «Шевченків Хутір» з подальшою пропозицією автоматизації таких процесів як організація роботи персоналу, створення системи для роботи з вакансіями та обробки заявок на роботу, відслідковування замовлень, ведення клієнтської бази, створення системи знижок та акцій. В ході виконання роботи було розроблено веб-орієнтовану систему для ведення ресторанного бізнесу. Дана система втілена у формі багатокористувацького веб-сайту, з розробленою системою ролей та дозволів, орієнтованого на клієнтів та персонал. Функціями такої системи є такі, що орієнтовані *на клієнта* (можливість отримати інформацію про заклад, зробити оцінку меню, забронювати столик) та *на персонал* (реєстрація, автентифікація та авторизація користувачів, система для перегляду та роботи з вакансіями і відправкою і обробкою запитів на роботу).

В розробленій системі для реалізації авторизації запропоновано концепцію RBAC (Role Based Access Control - контроль доступу на основі системи ролей). Згідно даної концепції, кожна роль – це певний набір дозволів, роль може містити в собі іншу роль, що дозволить унаслідувати всі дозволи з іншої ролі. Дозвіл може також містити в собі інший дозвіл, а також може бути зв'язаний з правилом – умовою, що здійснює задані обмеження для дозволу на виконання дії.



При розробці вебсайту було проаналізовано існуючі аналогічні вебсистеми, обґрунтовано вибір необхідного оточення, архітектури системи та інструментів розробки. Визначено системні та апаратні вимоги для повноцінної роботи вебсистеми. Розроблена система орієнтована на роботу з користувачами: персоналом та клієнтами, що надає можливість розширення своєї діяльності через мережу Web, впровадженню нових шляхів удосконалення маркетингової діяльності, залученню нових клієнтів і, як підсумок, підвищення якості обслуговування та збільшення прибутку.

УДК 621.398

Лімінович І.Д., здобувач, гр. КІ-3, ФІКТ
Локтікова Т.М., ст. викл. кафедри ІПЗ, ФІКТ
Кушнір Н.О., асист. кафедри ІПЗ, ФІКТ
Державний університет «Житомирська політехніка»

РОЗРОБКА БАГАТОФУНКЦІОНАЛЬНОГО МІКРОПРОЦЕСОРНОГО ПРИСТРОЮ ДЛЯ ІНФОРМАЦІЙНО-УПРАВЛЯЮЧОГО КОМПЛЕКСУ

Функціонування інформаційно-управляючого комплексу (ІУК) неможливе без використання мікроконтролера (МК), який управляє будь-яким його пристроєм. МікроЕОМ AT89S52 або її аналоги використовувалась у попередньому поколінні ІУК. У сучасних пристроях функціональні можливості розширились, тому до їх складу вводяться більш потужні та сучасніші МК. Наприклад, мікроконтролери компанії STM. Зокрема, високопродуктивний МК, заснований на архітектурі ARM Cortex M4 – STM32F407VET6. Це економний мікроконтролер, який належить до перспективної групи сигнальних мікроконтролерів, що підтримують DSP-інструкції. На базі вищевказаного мікроконтролера був розроблений багатофункціональний пристрій для сучасного ІУК. Було розроблено його алгоритм роботи та структурну схему. У складі пристрою можна виділити такі основні блоки: мікроконтролер; блок комутації аналогових сигналів (БКАС); блок нормалізації сигналів (БНС); блок введення дискретних сигналів (БВДС); блок управління реле (БУР); блок індикації (БІ); блок стабілізації напруги живлення АЦП (БСНЖ); інтерфейсний блок (ІБ); блок самоконтролю (БС); блок живлення (БЖ).

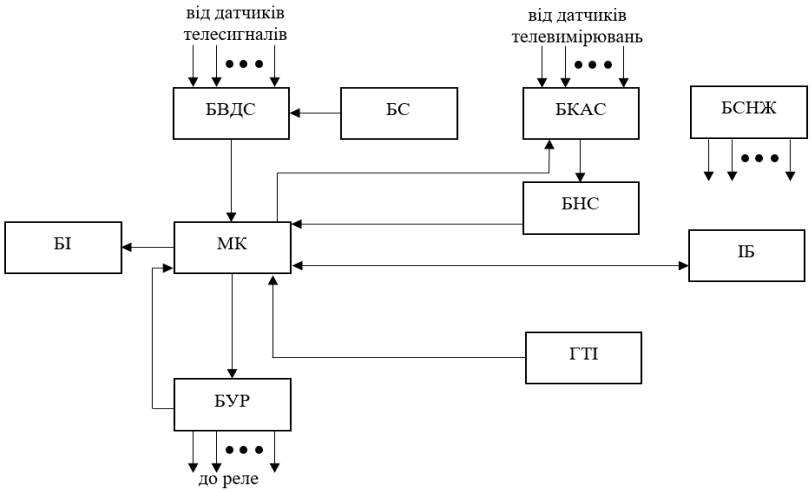


Рис. 1. Структурна схема багатофункціонального пристрою для ІУК

Розроблений багатофункціональний пристрій включає в себе три найважливіші функціональні модулі ІУК, а саме: модуль приймання команд телеуправління (ТУ), модуль введення телевимірювань поточних значень (ТВПЗ) параметрів та модуль введення дискретних сигналів (ДС). З боку ТУ даний пристрій має забезпечити перевірку прийнятої команди телеуправління та формувати вихідні сигнали для управління вбудованими в пристрій реле. З боку ТВПЗ розроблений пристрій має забезпечувати введення поточних значень сигналів від одного до чотирьох датчиків телевимірювань та супровід даних додатковою міткою часу. З боку ДС розроблений пристрій має фіксувати послідовності змін стану контрольованих об'єктів (подій) та супроводжувати «події» відносними мітками часу. Ці модулі забезпечують виконання трьох основних функцій телемеханіки – телеуправління, телевимірювання та телесигналізації.

Даний пристрій надає такі можливості при застосуванні: управління двома об’єктами; введення, перетворення та обробку аналогових сигналів від чотирьох датчиків телевимірювань 0…5мА, мінус 5…0…+5мА, 0…20мА, 4…20мА; введення дискретних сигналів від восьми датчиків телесигналів.

Також було розроблено програму для мікроконтролера та принципіальну електричну схему пристрою. Мовою програмування мікроконтролера було обрано мову С. Були проведені експериментальні дослідження розробленого пристрою.

Як висновок можна зазначити, що технічні характеристики даного пристрою викликані тим, що в залежності від застосування кількість датчиків, виконавчих механізмів, розміщуваних на пристрої контрольованого пункту, може бути невеликою. Тому доцільним є застосування багатофункціонального модуля, який забезпечує виконання декількох телемеханічних функцій, замість застосування декількох повноцінних функціональних модулів різного типу.

УДК 004

Венгловська Ю.В., студ., гр. КН-19-1, ФІКТ
Левківський В.Л., ст. викл. кафедри КН
Державний університет «Житомирська політехніка»

ГРАФІЧНІ СТИЛІ В КОМП'ЮТЕРНИХ ІГРАХ

Ігрова графіка пройшла довгий шлях від абстрактних геометричних фігур до сучасних моделей. Пару десятків років тому графіці не надавали особливого значення, в іграх більше звертали увагу на захоплюючий геймплей, атмосферу і сюжет, але вже тоді були плани на деякі графічні нововведення, але з технічних причин і через слабке обладнання, ідеї залишились тільки на папері. Очевидно, що ключове місце в поліпшенні графіки зіграв поступовий розвиток продуктивності комп'ютерів.

Pixel Art або піксельна графіка - напрямок цифрового мистецтва, який полягає в створенні зображень на рівні пікселів (мінімальної логічної одиниці, з якої складається зображення). Піксель-арт зараз повертається в ігри з основою із пофарбованих пікселів і сучасними ефектами. На рисунку 1 можна побачити зразки примітивної і сучасної піксельної графіки.

Рис. 1. Приклади піксельної графіки

«Плаский дизайн» або Flat design – сучасний стиль графіки, який відрізняється простотою та мінімалістичністю. Особливості:

- немає зайвих ефектів, всі зображення двомірні і знаходяться в одній площині, графіка не передбачає використання текстур, відблисків та ін;
- насичені колірні контрасти;
- легко впізнавана форма (спрощене схематичне зображення, але зрозуміле користувачеві).

Як приклад Flat design можна розглядати гру The Looppy.

2D стилізація – це принцип створення графіки у грі, коли не застосовується анімація персонажів, а промальовуються фони та рухи персонажів покадрово, як мультфільми. Приклад – гра Little Missfortune.

Коли техніка змогла підтримувати реалістичну 3D графіку почалася «ера реалізму», яка продовжується і зараз. Розробники створюють все більш і більш реалістичні ігри. Кожна маленька деталь дуже гарно промальована, анімація рухів чітка та правильна. Гра Spider-Man приклад 3D реалізму.

3D cartoon не потребує детальної розробки та великої кількості ресурсів, як реалістична графіка. Переважають спрощені форми та яскраві кольори.

Стилізований реалізм. На гіперболізованій, гротескній, або навіть «мультяшній» моделі використовують дуже реалістичні текстури. Такий стиль часто зустрічається у фентезі та постапокаліпсисах. Приклад – гра Rage 2.

Сел-шейдінг. Результатом являєтеся зображення, в деякій мірі імітуючи малювання вручну. Такий тип рендерингу часто використовується для одухотворення коміксів, для яких характерні жорсткі контури, обмежене число кольорів, неплавні переходи світлотіні.

Low poly напрямок живопису, що характеризується підкресленим використанням простих геометричних форм і роздроблення реальних об'єктів на стереометричні примітиви. Як і Flat design, Low poly переживає вже другу хвилю популярності.

Воксельна графіка – це звичайний растр в тривимірному просторі, тільки до стандартних для растра параметрам кольору і координат осей X і Y додають ще й вісь Z, тобто глибину. Вокселі є аналогами двовимірних пікселів для тривимірного простору.

Handmade стиль – коли гру створюють з підручних матеріалів (наприклад з пластиліну або паперу).

Графічний ігровий контент несе на собі кілька функцій: семантичну (смислову, прояснює ігрову механіку) і декоративну, що доповнює, урізноманітнювати гру. Також від якості графіки дуже залежить в тому числі і те, чи буде гравець «занурений» в атмосферу гри.

Оригінальний візуальний стиль завжди знаходиться в виграшному положенні в порівнянні з тисячами однакових ігор. Оригінальність може виражатися в незвичайній манері малювання текстур, в незвичайних рисах персонажів, в незвичайній геометрії моделей і так далі.

УДК 004

Менес Ю.В., студ., гр. КН-19-1, ФІКТ
Марчук Г.В., ст. викл. кафедри КН
Державний університет «Житомирська політехніка»

НАРАТИВ В КОМП'ЮТЕРНИХ ІГРАХ

Наратив – це повнота ігрового досвіду, який гравець може отримати, це унікальне проходження гри для кожного гравця та сукупність засобів та інструментів якими розробники вибудовують для гравця його досвід. Історія і сюжет можуть бути в грі, і тоді наратив – це спосіб «доставки» історії гравцеві. Але історії може і не бути, і тоді наратив дає гравцеві розуміння того, що ж тут відбувається, хто він в цій системі, які його цілі і інструменти. Іншими словами наратив – це те, що «створюється» самим гравцем при взаємодії з грою.

Коли говорять, що в грі хороший наратив, то мають на увазі, що у гравця не виникає людо-наративного дисонансу, добре працює занурення, ніщо не відволікає від отримання досвіду, гравець завжди розуміє: хто він, де він, що і навіщо він зараз робить і чого хоче досягти. А вищий пілотаж - це коли всі ці елементи складаються у гравця в голові в особисту індивідуальну історію проходження. Наприклад, в грі Minecraft – хороший наратив. Там все зроблено так, що навіть коротку ігрову сесію гравець може сприйняти вкрай емоційно і у фарбах переказати як історію власних пригод. Мається на увазі survival mode.

Коли говорять, що наратив в грі поганий – мається на увазі, що гра виглядає набором нескладних сутностей, відсутнє розуміння того, ким є персонаж в світі гри, що і навіщо він робить, і чому робить саме так. В такій грі гравця «вибиває» з занурення. При цьому, гра може залишатися захоплюючою по геймплею. Так що це питання цілей розробника – який саме досвід він хочете передати гравцеві. Якщо розробник хочете зробити абстрактну гру або, наприклад, передати досвід нестримного насильства – йому не потрібно працювати над якістю наративу. Але якщо він хочете зробити хорор або розповісти глибоку історію начебто To the Moon або Valiant Hearts, то доведеться рахуватися з наративом і почати в ньому розбиратися.

Підсумовуючи все віще сказане - наратив створює гравець своїми діями, одушевляючи гру, витягуючи, доливаючи, трансформуючи зміст своїх дій. Тобто переказ ігрової сесії - це наратив. Сюжет - це не наратив. Це частина наративу, але наратив більше сюжету (рис.1).

Рис. 1. Наратив і сюжет

Фахівець, який відповідає за історію і розповідь в розробці комп'ютерних ігор – це наративний дизайнер. Завданням наративного дизайнера є створення взаємовигідних відносин між історією гри і її механіками. Це означає, що для передачі історії гравцеві використовуються всі наявні засоби – це і арт (концепт-дизайн зайнятий багато в чому саме передачею сенсу через зовнішній вигляд персонажів і оточення), і анімація, і звуковий дизайн, і інтерфейси, і різні ефекти, і навіть – механіки і геймплей.

Чим же наративні механіки відрізняються від звичайних? Нічим, крім того, що обтяжені змістом. Ігрова механіка – це якась дія. Наприклад, раніше всі збирали кукурудзу з грядок клікаючи по ним, а гейм-дизайнери Hay Day додумалися водити пальцем по екрану, імітуючи зрізання колосків серпом. Дія стала символічною. У тому ж Hay Day є успішна геймплейна метафора риболовлі, що імітує процес набагато ближче по механіці, ніж просто: клікнути – закинути вудку, почекати рибу – клікнути – витягнути.

Навіщо потрібні ці механіки? Вони дають більш потужний і більш сильний засіб розповіді. До того ж наративні механіки універсальні з точки зору культури і не залежать від мовних бар'єрів. Це частина невербальної комунікації, яка виростає з людської біології та еволюційних процесів. Приклади тому – ігри без тексту, які добре сприймаються в усьому світі. Наприклад The Gardens Between – красива, атмосферна, ностальгічна і зворушлива розрахована на одного гра-головоломка. Розробникам вдалося домогтися щоб красиво, цікаво, а головне без слів, під приємну медитативну музику, розповідалася проста, ностальгічна і зворушлива історія про дружбу.

Як використовувати це в розробці ігор? Для початку поставити питання - чи відповідає геймплей тому, що за змістом відбувається з гравцем. І якщо не дуже відповідає - наприклад, збирання камінців по три в ряд ніяк не допомагає рятувати світ або вбивати монстра, то подумати, як вирішити цей людо-наративний конфлікт. Наприклад, збирати камінчики по три, тому що це елементи стихій, і вони заряджають ваші заклинання силою – як це зроблено в Puzzle Quest.

УДК 004.056.55

Щур Н.О., ст. викл. кафедри КІ та КБ
Державний університет «Житомирська політехніка»

ОСНОВНІ НАПРЯМИ РОЗВИТКУ ПОСТКВАНТОВОЇ КРИПТОГРАФІЇ

На сьогоднішній день практично усі цифрові комунікації захищені трьома криптографічними системами: шифрами із відкритим ключем, цифровими підписами та протоколами розподілу ключів. У сучасних комп'ютерних мережах ці системи реалізовані з використанням асиметричних криптографічних алгоритмів, таких як RSA, DSA, ECDSA, DH, ECDH. Їх безпека, як правило, ґрунтується на складності розкладання на прості множники великих чисел або ж розв'язанні задачі дискретного логарифмування. Тривалий час припускалося, що ці задачі не мають ефективного вирішення за поліноміальний час. Проте, такі припущення були засновані на обчислювальній потужності класичних комп'ютерів.

У 1994 році американський вчений Пітер Шор продемонстрував, що асиметричні криптосистеми можна легко зламати за допомогою досить потужного квантового комп'ютера і спеціального алгоритму, пізніше названого алгоритмом Шора. За оцінками експертів, протягом наступних 20 років буде побудований потужний квантовий комп'ютер, який зможе зламати багато криптосистем із відкритим ключем, що використовуються в даний час. Метою постквантової криптографії є розробка криптографічних систем, які захищені від зламу як на квантових, так і на класичних комп'ютерах і можуть взаємодіяти з існуючими протоколами зв'язку та мережами. У 2015 році агентством національної безпеки США (NSA) був анонсований план переходу до алгоритмів, стійких до атаки на квантовому комп'ютері. А у 2016 році національний інститут стандартів і технологій США (NIST) оголосив про запуск конкурсу на розробку та відбір найбільш оптимальних постквантових алгоритмів на міжнародному рівні. На участь у конкурсі подали заявки 69 команд з усього світу. Із запропонованих алгоритмів у другий етап пройшли 26. Вже 22 липня 2020 року були оголошені фіналісти другого етапу, які пройшли далі [1].

Отже, кандидатами на новий постквантовий стандарт цифрового підпису стали:

- CRYSTALS-DILITHIUM – представник криптографії на решітках. За основу взята схема Фіата-Шаміра з перериваннями. Має хорошу продуктивність і може бути ефективно реалізована на малоресурсних пристроях;
- FALCON – також є представником криптографії на решітках. Він має найкоротші підписи та відкриті ключі серед систем на базі решіток для певного рівня безпеки. Головним недоліком цієї схеми є складна програмна і апаратна реалізація;
- Rainbow – представник багатоваріантної поліноміальної криптографії, що основана на складності розв'язання систем багатомірних многочленів над кінцевими полями. Головною перевагою є розмір цифрового підпису. Але через великий розмір ключа цей алгоритм рекомендується використовувати тільки для специфічних завдань, де розмір ключів не критичний.

В наступний етап також пройшли такі алгоритми асиметричного шифрування:

- Classic McEliece – представник криптографії на базі теорії алгебраїчного кодування. Основна конструкція схеми була запропонована ще в 1979 році і добре вивчена. Має малі розміри шифротексту, але дуже великий розмір ключа;
- CRYSTALS-KYBER – є представником криптографії на решітках. Криптоаналіз зводиться до вирішення задачі MLWE (module learning with errors). Для забезпечення стійкості до атак на основі обраного шифротексту використовується перетворення Фуджісакі-Окамото;
- NTRU – є представником криптографії на решітках. За основу взята схема NTRUEncrypt, що вимагає використання певних рекомендованих параметрів для захисту від атак.
- SABER – є представником криптографії на решітках. Криптостійкість ґрунтується на складності вирішення задачі MLWR (module learning with rounding problem). Використовується перетворення Фуджісакі-Окамото, як і в CRYSTALS-KYBER.

Остаточні результати конкурсу будуть оголошені у 2023 році, але очевидним фаворитом серед запропонованих підходів є постквантова криптографія на решітках [2]. Цей напрям заснований на завданні дискретної оптимізації, а саме на пошуку найкоротшого шляху на багатовимірній решітці. У той час як інші завдання дискретної оптимізації, такі як розкладання великого числа на прості множники, вирішуються квантовим комп'ютером за поліноміальний час, на сьогоднішній день невідомо жодного квантового алгоритму, який здатний вирішити завдання на решітці за час менше експоненціального. Таким чином, ймовірно, саме криптографія на решітках в найближчі роки буде витісняти звичні нам RSA та ECDSA.

Список використаної літератури:

1. Post-Quantum Cryptography. Round 3 Submissions. URL: https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions
2. Basic Intro to Lattices in Cryptography. URL: https://qvault.io/cryptography/very-basic-intro-to-lattices-in-cryptography/

УДК 004.89

Лисогор Д.Ю., аспірант
Мєдвєдєв В.В., студ., гр. ПІ-61
Морозов А.В., к.т.н., доц.
Державний університет «Житомирська політехніка»

ПРО АВТОМАТИЗАЦІЮ КЛАСИФІКАЦІЇ ТЕКСТОВИХ ДАНИХ

В інформаційному просторі кожного дня створюється велика кількість інформації, аналіз якої людиною вручну не є неможливим. Дуже часто виникає задача класифікації чи групування схожих за певними ознаками текстових даних. Прикладом однієї з таких задач є задача розподілу новин на інформаційних сайтах за рубриками або категоріями. Ряд інших задач класифікації текстів може бути реалізований тими ж підходами та алгоритмами, що і задача розподілу текстів за категоріями. Тому важливою є розробка системи, яка б надала можливість автоматизувати класифікацію текстів за категоріями.

Задача класифікації – формалізована задача, яка містить множину об'єктів (ситуацій), поділених певним чином на класи. Задана скінченна множина об'єктів, для яких відомо, до яких класів вони належать. Ця множина називається вибіркою. До якого класу належать інші об'єкти невідомо. Необхідно побудувати такий алгоритм, який буде здатний класифікувати довільний об'єкт з вихідної множини.

Введемо позначення, які будуть зустрічатися при розв’язанні задачі класифікації текстів. Текст – загалом зв’язна і повністю послідовна кінцева множина слів.

Слово – найменша самостійна і вільно відтворювана в мовленні відокремлено оформлена значима одиниця мови, набір символів.

Для програмної реалізації алгоритмів було обрано мову програмування Python. Вибір зумовлений рядом переваг, які стали визначальними. Серед найбільш вагомих «плюсів» мови Python є наявність великої кількості бібліотек для роботи з алгоритмами штучного інтелекту, машинного навчання та аналізу даних, кросплатформеність та підтримка об’єктно-орієнтованого програмування.

Разом з тим, стандартні бібліотеки мови не адаптовані для підтримки української мови, тому пряме використання багатьох алгоритмів обробки україномовних текстів не є можливим. Тому для роботи з текстовим представленням даних було вирішено ряд допоміжних задач.

Робота з текстами включає попередню багатоетапну обробку даних. Основними етапами попередньої обробки даних є:

1) очистки тексту від чисел;

2) токенізація тексту, тобто виділення у тексті токенів (розбиття тексту на лексеми);

3) видалення знаків пунктуації (після цього етапу у тексті залишаються лише слова);

4) лематизація лексем (приведення слова до його початкової форми), що виконується за допомогою модуля pymorphy2;

5) видалення стоп-слів («шумових» слів, тобто слів, які самостійно не несуть змістовного навантаження).

Оскільки наявні бібліотеки мови Python не мають словників українських стоп-слів, то власноруч було сформовано такий словник і записано в окремий файл.

Для того, щоб визначити, який класифікатор показує найкращі результати проведено обчислювальний експеримент шляхом порівняння якості класифікації різних алгоритмів. Для цього було підготовлено дата сет розміром 10000 текстів, які були отримані в результаті збору новин з інформаційних веб-сайтів із зазначенням тематики кожної новини.

Кожний текст проходив попередню обробку. На наступному етапі за допомогою класу *CountVectorizer* з модуля *sklearn* виконується набору текстів в матрицю лексем, які знаходяться у тексті. Рядками матриці є тексти, по вертикалі – лексеми. На перетині рядків та стовпців – числа, які позначають кількість входжень відповідної лексеми у відповідний текст (таблиця 1).

Таблиця 1

Схематичний результат роботи CountVectorizer

	Лексема 1	**Лексема 2**	**…**	**Лексема M**
Текст 1	c_{11}	c_{12}	…	c_{1m}
Текст 2	c_{21}	c_{22}	…	c_{2m}
…	…	…	…	…
Текст N	c_{n1}	c_{n2}	…	c_{nm}

Далі за допомогою класу *TfidfTransformer* з модуля *sklearn* виконується визначення метрики *TF·IDF*. *TfidfTransformer* надає зручний спосіб оцінки важливості певної лексеми для конкретного тексту відносно всіх інших текстів. Принцип такий – якщо лексема зустрічається в деякому тексті часто, але при цьому зустрічаючись рідко в усіх інших документах – це слово має більшу значимість для того самого документу. Таким чином, метрика *TF·IDF* дає можливість виявити найбільш важливі слова, які визначають належність тексту до певного класу.

Після роботи *TfidfTransformer* маємо підготовлені дані для роботи класифікатора.

Далі вихідні дані (10000 текстів новин) ділимо на 2 частини – навчаючу та тестову вибірку, виходячи з пропорції 70/30. Таким чином, у навчаючу вибірку потрапило 7000, а у тестову – 3000 новин.

Для оцінки якості класифікації використовувались такі числові характеристики як точність та повнота.

Введемо позначення:

$Precision_c = tp_c / (tp_c + fp_c)$ – точність,

$Recall_c = tp_c / (tp_c + fn_c)$ – повнота,

де tp_c (truepositive) – кількість документів, правильно приписаних до класу *c,*

fp_c (falsepositive) – кількість документів, неправильно приписаних до класу *c,*

fn_c (falsenegative) – кількість документів, неправильно приписаних не до класу *c.*

Досліджувалися класифікатори, присутні в бібліотеці *scikit-learn* мови *Python*:

- NB (Naive Bayes classifier – наївний Баєсів класифікатор);
- KNN (K-nearest neighbours – к найближчих сусідів);
- SVM (Support-vector machine – метод опорних векторів);
- SGD (Stochastic Gradient Descent – метод стохастичного градієнту);
- DT (Decision Trees – метод дерев рішень);

Результати обчислювального експерименту наведено у таблиці 2.

Таблиця 2

Результати обчислювального експерименту

Метод	**Precision**	**Recall**
NB	0.5594	0.5035
KNN	0.5153	0.4515
SVM	0.5380	0.4880
SGD	0.6650	0.5055

Як видно з таблиці 2, класифікація методом SGD (стохастичного градієнту показує) найкращий результат на випадковій вибірці.

Переваги метода NB – висока швидкість роботи, підтримка інкрементального навчання, легка інтерпретованість результатів навчання. Недоліки методу: відносно низька якість класифікації і нездатність враховувати залежність результату класифікації від поєднання ознак.

Метод KNN показав такі переваги: можливість оновлення навчаючої вибірки без перенавчання класифікатора, легка інтерпретованість результатів роботи алгоритму. Недоліки методу: висока залежність результатів класифікації від вибраної метрики, довгий час роботи у зв'язку з необхідністю повного перебору навчаючої вибірки, неможливість розв'язання задач великої розмірності за кількістю класів та документів.

У метода SVM виявлено перевагу – можливість роботи з невеликим набором даних для навчання. Однак, метод має недоліки: складна інтерпретація параметрів алгоритму та нестійкість по відношенню до викидів у вихідних даних.

Метод SGD виявився найкращим, показав найкращу ефективність. Він має просту інтерпретованість результатів роботи алгоритму та порівняно з іншими алгоритмами швидке виконання навчання.

Описані методи добре справляються із задачами класифікації текстів за тематикою. Однак, у випадках, коли потрібно мати не просто віднесення тексту до певної категорії, а відсоткове значення ймовірності, доцільніше використовувати штучні нейронні мережі.

Отже, у роботі запропоновано методику попередньої обробки текстових даних за допомого мови програмування Python. Для обрання найкращого класифікатору проведено обчислювальний експеримент, у ході якого встановлено, що найкращі результати показав класифікатор SGD. Для експерименту зібрано дані з популярних новинних сайтів (10000 новин). Для класифікації текстів за тематикою та мовою написання пропонується використовувати SGDClassifier.

УДК 004.89

Білявський Н.А., група КІ-4
Русятинська А.О., група КІ-4
Плечистий Д.Д., к.т.н., доц.
Толстой І.А., асист.
Державний університет «Житомирська політехніка»

ОГЛЯД ТА ПОРІВНЯННЯ СИНТАКСИСУ CSS-ПРЕПРОЦЕСОРІВ

У великих вебпроєктах, часто виникає необхідність написання великої кількості CSS-стилів, які можуть розміщуватися у різних файлах. Незважаючи на постійний розвиток CSS, стандартних можливостей часто не вистачає. Для того, щоб мати розширені можливості при написанні стилів, які дають змогу скоротити обсяг CSS-коду, робити його декомпозицію, застосовувати елементи програмування тощо, використовують CSS-препроцесори.

CSS-препроцесор – це програма, яка дозволяє використовувати власний синтаксис (що має розширений набір можливостей з написання коду) і може генерувати з нього CSS-код. Сьогодні найбільш популярними CSS-препроцесорами є: 1) SASS/SCSS; 2) LESS; 3) Stylus.

SASS (Syntactically Awesome Style Sheets) – з'явився у 2006 році. На синтаксис SASS вплинула мова програмування Ruby, де вкладеність блоків визначається відступами. Трохи пізніше з'явився синтаксис SCSS, який дозволив використовувати можливості SASS, але у синтаксисі CSS.

LESS з'явився у 2009 році і багато у чому схожий на SCSS.

Stylus був розроблений у 2010 році і у ньому розробники спробували врахувати недоліки, які існували у SCSS та LESS.

Трансляцію коду, написаного з використанням препроцесора можна виконувати такими способами:

1) за допомогою візуальних трансляторів (PrePros, CodeKit та ін.);
2) автоматизованих консольних збірників (Gulp, Webpack, Rollup та ін.);
3) ручною збіркою з консолі;
4) підключенням JS-перетворювача безпосередньо до HTML-сторінки.

Однак, останній спосіб є неефективним, оскільки при кожному завантаженні сторінки буде відбуватися трансляція код у CSS.

SASS і Stylus використовують відступи для вказування вкладеності елементів і не вимагають написання крапок з комою в кінці рядків.

LESS та SCSS для вкладання елементів використовують фігурні дужки та крапки з комою.

Усі перераховані вище препроцесори, дозволяють:

1) створювати змінні;
2) вкладати стилеві правила;
3) створювати домішки з метою усунення дублювання коду;
4) використовувати розширення (наслідування);
5) застосовувати кольорові функції;
6) імпортувати стилів з інших файлів;
7) перевіряти умови;
8) виконувати повторення за допомогою циклів;

Для позначення змінних у LESS використовується символ «@», SASS та SCSS – «$», Stylus – перед змінними ніяких додаткових символів не вказується. Для оголошення домішок в SASS використовується символ «=», а для використання – вказується символ «+». В SCSS оголошення домішок здійснюється словом «@mixin», використання – словом «@include». В LESS для оголошення та застосування використовується символ «.», а в Stylus перед оголошенням домішки не потрібно вказувати ніяких додаткових символів. В усіх розглянутих препроцесорах для імпортування стилів використовується ключове слово «@import». Реалізація перевірки умови в Stylus здійснюється за допомогою ключових слів «if/else», SASS/SCSS – перед цими словами має бути розміщено символ «@», а ось в LESS використовуються ключові слова «when» та «when not». Цикли в SASS/SCSS реалізовуються ключовими словами «@for … from … through …», в LESS – шляхом рекурсивних викликів функцій. В Stylus для запису циклів використовується ключове слово «for … in …».

Проаналізувавши синтаксис та можливості SASS/SCSS, LESS, Stylus можна зробити такі висновки:

1) набільш зручним за синтаксисом є SCSS, оскільки його синтаксис є дуже схожим на CSS;
2) SASS дозволяє писати більш компактніший код, ніж SCSS за рахунок відсутності фігурних дужок та крапок з комою;
3) LESS має досить неявний синтаксис, маючи такі ж можливості, як і SASS/SCSS;
4) Styles має більше можливостей, ніж SASS/SCSS та LESS, тому у деяких випадках його використання може мати переваги.