

**Клименко М.В., магістр**  
**Безвершенко Є.І., старший викладач**  
ДВНЗ «Ужгородський національний університет»,  
м. Ужгород  
Кафедра «Комп'ютерних систем та мереж»

## МЕРЕЖЕВИЙ АНАЛІЗАТОР НА БАЗІ МІКРОКОМП'ЮТЕРА RASPBERRY PI

В даний час набули широкого розвитку мікрокомп'ютери, найпопулярнішим з яких є *RASPBERRY PI*.

*Raspberry Pi* - одноплатний комп'ютер розміром з банківську карту, спочатку розроблений як бюджетна система для навчання інформатиці, що згодом одержав набагато більш широке застосування і популярність, ніж очікували його автори. Він використовує архітектуру *System on Chip (SOC)* з швидким мікропроцесором, підтримує багатозадачність складних програмних додатків.

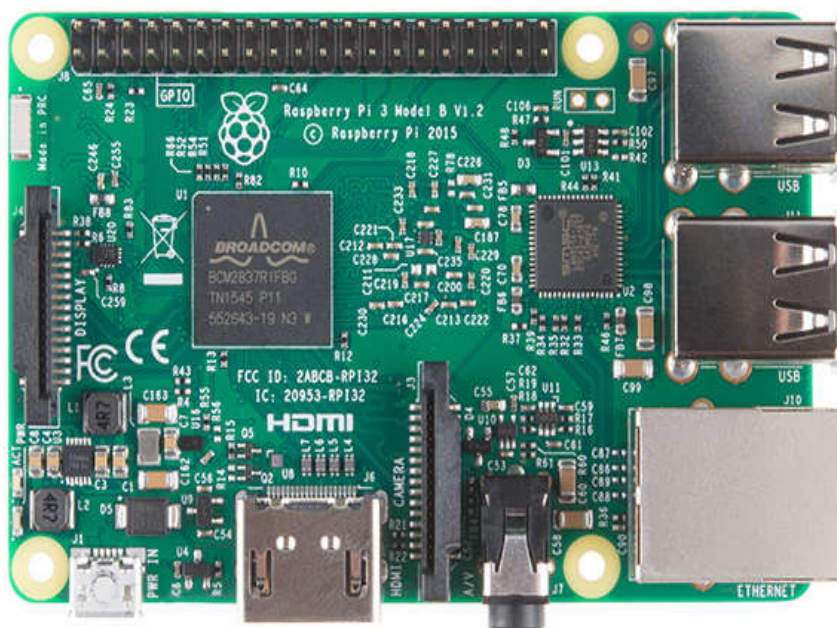


Рис. 1. Мікрокомп'ютер *Raspberry Pi 3B*.

Багато проектів, виконаних із використанням *Raspberry Pi* відкриті і добре задокументовані, що дозволяє проводити дослідження і розробку на базі існуючих проектів.

Аналіз мережевого трафіку завжди є актуальним питанням для провайдерів а також осіб які є власниками серверів, але мережеве обладнання часто занадто дороге і потребує багато енергії. Для вирішення проблеми великої ціни мережевих пристроїв та великого енергоспоживання можна використовувати мікрокомп'ютери *Raspberry Pi*, які дозволяють за низьку ціну та малу енергоспоживаність виконати всі поставлені на неї завдання.

Перевагами мережевого аналізатора на базі *Raspberry Pi* :

1) Відносна дешевизна;  
2) Підтримка технології WI-FI, що дає можливість легко підключатись в локальну мережу та використовувати мікрокомп'ютер в ролі маршрутизатора із *Firewall*.

3) Зручність. На базі *Raspberry Pi* крім мережевого аналізатора можна реалізувати також систему виявлення вторгнень (*Intrusion Detection System, IDS*), а також проводити налаштування мережевого обладнання.

В результаті дослідження проведений аналіз обчислювальної спроможності *Raspberry Pi*, а також порівняння енергозатрат мікрокомп'ютера та мережевого аналізатора на базі персонального комп'ютера. В процесі дослідження визначено, що використання мікрокомп'ютерів для аналізу мережевого трафіку є більш доцільним ніж використання персонального комп'ютера завдяки малому споживанні електроенергії мікрокомп'ютера, його низькій вартості та компактності.

#### Література:

- 1) Магда Ю.С. *Raspberry Pi*. Руководство по настройке и применению – М.: ДМК Пресс, 2014. – 188с.
- 2) Веб-сервер на Raspberry Pi 3. ЗА и ПРОТИВ [Электронный ресурс]. Режим доступа: <http://raznoe.su/veb-server-na-raspberry-pi-3-za-i-protiv>
- 3) А.Н. Андрончик, В.В. Богданов, Н.А. Домуховский, А.С. Защита информации в компьютерных сетях. 2008. – 248 с.
- 4) Стивен Норткат, Джуди Новак, Обнаружение нарушений безопасности в сетях (3-е издание), 2003. – 356 с
- 5) М.В. Веселовський Національний аерокосмічний університет імені М.С. Жуковського «ХАІ», Харків ПОБУДОВА СМАРТ-СИСТЕМ ЗА ДОПОМОГОЮ RASPBERRY PI.
- 6) Магістерська дисертація студента Національного технічного університету України «Київський Політехнічний Інститут» Чернацького Артема Юрійовича.

**Ковтун А.А.**

*Запорізький національний університет, місто Запоріжжя  
Кафедра програмної інженерії, студент*

## ОГЛЯД ТЕХНОЛОГІЇ FLUTTER

Flutter - це набір засобів розробки від Google для створення високоякісних натурних інтерфейсів для iOS та Android за рекордні терміни. Flutter працює з існуючим кодом, використовується розробниками та організаціями по всьому світу[1].

Уперше Google випустив Flutter 1.0 у грудні минулого року, після того, як він був у бета-режимі протягом 18 місяців. Додатки Flutter пишуться на Dart. Dart - мова програмування, що використовується для кодування програм Flutter. Dart трохи схожий на C і є об'єктно-орієнтованою мовою програмування. Dart використовується не тільки для розробки мобільних додатків, але є мовою програмування. Затверджений стандартом Ecma (ECMA-408), він

використовується для побудови майже будь-чого в Інтернеті, серверах, настільних комп'ютерах і, звичайно, мобільних додатках.

Дизайн користувацького інтерфейсу додатків Flutter зазвичай включає в себе використання або створення різних віджетів. Віджет Flutter є незмінним описом будь-якої частини призначеного для користувача інтерфейсу. Всі графічні об'єкти, включаючи текст, форми і анімацію, створюються за допомогою віджетів. Комплексні віджети можна створити, поєднавши безліч простіших, а додаток насправді є лише найбільшим віджетом із усіх (часто його називають "MyApp"). Віджет MyApp містить усі інші віджети, які можуть містити ще менші віджети, і разом вони складають додаток. Однак, створювати додатки Flutter можна і без віджетів, безпосередньо викликаючи методи бібліотеки Foundation для роботи з канвою. Фреймворк Flutter складається з двох наборів віджетів, які відповідають конкретним описам дизайну: Material design від Google і Cupertino для імітації дизайну додатків в Apple iOS[2].

Програма "Привіт, світ" у Flutter виглядає приблизно так:

```
import 'package:flutter/material.dart';

void main() => runApp(HelloWorldApp());

class HelloWorldApp extends StatelessWidget {
  @override
  Widget build(BuildContext context) {
    return MaterialApp(
      title: 'Hello World App',
      home: Scaffold(
        appBar: AppBar(
          title: Text('Hello World App'),
        ),
        body: Center(
          child: Text('Hello World'),
        ),
      ),
    );
  }
}
```

Рисунок 1 – Програма у Flutter

#### Література:

1. <https://flutter.dev/>
2. [https://en.wikipedia.org/wiki/Flutter\\_\(software\)](https://en.wikipedia.org/wiki/Flutter_(software))

## **УПРАВЛІННЯ РИЗИКАМИ ПРОЕКТУ СТВОРЕННЯ РОЗУМНОГО БУДИНКУ**

Технології «Розумного будинку» зараз дуже активно набирають популярність. Складовою частиною «Розумного будинку» є різного роду сигналізації і датчики (наприклад, датчики руху, задимлення, датчики відкритих дверей і вікон, системи відеоспостереження), які допомагають забезпечити безпеку квартир, котеджів і інших житлових приміщень, в яких встановлені дані системи. Всі ці компоненти керуються інформаційною системою «Розумного будинку». Також існує можливість запровадження спеціального вбудованого обладнання, що використовується правоохоронними органами та приватними охоронними підприємствами для охорони контрольної території. Переваги «Розумного будинку» розглянуті на порталі IQDim Львів [1]. Але, на жаль, крім великого числа переваг даної системи вона має і ряд недоліків. Згідно з рядом досліджень [2], даному типу систем притаманний ряд уразливостей. Також, в даний час прогнозується зростання числа правопорушень, пов'язаних з розумною технікою в цілому і розумними будинками зокрема.

Мета дослідження - виявлення найбільш вразливих частин управління проектом створення «Розумного будинку», ідентифікація та оцінка ризиків, а також вироблення рекомендацій щодо зменшення негативного впливу на результати таких проектів.

В основі дослідження було покладено державний стандарт ДСТУ ISO/IEC 27005:2015 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT) [3]. Для можливості його застосування в проведеному дослідженні довелося адаптувати процес управління ризиками. Для управління ризиками використовувалася схема, зображена на рисунку 1.

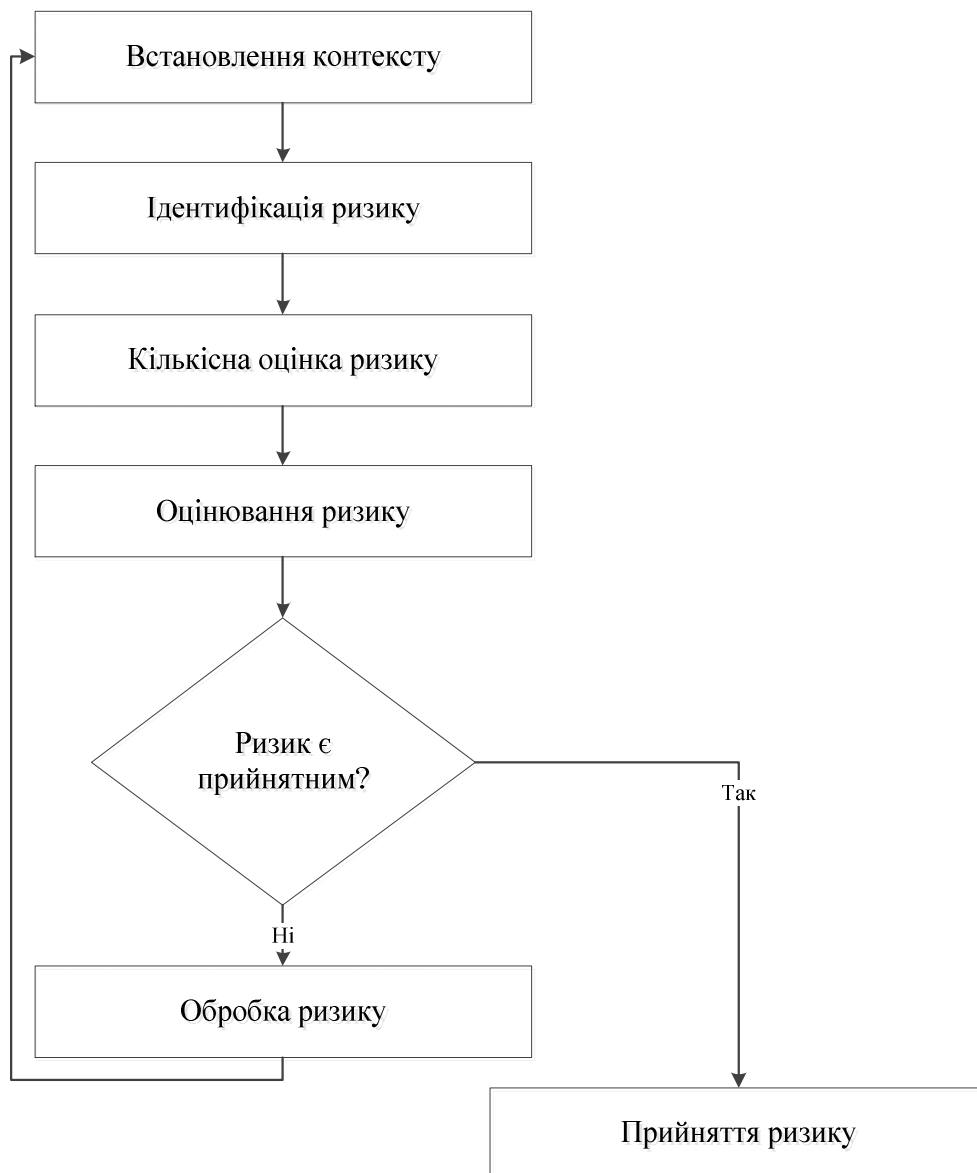


Рис. 1. Схема управління ризиками «Розумного будинку»

На етапі встановлення контексту шляхом експертної оцінки визначають шкали впливу ризикових подій на порушення цінностей активів. На етапі ідентифікації ризику в результаті оцінки були ідентифіковані уразливості, актуальні для систем, побудованих за технологією розумний будинок. В результаті актуальними були визнані 25 уразливостей, з яких вибрано дві, що подані в таблиці 1.

Таблиця 1

### Зіставлення загроз і пов'язаних з ними уразливостей

Загроза	Вразливість
Розкрадання документів і носіїв інформації	Недоліки фізичного захисту будівлі, вікон і дверей
	Неадекватне і недбале використання фізичного контролю доступу до будівлі та приміщень
	Незахищене зберігання
Помилка в використанні	Відсутність або недостатність механізмів моніторингу
	Недостатність вивчення питань безпеки

Наступним етапом було визначення актуальних загроз. Актуальними вважалися загрози, які порушують функціонування інформаційної системи (конфіденційність, цілісність або доступність). Всього було ідентифіковано 27 актуальних загроз. Найбільш небезпечними з них можна вважати наступні: фальсифікація прав, спотворення даних, втручання в програмні засоби, перехоплення і підміна переданих даних. В результаті зіставлення актуальних загроз, уразливостей, які використовуються при реалізації даних загроз і порушуваних властивостей активу було ідентифіковано 33 ризики, з яких вибрано три основні, що подані в таблиці 2.

Таблиця 2

### Основні ідентифіковані ризики

№	Загроза	Вразливість
1	Заподіяння шкоди вогнем / пожежею	Недоліки фізичного захисту будівлі
2	Значний інцидент (аварія)	Чутливість до перепадів напруги
3	Знищення обладнання або носіїв	Незахищене зберігання

Пропонується ряд заходів, які дають змогу вплинути на ідентифіковані ризики:

- 1) Використання в інформаційній системі «Розумний будинок» підсистеми розмежування доступу користувачів до об'єкта;
- 2) Розробка підсистеми конфіденційності зберігання і доступу до паролів користувачів інформаційної системи «Розумний будинок»;
- 3) Використання підсистеми шифрування даних інформаційної системи «Розумний будинок»;
- 4) Вироблення рекомендацій щодо конструкції вікон та дверей;
- 5) Періодичний перегляд прав доступу користувачів до управління інформаційною системою «Розумний будинок»;
- 6) Постійний моніторинг у системі системі «Розумний будинок» несанкціонованих вторгнень і міжмережевих екранів;
- 7) Постійний аналіз недоліків і уразливостей ПЗ, і своєчасне їх усунення;
- 8) Періодичний перегляд прав доступу до об'єкта.

### Висновки

Досліджена проблема незахищеності інформаційної системи «Розумний будинок», їх поточний стан в світі інформаційних технологій. Виконано ідентифікацію ризикових подій. В результаті були ідентифіковані загрози, характерні для систем, побудованих за технологією «Розумний будинок», а також актуальні уразливості. Всього було ідентифіковано 33 ризики. В результаті виконаних досліджень розроблений процес виявлення основних ризиків та вироблені рекомендації для їх зниження. Дотримання даних рекомендацій дозволить істотно підвищити рівень захищеності інформаційних систем, побудованих за технологією «Розумний будинок».

### Література:

1. Портал IQDim Львів [Електронний ресурс] - URL: <http://iqdim.com/perevagy-rozumnego-domu/> режим доступу: вільний (дата звернення 20.10.2019).
2. Огляд систем і технологій "Розумний будинок" [Електронний ресурс] - URL: <http://yakrobitiremont.pp.ua/sistema-rozumnij-budinok-visokointelektualne-zhitlo/> режим доступу: вільний (дата звернення 21.10.2019).
3. Сервіс документів [Електронний ресурс] - [http://online.budstandart.com/ua/catalog/doc-page.html?id\\_doc=66912](http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66912)

*Крикунова Г.Д.,  
студентка математичного факультету  
Запорізький національний університет  
м. Запоріжжя, Україна*

## ВИКОРИСТАННЯ ПРОТОКОЛУ OAuth2 ДЛЯ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧА У МОБІЛЬНИХ ДОДАТКАХ

Щоб безпечно отримати доступ до інтернет-сервісу, користувачі повинні пройти автентифікацію на службу – вони повинні надати підтвердження своєї особи. Для програми, яка отримує доступ до стороннього сервісу, проблема безпеки є ще складнішою. Для доступу до сервісу потрібно не тільки пройти автентифікацію користувача, але і додатку також потрібно дозволити діяти від імені користувача.

Галузевим стандартним способом роботи з автентифікацією сторонніх служб є протокол OAuth2. OAuth2 надає єдине значення, яке називається токеном автентичності, що представляє як особу користувача, так і дозвіл програми діяти від імені користувача.

Протокол OAuth2 використовується для:

- Отримання дозволу від користувача на доступ до онлайн-сервісу за допомогою акаунта користувача.

- Автентифікація онлайн-сервісу від імені користувача.

Передумовою використання OAuth2 є знання про:

- URL служби, до якої потрібно отримати доступ.
- Область автентифікації - це рядок, який визначає конкретний тип доступу, який запитує ваш додаток.

- Ідентифікатор клієнта та секрет клієнта - це рядки, що ідентифікують ваш додаток до сервісу. Потрібно отримати ці рядки безпосередньо у власника служби.

Порядок отримання дійсного auth token від Android Account Manager зображено на рис.1.

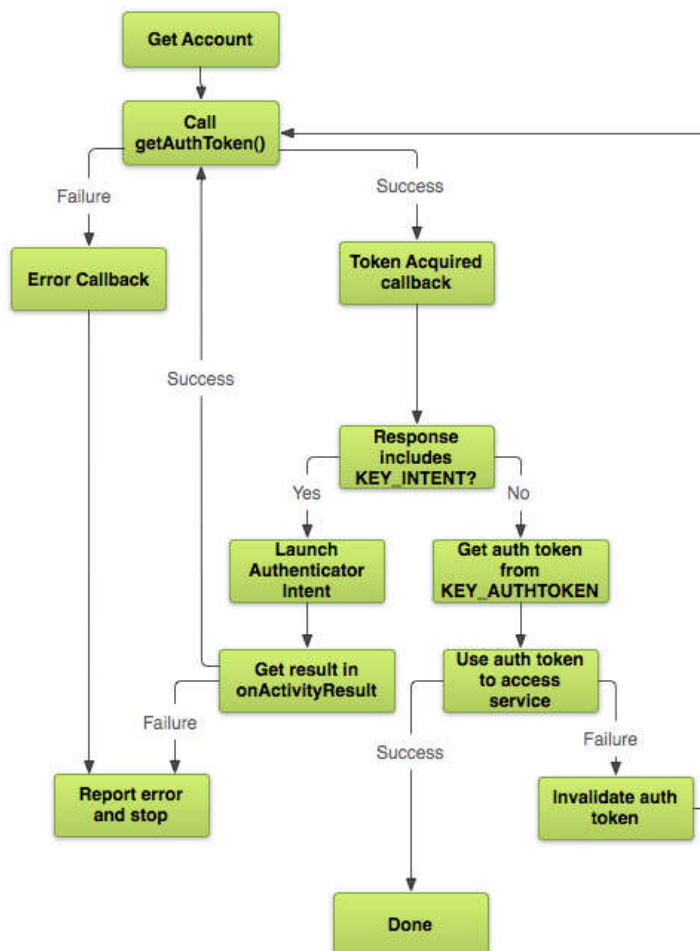


Рисунок 1 – Порядок отримання дійсного auth token

Наведений нижче приклад показує, як підключитися до сервера Google. Google використовує галузевий стандартний протокол OAuth2 для автентифікації запитів.

API Google вимагає, щоб було введено чотири значення з кожним запитом: ключ API, ідентифікатор клієнта, секрет клієнта та ключ авторизації. Перші три приходять з веб-сайту консолі Google API. Останнє - це значення рядка, яке отримали, викликавши `AccountManager.getAuthToken()`. Треба передати їх на сервер Google у рамках запиту HTTP.

```
URL url = new URL ("https://www.googleapis.com/tasks/v1/users/lists?key="
+ your_api_key);
```

```
URLConnection conn = (URLConnection) url.openConnection();
```

```
conn.addRequestProperty("client_id", your_client_id);
```

```
conn.addRequestProperty("client_secret", your_client_secret);
```

```
conn.setRequestProperty("Authorization", "OAuth " + token);
```

Якщо запит повертає код помилки HTTP 401, то токену відмовлено. Найпоширенішою причиною цього є те, що строк дії токену закінчився. Виправлення просте: треба викликати метод `AccountManager.invalidateAuthToken()`.

Отже, OAuth2 надає універсальний інтерфейс для доступу до різних сервісів, за допомогою якого можна здійснювати автентифікацію користувача



використовуючи різні облікові записи. OAuth2 - простий стандарт авторизації, заснований на базових принципах інтернету, що робить можливим застосування авторизації практично на будь-якій платформі.

#### Література:

1. Authenticate to OAuth2 services. URL:  
<https://developer.android.com/training/id-auth/authenticate>
2. Understanding OAuth2. URL:  
<http://www.bubblecode.net/en/2016/01/22/understanding-oauth2/>

*Кропенко Д.О.<sup>1</sup>, студент*

*Ходаковський О.В.<sup>2</sup>, к.т.н., доцент*

*Національний технічний університет України “Київський Політехнічний  
Інститут ім. Ігоря Сікорського”, м. Київ*

*<sup>1</sup>Кафедра автоматизації проектування енергетичних процесів і систем,  
студент*

*<sup>2</sup>Кафедра автоматизації проектування енергетичних процесів і систем,  
доцент*

## **ЗАХИСТ ШИФРОВАНОГО БЕЗДРОТОВОГО ЗВ'ЯЗКУ ПРИСТРОЇВ ВВЕДЕННЯ ІНФОРМАЦІЇ ВІД АТАК ПО ПОСТОРОННІМ КАНАЛАМ**

Оскільки бездротові технології стали для нас повсякденним явищем, ми часто вважаємо їх безпечними та все більше людей користуються бездротовими периферійними пристроями, оскільки останні вже практично зрівнялися за ціною з дротовими, однак мало хто замислюється, що такі пристрої не захищені від злому. Насьогодні відсутні стандарти, що регулюють безпеку бездротових периферійних пристроїв, з цієї причини питання захисту від злому залишається на виробниках [1].

Більш того, навіть захищений бездротовий зв'язок надійними та перевіреними алгоритмами шифрування даних є вразливим до атак по стороннім каналам: завдяки останнім досягненням в математиці є можливим проаналізувати зв'язок та частково або повністю відновити зміст передаючої інформації пристроями введення.

У доповіді буде описаний один із методів вилучення корисної інформації із трафіку захищеного бездротового зв'язку пристрою введення інформації та метод протидії подібним атакам.

Метою доповіді є демонстрація доступності виконання подібних атак та можливості їм протидії.

Подібний метод атаки згадується у вразливості CVE-2019-11184, де під час SSH сесії відправляються пакети у момент натискання клавіш на клавіатурі [2].

Даний метод атаки є атакою по часу — виконавши високоточний замір часу виконання різних подій та їх аналіз, можна розшифрувати захищені дані. Цей вид атаки є пасивним та неруйнівним [3].

Маємо пристрій введення інформації — клавіатуру Logitech K250, що використовує для з'єднання із комп'ютером донгл із радіоприймачем NRF24LU1. Для аналізу трафіку було використано RTL-SDR. Виявлено, що для передачі натискання клавіші відправляються два пакети — під час натискання клавіші та під час відпускання клавіші.

Варто відмітити, що затримки між натисканнями зазвичай залежать від положення клавіші на клавіатурі, можна з певною ймовірністю відтворювати інформацію, що вводиться. Наприклад, більшість людей зазвичай набирають "s" після "a" значно швидше, ніж "g" після "s". Маючи точні моменти передачі пакетів можна дати оцінку — наскільки ці моменти відповідають тому чи іншому слову [4].

Для подальшого аналізу необхідно отримати перевірочний набір моментів, кожен з яких відповідає певному слову. Отримати даний набір можна при звичайному введенні тексту на комп'ютері, зафіксувавши моменти натискання та відпускання клавіш.

Для оцінки використаємо формулу Евклідової відстані (1)[5]:

$$d = \sqrt{\sum_{i=1}^{2n} (x_i - y_i)^2}, \quad (1)$$

де  $d$  — відстань між словами;  $x_i$ ,  $y_i$  — моменти натискання для перевірного та отриманого слів;  $n$  — кількість букв у слові.

За допомогою формули отримаємо чисельний показник — наскільки моменти натискання отриманого слова відповідає моментам натискання перевірного слова. Виконуючи обчислення для усіх перевірочних слів можемо визначити отримане слово.

При великій кількості даних для пришвидшення обчислень можна використати простішу формулу, наприклад, Манхеттенську відстань (2)[5]:

$$d = \sum_{i=1}^{2n} |x_i - y_i| \quad (2)$$

Для протидії аналізу пропонується в ефір відправляти хибні пакети за допомогою пристрою. Даний пристрій можна створити на базі мікроконтролера ATMEGA-328P та радіопередавача NRF24L01. Схему з'єднання апаратних елементів пристрою зображено на рисунку 1.

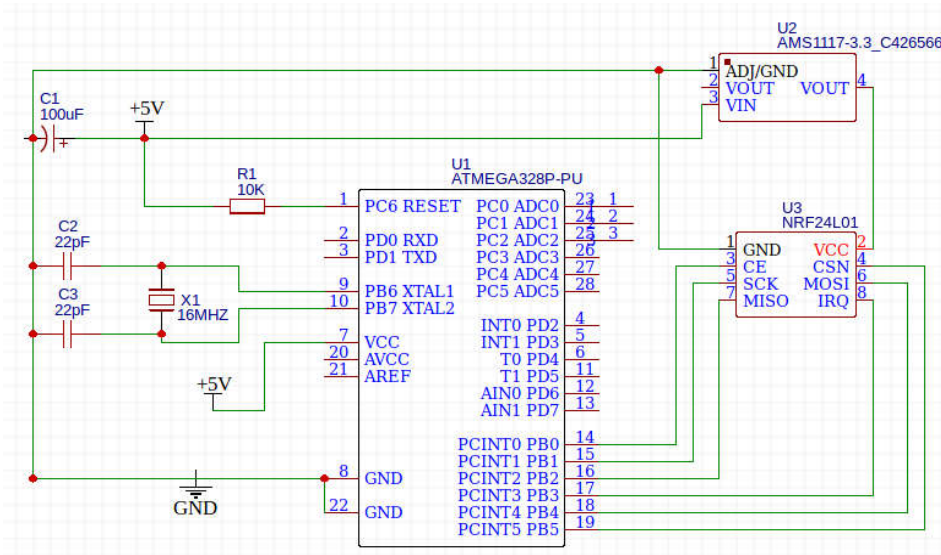


Рис. 1. З'єднання апаратних елементів

Передача хибних пакетів здійснюється із затримкою за розподілом Пуассона (3):

$$t = \frac{-\log\left(\frac{r}{r_{\max}}\right)}{\lambda}, \quad (3)$$

де  $\lambda$  — математичне очікування,  $r$  — невід'ємне випадкове число,  $r_{\max}$  — максимальне значення випадкового числа.

Завдяки використанню випадкової затримки згенерований трафік не заважає роботі пристроїв введення інформації та ускладнює аналіз трафіку для вилучення передаючої інформації.

### Висновки

Описано метод атаки на зашифрований зв'язок пристроїв введення інформації та аналіз трафіку. Запропоновано метод протидії подібним атакам, описано пристрій для захисту зв'язку.

Перспективами подальших досліджень у данному напрямку є дослідження можливості інтеграції описаного алгоритму захисту зв'язку при виробництві нових бездротових пристроїв введення інформації.

### Література:

1. Об опасностях беспроводных клавиатур и мышей [Електронний ресурс] — Режим доступу: <https://habr.com/company/pt/blog/325932/>
2. INTEL-SA-00290 [Електронний ресурс] — Режим доступу: <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html>
3. Обзор видов атак по побочным каналам на криптографические устройства. Подлеснов А. В. Молодой учёный. 2015. № 1. с. 187-189
4. Реализация DDIO в чипах Intel допускает сетевую атаку по определению нажатий клавиш в сеансе SSH [Електронний ресурс] — Режим доступу: <https://www.opennet.ru/opennews/art.shtml?num=51467>
5. Taxicab geometry world [Електронний ресурс] — Режим доступу: <http://www.ams.org/publicoutreach/feature-column/fcarc-taxi>

*Кузьмініх В.О., канд. тех. наук, доцент  
Національний технічний університет України  
“Київський політехнічний інститут імені Ігоря Сікорського”, м. Київ  
Кафедра автоматизації проектування енергетичних процесів і систем,  
доцент*

*Пивовар Н.О., студент ТВ-381мп  
Національний технічний університет України  
“Київський політехнічний інститут імені Ігоря Сікорського”, м. Київ  
Кафедра автоматизації проектування енергетичних процесів і систем,  
студент*

## **СИСТЕМА АНАЛІЗУ ЗБІЖНОСТІ ТЕКСТОВОЇ ІНФОРМАЦІЇ ДЛЯ ОЦІНКИ ПЛАГІАТУ**

Розвиток та розповсюдження засобів комунікації і доступу до мережі Інтернет сприяє збільшенню спектру інформації до якої людина має доступ. За допомогою звичайного смартфона можна здійснити пошук будь-якої інформації. Тим не менш, звідси виникає нова проблема: так як кожен може отримати доступ до будь-якої інформації, значно складніше оцінити чи є вона оригіналом чи взята з інших відкритих джерел. Досить часто у мережі Інтернет можна знайти джерела інформації (будь то статті, сайти, онлайн журнали і т.п.), які майже повністю складаються з фрагментів тексту інших джерел. Сьогодні існують такі програми як Advego Plagiatius, Etxt Antiplagiat та онлайн сервіси як UNPLAG, Content-Watch та інші. Проте мало які системи дають точні результати і рекомендується перевіряти результати у декількох системах. Так як для людини це досить не проста задача було прийнято рішення розробки системи аналізу збіжності текстової інформації для оцінки плагіату.

Проведений аналіз показав, що за допомогою програмного середовища Python [1] (а саме Flask, sklearn, numpy) можна розробити програмний продукт для пошуку і порівняння інформації з відкритих джерел. У якості алгоритму для оцінки збіжності було вирішено використати векторний метод із групуванням слів у тріади (3-грами) [2]. Це дозволило відстежувати не тільки ідентичні фрагменти тексту з інших джерел, а і мінімально трансформовані речення, у яких, наприклад, слова переставлені місцями. В той же час, такий алгоритм менш чутливий до омонімів і текстів зі схожим набором слів, але зовсім іншим сенсом. Варте уваги і те, що така модифікація алгоритму є більш складною задачею з точки зору обчислень, тому що тепер потрібно комбінувати слова у групи з по 3 елементи і зі збільшенням кількості слів збільшується і розмір вектору, а звідси збільшується час виконання алгоритму.

Розроблена система, отримавши запит на перевірку текста, починає пошук заданої теми у відкритих джерелах і завантажує тексту сторінок. Після цього відбувається виокремлення текстової інформації з HTML-коду і створення вектору. Вектори всіх знайдених джерел перевіряються на подібність і відбираються найбільш схожі методом косинусу подібності двох векторів [2]. Після цього система відображає користувачеві список посилань на джерела з

яких ймовірно взята інформація у тексті, що перевіряється. Блок-схема алгоритму зображено на рисунку 1.1.

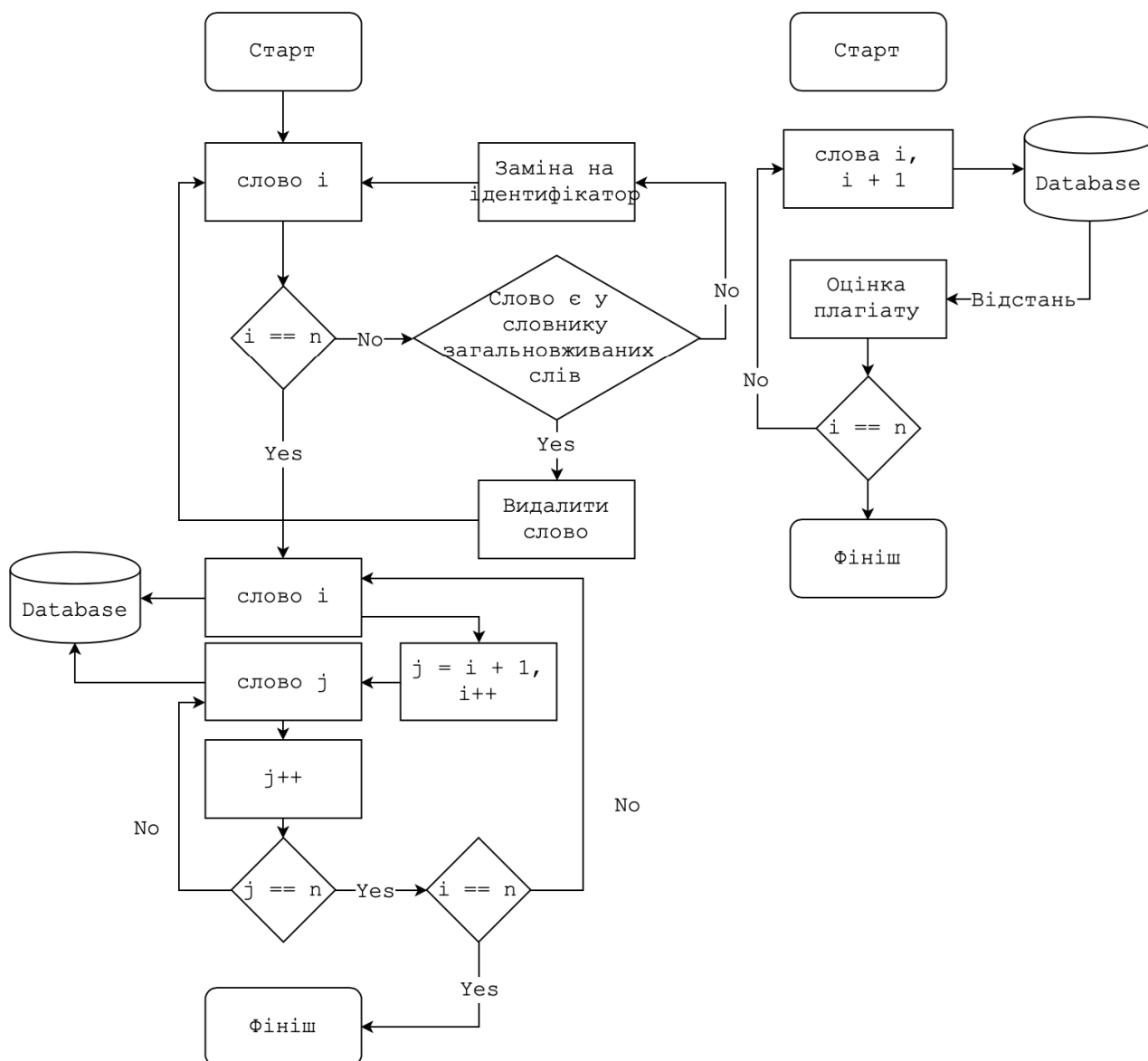


Рисунок 1.1

Розроблений підхід досить ефективно проводить перевірку тексту на плагіат або навіть пошук робіт, які були використані у тексті, що перевіряється.

#### Література:

1. Марк Лутц. Программирование на Python / Марк Лутц. — СПб.: Символ-Плюс, 2011. — 992 с.
2. sklearn.metrics.pairwise.cosine\_similarity — scikit-learn 0.21.3 documentation [Електронний ресурс]: — Режим доступу: [https://scikit-learn.org/stable/modules/generated/sklearn.metrics.pairwise.cosine\\_similarity.html](https://scikit-learn.org/stable/modules/generated/sklearn.metrics.pairwise.cosine_similarity.html).

*Лук'янова Г.Ю., старший викладач  
Балаклійська філія Комунального закладу  
«Харківська гуманітарно-педагогічна академія» Харківської обласної  
ради,  
м. Балаклія  
Початкова освіта, викладач*

## **ФОРМУВАННЯ ПРОФЕСІЙНИХ КОМПЕТЕНЦІЙ МАЙБУТНЬОГО ПЕДАГОГА ЗА ДОПОМОГОЮ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

Підготовка компетентного педагога з високим рівнем загальної та професійної культури, фундаментальними знаннями в області методології, педагогіки, системним баченням педагогічних проблем в освіті направлена на вдосконалення і формування у майбутніх вчителів власного стилю творчої педагогічної діяльності.

Технологічна підготовленість вчителя є важливою ланкою в розумінні категорії «педагогічна компетентність», що є суттю педагогічної культури, яка виконує функції відтворення і збереження педагогічної реальності. Технологічна культура майбутнього вчителя, що розглядається сьогодні як основоположна ланка успішності в майбутній професійній діяльності, є процесом творчої самореалізації внутрішніх сил студентів.

Незалежно від спеціалізації та характеру майбутньої професійної діяльності, будь-який фахівець-початківець має володіти фундаментальними знаннями, професійними вміннями й навичками. Важливе значення в придбанні цих знань, умінь і навичок мають досвід творчої, дослідницької та самостійної діяльності, що дозволяє майбутньому фахівцеві визначити свою позицію з того або іншого професійно-орієнтованого питання або проблеми.

Для досягнення високого рівня науково-практичної підготовки студентів, необхідно розв'язати дві головні проблеми: забезпечити можливість здобуття студентами глибоких фундаментальних знань; змінити підходи до організації самостійної роботи студента. Сьогодні актуальна самостійна робота студента з використанням інформаційних технологій, що дозволяє поставити самостійну роботу студента на новий рівень самостійності суб'єкта вчення.

Використання інформаційних технологій в процесі навчання дозволяє змінити характер освітньої діяльності студентів, активізувати самостійну роботу студентів з різними електронними засобами навчального призначення.

У системі вишівській підготовки фахівців важлива орієнтація майбутнього вчителя на поєднання навчально-виховної роботи в школі з науковими пошуками. Процеси кардинальних перетворень в сучасній школі вимагають від вчителя переорієнтації його діяльності на нові педагогічні цінності, адекватні характеру наукової творчості, що, у свою чергу, висвічує одну з основних проблем вищої освіти – формування науково-дослідницької культури вчителя.

Актуалізує тему формування професійних компетенцій майбутнього педагога технічний і технологічний процес, який спричиняє появу нового виду інформаційних продуктів, що об'єднують текст, звук, зображення, а також нового виду інформаційних послуг. Використання сучасних інформаційних систем у сфері освіти забезпечує принципово новий рівень здобуття і узагальнення знань, їх поширення і використання в самостійній і науково-дослідницькій діяльності студента.

Включення інформаційних технологій в навчальний процес у закладах вищої освіти вирішує наступні завдання:

- забезпечення інформацією студентів в навчальному процесі;
- формування ключових компетенцій студентів;
- інтеграція базової та додаткової освіти;
- підвищення мотивації студентів до вчення й ін.

Головним завданням сьогодення у сфері вищої професійної освіти є виховання таких людей, які були б здатні застосовувати свої знання в умовах, що змінюються, і чия основна компетенція полягала б в умінні включитися в постійне самонавчання впродовж всього свого життя.

*Мазниченко Н.І.*

*Національний юридичний університет імені Ярослава Мудрого, м. Харків  
Кафедри криміналістики, старший викладач*

## **МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ КОМП'ЮТЕРНОЇ ІНФОРМАЦІЇ ОБМЕЖЕНОГО ДОСТУПУ В ЮРИДИЧНІЙ ДІЯЛЬНОСТІ**

У зв'язку з розповсюдженням та впровадженням інформаційно-комунікаційних технологій в будь-які сфери діяльності людини значно збільшуються можливості для створення, обробки, збереження, поширення, передачі різноманітної інформації. Сьогодні неможливо уявити діяльність юристів без використання сучасних технологій. В різноманітних комп'ютерних системах та сучасних цифрових засобах зберігаються величезні обсяги інформації, що мають відношення до їх професійної діяльності. Серед такого обсягу може бути інформація, що має статус обмеженого доступу. Згідно зі ст. 6 Закону України «Про доступ до публічної інформації» та ст. 21 Закону України «Про інформацію») до інформації обмеженого доступу належить конфіденційна, таємна та службова інформація. Професійна діяльність юристів незалежно від спеціалізації обов'язково буде пов'язана з опрацюванням інформації обмеженого доступу. До такої інформації належить, наприклад, лікарська таємниця, таємниця листування, таємниця слідства, таємниця усиновлення (удочеріння), нотаріальна таємниця, комерційна та банківська таємниця, адвокатська таємниця, конфіденційна інформація про особу, інформація, що зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності і тощо. За розголошення, поширення, розповсюдження деяких різновидів такої інформації в законодавстві України передбачена

відповідальність, в тому числі і кримінальна. Тобто, мова йде не про можливість, доцільність, бажаність, а про обов'язковість захисту такої інформації. Забезпечення правомірного використання інформації обмеженого доступу та захист від неправомірного використання – складова професійної діяльності юристів.

Якщо захистом інформації обмеженого доступу в деяких державних реєстрах та базах даних займаються відповідні структурні підрозділи інформаційної безпеки, співробітники яких зобов'язані забезпечувати надійний захист зазначених інформаційних ресурсів, на власних комп'ютерних системах звичайні юристи повинні самостійно дбати про захищеність такої інформації, якщо вона міститься в поточних робочих документах. Для досягнення цієї мети кожен юрист повинен бути обізнаним в сучасних технологіях захисту інформації, що зберігається в комп'ютерних системах та передається по мережах. Спробуємо розглянути особливості, переваги та недоліки кожного з захисних механізмів та систематизувати їх.

Першою розглянемо технологію захисту інформації обмеженого доступу на основі систем ідентифікації користувачів. Дана технологія обмежує доступ на основі унікального ідентифікатора, яким володіє легітимний (авторизований) користувач.

В якості ідентифікатора в сучасних системах можуть бути використані [1, с. 216]: або унікальні знання (парольна ідентифікація), або унікальна фізіологічна чи поведінкова характеристика (біометрична ідентифікація), або унікальний предмет – електронний ключ (апаратна ідентифікація).

Найпоширенішою на сьогоднішній день є парольна ідентифікація завдяки простоті реалізації і застосування. Але в той же час така ідентифікація є найслабшою, враховуючи людський фактор та спектр програмних засобів, спрямованих на визначення пароля.

Щодо біометричної ідентифікації, то можна відмітити, що на сьогоднішній день для обмеження доступу до сучасних комп'ютерних систем та інформаційних ресурсів найчастіше використовують такі характеристики, як відбиток пальця, сітківка ока, райдужна оболонка ока, зображення обличчя, голос і т. і. Головною перевагою біометричних технологій є найвища надійність завдяки унікальності кожної такої характеристики для окремої людини. Основним недоліком біометричної ідентифікації є потреба в придбанні додаткового обладнання (сканера) для отримання відповідної характеристики.

Враховуючи тенденції розвитку сучасних цифрових пристроїв, наявність сенсорного екрану, вбудованої камери, вбудованого мікрофону, можна припустити, що будуть запитані такі біометричні характеристики, як відбиток пальця (touch ID), зображення обличчя (face ID), голос, графічний підпис, тому що для отримання перерахованих ознак не потрібне додаткове обладнання.

Системи апаратної ідентифікації ґрунтуються на визначенні особи користувача по якомусь предметі, ключу, що перебуває в його ексклюзивному користуванні. На даний момент найбільше поширення одержали два типи пристроїв: різноманітні карти (проксиміті-карти, смарт-карти, магнітні карти і т.д.) та так звані токени (token), які підключаються безпосередньо до одного з



портів комп'ютера. Головним достоїнством застосування апаратної ідентифікації є досить висока надійність. Найбільш серйозною небезпекою у випадку використання апаратної ідентифікації є можливість крадіжки зловмисниками токенів або карт у зареєстрованих користувачів. Також вони можуть бути втрачені, передані іншій особі, дубльовані.

Слід відзначити, що останнім часом для підвищення рівня захищеності інформаційних ресурсів комп'ютерних систем використовують комплексні або багатофакторні системи ідентифікації [2]. В таких системах для визначення особи користувача комп'ютерної інформаційної системи застосовується відразу кілька параметрів, що в свою чергу підвищує рівень захищеності інформаційних ресурсів.

Останнім часом все більшої популярності як ідентифікаційна ознака набуває електронний підпис. Найчастіше така характеристика використовується для доступу до інформації деяких державних реєстрів, до власних електронних кабінетів при роботі з деякими сервісами в режимі online і т.д., але для захисту інформації обмеженого доступу на локальних комп'ютерах така ідентифікаційна ознака не застосовується.

Наступною технологією захисту комп'ютерної інформації розглянемо шифрування (криптографія) – оборотне перетворення інформації з метою приховування від неавторизованих осіб, з наданням, в той же час, авторизованим користувачам доступу до неї. Для реалізації шифрування потрібні алгоритм та ключ. Алгоритм – це правило перетворення інформації в зашифровану. Ключ підтверджує вибір конкретного перетворення із сукупності можливих для даного алгоритму. Ключ – інформація, необхідна для здійснення процесу шифрування і дешифровки текстів.

За особливостями алгоритму шифрування буває симетричним та асиметричним. В симетричних криптосистемах один той самий ключ використовується для шифрування та дешифрації (повернення інформації в початковий стан). Доцільно використовувати для збереження інформації в захищеному виді на локальному комп'ютері (немає потреби передавати ключ іншому користувачеві). В асиметричних криптосистемах (системах з відкритим ключем) використовується два ключі: відкритий ключ – для шифрування та відповідний йому секретний – для розшифрування. Доцільно використовувати при необхідності передачі конфіденційної інформації по комп'ютерним мережам, оскільки передача партнерові за перепискою по мережі відкритого ключа не представляє небезпеки. На сьогоднішній день асиметричне шифрування вважається найбільш надійним способом захисту комп'ютерної інформації.

Наступною технологією, що застосовується в області захисту конфіденційної інформації, розглянемо цифрову стеганографію, що активно розвивається останніми роками. Стеганографія (з грецької – тайнопис) – наука про приховану передачу інформації шляхом збереження в таємниці самого факту передачі. Цифрова стеганографія заснована на надмірності мультимедійних даних, представлених в цифровій формі, які спочатку мали аналогову природу (зображення, відео, звук) [3, с. 183]. Внесення змін в такі

об'єкти знаходяться нижче порога чутливості середньо статистичної людини і не помітні для загального сприйняття. Цифрова стеганографія має декілька напрямків застосування, одним з яких є вбудовування інформації з метою її прихованої передачі. Захист інформації обмеженого доступу здійснюється за рахунок приховування секретної інформації в цифровій формі всередині іншої інформації в цифровій формі від необізнаного користувача. Основна мета – непомітність впровадження секретної інформації в інший файл (контейнер), яка реалізується за рахунок психовізуальної надмірності, що є в цифрових сигналах (графіка, звук, відео, текст). Тобто, після впровадження секрету в файл-контейнер (отримаємо стегоконтейнер) необізнаний користувач звичайними органами чуття ніяких змін не помітить. Таким чином можна передавати по мережах конфіденційну інформацію. Користувач, для якого ця інформація призначалась, зможе її отримати.

У зв'язку з особливостями професійної діяльності кожен юрист повинен дбати про захист інформації обмеженого доступу, що зберігається в комп'ютерних системах та передається по мережах. Для досягнення цієї мети доцільно: 1) максимально об'єктивно оцінити рівень небезпек та загроз для такої інформації в кожній конкретній ситуації; 2) після аналізу обрати ту технологію захисту, що є найбільш ефективною і забезпечить достатній рівень захисту; 3) придбати та встановити програмне забезпечення, що реалізує обрану технологію (в разі потреби, якщо дана технологія не є вбудованою). Також слід пам'ятати, що сучасні версії операційних систем мають достатньо вбудованих захисних механізмів, якими не варто нехтувати.

#### **Література:**

1. Кошева Н.А., Мазниченко Н.І. Ідентифікація користувачів інформаційно-комп'ютерних систем: аналіз і прогнозування підходів // Системи обробки інформації. Випуск 6 (113). – Харків: Харківський університет Повітряних Сил імені Івана Кожедуба, 2013. – 320 с. – С. 215-223.
2. Шрамко В.Н. Комбинированные системы идентификации и аутентификации [Электронный ресурс] // PCWeek/RE. – 2004. – №45. – Режим доступа: <https://www.itweek.ru/infrastructure/article/detail.php?ID=69114>
3. Абазина Е. С., Ерунов А. А. Цифровая стеганография: состояние и перспективы // Системы управления, связи и безопасности. Научный журнал. – № 2, 2016. С. 182-201.

**Мартовицкий В.А., ст. преподаватель**  
**Осипова Д.Ю., студент**

*Харьковский Национальный Университет Радиоэлектроники, г. Харьков*  
*Кафедра Электронных вычислительных машин*

## **ШАБЛОН CQRS В СОВРЕМЕННЫХ WEB-ПРИЛОЖЕНИЯХ**

Основной подход, который люди используют для взаимодействия с информационной системой, это рассмотрение этой системы как хранилище данных, поддерживающие CRUD. CRUD – акроним, обозначающий четыре

базовые функции, используемые при работе с базами данных: создание (англ. *create*), чтение (англ. *read*), модификация (англ. *update*), удаление (англ. *delete*). То есть, подразумевается, что существует модель некоторой базы данных, в которой мы можем создавать новые записи, читать записи, обновлять существующие записи и удалять записи. В простейшем случае все наши действия связаны с хранением и извлечением этих записей. Поскольку потребности разработки становятся все сложнее, от такой модели постепенно стараются отойти. Например, может понадобиться взглянуть на информацию иначе, чем на тривиальное хранилище записей. Чтение данных сложив несколько записей в одну или сформировав виртуальные записи путем объединения информации для разных мест, а в обновление данных добавить правила проверки, которые позволяют хранить только определенные комбинации данных. Чтобы реализовать такие изоцированные запросы, разработчики изобрели много шаблонов: объектно-ориентированная парадигма разработки, шаблоны проектирования, разработка через тесты (Test-Driven Development, TDD), предметно-ориентированное проектирование (Domain-Driven Design, DDD), а также CQRS.

CQRS – Command Query Responsibility Segregation, что означает дословно распределение ответственности между командами и запросами. В значении разработки программного обеспечения CQRS это стиль архитектуры, в котором операции чтения отделены от операций записи. [1]

CQRS происходит из идеи шаблона CQS (англ. Command Query Separation). Основная идея CQS заключается в том, что все методы должны быть либо функциями (запросы) или процедурами (команды):

- **Запросы:** метод возвращает результат выполнения и не имеет побочных эффектов;
- **Команды:** методы выполняет некоторое действие и не возвращает результат;

Важные причины разделения команд и запросов заключаются в следующем:

- Сильный дисбаланс между количеством чтений и записей при работе с большим объемом информации. Операций на чтение существенно больше чем на изменения;
- Одна программная модель, включающая в себя и запись и чтение, в случае с массивными данными работает недостаточно хорошо;

В подходе CQS эта идея применяется на уровне архитектуры приложения, разделяя ее на две части: чтение и запись, а идея паттерна CQRS поднимается на уровень объекта, а не методов. Используя CQRS в реальном приложении, можно добиться того, что бизнес-логика не будет ничего знать про тип источника данных. Она будет оперировать только Запросами и Командами. При правильном подходе, это может существенно упростить создание и дальнейшее сопровождение приложения.

## CQRS Pattern

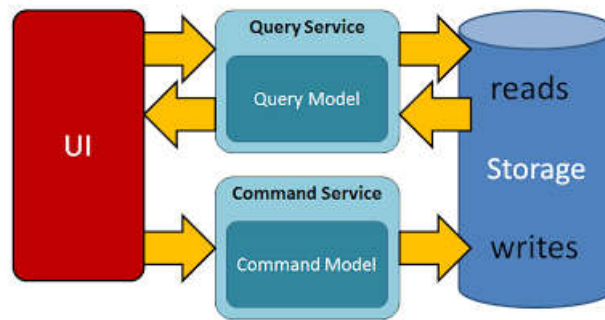


Рис. 1 – Схема работы шаблона CQRS [2]

На небольшом примере рассмотрим, как может выглядеть реализация CQRS.

Условие – необходимо хранить список пользователей.

```
public class User
{
    public int Id { get; set; }
    public string Url { get; set; }
}
```

Рис. 2 – Листинг класса User

Реализация Запроса, возвращающего пользователя по его *Id*. В конструкторе передадим источник данных, а метод *Execute()* будет возвращать нужный объект.

```
public class GetUrlByIdQuery
{
    private readonly IEnumerable<User> _dataSource;

    public GetUrlByIdQuery(IEnumerable<User> dataSource)
    {
        this._dataSource = dataSource;
    }

    public Link Execute(int id)
    {
        return this._dataSource.FirstOrDefault(e => e.Id == id);
    }
}
```

Рис. 3 – Листинг запроса GetUrlByIdQuery

Реализация команды. [3]

```

public class AddUserCommand
{
    private readonly ICollection<User> _dataSource;

    public AddUserCommand(ICollection<User> dataSource)
    {
        this._dataSource = dataSource;
    }

    public void Execute(string url)
    {
        int maxId = this._dataSource.Max(e => e.Id) + 1;
        this._dataSource.Add(new User() {
            Id = maxId,
            Url = url
        });
    }
}

```

Рис. 4 – Листинг команды AddUserCommand

Сравнение достоинств и недостатков системы CQRS.

Достоинства:

- Меньше зависимостей в каждом классе;
- Соблюдается первый принцип SOLID – Single Responsibility

Principle

- Легко заменяем на другой шаблон проектирования
- Легко тестируется
- Легко расширяемая функциональность.

Недостатки:

- Подход появился относительно недавно, поэтому слабо распространен.
- Если в команде и запросе появляется общая логика, дизайн системы усложняется, так как приходится использовать композицию, наследование, агрегацию.
- Сложно целиком придерживаться CQS и CQRS.
- Плохо взаимодействует с CRUD-приложениями.

Чтобы приложения были по-настоящему эффективными, они должны подстраиваться под требования бизнеса. Архитектура, основанная на CQRS, значительно упрощает расширение и модификацию рабочих бизнес-процессов и поддерживает новые сценарии.

#### Литература:

1. Microsoft Azure. [Электронный ресурс]. 2005. Дата обновления: 14.05.2019. URL: <https://docs.microsoft.com/ru-ru/azure/architecture/patterns/cqrs> (дата обращения: 09.11.2019)
2. Medium. [Электронный ресурс]. 2017. Дата обновления: 05.12.2017. URL: <https://medium.com/@domagojk/patterns-for-designing-flexible-architecture-in-node-js-cqrs-es-onion-7eb10bbefe17> (дата обращения: 09.11.2019)
3. Refactoring GURU. [Электронный ресурс]. 2014. Дата обновления: 10.09.2019. URL: <https://refactoring.guru/ru/design-patterns/command> (дата обращения: 09.11.2019).

*Медведєв Р.Б., к.т.н., професор*  
*Складанний Д.М., к.т.н., доцент*  
*Крайнік А.Р., магістрант*  
Національний технічний університет України  
«Київський політехнічний інститут імені Ігоря Сікорського», м. Київ.  
Кафедра кібернетики хіміко-технологічних процесів

## АЛГОРИТМ ВИЯВЛЕННЯ ПАРИ У ТЕПЛОНОСІЇ ПЕРШОГО КОНТУРУ ВОДО-ВОДЯНОГО РЕАКТОРА АЕС

Пароутворення є однією з найнебезпечніших явищ, яке може статися у теплоносії першого контуру водо-водяного реактора атомної електростанції [1, 2]. Встановлена у контурі система компенсації об'єму запобігає аварійним ситуаціям у випадку випаровування теплоносія, але під час інтенсивного випаровування може виявитися недостатньою. Тому важливим є виявлення пари в теплоносії на ранніх етапах пароутворення з метою термінового вжиття відповідних заходів [1, 2]. Тому задача створення алгоритму оцінювання ймовірності появи пари є актуальною.

Під час розроблення алгоритму слід врахувати, що щодо теплоносія першого контуру з метою запобігання корозії обладнання продуктами радіоактивного розпаду води, застосовується процедура борного регулювання. Розчин борної кислоти, який в результаті утворюється добре проводить електричний струм. Тому для фіксації появи пари пропонуємо скористатися наступним алгоритмом:

У випадку, якщо борне регулювання проводилося (це можна встановити за записами реєстрації дій, які ведуться на АЕС), вимірювання електропровідності потрібно здійснювати вздовж та впоперек трубопроводу. Відстань між електродами в обох випадках має бути однаковою. Ймовірність появи пари у такому випадку пропонується визначати за сигмоїдальною функцією (1) [3]:

$$Pr = \frac{1}{1 + \exp(-0,9 \cdot (x - 5,6))} \quad (1)$$

У якості аргументу сигмоїдальної функції приймемо збільшене у 100 разів відносне відхилення між електропровідністю в повздовжньому та поперековому напрямі (2). Очевидно, що електропровідність у повздовжньому напрямі буде не меншою, ніж у поперековому.

$$x = \frac{E_{\text{ПД}} - E_{\text{ПП}}}{E_{\text{ПД}}} \cdot 100 \quad (2)$$

де  $E_{\text{ПД}}$  – електропровідність вздовж трубопроводу,  $E_{\text{ПП}}$  – поперек трубопроводу.

У випадку відсутності борної кислоти (борне регулювання не проводилося), електропровідність розчину забезпечується власною провідністю води і розчинених і ній продуктів радіолізу та корозії. Ймовірність появи пари у такому випадку вираховується сигмоїдальною функцією (3) [3]:

$$Pr = \frac{1}{1 + \exp(90 \cdot (E - 0,11))} \quad (3)$$

де  $E$  – електропровідність, в цьому випадку єдина, вимірювана поперек трубопроводу.

Для проведення імітаційного експерименту оберемо режим борного регулювання, за якого до контуру вводиться чиста вода. Концентрація борної кислоти у такому випадку буде змінюватися за рівнянням (4).

$$C(t) = C_0 \exp\left(\frac{-Q_{\text{пр}}}{V} t\right) \quad (4)$$

Результати такого імітаційного експерименту наведено на рисунку 1.

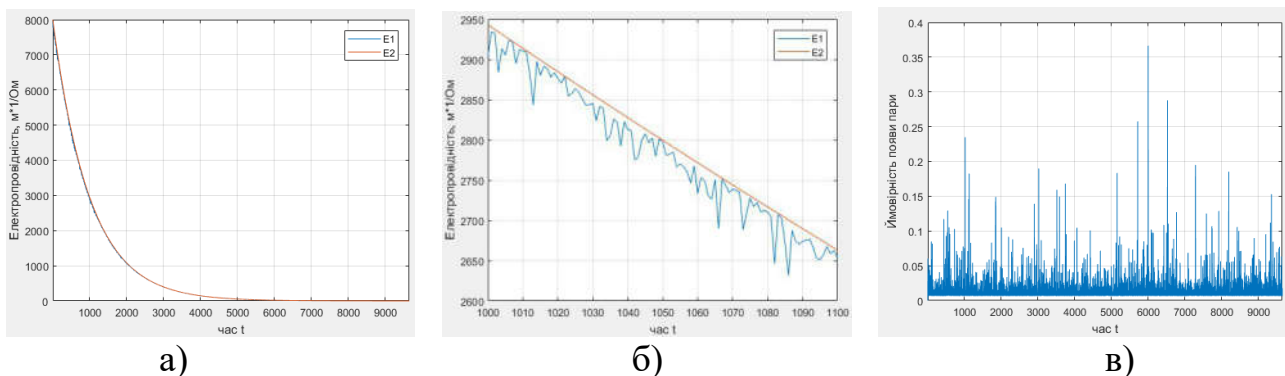


Рисунок 1. Результати імітаційного експерименту за наявності борної кислоти (режим додавання чистої води): а) розіграш електропровідності; б) ділянка 1000 ÷ 1100 графіку а. в) розрахунок ймовірності пароутворення.

На рисунку 2 наведено результати аналогічного імітаційного експерименту, проведеного за умов повної відсутності борної кислоти в теплоносії першого контуру.

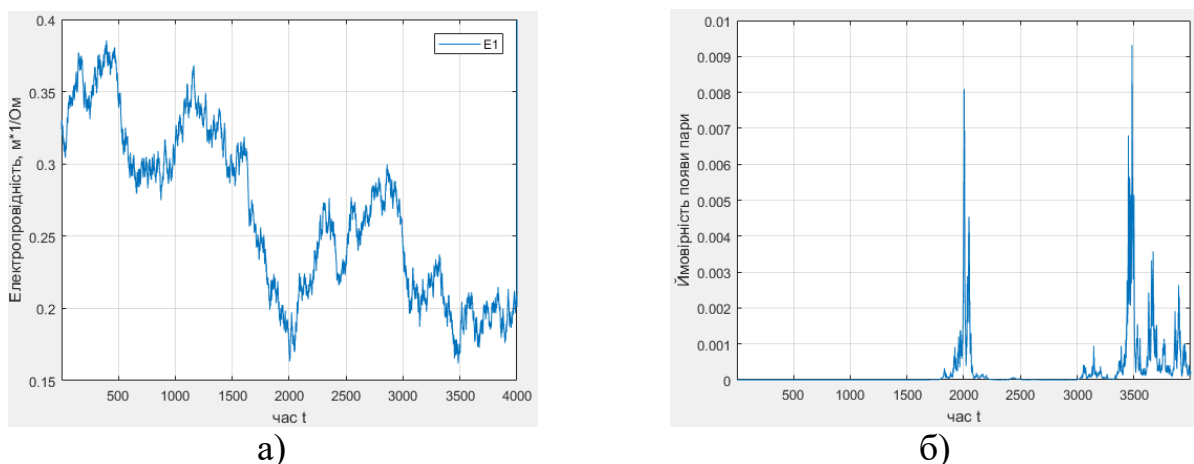


Рисунок 2. Результати імітаційного експерименту за відсутності борної кислоти: а) розіграш електропровідності; б) розрахунок ймовірності пароутворення.

Таким чином, запропонований алгоритм, за умови наявності нескладних технічних засобів, може успішно вирішувати задачу виявлення пари у потоці теплоносія першого контуру водо-водяного ядерного реактора.

### Література:

1. ВВЭР-1000: физические основы эксплуатации, ядерное топливо, безопасность / Афров А.М. та ін. Москва, 2006, 488 с.
2. АЭС с реактором типа ВВЭР-1000. От физических основ эксплуатации до эволюции проекта / Андрущечко С.А. та ін. Москва, 2010, 604 с.
3. *Медведев Р.Б.* Функція приналежності для алгоритму виявлення водяної пари у теплоносії першого контуру АЕС з реактором ВВЕР-1000 / Р.Б. Медведев, Д.М. Складанний, А.Р. Крайнік // Збірник наукових статей КМХТ 2019, Київ, 2019, С. 111-112.

*Міхєєв О.С.*

*Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ  
Кафедра автоматизації проектування енергетичних процесів і систем,  
студент*

## **ДЕЦЕНТРАЛІЗАЦІЯ ФУНКЦІЙ СЛУЖБИ КАТАЛОГІВ МУЛЬТИАГЕНТНОЇ СИСТЕМИ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ З МЕТОЮ ПІДВИЩЕННЯ ГОРИЗОНТАЛЬНОЇ МАСШТАБОВАНOSTІ ТА СТАБІЛЬНОСТІ СИСТЕМИ**

Служба каталогів - це компонент мультиагентної платформи, який надає агентам послуги з жовтими сторінками. Основною метою служби каталогів є надійне збереження інформації щодо стану агентів активної системи, а також підтримання точного, повного та актуального переліку агентів. Тобто, служба каталогів надає найактуальнішу інформацію про будь-якого агента свого каталогу на недискримінаційній основі всім уповноваженим агентам.

Кожен агент, який хоче оприлюднити свої послуги іншим агентам, повинен знайти відповідну службу каталогів та запросити реєстрацію його опису. Для реєстрації необхідно надати опис агента, що містить обов'язкові параметри опису. Також можуть бути надані необов'язкові та приватні параметри, що містять стандартизовану інформацію, яку розробник агента вважає необхідною до збереження у каталозі. Не передбачено майбутніх зобов'язань чи зобов'язань з боку зареєстрованого агента. Наприклад, агент може відмовити в запиті на виконання функції, яка зареєстрована через «Службу каталогів». Крім того, служба каталогів не може контролювати життєвий цикл будь-якого з зареєстрованих агентів.

Наявність каталогу агентів і єдиного головного контейнера платформи дозволяє агентам спілкуватися (обмінюватися інформацією) між собою. При цьому така взаємодія можливо всередині контейнера, між контейнерами однієї платформи (між агентами різних контейнерів на одній платформі) і між платформами (між агентами в контейнерах різних платформ). Обмін повідомленнями здійснюється асинхронно, з використанням черг.

Служба каталогів є найбільш навантаженим агентом мультиагентної системи через постійні звернення за інформацією з боку інших учасників системи. Стандарт FIPA передбачає наявність декількох служб каталогів з



метою зменшення навантаження на кожен з каталогів. Такий підхід збільшує час обробки інформації з метою прийняття рішень з боку функціональних агентів, що може призвести до непередбачуваних наслідків у рамках енергетичної інфраструктури.

Одним із варіантів розподілу навантаження на службу каталогів є децентралізація функцій реєстрації та дереєстрації між агентами-учасниками системи. Кожен агент містить інформації про свої функціональні можливості та локально зберігає інформацію лише про необхідних йому агентів або служб. Використання протоколу UDP дозволяє зменшити залежність між агентами та обмінюватись інформацією про актуальний стан системи без встановлення з'єднання за допомогою широкомовних повідомлень. Для передачі подібних повідомлень між локальними підмережами або глобальними мережами є можливість організувати агент типу проксі, метою та єдиною функцією якого буде передача будь-яких повідомлень між агентами подібного типу.

Даний підхід вирішує наступні проблеми: зменшення часу на прийняття рішення за рахунок збільшення швидкості отримання інформації про агента-виконавця, зменшення залежності агент-сервіс за рахунок використання UDP повідомлень, що передбачає також зменшення витрат на організацію та підтримку системи, зменшує необхідність у вертикальному масштабуванні системи адже кожен агент одночасно є сервісом каталогів.

#### **Література:**

1. FIPA Agent Management Specification [Електронний ресурс] – Режим доступу до ресурсу: [http://www.fipa.org/specs/fipa00023/SC00023K.html#\\_Toc75950983](http://www.fipa.org/specs/fipa00023/SC00023K.html#_Toc75950983).
2. Postel J. INTERNET STANDARD [Електронний ресурс] / Postel. – 1980. – Режим доступу до ресурсу: <https://tools.ietf.org/html/rfc768>.

***Ніколаєнко Р.С.,***

*Національний Технічний Університет України “Київський політехнічний інститут ім. Ігоря Сікорського”, м. Київ  
Кафедра автоматики та управління в технічних системах, студент*

## **ЗАХИЩЕНА P2P КОМУНІКАЦІЯ НА ОСНОВІ ТЕХНОЛОГІЇ BLOCKCHAIN**

На сьогодні обмін повідомленнями є найбільш використовуваною мережевою функцією, і аутентифікація між користувачами є життєво важливою властивістю. Найпоширенішими підходами до забезпечення цієї властивості є протоколи шифрування PKI та S/MIME, але вони вразливі до атак MITM та атаки EFAIL. Блокчейн - це інноваційна технологія, яка долає ці загрози і дозволяє децентралізувати чутливі операції, зберігаючи високий рівень безпеки. Це усуває необхідність для довірених посередників. Блокчейн доступний для всіх мережевих вузлів і відслідковує всі вже здійснені транзакції. Блокчейн пропонує модель дизайну повідомлень, що забезпечують ефективність та

безпеку даних. використовуючи смарт-контракт для перевірки особи та пов'язаних з ними публічних повідомлень, а також перевірки сертифіката користувачів. Система повністю децентралізована і дозволяє користувачам безпечно обмінюватися повідомленнями.

Така система наділена такими властивостями, як:

1. Конфіденційність - гісля того, як канал зв'язку між користувачами захищений, може бути встановлено однорангове шифрування між кінцевими точками, і лише авторизовані користувачі матимуть доступ до обміну повідомленнями.

2. Цілісність повідомлення та аутентифікація - система перевіряє недійсність підпису, перш ніж зберігати. Інша особа не може змінити підписаний договір або повідомлення під час транзакції. Кожен користувач має сертифікат, що зберігається на блокчейні. Розумний контракт перевіряє сертифікат і підтверджує особу користувачів. Всі обмінні повідомленнями підписуються приватними ключами, пов'язаними з публічним ключем на сертифікатах, використовуючи алгоритм ECDSA.

3. Надійність - неможливо одночасно вимкнути всі комп'ютери, що беруть участь у блокчейні. Як результат, ця база даних завжди в Інтернеті, і її робота ніколи не припиняється.

Однорангові мережі (P2P) допомагають подолати багато проблем, які виходять за рамки традиційних підходів клієнт-сервер, але ці функції також запроваджують нові архітектурні рішення, наприклад, як встановити довірчі відносини в P2P-мережах. Блокчейн Ethereum - це платформа для децентралізованих додатків, що називаються смарт-контрактами. Оскільки адреси Ethereum є унікальними ідентифікаторами, права власності яких не змінюються, їх активність можна відстежувати та аналізувати. Розумний контракт - це виконуваний код, який працює над блокчейном, що дозволяє автоматично виконувати угоду між двома сторонами, без однієї зі сторін можливість перешкоджати його виконанню.

Нижче наведено формальний алгоритм для верифікації повідомлення:

Коли користувач Боб хоче надіслати повідомлення Алісі, Боб представляє лише  $ID^B$ , попередньо записаний на блокчейн, і  $ID^A$  Аліси з часовою міткою  $T$  в блокчейн, де  $ID$  — хеш публічного ключа. Кожне повідомлення повинно містити часову мітку.

1. Боб відправляє транзакцію  $T_B = [ID^B, ID^A, T, S^{\text{user}^B}_{\text{pri}}(ID^B, ID^A, T)]$ , де  $S$  — функція підпису приватним ключем. Розумний контракт отримує запит від Боба.

2. Розумний контракт перевіряє, чи є представлений  $ID^B$  та  $ID^A$  в блокчейні. Контракт читає та аналізує записи Аліси та Боба. Якщо проходить валідацію, то повертає true

3. Боб надсилає транзакцію  $T^1_B = [ID^B, ID^A, T, E^{\text{user}^A}_{\text{pub}}(ID^B, ID^A, T, K^{\text{user}^B}_{\text{pub}})]$ , де  $E$  — функція шифрування приватним ключем,  $K$  — ключ, на адресу Аліси.

4. Потім Аліса перевіряє транзакцію своїм приватним ключем, і надсилає на адресу Боба транзакцію  $T_A^2 = [ID^A, ID^B, T+1, E_{pub}^{user^B}(ID^A, ID^B, T+1, K_{pub}^{user^A})]$ .

5. Після отримання транзакції Бобом, здійснюватиметься однакова перевірка, і встановлюється взаємна аутентифікація між двома суб'єктами.

#### Список використаних джерел:

1. Ethereum Whitepaper [Електронний ресурс] – Режим доступу: <https://github.com/ethereum/wiki/wiki/White-Paper>
2. Understanding Ehtereum P2P network [Електронний ресурс] – Режим доступу: <https://medium.com/shyft-network-media/understanding-ethereums-p2p-network-86eeaa3345>
3. How to defend yourself against MITM or Man-in-the-middle attack [Електронний ресурс] – Режим доступу: <https://hackerspace.kinja.com/how-to-defend-yourself-against-mitm-or-man-in-the-middl-1461796382>

*Палюх В.М., студент 6 курсу*

*Національний університет «Львівська політехніка», м. Львів*

*Кафедра програмного забезпечення*

## ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ РЕКРЕАЦІЙНОЇ ДІЯЛЬНОСТІ ПАРКУ «ШЕВЧЕНКІВ ГАЙ»

Для ефективного планування рекреаційної діяльності установ ПЗ "Шевченківський гай" адаптовано імітаційну економіко-математичну модель [1], за допомогою якої можна оптимізувати використання і відтворення природно-заповідних рекреаційних ресурсів. Адаптація моделі до конкретних ПЗ "Шевченківський гай" здійснюється через систему обмежень екологічного та господарського характеру [2], а саме, обмеження на місткість територій та об'єктів ПЗ "Шевченківський гай", на рівень розвитку їх рекреаційних інфраструктур, сфер обслуговування відвідувачів та попит на рекреаційні послуги. Розглянута нижче модель призначена для максимізації очікуваного прибутку установи ПЗ "Шевченківський гай" шляхом надання оптимальних видів рекреаційних послуг.

Таким чином, при виборі установою ПЗ "Шевченківський гай" оптимальних видів рекреаційних послуг максимум очікуваного прибутку буде складатися з таких структурних компонентів, грн./день

$$\sum_{i=1}^{N^e} p_i^{(t,d)} \cdot w_i^{(d)} + \sum_{f=1}^{F^e} k_f^{(t,d)} \sum_{i=1}^{N^e} n_{fi}^{(d)} + \sum_{j=1}^{J^{pn}} o_j^{(t,d)} \cdot n_j^{pn} \rightarrow \max : t \in T; d \in M^o, \quad (1)$$

де:  $T$  – категорії періодів відпочинку (літній, осінній, зимовий, весняний);

- $N^e$  – категорії відвідувачів (дорослі, діти, пільгові категорії);
- $M^o$  – категорії днів відпочинку (будні, вихідні, святкові);

•  $\overline{P^{(t,d)}} = \{p_i^{(t,d)}, i = \overline{1, N^a}\}: t \in T; d \in M^a$  – фактична кількість відвідувачів  $i$ -ої категорії, що знаходяться на території чи біля об'єктів ПЗ "Шевченківський гай" у  $d$ -ту категорію дня відпочинку для  $t$ -го періоду, люд.;

•  $\overline{W^{(d)}} = \{w_i^{(d)}, i = \overline{1, N^a}\}: d \in M^a$  – вхідна плата для відвідувачів  $i$ -ої категорії в  $d$ -ту категорію дня відпочинку, грн.;

•  $N^e$  – види екскурсійних послуг;

•  $\overline{K^{(t,d)}} = \{k_f^{(t,d)}, f = \overline{1, N^e}\}: t \in T; d \in M^a$  – кількість екскурсійних послуг  $f$ -го виду, що надається відвідувачам у  $d$ -ту категорію дня відпочинку для  $t$ -го періоду, од.;

•  $\overline{I^{(d)}} = \{\overline{I_f^{(d)}} = \{i_{fi}^{(d)}, i = \overline{1, N^a}\}, f = \overline{1, N^e}\}: d \in M^a$  – прибуток від надання екскурсійних послуг  $f$ -го виду відвідувачам  $i$ -ої категорії, що знаходяться на території чи біля об'єктів ПЗ "Шевченківський гай" у  $d$ -ту категорію дня відпочинку, грн.;

•  $J^{pn}$  – види рекреаційних послуг;

•  $\overline{O^{(t,d)}} = \{o_j^{(t,d)}, j = \overline{1, J^{pn}}\}: t \in T; d \in M^d$  – обсяг  $j$ -ої рекреаційної послуги: катання на човнах, катамаранах, конях, кареті тощо (у т.ч. по сфері обслуговування відвідувачів: кафе, готель, ресторан, стоянка тощо), наданої у  $d$ -ту категорію дня відпочинку для  $t$ -го періоду, од.;

•  $\overline{I^{\delta i}} = \{i_j^{\delta i} = \delta_j^{\delta i} - \zeta_j^{\delta i}, j = \overline{1, J^{\delta i}}\}$  – прибуток від  $j$ -ої рекреаційної послуги, наданої у  $d$ -ту категорію дня відпочинку, грн.

Система обмежень запропонованої моделі враховує наявні можливості кожного з її структурних компонентів [3].

1. Фактична кількість відвідувачів територій та об'єктів ПЗ "Шевченківський гай" обмежена:

• місткістю територій та об'єктів ПЗ "Шевченківський гай", що не надають екскурсійні послуги

$$\sum_{i=1}^{N^a} p_i^{(t,d)} \leq Q^{(t)} : t \in T; d \in M^a; \quad (2)$$

• пропускними спроможностями екологічних стежок, туристичних маршрутів і паркових комплексів, які надають екскурсійні послуги

$$\sum_{i=1}^{N^a} p_i^{(t,d)} \leq E^{(t)} : t \in T; d \in M^a. \quad (3)$$

$$\text{Тому } \sum_{i=1}^{N^a} p_i^{(t,d)} \leq \min\{Q^{(t)}; E^{(t)}\} : t \in T; d \in M^a. \quad (4)$$

Місткість територій та об'єктів ПЗ "Шевченківський гай" для  $t$ -го періоду, що не надають екскурсійні послуги, визначається за такою формулою, люд./день:

$$Q^{(t)} = \sum_{g=1}^{G^d} s_g \cdot r_g^{(f,h)} + \sum_{j=1}^{J^i} \left( t_j^{(t)} - \frac{l_j^i}{v_j^{(t)}} \right) \cdot \tilde{n}_j^a \cdot v_j^{(t)}, \quad (5)$$

де:  $\overline{R^{(f,h)}} = \{r_g^{(f,h)}, g = \overline{1, G^\delta}\}: h \in H; f \in F$  – норма рекреаційного навантаження для  $g$ -го ландшафтного району з  $f$ -им ступенем стійкості природних комплексів та  $h$ -ою стадією рекреаційної дигресії, люд.-день/га;

•  $\overline{S} = \{s_g, g = \overline{1, G^\delta}\}$  – площа  $g$ -го ландшафтного району, га;

•  $\overline{T^{(t)}} = \{t_j^{(t)}, j = \overline{1, J^i}\}: t \in T$  – тривалість відкритого  $j$ -го маршруту для  $t$ -го періоду, год;

•  $\overline{L^i} = \{l_j^i, j = \overline{1, J^i}\}$  – довжина відкритого  $j$ -го маршруту, км;

•  $\overline{V^{(t)}} = \{v_j^{(t)}, j = \overline{1, J^i}\}: t \in T$  – швидкість руху відвідувачів  $j$ -им маршрутом для  $t$ -го періоду, км/год;

•  $\overline{\tilde{N}^{\hat{a}}} = \{\tilde{n}_j^{\hat{a}}, j = \overline{1, J^i}\}$  – щільність відвідувачів на  $j$ -му маршруті, люд./км;

•  $\sum_{j=1}^{J^i} \left( t_j^{(t)} - \frac{l_j^i}{v_j^{(t)}} \right) \cdot \tilde{n}_j^{\hat{a}} \cdot v_j^{(t)}$  – пропускна спроможність маршрутів не

екскурсійного типу, люд./день.

Пропускна спроможність паркових комплексів екскурсійного типу визначається за такою формулою, люд./день

$$E^{(t)} = \frac{m^{\pm\Delta} \cdot g^{(t)}}{G^{\pm\Delta}} \cdot (n - k \cdot (n - 1)), t \in T, \quad (6)$$

де:  $m^{\pm\Delta}$  – середня кількість людей в екскурсійній групі, люд.;

•  $g^{(t)}, t \in T$  – тривалість робочого дня об'єкту огляду для  $t$ -го періоду, год.;

•  $G^{\pm\Delta}$  – тривалість огляду основних композиційних вузлів парку по екскурсійному маршруту, год.;

•  $n$  – одночасна кількість екскурсійних груп у парку, шт.;

•  $k$  – коефіцієнт, який враховує необхідний розрив у часі між екскурсійними групами, в частках год.

2. Фактична кількість екскурсійних послуг, що може бути надана у день відпочинку, обмежена:

• кількістю екскурсиводів

$$\sum_{f=1}^{N^e} k_f^{(t,d)} \leq \sum_{f=1}^{N^e} u_f^{(t,d)} \cdot m_f^e : t \in T; d \in M^{\bar{a}}; \quad (7)$$

• попитом відвідувачів на екскурсійні послуги

$$\sum_{f=1}^{N^e} k_f^{(t,d)} \leq \sum_{f=1}^{N^e} y_f^{(t,d)} : t \in T; d \in M^{\bar{a}}. \quad (8)$$

Тоді, фактична кількість екскурсійних послуг, що може бути надана у день відпочинку, становить

$$\sum_{f=1}^{N^e} k_f^{(t,d)} \leq \min \left\{ \sum_{f=1}^{N^e} u_f^{(t,d)} \cdot m_f^e; \sum_{f=1}^{N^e} y_f^{(t,d)} \right\} : t \in T; d \in M^{\bar{a}}, \quad (9)$$

де:  $\overline{U^{(t,d)}} = \{u_f^{(t,d)}, f = \overline{1, N^e}\}: t \in T; d \in M^{\bar{a}}$  – кількість екскурсиводів, які проводять екскурсії  $f$ -го виду у  $d$ -ту категорію дня відпочинку  $t$ -го періоду, шт.;

•  $\overline{M^e} = \{m_f^e, f = \overline{1, N^e}\}$  – кількість екскурсійних послуг  $f$ -го виду, що може надати у день один екскурсивод, шт.;

•  $\overline{Y^{(t,d)}} = \{y_f^{(t,d)}, f = \overline{1, N^e}\}: t \in T; d \in M^{\bar{a}}$  – попит на екскурсійні послуги  $f$ -го виду у  $d$ -ту категорію дня відпочинку для  $t$ -го періоду, шт.

Прибуток від надання екскурсійних послуг  $f$ -го виду відвідувачам  $i$ -ої категорії, що знаходяться на території чи біля об'єктів ПЗ "Шевченківський гай" у  $d$ -ту категорію дня відпочинку, грн.

$$\bar{i}_{fi}^{(d)} = \begin{cases} \bar{a}_{f,\min}^{(d)} - (w_i^{(d)} \cdot k) - v_f^e, & \text{для } k \leq 4 \\ z_f^e \cdot (\bar{\delta}_{fi}^{\hat{a}\hat{o}} - w_i^{(d)}) - v_f^e, & \text{для } k \geq 5 \end{cases}, \quad (10)$$

де:  $\bar{A}_{\min}^{(d)} = \{\bar{a}_{f,\min}^{(d)}, f = \overline{1, N^e}\}: d \in M^{\bar{a}}$  – мінімальна вартість екскурсійних послуг  $f$ -го виду для групи відвідувачів з обмеженою кількістю осіб у  $d$ -ту категорію дня відпочинку, грн.;

•  $\overline{V^{\bar{a}}} = \{v_f^{\bar{a}}, f = \overline{1, N^e}\}$  – середні витрати за надання екскурсійних послуг  $f$ -го виду, грн.;

•  $\overline{Z^{\bar{a}}} = \{z_f^{\bar{a}}, f = \overline{1, N^e}\}$  – фактична кількість осіб у групі відвідувачів, що отримують екскурсійні послуги  $f$ -го виду, шт.;

•  $\overline{\bar{O}^{(d)}} = \{\bar{O}_f^{(d)} = \{\bar{\delta}_{fi}^{(d)}, i = \overline{1, N^{\bar{a}}}\}, f = \overline{1, F^e}\}: d \in M^{\bar{a}}$  – середня ціна за надання екскурсійних послуг  $f$ -го виду для відвідувачів  $i$ -ої категорії у  $d$ -ту категорію дня відпочинку, грн.;

•  $\overline{W^{(d)}} = \{w_i^{(d)}, i = \overline{1, N^{\bar{a}}}\}: d \in M^{\bar{a}}$  – вартість вхідної плати для відвідувачів  $i$ -ої категорії в  $d$ -ту категорію дня відпочинку, грн.;

•  $k$  – розрахункова кількість осіб в екскурсійній групі, шт.

3. Обсяг надання рекреаційних послуг обмежений:

• рівнем розвитку рекреаційної інфраструктури

$$o_j^{\delta i} \leq k_j^{\delta i} \cdot n_j^{\pm \Delta}, j = \overline{1, J^{\delta i}}; \quad (11)$$

• попитом рекреантів

$$o_j^{(t,d)} \leq d_j^{(t,d)}, j = \overline{1, J^{\delta i}}: t \in T; d \in M^{\bar{a}}. \quad (12)$$

Тоді обсяг надання рекреаційних послуг становитиме

$$\overline{O^{(t,d)}} = \{o_j^{(t,d)} = \min\{k_j^{\delta i} \cdot n_j^{\pm \Delta}; d_j^{(t,d)}\}, j = \overline{1, J^{\delta i}}\}: t \in T; d \in M^{\bar{a}}, \quad (13)$$

де:  $\overline{K^{\delta i}} = \{k_j^{\delta i}, j = \overline{1, J^{\delta i}}\}$  – кількість рекреаційного обладнання (інвентарю) для  $j$ -го виду рекреаційних послуг, шт.;

•  $\overline{N^{\pm \Delta}} = \{n_j^{\pm \Delta}, j = \overline{1, J^{\delta i}}\}$  – змінність використання рекреаційного обладнання (інвентарю) у  $d$ -ту категорію дня відпочинку, од.;

•  $\overline{D^{(t,d)}} = \{d_j^{(t,d)}, j = \overline{1, J^{\delta i}}\}: t \in T; d \in M^{\bar{a}}$  – попит на  $j$ -ту рекреаційну послугу у  $d$ -ту категорію дня відпочинку для  $t$ -го періоду, од.

Функція мети (1) визначає вимогу отримання максимального прибутку, який можна одержати шляхом надання оптимального набору рекреаційних

послуг як особливого виду "продукції" ПЗ "Шевченківський гай". Умови (4), (9), (13) утворюють систему обмежень екологічного та господарського характеру моделі. За допомогою розрахункових формул (5), (6), (10) визначають окремі показники моделі.

Процес розрахунку оптимального набору рекреаційних послуг за допомогою запропонованої імітаційної економіко-математичної моделі передбачає виконання таких основних, як визначення зі змінними факторами та діапазонами їх варіювання, проведення основного експерименту та виконання статистичного оброблення отриманих результатів спостережень, розрахунку коефіцієнтів регресії математичної моделі, а також перевірки її на адекватність. Після детального аналізу отриманих результатів необхідно прийняти науково обґрунтовані рішення про доцільність надання певних видів рекреаційних послуг з метою оптимізації прибутку установ ПЗ "Шевченківський гай". Безумовно, запропонована оптимізаційна модель повинна розглядатися як попередня і така, що потребує апробації і подальшого удосконалення.

#### **Література:**

1. Грицюк Ю.І. Об'єктно-орієнтоване програмування: Настанова і завдання до виконання курсової роботи (в.2) . – Львів: НЛТУУ. – 2007. – 72 с.
2. Демидович Б.П., Марон Н.А. Основы вычислительной математики. – М.: Наука, 1966. – 664 с.
3. Гихман И.И., Скороход А.В., Ядренко М.И. Теория вероятности и математическая статистика. – 2-е изд., перераб. и доп. – К.: Выща шк., 1988. – 439 с.

***Прокопович-Ткаченко Д.І., канд. тех. наук, доцент***

*Університет митної справи та фінансів, м. Дніпро*

*Кафедра кібербезпеки та інформаційних технологій, завідувач кафедри*

***Стелюк Б.Б., канд. тех. наук, доцент***

*Університет митної справи та фінансів, м. Дніпро*

*Кафедра кібербезпеки та інформаційних технологій, доцент*

***Солянніков В.Г., студент Б16-1***

*Університет митної справи та фінансів, м. Дніпро*

*Кафедра кібербезпеки та інформаційних технологій, студент*

## **ПІДХОДИ ДО АВТОРИЗАЦІЇ ТА АВТЕНТИФІКАЦІЇ БЕЗПРОВОДОВОГО ДОСТУПУ КОМУНІКАЦІЙНИХ СИСТЕМ**

Розвиток та вдосконалення телекомунікаційних систем і мереж України здійснюється відповідно до Концепції розвитку телекомунікацій України із застосуванням новітніх технологій, які відповідають міжнародним стандартам, з урахуванням технологічної цілісності всіх мереж та телекомунікаційних засобів, підвищення ефективності та сталості функціонування. Стратегічно важливе значення має забезпечення захисту від несанкціонованого втручання в режими функціонування обладнання телекомунікаційних систем і мереж.

Проведений аналіз [1] показав, що для забезпечення безпеки безпроводових телекомунікаційних систем і мереж застосовуються різні механізми захисту.

У якості основи при розробці методу авторизації та автентифікації безпроводового доступу використано відомий метод, який полягає в комплексному застосуванні процедур та операцій організаційного та технічного характеру із створення встановленого режиму авторизації та автентифікації для підвищення безпеки телекомунікаційних систем та мереж [1]. Основним відмінним елементом методу є застосування генераторів псевдовипадкових послідовностей максимального періоду для формування ключів авторизації доступу, тобто замість спеціальної функції Dot16KDF, колізійні властивості якої є незадовільними, пропонується використовувати більш досконалу функцію генерації послідовностей. Застосування генераторів псевдовипадкових послідовностей максимального періоду за рахунок забезпечення потрібних колізійних властивостей формованих ключів авторизації дозволяє підвищити безпеку телекомунікаційних систем та мереж.

Структурна схема методу представлена на рис. 1, на якому наведено сукупність процедур і функцій відомого методу та введені нові елементи.



Рис. 1. Схема методу авторизації та автентифікації безпроводового доступу телекомунікаційних систем та мереж



Метод авторизації та автентифікації безпроводового доступу складається з визначених: – процедур та операцій передачі даних, які будуються із використанням методів та засобів телепередачі даних і стандартизованих телекомунікаційних протоколів; – процедур та операцій організації безпечних з'єднань, які будуються із використанням методів та засобів симетричної криптографії та певних механізмів забезпечення безпечного з'єднання, які налаштовуються, зокрема, за встановленим криптографічним комплексом, із визначеними векторами ініціації, секретними ключами та часом їх життя; – процедур та операцій організації автентифікації користувачів та пристроїв, які будуються із використанням методів та засобів асиметричної криптографії, інфраструктури відкритих ключів, цифрових сертифікатів, тощо, та відповідних протоколів автентифікації та авторизації, зокрема RSA авторизації, EAP-авторизації та сумісної RSA-EAP авторизації; – процедур та операцій формування ключів авторизації доступу, які будуються із використанням методів та засобів (генераторів) псевдовипадкових послідовностей із застосуванням удосконалених механізмів, а саме:

– процедур контролю векторів ініціації для виконання першої сформульованої вимоги щодо відсутності колізій (збігів) в вхідних послідовностях;

– безпечних генераторів послідовностей максимального періоду для виконання другої сформульованої вимоги щодо періодичних властивостей ключів авторизації.

Запропоновані процедури контролю векторів ініціації реалізуються шляхом введення до функції генерації ключів авторизації доступу додаткового параметра *i* (аргументу функції генерації), який визначається за порядковим номером ключа авторизації. Таким чином, для кожного наступного виклику функції генерації використовується унікальний номер, що *i* забезпечує виконання першої вимоги стосовно відсутності колізій (збігів) в вхідних послідовностях.

#### **Література:**

1. Прокопович-Ткаченко Д.І. Дослідження протоколів автентифікації та авторизації доступу в безпроводових телекомунікаційних системах та мережах / Д.І. Прокопович-Ткаченко / Системи озброєння і військова техніка, 2013, № 1(33). – С. 119-122.

***Рихтюк Е.Ю.***

*Національний університет «Львівська політехніка», м.Львів.*

*Кафедра «Програмне забезпечення», студент - магістр*

## **АВТОМАТИЗОВАНИЙ СЕРВІС ПІДБОРУ ІТ-ПЕРСОНАЛУ В КОМПАНІЇ**

Основна проблема в процесі підбору персоналу на ту чи іншу посаду в ІТ-компанії або команді розробників – це «людський фактор». Людина яка оцінює кандидата (зазвичай це одна-дві людини) не може охопити всі моменти при

оцінюванні і найчастіше допускаються помилки, які ніяк не можна з прогнозувати, саме від цього при оцінюванні кандидата і формуванні експертної заключення (що зазвичай є ручним процесом) відбувається свого роду «лотерея» де шанси на максимально ефективну і оптимізовану роботу працівником – 50 на 50 [1].

Суть роботи полягає в тому, щоб скомбінувати декілька окремих процесів в одну автоматизовану систему. Для оцінювання кандидатів було вибрано метод оцінювання за типом інформаційного метаболізму людини, що являється її соціотипом та психотипом, що грає основну роль при оцінці компетентності кандидата. Для початку було відокремлено основні ролі в ІТ-компаніях і встановлено їм необхідні типи інформаційного метаболізму які складаються з абривіатур. Абривіатури рекомендуємих соціонічних типів, які складаються з трьох букв, перша з яких, демонструє найважливішу основну функцію (Л – логіка, С – сенсорика, Е – етика, І – інтуїція), друга демонструє творчу функцію (Л – логіка, С - сенсорика, Е – етика, І – інтуїція) і третя – виконує роль сприйняття навколишнього світу (І – інтроверсія, Е – екстраверсія) [3]. Далі важливим процесом є регулярне оцінювання кандидата всіма з ким він комунікує в ході виконання своїх обов'язків, а саме оцінюються особисті якості (креативність, лідерство, комунікабельність, прагнення до саморозвитку, тощо) та професіональні (знання технологій, вміння проектування, мотивація до самореалізації, тощо). Процес прийняття рішення базується на опрацювання всіх оцінок виставлених кандидату за весь цикл його професійної діяльності та буде зводитись до одного показника компетентності який вираховується за наступною формулою [2].

$$K_p = \left( \frac{\sum_{i=1}^{15} L_i * K_{vi}}{\sum_{i=1}^{15} K_{vi}} \right) / 100$$

Де  $K_p$  – показник «компетентності»;  $L_i$  – значення певної якості кандидата;  $K_{vi}$  – значення коефіцієнта певної якості кандидата. Показник компетентності аналогічним чином виставляється і для наявних посад, проте на відміну від показника кандидата, змінюватися він не буде. В ході дослідження було проведено експеримент з кандидатами в реальному робочому процесі. Перш за все кандидата направляли на посаду, старим способом, а саме туди де є вакантна посада і характеристики кандидата, хоча б наближено відповідали вимогам. Протягом робочого тижня кандидату виставлялися оцінки всіх хто був, хоча б якимось зв'язаний з його робочим процесом тому, щодня кандидат мав оцінку компетентності. На другий тиждень експерименту було співставлено показник компетентності кандидата, то наявних посад і кандидата назначили на відповідну для його показника посаду. Результати таких самих оцінювань показали, що рівень ефективності кандидата стрімко пішов в гору. Експеримент можна рахувати вдалим, тому що за 2 робочих тижня вдалося явно побачити рівень компетентності кандидата і направити його вміння в правильне «русло».

### Література:

1. Квалификационные требования (профессиональный стандарт) в области информационных технологий «Специалист по системному администрированию» [Электронный ресурс]. – Режим доступа: <http://www.apkit.ru/committees/education/meetings/standarts.php>. Дата обращения: 30.03.2014.
2. Kramskoy S.A. Approaches and stages of assessment of role of specialists for IT-companies using fuzzy logic [Текст] / С.А. Крамской // Тези доповідей XIII міжнар. наук.-практ конф. «Управління проектами у розвитку суспільства». – К.: КНУБА, 2016. – С. 36-38.
3. Шевченко Т.В. Нестандартные методы оценки персонала / Т.В. Шевченко. – М.: Ай Пи Эр Медиа, 2010. – 128 с.

**Рожков Є.І.**

*Машинобудівний коледж Донбаської державної машинобудівної академії,  
м. Краматорськ*

*Комп'ютерні науки, студент*

**Новікова Н.В., викладач-методист**

*Машинобудівний коледж Донбаської державної машинобудівної академії,  
м. Краматорськ*

*Комп'ютерні науки, викладач*

## ЧИСЛА ФІБОНАЧЧІ В ВЕБДИЗАЙНІ

На сьогоднішній день вебдизайн - це галузь веброзробки, що охоплює цілий ряд напрямів і дисциплін із створення та супроводу сайтів або вебзастосунків, таких як графічний вебдизайн, проектування інтерфейсів, авторинг (у тому числі стандартизований код і власницьке програмне забезпечення), використання та оптимізація для пошукових систем.

Розглянемо деякі конструкції вебдизайну на основі послідовності чисел Фібоначчі. За означенням, перші два числа є 0 і 1, і кожне наступне число дорівнює добутку двох попередніх. Послідовність чисел виглядає наступним чином: 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144...

Ці числа знайшли достатньо широке застосування в різних галузях науки, в природі та на підприємствах. Так їх використовують в музиці для настроювання інструментів, в архітектурі для обчислення гармонійних пропорцій, наприклад співвідношення висоти приміщення до висоти декорування стін різними матеріалами. Відстані між листям (або гілками) на стовбурі рослини відносяться приблизно як числа Фібоначчі.

Основна ідея конструкції для вебдизайну полягає в використанні чисел при вирішенні питання про розміри і зміст основної і бічної області. І ці числа і Золотий перетин рівнозначні в даному контексті і дизайнери використовують те, що їм зручніше.

Загалом, макети досить легко побудувати з використанням послідовності чисел Фібоначчі. Ви вибираєте певну ширину бази першого контейнеру. Потім, при визначенні розмірів інших контейнерів, ви перемножуєте ширину бази з

числами Фібоначчі. Подивимося на зразок блогу друкарні, який має мінімалістський дизайн на основі чисел Фібоначчі.

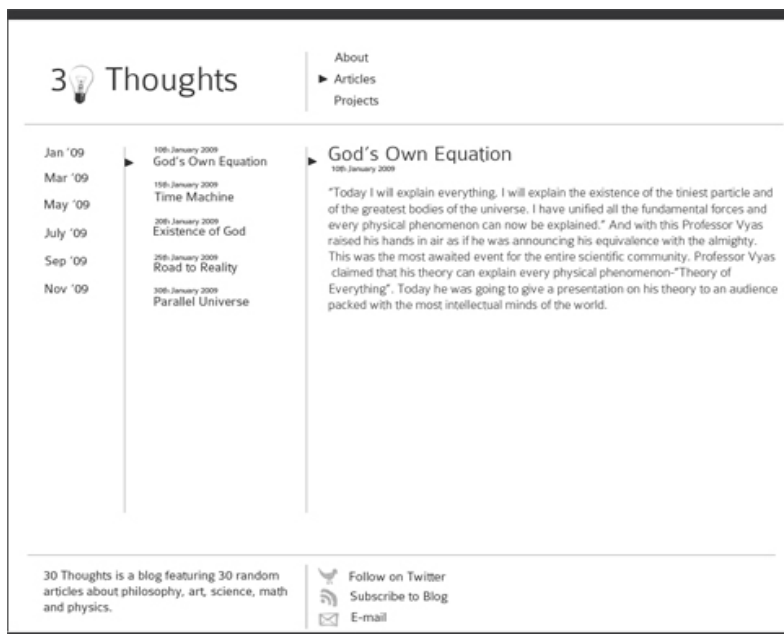


Рис. 2. Мінімалістський блог друкарні на основі чисел Фібоначчі

Ми можемо бачити, що сторінка розділена на три стовпці. Кожен стовпець відповідає числу Фібоначчі. Для цього дизайну ми використовували базову ширину 90 пікселів. Перший стовпець має ширину 180 пікселів ( $90 \times 2$ ); ширина другого становить 270 пікселів ( $90 \times 3$ ), а ширина третього стовпчика - 720 пікселів ( $90 \times 8$ ). Розмір шрифту також відповідає числу з даного ряду.

Якщо сайт має фіксовану ширину, наприклад тисячу пікселів, то числа Фібоначчі не дуже зручно використовувати. Остільки найближче до тисячі число з цього ряду це 987 (... , 610, 987, 1597 ...), то саме на основі цього числа доведеться проводити обчислення для ширини блоків сайту. У таких ситуаціях краще всього скористатися правилом Золотого перетину ( $1000 \times 0,618 = 618px$ ) і виходячи з нього визначити ширину блоків.

Числа Фібоначчі найкраще підходять для дизайну блогів і журнальних макетів. Знову ж таки, варто відзначити, що слід спиратися на творчий підхід при використанні послідовності Фібоначчі у роботі, інакше макети будуть здаватися занадто складними і, отже, будуть складні у використанні і навігації.

#### Література:

1. Веб-дизайн: підруч. для студ. вищ. навч. закл. / О. В. Пасічник, В. В. Пасічник ; за заг. ред. В. В. Пасічника ; М-во освіти і науки України. — Л. : Магнолія 2006, 2010. — 519 с
2. Н. Н. Воробйов. Числа Фібоначчі. - Наука, 1978. - Т. 39.
3. Вебдизайн [Електронний ресурс]: <https://uk.wikipedia.org/wiki/Вебдизайн>

## **АЛГОРИТМ ПОШУКУ ЕЛЕМЕНТІВ НА СТОРІНЦІ ЗІ ЗМІНЮВАНОЮ СТРУКТУРОЮ**

Задача пошуку елементів на сторінках із динамічною структурою виникає з потреби прив'язання певних сторонніх елементів (підказок, тощо) до елементів веб-сторінки й збереження цього прив'язання зі зміною структури сторінки. Для цього необхідно мати змогу ідентифікувати той елемент на змінній сторінці, що якого було раніше прив'язано підказку.

Для вирішення поставленої задачі необхідно розробити алгоритм, що враховує всі можливі шляхи знайдення певного елемента на сторінці від кореневого елемента, оскільки положення кореневого елемента на сторінці завжди відомо, а врахування всіх можливих шляхів від кореневого елемента до обраного елемента дозволить врахувати будь-які переміщення обраного елемента на сторінці відносно кореневого, адже його все ще можна буде знайти на сторінці за деякими шляхами, за якими його можна було знайти раніше.

Наприклад, якщо на сторінці знаходиться кореневий елемент `<body>`, всередині якого знаходиться елемент `<div>`, що має атрибут `class="myDivClass"`, всередині якого знаходиться інший елемент `<div>` з класом `"myDivClass2"`, всередині якого знаходиться шуканий елемент `<a>`, то дійти до елемента `<a>` від кореневого елемента, використовуючи такий метод, як `document.querySelector`, можна наступними шляхами:

- `body > div.myDivClass > div.myDivClass2 > a;`
- `body > div.myDivClass > a;`
- `body div.myDivClass > a;`
- `body div.myDivClass a;`
- `body div.myDivClass2 > a;`
- `body > div > div > a;`
- `body > div.myDivClass > div.myDivClass2 > *;`
- `body > div.myDivClass > div > *;`
- `body div.myDivClass2 > *;`
- `body > a;`
- `body > div.myDivClass > div.myDivClass2 > a;`
- `body > div.myDivClass > div.myDivClass2 > a.`

У деяких з цих можливих шляхів від кореневого елемента до шуканого відсутній перший елемент `<div>`, у деяких з них відсутній другий елемент `<div>`, у деяких з них відсутні обидва елементи. Це означає, що частина з

можливих шляхів дозволить знайти шуканий елемент за будь-яких змін структури сторінки.

Також, частина шляхів до елемента може відкидати певні атрибути чи тег обраного елемента або його батьків. Наприклад, розглянемо наступні два шляхи від кореневого елемента `body` до обраного елемента `a`:

- `body > div > div > a`;
- `body > div > div > *`.

У першому випадку елемент буде знайдено на сторінці лише за умови якщо він не змінить свій тег з `<a>` на будь-який інший. Другий шлях знайде елемент навіть якщо тег елемента буде змінено на, наприклад, `<div>`.

Використовуючи ідею про прокладення усіх можливих шляхів від кореневого елемента до обраного елемента, розглянемо етапи роботи алгоритму, що прокладає дані шляхи, перевіряє, чи усі вони ведуть до шуканого елемента, й після зміни сторінки використовує усі ці шляхи для знайдення елемента, обираючи той елемент, на який вказує більшість з згенерованих шляхів.

Нижче наведені етапи роботи алгоритму побудови усіх можливих шляхів до елемента:

- знайти усі елементи між кореневим елементом та шуканим елементом;
- використовуючи усі можливі комбінації множини проміжних елементів, скласти множину можливих шляхів, частина з яких включає лише частину проміжних елементів;
- знайти усі атрибути для шуканого елемента та для кожного з проміжних елементів;
- використовуючи комбінації множини для атрибутів кожного з проміжних елементів та для атрибутів шуканого елемента, а також декартовий добуток множин, розширити множину можливих шляхів до шуканого елемента таким чином, що частина зі шляхів буде використовувати лише частину з атрибутів елемента;
- продублювати шляхи для кожного з проміжних елементів та для шуканого елемента, відкидаючи вимоги відносно тегу елемента.

#### Список використаних джерел:

1. `Document.querySelector` [Електронний ресурс] – Режим доступу: <https://developer.mozilla.org/ru/docs/Web/API/Document/querySelector>
2. `Document Object Model` [Електронний ресурс] – Режим доступу: [https://ru.wikipedia.org/wiki/Document\\_Object\\_Model](https://ru.wikipedia.org/wiki/Document_Object_Model)
3. `What is the Document Object Model?` [Електронний ресурс] – Режим доступу: <https://www.w3.org/TR/DOM-Level-2-Core/introduction.html>

*Сав'як Назар Тарасович*

*Студент магістратури факультет управління фінансами та бізнесу  
Львівський національний університет імені Івана Франка  
Задорожна Анна Володимирівна к. ф.-м. н., доцент кафедри  
економічної кібернетики факультет управління фінансами та бізнесу  
Львівський національний університет імені Івана Франка*

## **ОГЛЯД ПЕРСПЕКТИВНИХ ФРЕЙМВОРКІВ ТА БІБЛІОТЕК ДЛЯ РОЗРОБКИ ВЕБ-САЙТІВ**

На сьогоднішній день складно уявити життя без Інтернету. Він являє собою всесвітню систему сполучених комп'ютерних мереж. Ця павутина наповнена веб-сайтами, які дозволяють користувачам оперативно отримувати відповіді на різноманітні питання. Створення сайтів передбачає наявність у веб-розробника не тільки прекрасних технічних навичок та логічного мислення, але й розвиненої креативності. Складність роботи над веб-сайтом полягає у тому, що вона містить як технічну складову, так і творчу, оскільки потрібно не тільки розробити дизайн сайту, а й наповнити його різноманітними матеріалами.

Щоби написати код для веб-сайту, потрібні фреймворки та бібліотеки, яких є чимало видів. Дамо порівняльну оцінку основним з них:

jQuery – достатньо відома бібліотека, яка містить серцевий код. Суть цієї бібліотеки полягає у полегшенні навігації через такий елемент, як DOM, створенні AJAX-застосунків, анімацій та обробки подій.

AngularJS – на даний момент знаходиться у топі найпопулярніших фреймворків. Одна з його характеристик – відкритість програмного коду. Перевагами є: можливість у створенні та зберіганні частин коду, котрі можна використовувати у подальшому, також утворення нових HTML-елементів та чимала кількість інструментів для текстів.

ReactJS – розроблений і підтримується командами Instagram, Facebook. ReactJS підходить якщо ви прагнете розвиватись у сфері фронтенд-розробки, то саме ця бібліотека буде хорошим початком.

Vue.js – доволі креативний фреймворк, котрий містить кореневу бібліотеку, яка спершу впорається із завданнями уяви, а щодо створення односторінкових додатків, то за це відповідає підсистема додаткових бібліотек.

BackboneJS – хороший фреймворк для початківців завдяки своїй легкості у користуванні.

MeteorJS – підходить для управління базами даних, а також для рендерингу та фронт- і бекенду, адже є доволі функціональним. Також перевагою є те, що він має достатньо інструментів, щоби створити багатofункціональні додатки.

Skel – попри його абсолютну приналежність до JavaScript, він не є досить популярним, проте для створення веб-сайтів та додатків він чудово підійде. Містить функції API і нормалізації стилів браузера.

KnockoutJS – досить легка у використанні JavaScript платформа, яка взаємодіє із моделлю MVVM.

Щодо різниці між бібліотеками та фреймворками, то фреймворк задає розробку архітектури додатку, формує поведінку за умовчанням та каркас, тоді як бібліотека використовується як об'єкт із декількома системами та не впливає на основний програмний продукт.

Переваги фреймворків:

- розробка допомагає простіше супроводжувати проект на фреймворку;
- бізнес-процеси можуть реалізуватись із будь-якою послідовністю;
- швидкість та витривалість;
- безпека. Рішення тут набагато безпечніші, ніж в самописних системах.

Недоліки:

- щоби розробляти продукт на фреймворку, потрібно мати знання тих бізнес-процесів, над якими працюєш;
- набагато більше часу займає створення функціоналу.

Отже, для того, щоби веб-сайт був ефективний та функціональний, потрібно дотримуватися логічного структурування та композиційного впорядкування всіх елементів на веб-сторінках відповідно до їх значущості; проектувати інтерфейс веб-сайту таким чином, щоби користувач міг легко зрозуміти та розібратись із тим, куди йому необхідно перейти для бажаного результату; створювати такий зовнішній вигляд сайту, який би відповідав змісту, характеру і призначенню сайту.

Для того, щоби можна було із легкістю виконати ці умови, потрібно використовувати бібліотеки і фреймворки, яких зараз є досить багато, тому можна обрати той, який підходить розробнику для конкретної задачі.

#### Література:

1. Фреймворки в веб разработке [Електронний ресурс]. – Режим доступу до ресурсу: [https://web-creator.ru/articles/about\\_frameworks](https://web-creator.ru/articles/about_frameworks)
2. [Електронний ресурс]. – Режим доступу: <https://habr.com/>
3. [Електронний ресурс]. – Режим доступу: <https://tproger.ru/>
4. Знайомство з фреймворками [Електронний ресурс]. – Режим доступу до ресурсу: <http://weplib.com.ua/blog/29>

**Самойлов В.В., бакалавр, студент**

*Мелітопольський державний педагогічний університет, м. Мелітополь  
Кафедра інформатики і кібернетики, студент*

### ОПИС ТЕКСТОВОГО РЕДАКТОРА SUBLIME TEXT 3

Sublime Text 3 — швидкий кросплатформний текстовий редактор. Підтримує плагіни, розроблені за допомогою мови програмування Python. Sublime Text 3 не є вільним чи відкритим програмним забезпеченням, але деякі його плагіни розповсюджуються з вільною ліцензією, розробляються і підтримуються спільнотою розробників.



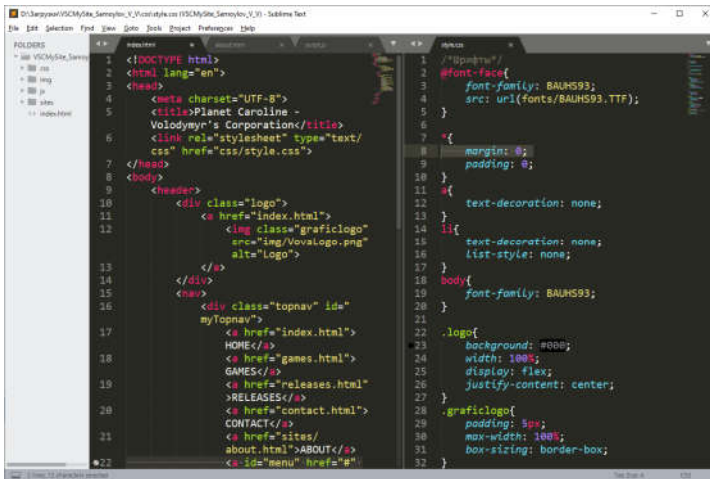


Рисунок 1 - Sublime Text 3

Екран ділиться не тільки навпіл, але і на чотири колонки, наприклад у кожному стовпчику можливо відкрити окремий файл. Справа у кожному вікні є смуга прокрутки у вигляді карти коду, її можна прибрати у налаштуванні програми, якщо немає в ній потреби. Так само можна вивести або прибрати панель проєктів або відкритих файлів - вона розташовується зліва. Наприклад в ній можна створити новий файл, перейменувати існуючий або видалити його. Відкритий проєкт представлений у вигляді дерева папок і файлів як у файловому менеджері. У Sublime Text 3 ви можете переглядати файл зображення, це зручно і прискорює пошук потрібного, наприклад при верстці сайту.

На цей текстовий редактор існує безліч плагінів, які безмежно розширюють його функціонал. На офіційному сайті і в співтовариствах цього редактора ви зможете знайти плагіни, які розширять функціонал цього редактора в тій сфері, в якій потрібно вам.

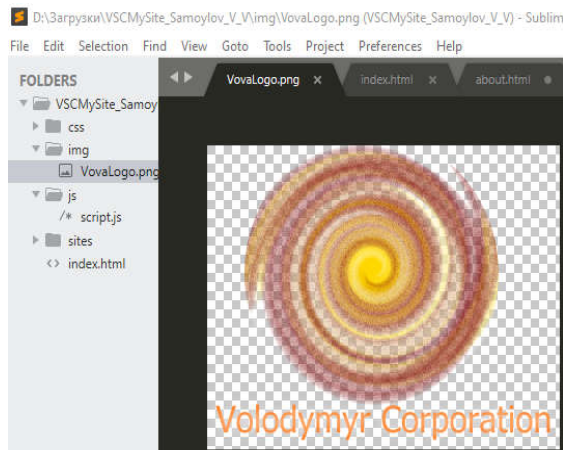


Рисунок 2 - Перегляд зображення

Найголовніший плагін - це Package control, який встановлюється в першу чергу і в подальшому за допомогою нього ви зможете встановлювати або видаляти всі наступні плагіни. Завантажувати їх не треба, просто набираємо назву потрібного плагіну в пошуку через Package control. У рядку пошуку пишемо потрібний, потім вибираємо необхідний. Обраний плагін автоматично завантажиться і встановиться. (Натискаємо Ctrl + Shift + P, пишемо install, тиснемо Enter або вибираємо пункт «Package Control: Install Package»)

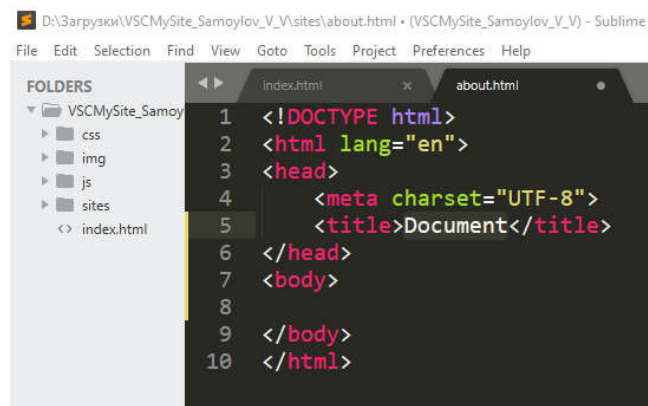
Другий за популярністю плагін - Emmet. Цей плагін сильно прискорює написання коду, тому для верстальника це просто чудо. Наприклад набравши всього один символ “!” і після цього натиснувши TAB ми отримуємо такий код:

Деякий час назад в якості альтернативи знаменитому Notepad++, був встановлений редактор Sublime Text 3. Після роботи на ньому протягом деякого часу стало зрозуміло, що він залишиться головним редактором, а Notepad++ відійде на другий план в якості запасного варіанту.

У редакторі можливе відкриття декількох вікон одночасно і поділ екрану як по горизонталі, так і по вертикалі.

Плагін Alignment - вирівнює код. Дуже зручно коли ви відкриваєте чужий файл і намагаєтеся в ньому розібратися, виділяємо код і тиснемо Ctrl + Alt + A і код стало приємно читати.

Так само є безліч плагінів, які не тільки розширюють функціонал, але і змінюють зовнішній вигляд. Ви зможете надати зовнішній вигляд в стилі який вам подобається.



```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <title>Document</title>
6 </head>
7 <body>
8
9 </body>
10 </html>
```

Рисунок 3 - Приклад коду

### Література:

1. Sublime Text [Електронний ресурс] - [https://uk.wikipedia.org/wiki/Sublime\\_Text](https://uk.wikipedia.org/wiki/Sublime_Text).
2. Документація Sublime Text [Електронний ресурс] - <https://www.sublimetext.com/docs/3/>.

*Саніжак І.М., магістр*

*Івано-Франківський національний технічний університет нафти і газу,*

*м. Івано-Франківськ*

*Кафедра інженерії програмного забезпечення, магістр*

## РОЗРОБКА СЕРВІС-ОРІЄНТОВАНОЇ СИСТЕМИ В ІНТЕРНЕТ-МЕДІА СФЕРІ

Попри велику кількість медіа контенту в мережі Інтернет, радіо через всесвітню павутину у сьогоднішні не лише не втрачає своїх позицій, а й навпаки знаходить все більше й більше прихильників.

За даними статистики, кількість інтернет радіослухачів у США станом на 2018 рік була близькою до 180 мільйонів осіб, що складає близько 50% всього населення Сполучених Штатів, та близько 67% американців, що користуються інтернетом. Разом із тим зростає час, який користувачі проводять слухаючи онлайн-радіо [1].

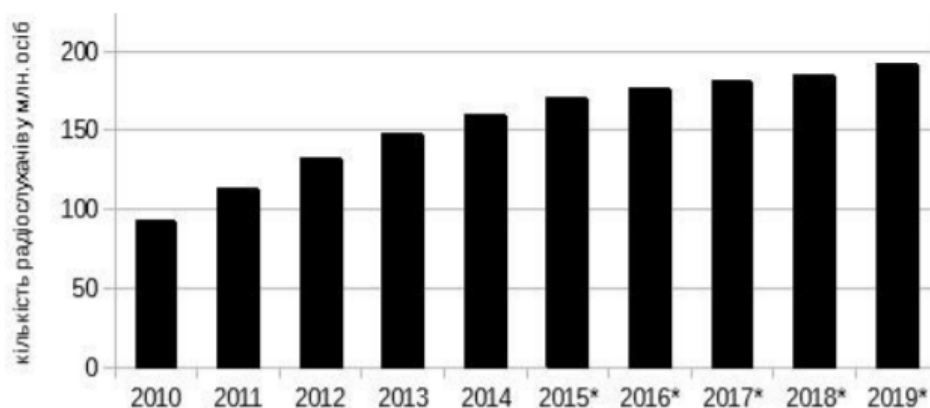


Рис. 1. Графік збільшення кількості інтернет-радіослухачів(\* - прогнозоване збільшення) [2]

Оскільки тема є актуальною, метою роботи є розробка працюючого інтернет радіо медіа серверу, що буде приймати сигнал від певного джерела, та розсилати всім користувачам, що будуть до нього підключенні.

Для великих сайтів потокового мовлення використовується кілька медіа серверів, розосереджених географічно, так щоб клієнт міг підключитися до найближчого, для зменшення затримок мережі [3]. Отже основними компонентами Інтернет радіо є:

- радіостанція, що створює потік та відправляє його на медіа сервер;
- медіа сервер, що приймає потік від радіостанції та відправляє усім підключеним клієнтам;
- програвач клієнта, що підключається до медіа серверу, отримує та відтворює аудіо потік.

При передачі аудіо даних використовується буферизація на стороні клієнта, що дозволяє знизити вплив джиттера. Буферизація 10-15 с звучання до початку програвання дозволяє зробити мовлення безперервним навіть за умови помітного джиттера у мережі. До тих пір, доки пакети прибувають раніше, ніж вони реально необхідні, немає ніякого значення, коли саме вони прибувають.

Для програвання ефіру, що йде від медіа серверу усе що потрібно на сайті це тег `<audio></audio>`. У даного тегу є певні можливі атрибути, а саме:

- `autoplay` – при наявності даного атрибута аудіо потік буде відтворюватися одразу ж після завантаження сторінки. У якості значення вказується «autoplay», також можна взагалі не вказувати жодного значення;
- `controls` – атрибут, що додає панель керування до аудіо треку. Вид панелі та її зміст залежить від браузеру і може включати в себе: кнопку відтворення, паузи, полосу перемотки, повзунок для зміни рівня гучності та ін. У якості значення вказується «controls», також можна писати атрибут без значення;
- `loop` – зациклює аудіо, у випадку якщо програватиметься файл, аби воно нескінченно повторювалось після завершення. У якості значення вказується «loop», також можна писати атрибут без значення;
- `muted` – вимикає звук при відтворенні музики. У якості значення вказується «muted», також можна взагалі не вказувати жодного значення;
- `preload` – атрибут використовується для завантаження аудіо файлу разом із завантаженням веб-сторінки. Ігнорується, якщо встановлений атрибут «autoplay».

Незважаючи на велику кількість протоколів, створених для багатоадресної передачі потокового медіа контенту, радіомовлення через мережу використовує звичайний TCP для встановлення з'єднання між клієнтом та сервером та надійної передачі даних.

Проаналізувавши методи створення аудіо файлів та визначивши їх переваги і недоліки можна сказати, що для Інтернет радіомовлення найбільш підходящими є формати із стисненням та втратами, такі як MP3, AAC, OGG Vorbis.

Першим, що необхідно будь-якій радіостанції у мережі Інтернет це програмне забезпечення, що зможе віддавати свій аудіо потік у мережу [4]. Існує багато програм для рішення даної задачі. Найбільш розповсюдженими є:

- Для комп'ютерів під управлінням ОС Windows:
  - RadioBOSS
  - Winamp + плагін до ShoutCast (програмне забезпечення медіа серверу)
- Для комп'ютерів під управлінням ОС Linux:
  - Ices
  - PulseAudio

Отже проаналізувавши варіанти реалізацій медіа серверів можна сказати, що досить великих відмінностей у плані функціоналу та підтримки немає. Проте мала необхідність у ресурсах серверу IceCast робить його більш вигідним варіантом для використання. Ще однією перевагою є те, що даний сервер створений тією ж компанією, що й кодек OGG Vorbis, тому він підтримує цей поки що не досить широко використовуваний, але дуже якісний, формат. Платні сервери мають додаткові функції, що робить цей вид реалізації більш підходящим для комерційних користувачів.

Програмне забезпечення медіа серверів основну функцію виконують однаково, проте через низьку необхідність у ресурсах кращим вибором є IceCast[5]. Серед програм, що можуть створювати аудіо потік можна виділити PulseAudio, що має такі особливості:

- можливість роботи з декількома джерелами і приймачами звуку;
- синхронізація потоків відтворення;
- модуль придушення акустичного відлуння для VoIP;
- кросплатформеність.

Усі існуючі програвачі, що можуть відтворювати аудіо потоки, які йдуть з мережі, за своїм функціоналом є приблизно однаковими.

Після вибору реалізації медіа серверу, було досліджено можливість підключення до цього програмного модулю із сайту кафедри. Було проаналізовано спосіб отримання аудіо потоку, як з використанням стандартних HTML тегів, так і з використанням спеціального модуля для системи керування вмістом.

Результати роботи серверу показали, що він коректно передає аудіо потік від радіостанції до користувачів, що підключаються. Також виводиться метадані музичного файлу, що програвється. У адміністративній панелі серверу доступна більш детальна інформація про використання мережі, кількості радіостанцій, що віщають через медіа сервер, та кількість клієнтів, що зараз прослуховують кожну радіостанцію.

#### Література:

1. Internet Radio Trends Report 2015. – Режим доступу: [http://xappmedia.com/wp-content/uploads/2015/01/Internet-Radio-TrendsReport-2015\\_january.pdf](http://xappmedia.com/wp-content/uploads/2015/01/Internet-Radio-TrendsReport-2015_january.pdf). – Дата доступу: 09.09.2019

2. Number of monthly digital radio listeners in the United States from 2010 to 2019. – Режим доступу: <http://www.statista.com/statistics/191657/us-weeklyinternet-radio-listeners-since-2009/>. – Дата доступу: 09.09.2019
3. Таненбаум Э. Компьютерные сети 5-е издание / Эндрю Таненбаум. – Санкт Петербург : «Питер», 2012. -С. , 739-745, 763-767
4. Шеренковський А.О. Програмне забезпечення медіа-серверу Інтернет радіо / Шеренковський А.О. // Системний аналіз та інформаційні технології : 18- 80 а Міжнародна науково-технічна конференція «SAIT 2016», Київ, 30 травня – 2 червня 2016 р. / ННК “ІПСА” НТУУ “КПІ”. – К.: ННК “ІПСА” НТУУ “КПІ”, 2016. – С. 429
5. Документація медіа серверу IceCast 2. – Режим доступу <http://icecast.org/docs/>. – Дата доступу: 09.09.2019

*Сусуловська М.Р., студентка-магістр  
Національний університет «Львівська Політехніка», м. Львів  
Кафедра прикладної лінгвістики, студент*

## **КОМП'ЮТЕРНИЙ ПЕРЕКЛАД МЕДИЧНИХ ТЕРМІНІВ**

Дослівно переклад – це вид посередництва у мовах, коли зміст іншомовного тексту оригіналу передається па іншу мову шляхом створення на ньому комунікативно рівноцінного тексту. Для перекладу з однієї мови на іншу мову можуть застосовуються такі програми: 1) словники, 2) перекладачі текстових документів, 3) перекладачі тексту веб-сторінок із збереженням дизайну. Розрізняють автоматизований, машинний і статистичний переклади.

Комп'ютерний переклад текстів - одна з найцікавіших і потрібніших інформаційних технологій. Комп'ютерний переклад є й однією з найскладніших для програмістів задач.

Коли мова йде про використання програм для перекладу окремих слів - це для комп'ютера не проблема: в пам'яті можуть зберігатись десятки словників найбільшого обсягу. Комп'ютерний словник може надати всі можливі значення слова, яке потрібно перекласти. Ця можливість активно використовується користувачами у різних фахових напрямках.

Однак медичний переклад – це надзвичайно складне явище, позначене системою різноманітних жанрів та долучених дисциплін, що викликає розбіжності в номенклатурі. За рахунок розширення рамок самого поняття зростає і поле термінологічної лексики та зразків текстів, які так чи інакше підходять під визначення "медичних перекладів".

Критеріями адекватності саме медичного перекладу, за М. Руло, є: 1) точна передача основної думки (message) оригіналу, 2) дотримання прийнятих у момент створення перекладу граматичних норм, 3) ідіоматичність, 4) відтворення емоційної тональності оригіналу, 5) зрозумілість для читача, який належить до іншої культури [4].

Проте, він також зазначає і шість основних проблем перекладу медичного

тексту: особливості сталих виразів, включаючи метонімічне вживання термінів і переважне вживання певних частин мови; багатозначність термінології; проблеми перекладу епонімів; розбіжність афіксів в словах загального походження; недостатньо висока якість спеціалізованих багатомовних словників[4].

Проблема відтворення жанрових особливостей фармацевтичних текстів знайшла відображення в дисертаційному дослідженні Боцмана А.В. У досліджуваних текстах було виділено чотири інформаційні зони: інтродуктивно-дескриптивну, регламентативно-директивну, зону попереджень та референціальну. Фармацевтичні тексти також мають індикатори безпосередньої (поділяються на індикатори для фахівців у галузі медицини, фахівців у суміжних природничих галузях, пацієнтів) та опосередкованої спрямованості. Індикатори групуються з урахуванням вікових, статевих характеристик, функції (дозволяючі, попереджуючі, забороняючі) й виконують текстотвірну або текстоформлювальну ролі [1].

Серед вимог до медичних перекладачів необхідно згадати й конфіденційність, оскільки найчастіше їм доводиться мати справу з лікарською таємницею.

Крім цього, професійний медичний перекладач постійно вдосконалює свою майстерність шляхом віднайдення найкращих еквівалентів у мові перекладу. Це особливо важливо, коли переклад здійснюється мовами, що мають кілька діалектів (наприклад, британський і американський варіанти англійської мови) [3].

Однозначної відповіді на питання "Чи повинен медичний перекладач мати медичну освіту?" не існує. Перекладачі з медичною освітою вважають, що вона незамінна в цьому виді діяльності, перекладачі без неї не бачать у ній необхідності. Однак, у будь-якому випадку, основи медичних знань необхідні, щоб розуміти предмет перекладу. Очевидно і те, що лікар, який володіє іноземною мовою, також не може бути гарним перекладачем, оскільки перекладач – це окрема професія, якій необхідно вчитися.

Однак навіть медичні тексти з однаковою спрямованістю, скажімо інструкції для застосування лікарських засобів, які принципово призначені для одного і того самого кола реципієнтів – для пацієнтів, матимуть різне семантичне і синтаксичне оформлення, що, в свою чергу, слід урахувати при виконанні перекладу. Крім того, зустрічаються тексти зі змішаною спрямованістю або спрямованість тексту оригіналу не відповідає спрямованості тексту перекладу, що дуже часто впливає з культурних розбіжностей відповідних цільових аудиторій. В Україні під інструкцією для вживання лікарського препарату підписується академік, який нібито підтверджує якість його, тоді як у Німеччині в інструкції – жодного прізвища. В Україні подекуди досі вдаються до конотативно забарвленого терміна "хворий" замість нейтрального терміна "пацієнт" [2].

Оскільки медичні тексти написані у специфічному стилі, з великою питомою часткою термінів, перекладач має бути фахівцем у галузі та знавцем національної термінологічної системи, а також формату відповідної документації національною мовою.

Однак, щодо інструкцій, то досє про схвалення нової продукції часто містять такі фрагменти, як графіки, таблиці, комп'ютерні проектування, відскановані підписи пацієнтів, що супроводжуються текстовими коментарями.

І тому, залежно від характеру документів, може знадобитися і складний технічний переклад. Наприклад, переклад інструкції по використанню обладнання. Значну складність представляє будь-який юридичний переклад або медичний. Це пояснюється великою кількістю спеціальних термінів і необхідністю передати саму суть даних термінів.

З появою комп'ютерних технологій, виконання перекладів значно спростилося. Наприклад, з'явилися різноманітні програмні продукти.

Завдяки сучасним технологіям істотно спростився сам процес перекладу. Стало набагато простіше знаходити кваліфікованих фахівців, взаємодіяти з ними. Наприклад, машинний переклад ближче до дослівного перекладу. Відбувається процес поступового перекладу слова за словом. Однак, без повного розуміння медичної термінології та медичних концепцій - неможливо виконати точний переклад, щоб правильно передати зміст оригінального тексту медичної сфери.

Тому важливо підсумувати, що медичний переклад можна з впевненістю здійснювати за допомогою комп'ютерних технологій, але це дуже відповідальне завдання. Інструкції застосування до ліків, інструкції з експлуатації обладнання, приладів, виписані рецепти та інші тексти, повинні бути грамотно і без похибок перекладені з однієї мови на іншу, оскільки від цього може залежати здоров'я і життя людини, або навіть людей.

#### **Список використаних джерел:**

1. Боцман, А.В. (2006). Структурно-семантичні та прагматичні особливості фармацевтичних текстів. (Автореф. дис. канд. філол. наук). Київський національний ун-т ім. Тараса Шевченка, Київ.
2. Макеєв, К.С. (2009) Жанрові особливості фармацевтичних текстів у німецько-українському перекладі. (Автореф. дис. канд. філол. наук). Київський національний ун-т ім. Тараса Шевченка, Київ.
3. Txabarriaga, R. (2009). IMIA Guide on Medical Translation. Retrieved from: <http://www.imiaweb.org/uploads/pages/438.pdf>
4. Beddies, Th, Brinkschulte, E., Brumme, M, Hess, V, Marz, I., Müller, Th. (2008). Skript für das Praktikum der Medizinischen Terminologie, hrsg. vom Institut für Geschichte der Medizin im Charite Centrum für Human- und Gesundheitswissenschaften der Charite. Universitätsmedizin Berlin.

*Танасюк Ю.В.<sup>1</sup>, канд. фіз.-мат. наук, доцент  
Гарвасюк Р.В.<sup>2</sup>, спеціальність «комп'ютерна інженерія», студент  
Чернівецький національний університет імені Юрія Федьковича, м. Чернівці  
<sup>1</sup>Кафедра комп'ютерних систем та мереж, доцент  
<sup>2</sup>Кафедра комп'ютерних систем та мереж, студент*

## **АЛГОРИТМ ДЛЯ ФОРМУВАННЯ НАВЧАЛЬНОГО РОЗКЛАДУ**

Процес формування розкладу є важливим етапом перд початком кожного семестру у всіх навчальних закладах, який вимагає значних витрат часу. Потрібно враховувати досить багато змінних, таки як різна кількість студентів, викладачів, предметів щороку та багато інших факторів. Проте, цей процес можна автоматизувати і покращувати.

Розроблено алгоритм та програмне забезпечення для формування навчального розкладу занять на основі початкових даних, таких як: кількість студентів, викладачів, аудиторій, занять, тип занять. Алгоритм враховує розмір аудиторій, зайнятість викладачів, зміни навчання по часу та розподіл навантаження впродовж тижня, Також розроблене програмне забезпечення для створення, перегляду та редагування розкладу на ОС Android і веб інтерфейс для виконання вище прелічених операцій у браузерях.

Подання готового розкладу студентам також залишає бажати кращого. Тому для того, щоб зробити цей процес більш зручним та зрозумілим, було розроблено програмний продукт, який дозволяє переглядати студентам розклад, створений викладачами.

Для перегляду занять доступний Android додаток зі зручним та інтуїтивним інтерфейсом, де відображаються всі потрібні деталі заняття (де, коли, з ким і як довго). Розклад відсортований по університетах, факультетах і групах. Також додаток дозволяє користувачам створити власний розклад, який синхронізується між усіма пристроями на базі ОС Android.

Для створення розкладу викладами доступний програмний продукт для браузерів, інтерфейс якого створений з використанням бібліотеки ReactJS. Даний продукт дозволяє як створювати розклад автоматично, використовуючи алгоритм для створення розкладу, так і вручну. Для збереження створеного розкладу потрібне з'єднання з мережею Інтернет.

Дані розкладу занять зберігаються у базі даних Cloud Firestore. За збереження даних відповідає серверна чатина продукту, написана на NodeJS. Спілкування фронт- і бекенду відбувається через спеціальні API.

З'єднання Android додатку з базою даних відбувається напряду без додаткового сервера.

Нижче представлений загальний алгоритм створення розкладу.

На початку роботи алгоритму аналізується кількість занять, які потрібно розташувати в розкладі. Береться до уваги кількість вільних місць в розкладі деякої групи, кількість вільних аудиторій, тип аудиторій (лабораторні, лекційні і т. д.), а також наявність викладачів, які доступні в даний час для проведення заняття.



Особливістю даного алгоритму є те, що він враховує навантаження впродовж тижня або дня і номер курсу. Наприклад, якщо пари для першого курсу будуть розміщуватися в першій половині дня, починаючи з першої, то заняття для старших курсів розташуються пізніше, враховуючи наявність доступних аудиторій і викладачів по мірі збільшення порядкового номеру курсу.

Щодо розподілу навантаження, в алгоритмі враховано тип заняття. Оскільки чотири лабораторних пари поспіль були б не дуже доцільними в плані продуктивності студентів, Алгоритм буде «розбавляти» їх лекційними заняттями, а лабораторні чи практичні - переносити на наступні дні.

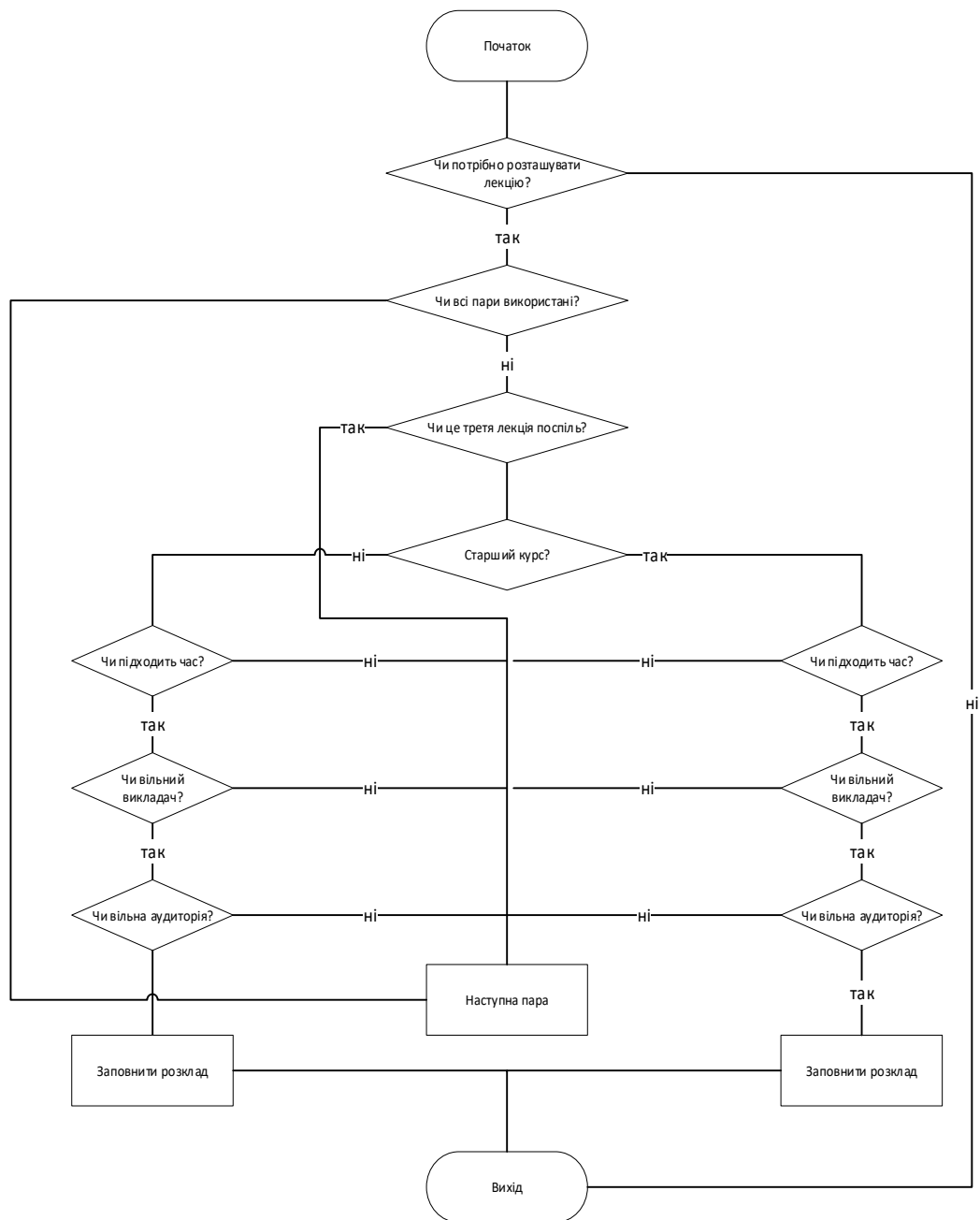


Рис. 1. Загальний алгоритм створення розкладу

### Література:

1. Кренке Д. Теория и практика построения баз данных [Електронний ресурс] / Д. Кренке // Питер. – 2003. – Режим доступу до ресурсу: <http://padaread.com/?book=22475>.
2. Almond M. An algorithm for constructing University timetables / Mary Almond. // The Computer Journal. – 1966. – 4. – С. 331–340.
3. Sedgewick R. Algorithms [Електронний ресурс] / R. Sedgewick, K. Wayne // 4th Edition. – 2013. – Режим доступу до ресурсу: <https://algs4.cs.princeton.edu/home/>.
4. Parlante N. Linked List Basics [Електронний ресурс] / Nick Parlante // Nick Parlante. – 2001. – Режим доступу до ресурсу: <http://cslibrary.stanford.edu/103/LinkedListBasics.pdf>.

*Танасюк Ю.В., канд. фіз.-мат. наук, доцент  
Головайко Р.А., спеціальність «Комп'ютерна інженерія», студент 6 курсу  
Чернівецький національний університет імені Юрія Федьковича, м. Чернівці  
Кафедра комп'ютерних систем та мереж*

## ВІРТУАЛЬНИЙ ТУР ПО НАВЧАЛЬНОМУ КОРПУСУ ЧЕРНІВЕЦЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ІМЕНІ ЮРІЯ ФЕДЬКОВИЧА

Віртуальна реальність зараз надзвичайно популярна і використовується в багатьох сферах повсякденного життя, як наприклад, відеоігри, кіно і серіали, продаж товарів і нерухомості, медицина, навчання, військова промисловість, а також проектування. Зокрема, засоби віртуальної і доповненої реальності стають дедалі популярнішими для створення віртуальних турів і планів будівель. Це пояснюється багатьма причинами. До прикладу, можна, не виходячи з дому, віртуально відвідати будь-який музей або пам'ятку на Землі. Також з'являється можливість створити план будівлі і побачити можливі недоліки. У квартирі чи аудиторії школи або університету спланувати дизайн, розташування меблів і техніки. А також допоможе в плані орієнтування у незнайомих будівлях, особливо людям з обмеженими можливостями. Саме тому, виконання даної теми є надзвичайно актуальним.

Як аналоги програм-навігаторів у приміщеннях для ОС Android можна коротко розглянути такі:

1) Path Guide (рис.1) – це додаток-карта для мобільних пристроїв розроблений Microsoft. Додаток не потребує GPS або будь-яких інших датчиків позиціонування для навігації у будинках. Path Guide використовує барометр та магнітометр смартфона для обчислення відстаней та створення карт необхідної будівлі. Більшість смартфонів потребують лише магнітометра або крокомірів для встановлення напрямків, але барометр допомагає додатку визначити висоту, що сприяє точнішому відтворенню структури будівлі. Під час кожного переходу або повороту є можливість додавання зображення для спрощення процесу навігації для користувачів. Недоліком цього додатку є потреба попереднього створення карти будівлі чи промислового об'єкту.

2) Google Indoor Maps (рис. 2) – функція вбудована в Google Maps і це плюс – не потрібно встановлювати додаткові програми. Мінусом, як і в

минулому додатку є відсутність готових карт будівель. Потрібно створити карту і надіслати її на відповідну пошту, щоб її додали до загальної карти світу.

3)

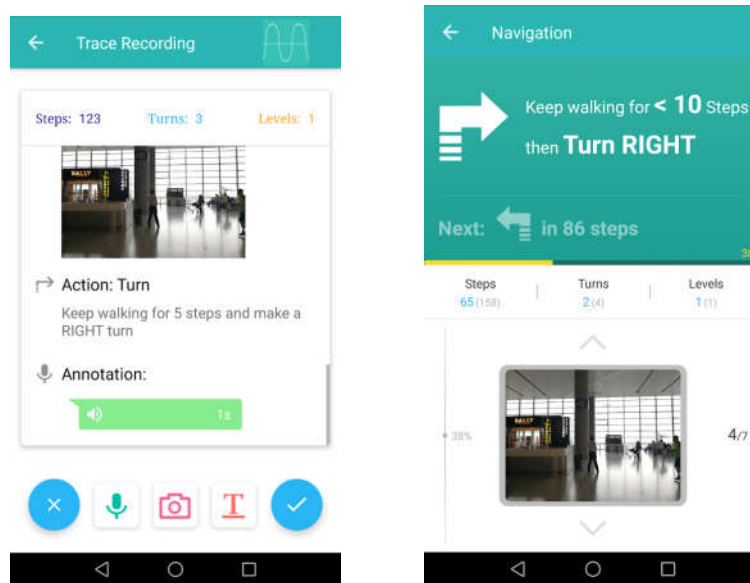


Рис. 1. Знімок екрана додатка Path Guide

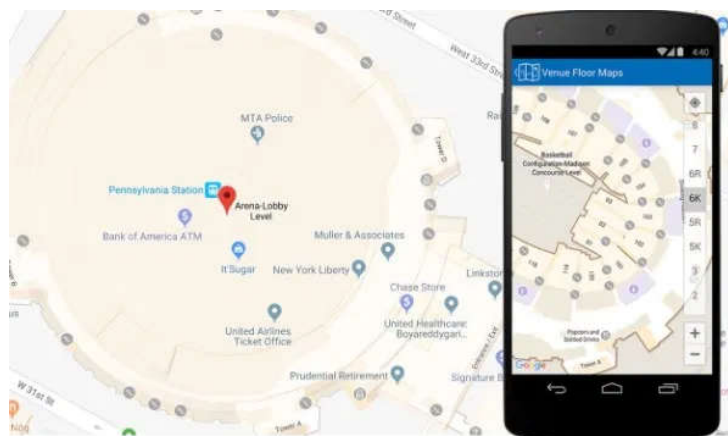


Рис. 2 Знімок екрана додатка Google Indoor Maps

Є ще кілька аналогів:

- 4) Situm Mapping Tool
- 5) HERE Indoor Radio Mapper
- 6) IndoorAtlas MapCreator 2

Проте, в цих аналогах, окрім потреби у створенні карти, обов'язкова реєстрація, що не завжди прийнятна.

Враховуючи наявні програмні розробки та можливості, які вони забезпечують, мета даної роботи полягала у створенні віртуальної 3D-моделі навчальних приміщень, яка б дозволила полегшити орієнтування у корпусі, виконувати пошук необхідних приміщень та прокладати до них оптимальні маршрути.

Представлена розробка створена за допомогою Unity 2018.3.7f1 Personal, а також програмного середовища Microsoft Visual Studio Community 2017 з використанням мови програмування C#. Середовище Unity зарекомендувало

себе як доволі простий, безкоштовний кросплатформовий двигун візуальної розробки. Розроблений додаток повинен допомагати студентам молодших курсів, а також просто відвідувачам навчального корпусу, орієнтуватись у ньому. Програма доступна для використання на платформах Windows і Android.

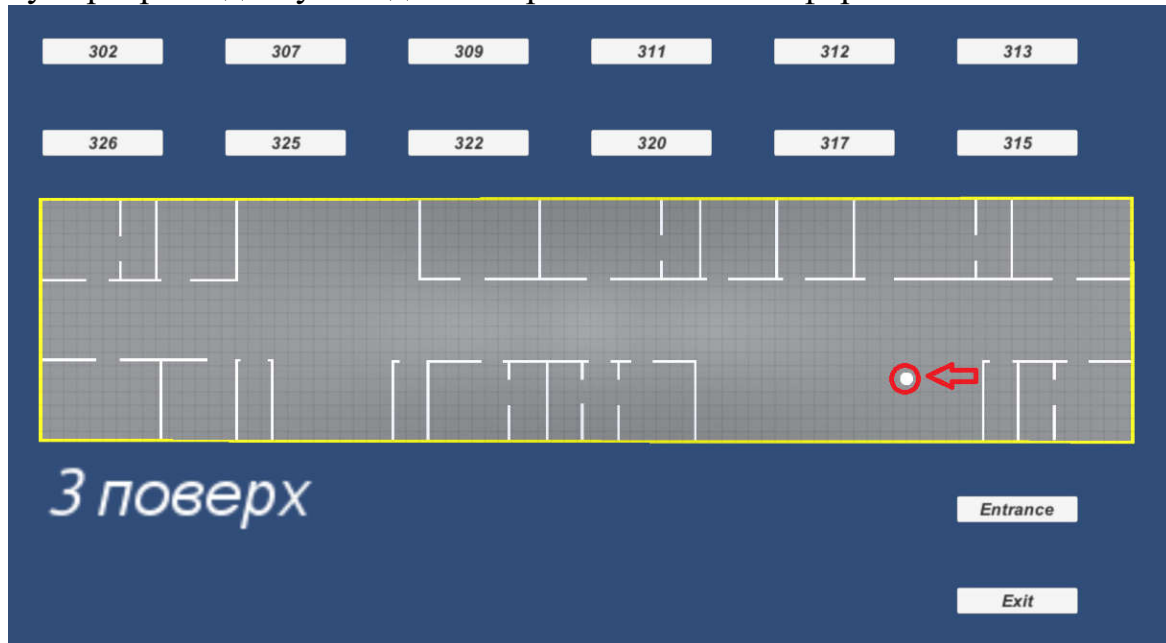


Рис. 3 Знімок екрана розробленого додатку на початку роботи

Розглянемо в якості прикладу третій поверх корпусу. На рис. 3 показано початкове розташування відвідувача, який піднявся на поверх сходами. Щоб дізнатися, де знаходиться потрібна аудиторія, натискаємо на кнопку з відповідним номером і фігура, яка позначає відвідувача, почне рухатись до обраної аудиторії. При цьому також відображається рекомендований шлях пересування. Так, обравши аудиторію № 307, бачимо де вона знаходиться (рис. 4). Також, в разі потреби є можливість повернутись на початок, тобто до входу на поверх зі сходів (кнопка Entrance), і кнопка виходу з програми (Exit).

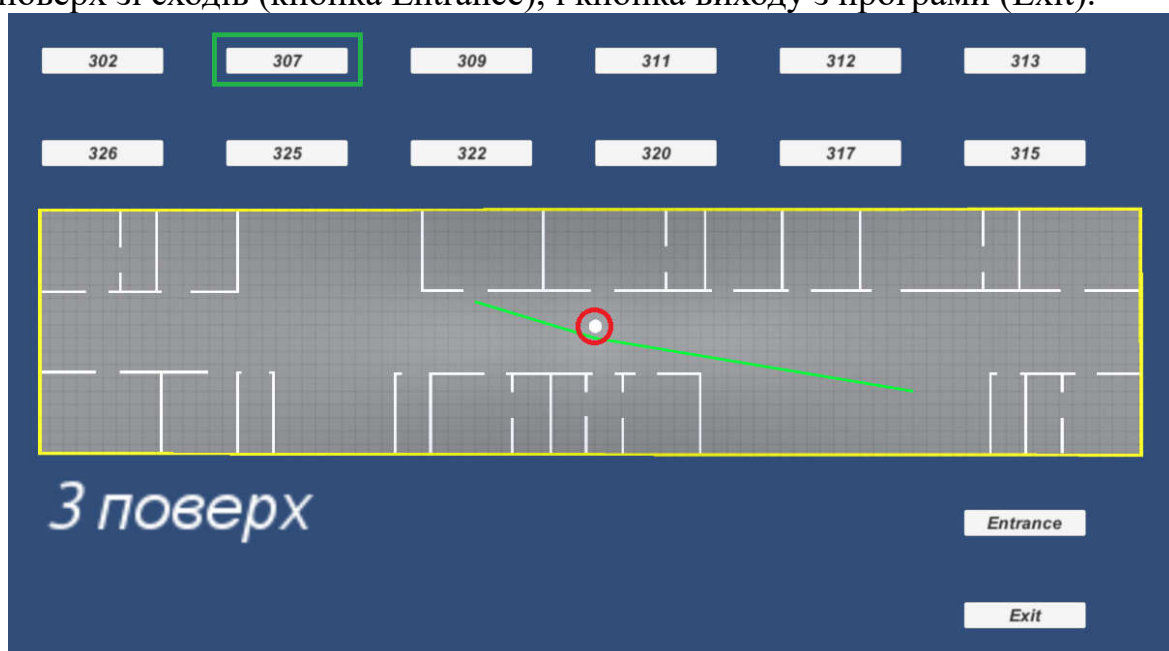


Рис. 4. Знімок екрана розробленого додатку після вибору аудиторії

Окрім зазначених функцій, розроблена програма забезпечує такі можливості:

- 1) Підсвічування обраної аудиторії.
- 2) Надання короткого опису об'єкту пошуку.
- 3) Прокладання шляху по декількох поверхах.

#### **Література:**

1. Unity in Action: Multiplatform Game Development in C# with Unity 5/ Joe Hocking. - Manning Publications, 2015. - 352 с.
2. Unity Game Development in 24 Hours, Sams Teach Yourself (2nd Edition) / Ben Tristem, Mike Geig.- Sams Publishing. - 2015. - 432 с.
3. Інтернет ресурс: <https://learn.unity.com>
4. Відео ресурс: <https://www.youtube.com/user/Brackeys>
5. Інтернет ресурс: <https://docs.microsoft.com/en-gb/dotnet/csharp/>

***Тарбай Б.В., Воропаєва С.Л., Поповецька Л.І.**  
Чернівецький національний університет імені Юрія Федьковича,  
м. Чернівці  
Кафедра комп'ютерних систем та мереж  
ДВНЗ “Чернівецький індустріальний коледж”*

## **ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ІНТЕГРАЦІЇ C# ТА AUTOCAD ПРИ ТРИВИМІРНОМУ МОДЕЛЮВАННІ**

При графічній взаємодії, проектувальника з технічними і програмними засобами, завдання автоматизації проектування дає можливість вирішувати інтерактивно. Головну роль при цьому відіграє графічне сприйняття і здатність оперувати графічними примітивами, що створюють графічний образ.

На сьогоднішній день існує велика кількість графічних редакторів та програм геометричного моделювання [1]. Система автоматизованого проектування AutoCAD являється однією з найпопулярніших платформ в світі. AutoCAD являється потужним графічним ядром, на якому базуються багато прикладних пакетів, як від самої фірми AutoDESK, так і від незалежних розробників.

Система AutoCAD в базовому виді дозволяє виконувати креслярські і конструкторські роботи використовуючи тільки стандартні засоби. За допомогою простих примітивів (відрізків, кіл, дуг та ін.) можна накреслити практично будь-який необхідний елемент. Однак кінцевим користувачам (інженерам, конструкторам та проектувальникам) необхідно створювати не просто примітиви, а конкретно визначені об'єкти (деталі обладнання, електричні та принципові схеми, будівельні плани та ін.). Здійснювати це необхідно якісно, швидко та ефективно відповідно до стандартів відповідної галузі виробництва.

Врахувати всі необхідні моменти для кінцевих користувачів та включити їх до складу системи просто неможливе завдання. Саме тому фірма AutoDESK

вдосконалила свою базову системи спеціальними засобами розробки нових практичних систем. Застосовуючи ці засоби користувач здатний створювати свої власні підпрограми для забезпечення автоматизації роботи в напрямках інженерної діяльності.

Система AutoCAD організована таким чином, що всі елементи в ній представлені в вигляді об'єктів. Кожен об'єкт має свої властивості та функції. Дана система розроблена з врахуванням концепції СОМ, що дозволяє звертатися до об'єктів AutoCAD з інших систем і їх додатків [2]. Технологія СОМ (Component Object Technology) – об'єктно-орієнтована програмна специфікація, представлена компанією Microsoft. Дана технологія призначена для підвищення надійності взаємодії програмних продуктів між собою. Технологія СОМ містить в своїй основі ідеї поліморфізму та інкапсуляції об'єктно-орієнтованих мов програмування. Саме завдяки даній технології можна здійснювати маніпуляції над об'єктами AutoCAD. Програми побудовані на стандарті СОМ, фактично не являються автономними програмами, а представляють собою набір взаємодіючих між собою СОМ-компонентів. Взаємодія СОМ-об'єктів забезпечується набором визначених підпрограм, які називаються інтерфейсами. Доступ до них забезпечується через унікальні ідентифікатори інтерфейсів GUI (Global Unique Interface Identifier), унікальність яких гарантує операційна система. Такий механізм схожий з використанням вказівників при доступі до об'єктів в об'єктно-орієнтованих мовах програмування, що дає можливість прозорого керування об'єктами, тому що доступ до них забезпечується через вказівники. На рис. 1 представлена діаграма, яка описує механізм використання СОМ-технології в додатках AutoCAD.

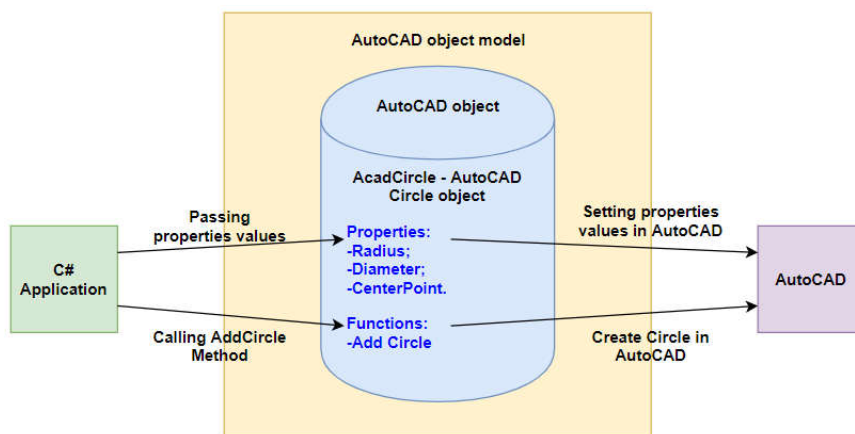


Рис. 1. Діаграма опису механізму взаємодії технології СОМ з додатками

Об'єктна модель AutoCAD є сукупністю об'єктів, властивостей, методів і подій. Для кожного з елементів цієї моделі є своя реалізація у вигляді даних і функцій, які забезпечують взаємодію з користувачем [3].

Об'єктна модель AutoCAD являється деревовидною структурою. На вершині цієї структури знаходиться об'єкт Application – AutoCAD. Об'єкти в AutoCAD розглядаються як ієрархія, яка містить не тільки примітиви, але і інші елементи (таблиці, словники та ін.). Однотипні об'єкти об'єднуються в сімействами (Collections) [2].

До складу кожного з документів входять колекції, які містять певний набір об'єктів. Наприклад, ModelSpace – колекція, яка містить всі об'єкти в просторі моделі.

Для реалізації базових інструментів об'єктної технології в моделі передбачені компоненти, які називають інтерфейсами. Кожний клас реалізується за допомогою свого інтерфейсу, який являється нащадком відповідного базового інтерфейсу. В базовому інтерфейсу описуються всі типізовані властивості та методи [2].

Розроблена система може розглядатися як демонстративний примірник, який містить набір функцій, що впливає на основні об'єкти системи AutoCAD для виконання певних конструкторських завдань.

#### **Література:**

1. Т. Соколова, AutoCAD 2016. Двухмерное и трехмерное моделирование. Учебный курс . – М.: ДМК Пресс, 2016. – 754 с.
2. Полещук Н. Н. Программирование для AutoCAD 2013–2015. – М.: ДМК Пресс, 2015. – 462 с.
3. AutoCAD .NET Developer's Guide. [Electronic resource]. – Access mode: <http://docs.autodesk.com>
4. Д. Скитт, С#. Программирование для профессионалов. – «Вильямс», 2008 – 544 с.
5. О. Ransen AutoCAD Programming in C/C++ –Wiley. 1997. – 510 с.

***Телишева Т.О., канд. техн. наук, доцент**  
Національний Технічний Університет України  
«Київський Політехнічний Інститут імені Ігоря Сікорського», м. Київ  
Кафедра автоматизованих систем обробки інформації та управління,  
доцент*

***Камінський О.В., студент ІС-81мп**  
Національний Технічний Університет України  
«Київський Політехнічний Інститут імені Ігоря Сікорського», м. Київ  
Кафедра автоматизованих систем обробки інформації та управління,  
студент*

## **АВТОМАТИЗАЦІЯ ПРОЦЕСУ ВИЗНАЧЕННЯ ІВАН В БАНКІВСЬКИХ СИСТЕМАХ**

Контрольні знаки (розряд) - це форма перевірки надмірності, яка використовується для виявлення помилок на ідентифікаційних номерах, які використовуються в випадках, коли принаймні іноді ідентифікаційні номери будуть вводитися вручну. Перевірка правильності введеного номеру широко запроваджується і в цифровому середовищі. Особове місце автоматизована перевірка займає в банківській сфері, де це пов'язано з розрахунковими та іншими операціями.

Згідно з текстом телеграми НБУ від 06.08.2019 р. №52-0011/40388 у ході впровадження міжнародного коду (IBAN) в Системі Електронних Платежів

(СЕР) виявлено, що деякі учасники СЕР невірно формують контрольний розряд у кодї ІВАН. Це приводить до збою в платіжних операціях СЕР.

Контрольний розряд складається з однієї або декількох цифр, обчислених за алгоритмом[1] і дуже часто використовується в різних номерах, з якими ми стикаємося як в житті, так і в інформаційних системах:

- номер РНН;
- номер ПН / БН;
- номер пластикової карти;
- номер банківського рахунку ІВАН;
- штрих - код товару EAN-13;
- код книги ISBN.

Як правило, контрольний розряд в невеликих номерах (довжиною 10-13 цифр) - це тільки одна остання цифра. У номерах достовірніше - це можуть бути вже кілька цифр

Найголовніше - контрольний розряд повинен давати захист від так званих "одноразових помилок". Одноразова помилка - це помилка тільки в одній цифрі з усіх. Але це програма-мінімум. Однак чим більше всяких різних помилок можливо відловити - тим краще. Адже людина може помилитися двомастами тридцятьма п'ятьма різними способами. За допомогою контрольного розряду можна виявити прості помилки у введенні ряду символів (як правило, цифр), таких як одна помилкова цифра або деякі перестановки двох послідовних цифр.

Необхідність стандартизації систем контрольних символів визначалася наступними міркуваннями:

а) з безлічі використовуваних систем багато хто мають дуже схожі характеристики, і значна частина різноманіття не дає суттєвої користі;

б) мало існуючих систем були ретельно перевірені математично, а в деяких є серйозні дефекти;

в) різноманітність систем підриває економію продуктів, які генерують або підтверджують контрольні символи, і часто заважає перевіряти взаємозамінні дані. [2]

Стандарт ISO / ІЕС 7064: 2003 (далі – Стандарт) визначає набір систем контрольних символів, здатних захищати рядки від помилок, які виникають при копіюванні або введенні даних. Рядки можуть мати фіксовану або змінну довжину і можуть мати набір символів:

- числовий (10 цифр: 0 до 9);
- алфавітний (26 літер: від А до Я);
- буквено-цифрові (літери та цифри).

Вбудовані пробіли та спеціальні символи ігноруються. Стандарт визначає вимоги відповідності до продуктів, описаних як генерування контрольних символів або контрольних рядків, використовуючи системи, наведені в цьому Міжнародному стандарті.

Системи контрольних символів, визначені в Стандарті, можуть виявляти:

- всі поодинокі помилки підстановки (підміна одного символу іншим, наприклад 4234 для 1234);



- всі або майже всі поодинокі (локальні) помилки переміщення (переміщення двох одиночних символів, суміжних або з одним символом між ними, наприклад, 12354 або 12543 для 12345);
  - всі або майже всі помилки зсуву (зсуви всієї струни вліво або вправо);
  - висока частка подвійних помилок підстановки (дві окремі похибки однієї заміни в одній і тій же рядку, наприклад 7234587 для 1234567);
  - висока частка всіх інших помилок.
- Рядок символів задовольняє перевірку, коли:

$$\sum_{i=1}^n [a_i \times r^{(i-1)}] \equiv \mathbf{1(modM)} \quad (1)$$

де

$n$  - кількість символів у рядку, включаючи контрольні символи;

$i$  - індекс позиції символів, що починається справа (тобто для самого правого символу,  $i = 1$ ), не враховуючи пробілів та роздільників;

$a_i$  - значення символу в позиції  $i$ ;

$r$  - радіакс (тобто основа для геометричної прогресії); [3]

У рекурсивному методі рядок обробляється символом зліва направо.

З індексом  $j = \mathbf{1} \dots n$ , де  $n$  - кількість символів у рядку, що включає контрольний символ,  $i$  визначаючи  $P_j = \mathbf{0}$  для  $j = \mathbf{1}$ , обчислюється за формулою:

$$S_j = P_j + a_{(n-j+1)} \quad (2)$$

$$P_{(j+1)} = S_j \times r \quad (3)$$

де

$S_j$  - проміжна сума;

$P_j$  - продукт, висунутий вперед;

$a_{(n-j+1)}$  - значення символу;

$r$  - радіакс [3]

Для перевірки рядок приймається як правильний, якщо:

$$S \equiv \mathbf{1(modM)} \quad (4)$$

Змоделюємо алгоритм розрахунку контрольного розряду на прикладі формування міжнародного номера банківського рахунку.

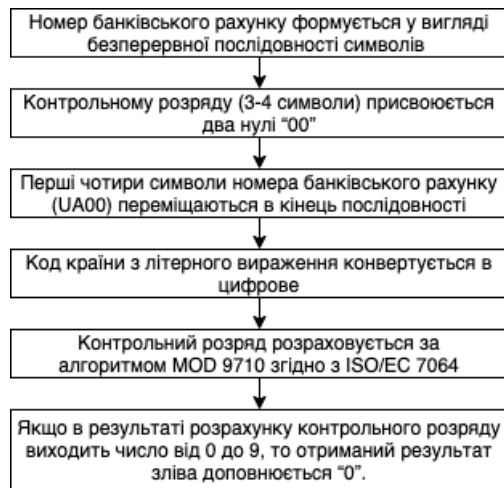


Рис. 1. Послідовність розрахунку контрольного розряду

У зв'язку з переходом на міжнародний номер банківського рахунку згідно постанови Правління Національного банку України від 28 грудня 2018 року № 162 [5], банківські установи повинні з 1 листопада формувати клієнтам міжнародні номери банківського рахунку.

Для формування міжнародного номера банківського рахунку розраховується контрольний розряд згідно з алгоритмом MOD97-10 системи контрольних знаків.

Наведемо діаграму послідовності програмної реалізації методу розрахунку контрольного розряду.

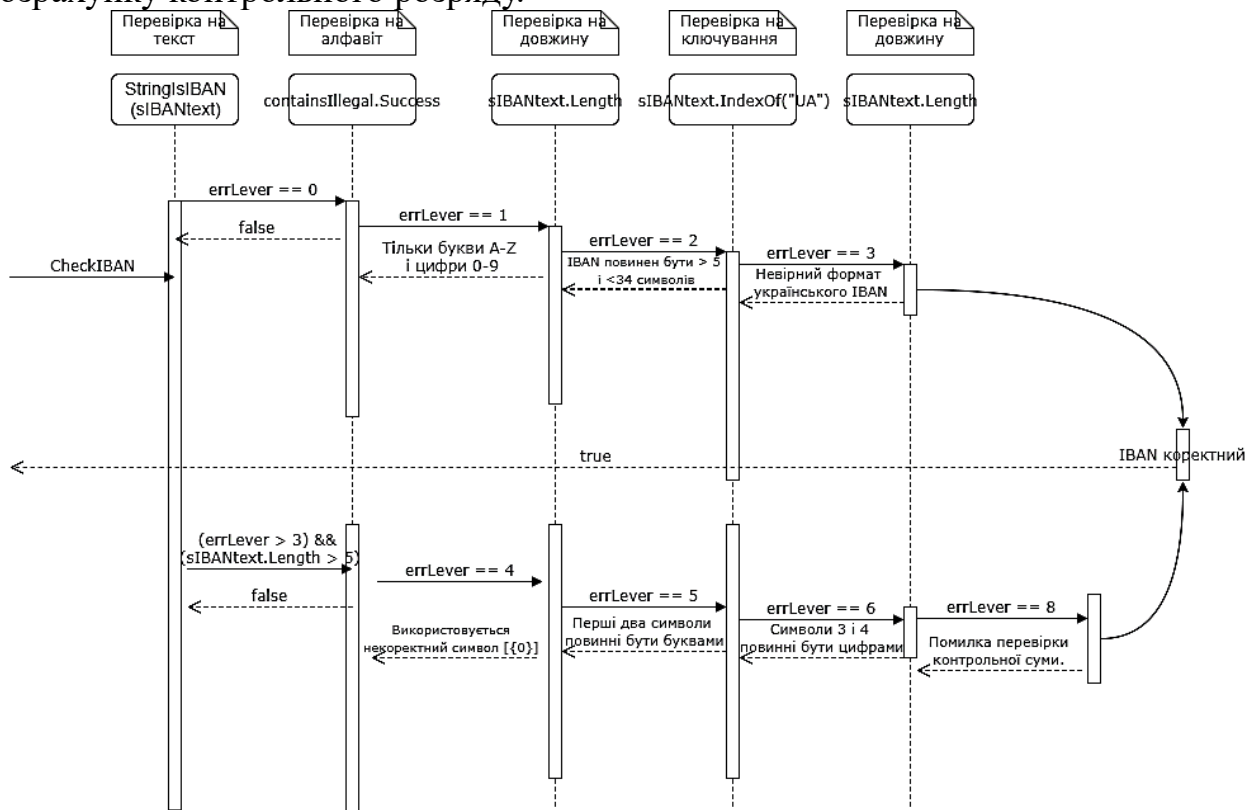


Рис. 2. Діаграма послідовності перевірки коректності міжнародного номеру банківського рахунку

Завдяки наведеної програмної реалізації, можна побачити, що завдяки імплементації алгоритму MOD9710 системи контрольних знаків у процес формування номеру рахунку клієнта, можна виключити типові помилки, які створюють клієнти під час роботи.

Також, завдяки цьому збільшується швидкість роботи програмного забезпечення банку, бо ідентифікації рахунку проходить швидше, що дозволяє пришвидшити усі операції банку та надає йому конкурентну спроможність у питанні стратегічного розвитку.

Актуальність теми обумовлюється тим, що згідно постанови Правління Національного банку України від 28 грудня 2018 року № 162 всі банки України мають перейти на IBAN, однак є помилкові перерахунки, які знаходять захисні системи СПС і необхідним є приведення у відповідність до стандартів АБС, які допускають помилки. В тезах наведені теоретичні відомості про контрольні розряди і методи їх створення. Для уніфікації запропонований алгоритм, який підтримує стандарт ISO / IEC 7064: 2003.

Був проведений огляд міжнародного стандарту систем контрольних знаків, що використовуються для збереження цілісності ідентифікаційних номерів, особливо банківських рахунків.

Була наведена діаграма послідовності методу розрахунку контрольного розряду для міжнародного номеру банківського рахунку.

#### **Список літератури:**

1. R.-H. Schulz. Some check digit systems over non-abelian groups. Mitt.der Math.Ges.Hamburg, 12(3):819–827, 1991.
2. ISO/IEC 7064:2003 Information technology — Security techniques — Check character systems.
3. R.-H. Schulz. On check digit systems using anti-symmetric mappings. In I. Althofer et al., editor. Numbers, Information and Complexity, pages 295–310. Kluwer Acad.Publ. Boston, 2000.
4. Грицак І. І. Управлінський облік у системі менеджменту підприємства: особливості організації та оцінювання / І. І. Грицак, В. М. Чубай // Науковий вісник НЛТУ України. – 2012. – Вип. 22.12. – С. 219–226.
5. Законодавство України. - [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/v0162500-18>

*Фуцур Д.А., магістр,  
Далекорей А.В., старший викладач  
ДВНЗ «Ужгородський національний університет», м. Ужгород  
Кафедра комп'ютерних систем та мереж*

## **ТЕХНОЛОГІЯ “BLOCKCHAIN” ДЛЯ ЗБЕРІГАННЯ ПЕРСОНАЛЬНИХ ДАНИХ**

Наразі до вже існуючих цінностей додаються такі як простота, прозорість та відкритість. І тому не дивно, що розвиток такої технології як blockchain припав саме на цей час.

Пояснення фундаментальних принципів роботи цього концепту лежить у його назві — блокчейн (англ. – blockchain «ланцюг блоків»). Ідея полягає в об'єднанні певного набору інформації (“блоки”) у глобальний розподілений реєстр (“ланцюг”). Така проста зовні технологія уже зробила переворот у багатьох сферах людського життя починаючи від фінансів і аж до системи охорони здоров'я. Блокчейн - це технологія, яка набрала популярності завдяки її використанню при побудові криптовалюти Bitcoin.

Основа технології блокчейн - в розподіленому зберіганні інформації. Це дозволяє зберігати важливу інформацію одночасно на багатьох серверах (у всіх учасників мережі), при цьому зберігати її відкрито і безпечно. Наприклад, на базі цієї технології можна зберігати як історію банківських транзакцій клієнтів, так і базу контрактів, результати голосувань, відбитків пальців або історій хвороб. Інформацію, яка одночасно зберігається у багатьох місцях неможливо підробити, неможливо вкрати, тому що оригінальні записи тут же можуть бути відновлені з сусідніх джерел.

Ціла система це журнал з фактами, що знаходиться на кількох комп'ютерах, об'єднаних в мережу рівноправних вузлів (P2P). Фактами може бути що завгодно, від фінансових операцій та до підписання контракту. Всі комунікації всередині мережі використовують криптографію, щоб надійно ідентифікувати відправника і одержувача.

Блокчейн — це принципово нова надійна технологія зберігання записів, яка може кардинально змінити підхід до формування і зберігання баз даних.

Учасники блокчейн - мережі мають доступ до інших комп'ютерів мережі, завдяки чому можна обмінюватися даними. Кожен користувач перевіряє коректність нових даних. Якщо вони достовірні, він зберігає їх і передає далі по мережі.

Дана технологія має величезний потенціал з точки зору спрощення та підвищення ефективності за рахунок створення принципово нової інфраструктури фінансових сервісів. Ця технологія може успішно використовуватися банками для проведення внутрішніх взаєморозрахунків і здійснення міжбанківських операцій, а також при проведенні мікроплатежів між фізичними особами.

При цьому вона може значно спростити відстеження підозрілих транзакцій і в цілому підвищити прозорість угод. По суті це технологія розподіленого підтвердження транзакцій, яка представляє собою величезну розподілену базу даних. При цьому перевіркою достовірності транзакцій займаються самі учасники, вони ж підтверджують їх справжність та формують блоки записів.

Такий підхід цікавий перш за все тим, що відпадає необхідність в посередниках в особі платіжних систем, що здійснюють процесування транзакцій і, як наслідок, підвищується швидкість обробки операцій і знижується вартість для кінцевого споживача.

### **Література:**

1. Roger Wattenhofer. The Science of the Blockchain - CreateSpace Independent Publishing Platform; 1 edition (January 27, 2016).
2. Blockchain Contracts and Cyberlaw - Pavan Duggal - SAAKSHAR LAW PUBLICATIONS (December 23, 2015).
3. «Decentralized Applications: Harnessing Bitcoin's Blockchain Technology» 1-е видання; Siraj Raval; 150 стр.; 2016 г.

*Шлапак С.С.*

*Національний Технічний Університет України “Київський політехнічний інститут ім. Ігоря Сікорського”, м. Київ  
Кафедра автоматики та управління в технічних системах, студент*

## **ПОРІВНЯННЯ СТАНДАРТІВ БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ**

У захищеній від MACsec мережі кожен вузол має щонайменше один захищений канал передачі. Цей захищений канал передачі пов'язаний з ідентифікатором: ідентифікатором захищеного каналу (SCI). Захищений канал передачі також зберігає різні параметри конфігурації, наприклад, чи потрібно виконувати захист відтворення або включити шифрування. Кожен вузол, який очікує отримання трафіку, що надсилається через певний захищений канал передачі, повинен налаштувати відповідний захищений канал прийому. Цей прийом захищеного каналу повинен мати SCI, відповідний SCI захищеного каналу передачі однорангового.

У межах кожного захищеного каналу (і передачі, і прийому) визначаються захищені асоціації. Захищені асоціації містять ключі шифрування та ідентифікуються за номером їх асоціації. З кожним захищеним об'єднанням пов'язаний ще один важливий параметр: номер пакету. На стороні передачі цей номер пакета вводиться в заголовок MACsec і використовується в процесі шифрування. На стороні прийому номер пакета із заголовка MACsec може бути перевірений на номер пакету, локально збережений у відповідній захищеній асоціації, щоб виконати захист відтворення.

### ***IPsec***

Перш за все, MACsec і IPsec працюють на різних мережевих шарах. IPsec працює над IP-пакетами, на рівні 3, тоді як MACsec працює на рівні 2, на кадрах Ethernet. Таким чином, MACsec може захищати весь трафік DHCP та ARP, який IPsec не може захистити. З іншого боку, IPsec може працювати через маршрутизатори, тоді як MACsec обмежений локальною мережею.

Як MACsec, так і IPsec, користувацькі програми не потребують змін, щоб скористатися гарантіями безпеки, які надають ці стандарти. У Red Hat Enterprise Linux підтримка IPsec надається libreswan

### ***SSL/TLS***

SSL / TLS працює на ще одному шарі, а саме на п'ятому (додатковому) шарі. Таким чином, безпека програм може вимагати змін програми, що може виявитися досить проблематичним. З іншого боку, вставлення

криптографічного шару безпосередньо в додатки також пропонує деякі переваги. Програмне забезпечення може самостійно перевіряти стан шифрування та справжність на основі політики та може відповідно реагувати. Перевірка цих властивостей безпеки безпосередньо в додатку може забезпечити захист від кінця до кінця. У Red Hat Enterprise Linux SSL / TLS надається декількома бібліотеками, такими як GnuTLS, NSS, OpenJDK / JSSE та OpenSSL (в алфавітному порядку).

#### Список використаних джерел:

- 1.Enhancing Network Security with MACsec [Електронний ресурс] – Режим доступу: <https://www.curtisswrightds.com/news/blog/enhancing-network-security-with-macsec.html>
- 2.What is ipsec ? [Електронний ресурс] – Режим доступу: <https://searchsecurity.techtarget.com/definition/IPsec-Internet-Protocol-Security>
- 3.Transport Layer Security [Електронний ресурс] – Режим доступу: [https://en.wikipedia.org/wiki/Transport\\_Layer\\_Security](https://en.wikipedia.org/wiki/Transport_Layer_Security)

**Шматок В.В., магістр,  
Сватюк О.Я., ст.викладач**  
*ДВНЗ «Ужгородський національний університет», м. Ужгород  
Кафедра комп'ютерних систем та мереж*

## ТЕХНОЛОГІЯ ДОПОВНЕНОЇ РЕАЛЬНОСТІ

Доповнена реальність – це середовище з прямим або непрямим доповненням фізичного світу цифровими даними. Процес додавання об'єктів доповненої реальності відбувається в режимі реального часу, а провідником служать цифрові пристрої – планшети, смартфони, «розумні» окуляри або аксесуари зі спеціальним програмним забезпеченням. Пристрій через камеру або інший інтерфейс (наприклад, *Bluetooth* або *GPS*) розпізнає об'єкти, особливі мітки на них або місце розташування користувача. Маркером може бути як спеціальний радіомаячок з вбудованим чіпом, так і звичайний *QR*-код. Для того, щоб відбулося доповнення, користувачеві потрібно потрапити в зону дії цього маячка або зчитати *QR*-код.

Додатки на основі доповненої реальності можуть допомогати людині фокусувати увагу на певних елементах зображення, що отримується з камери; покращувати розуміння об'єктів оточуючого світу шляхом надавання необхідної інформації, що накладається на зображення у вигляді текстового повідомлення або візуального образу.

На сьогодні доповнена реальність використовується у таких сферах діяльності: освіта, медицина, військова справа, авіація, маркетинг, туризм, дизайн та ігри. У сфері освіти доповнена реальність допомагає дітям пізнавати світ, оскільки вони можуть навести камеру телефону на предмет зацікавленості і побачити детальну інформацію про нього. У військовій справі доповнена реальність допомагає у підготовці військовослужбовців шляхом навчання на спеціальних полігонах з використанням доповненої реальності. У авіації

доповнена реальність допомагає навчати нових пілотів, а також слугує навігатором. У сфері маркетингу доповнена реальність допомагає продавати різноманітні товари та послуги шляхом показу цих товарів за допомогою спеціальної реклами. У сфері туризму доповнена реальність може допомагати користувачеві у пошуку шляху та знаходити і виводити інформацію про архітектурну будівлю або інший туристичний об'єкт, на який користувач наводить свій мобільний телефон. У сфері дизайну за допомогою доповненої реальності можна, наприклад, зручно презентувати архітектуру розробленої будівлі будь-якого розміру.

Отже, доповнена реальність має широке коло застосувань. Проте, на сьогодні важливою є проблема якісного відображення об'єктів у доповненій реальності.

### **Існуючі технології для роботи з AR**

*OpenCV* - бібліотека алгоритмів комп'ютерного зору, обробки зображень та чисельних алгоритмів загального призначення з відкритим кодом. Реалізована на C / C ++, також розробляється для *Python*, *Java*, *Ruby*, *Matlab*, *Lua* та інших мов. Може вільно використовуватися в академічних та комерційних цілях - поширюється в умовах ліцензії *BSD*.

*Vuforia SDK* - це програмне забезпечення для мобільних пристроїв, яке дозволяє створювати додатки доповненої реальності. Воно використовує технологію комп'ютерного зору для того, щоб розпізнавати і відстежувати плоскі зображення і прості 3D-об'єкти в режимі реального часу. Ця можливість реєстрації зображень дозволяє визначати розташування й орієнтації віртуальних об'єктів, таких як 3D-моделі, в реальному світі, коли вони розглядаються через камеру мобільного пристрою. Положення і орієнтація віртуального об'єкта відстежується в реальному часі, так що точки зору глядача на об'єкт співвідноситься з їх точкою зору на зображення, так, що здається, що віртуальний об'єкт є частиною реальної сцени світу.

*Vuforia SDK* підтримує різні 2D і 3D цільові типи, включаючи безмаркерні цілі. Додаткові можливості *SDK* включає локалізовані виявлення оклюзії за допомогою "віртуальних кнопок, зображень виконання цільового відбору, а також можливість створити і змінити цільові набори програмно під час виконання.

*Vuforia* забезпечує *API* для C++, *Java*, *Objective-C*, і *.Net* мов. Є розширення ігрового движка *Unity*. Таким чином, *SDK* підтримує як рідні для *IOS* і *Android* мови, так і одночасно дозволяє розробляти додатки доповненої реальності в *Unity*, які можна легко портувати на обидві платформи. Саме тому, додатки, розроблені з використанням *Vuforia*, сумісні з широким спектром мобільних пристроїв, включаючи *iPhone*, *iPad*, *Android* - телефонів і планшетів під управлінням ОС *Android* версії 2.2 або вище і *ARMv6* або 7 процесор з *FPU*.

*ARToolkit* - це бібліотека комп'ютерного стеження для створення додатків з доповненою реальністю Для цього він використовує можливості відео спостереження, розрахунок реального стану та орієнтації камери по відношенню до квадратного фізичного маркеру в режимі реального часу. Коли реальний стан камери відомо, віртуальна камера може бути розташована в тій же точці і 3D

модель накладається на реальний маркер. Так ARToolKit вирішує дві ключові проблеми в доповненій реальності: відстеження погляду і віртуальної взаємодії об'єктів.

*ARToolKit* був спочатку розроблений *Hirokazu Kato Nara* інституту науки і технологій в 1999 році і був випущений в університеті Лабораторія НІТ, у Вашингтоні. В даний час він функціонує як проект з відкритим розміщенням на *SourceForge* з комерційною ліцензією доступна *ARToolWorks*. *ARToolKit* дуже широко використовується (бібліотека з більш ніж 160000 завантажень з 2004 року).

*Metaio SDK* - готова бібліотека для створення мобільних додатків доповненої реальності. Використовує *OpenGL* використовує *SLAM* методи для більш точної роботи.

*String* - бібліотека для створення мобільних додатків орієнтована на *iOS* пристрою.

#### Література:

1. Buerli M., Misslinger S. Introducing ARKit-Augmented Reality for iOS//Apple Worldwide Developers Conference (WWDC'17). – 2017. – С. 1-187.
2. Gao L. et al. Real-time visual representations for mobile mixed reality remote collaboration //SIGGRAPH Asia 2018 Virtual & Augmented Reality. – ACM, 2018. – С. 15.
3. Karrie Karahalios. GaitAid Virtual Walker for Movement disorder patients Augmented Reality, 2007

**Юскович-Жуковська В.І., к.т.н., доцент,  
Соловей Л.Я., старший викладач,  
Міжнародний економіко-гуманітарний університет  
імені академіка Степана Дем'янчука, м.Рівне  
Кафедра інформаційних систем та обчислювальних методів**

### **НАПРЯМКИ ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ У ПІДГОТОВЦІ ІТ-ФАХІВЦІВ**

Стратегічним завданням вищої освіти являється підготовка високопрофесійних кадрів, здатних працювати в інформаційному, дедалі більш цифровому суспільстві. Конкурентноспроможний ІТ-фахівець повинен вміти самостійно застосовувати у своїй майбутній ІТ-діяльності новітні інформаційно-комунікаційні технології. Проблемам інформатизації освіти присвячені дослідження багатьох вітчизняних науковців: Гриценко В.І., Манако А.Ф., Биков В., Жалдак М.І., Литвинова С.Г, Овчарук О.В. Дослідженням побудови методів та засобів формування відкритого електронного середовища обміну інформацією присвячені роботи Міхайленка В.М., Білощицького А.О., Рача В.Я., Пелешишина А.М. та ін.

Розвиток соціальних мереж є похідним від розвитку інформаційного суспільства. WWW перетворюється на ефективний електронний простір для викладацько-студентського спілкування в позаурочний час. Соціальні мережі



насичені інформаційними ресурсами закладів вищої освіти. Тренди та спеціальності університетів охоплюють значну Internet-аудиторію абітурієнтів при профорієнтаційній роботі та вступній кампанії.

Віртуальні спільноти абітурієнтів та студентів стають визначальними у сприйнятті того чи іншого ЗВО в інформаційному суспільстві. Сервіси соціальних мереж надають змогу організувати взаємодію викладачів зі студентами, приймати участь у професійних on-line спільнотах. Впровадження новітніх IT та нестандартні підходи у практичній реалізації зумовлює процес на випередження, що відповідає інтересам інформаційного суспільства та потенційних роботодавців.

При підготовці IT-фахівців у ЗВО варто використовувати соціальні мережі і блоги, відео-чати і відео-конференції, 3D-комунікації, які допоможуть створити теоретичну базу для будь-якого on-line курсу. Internet-комунікації надають можливість віддалено спілкуватися викладачу зі студентом у режимі реального часу за допомогою не лише комп'ютера чи ноутбука, а також за допомогою планшетів та смартфонів. Практично всі популярні соціальні мережі надають можливість організувати такі взаємодії.

Насьогодні практично всі користувачі Internet користуються однією з соціальних мереж: Facebook, Twitter, Instagram, Google +, Telegram тощо. Переважна кількість українських викладачів та студентів регулярно використовують соціальні мережі для спілкування, обміну фото та відеофайлами, цікавою інформацією навчального, наукового та професійного характеру. Студентам в галузі IT-технологій викладаються курси з програмування, web-програмування та web-дизайну. Отже, соціальні мережі є потужним інструментом для підготовки IT-фахівців.

Різноманітні сервіси та інструменти соціальних мереж здатні забезпечувати спільну роботу викладачів та студентів під час проведення аудиторного або позааудиторного заняття в інтерактивному режимі. При цьому в освітньому процесі підвищується якість наукових, навчальних, методичних, виховних та організаційних робіт. В соціальних мережах можна організувати безперервну освіту та самоосвіту, відпрацювання пропущених занять, конференції та семінари, симпозіуми, дискусії та діалоги з різних навчальних дисциплін професійного спрямування.

Так, за допомогою соціальних мереж можна створити групи з вивчення навчальних дисциплін з алгоритмізації та програмування, баз даних тощо. У створеній групі розміщується конспект лекцій, надаються приклади розв'язання практичних завдань з написання програмного коду або приклади виконання лабораторних робіт, мультимедійний контент до кожної теми, даються посилання на інформаційні ресурси, електронні підручники тощо. В соціальних мережах проводяться обговорення теми, дискусії, діалоги, опитування. Результати виконаних завдань можуть бути доступними для інших учасників групи, яким дозволяється коментувати. Студенти стають творцями власного програмного продукту. Тобто навчальний процес підготовки IT-фахівців можна реалізувати як за індивідуальною формою навчання так і за груповою. На думку

Тишкової О.В. в мережі Internet існує незліченна кількість спільнот, що надають можливість самонавчатися [1].

Так, функціональні можливості відомих соціальних мереж: Facebook, Twitter, Instagram, Google +, Telegram, надають можливість викладачам при підготовці IT-фахівців надавати доступ до своїх інформаційних ресурсів. Перевагою соціальних мереж є можливість студентам виконувати завдання в режимі on-line та отримувати досвід провідних IT-фахівців та IT-компаній світу. Всі наявні матеріали розміщені у вільному доступі. Велика інформативність та вседоступність, інтерактивність та більша мобільність електронного середовища роблять вивчення дисциплін в галузі знань 12 «Інформаційні технології». Через спільну практичну діяльність у команді, студенти в групі можуть бути учасниками міжнародних IT-проектів.

Візуалізація матеріалів з програмування дозволяє демонструвати їх в електронному вигляді наочно, доступ можливий із будь-якого мобільного телефону, планшета, ноутбука, смартфона, тощо.

Таким чином соціальні мережі дозволяють студентам в IT-галузі самостійно здобувати знання, ефективно навчатися на якісно новому рівні, формувати ІКТ-компетентності.

#### **Література:**

1. Тишкова О.В. Соціальні мережі як виклик сучасності в освітньому середовищі / О.В. Тишкова // Вісник Інституту розвитку дитини. Вип. 34. Серія: Філософія, педагогіка, психологія: Зб. наук. праць. – К.: Вид-во НПУ імені М.П. Драгоманова, 2014. – С. 63-72.

***Mykytas Anton Oleksandrovych***

*Kharkiv National University of Radio Electronics, Kharkiv  
«Computer Engineering and Management», student*

***Kononenko Oleksandr Mykolaiovych***

*Kharkiv National University of Radio Electronics, Kharkiv  
«Computer Engineering and Management», student*

***Bratyshchenko Mykyta Ruslanovych***

*Kharkiv National University of Radio Electronics, Kharkiv  
«Computer Engineering and Management», student*

## **ІНФОРМАЦІЙНА БЕЗПЕКА**

У зв'язку з розвитком інформаційних технологій і комп'ютеризацією економіки одним з найважливіших питань в діяльності компанії стає забезпечення інформаційної безпеки. Інформаційна безпека (ІБ) - це стан інформаційної системи, при якому вона найменш сприйнятлива до втручання і нанесення збитку з боку третіх осіб. Безпека даних також має на увазі управління ризиками, які пов'язані з розголошенням інформації або впливом на апаратні і програмні модулі захисту.

## **Модель системи безпеки**

Інформація вважається захищеною, якщо дотримуються три головні властивості.

Перша - цілісність - передбачає забезпечення достовірності і коректного відображення охоронюваних даних, незалежно від того, які системи безпеки і прийоми захисту використовуються в компанії. Обробка даних не повинна порушуватися, а користувачі системи, які працюють з захищеними файлами, не повинні стикатися з несанкціонованою модифікацією, знищенням ресурсів або збоями в роботі програмного забезпечення.

Друге - конфіденційність - означає, що доступ до перегляду та редагування даних надається виключно авторизованим користувачам системи захисту.

Третє - доступність - має на увазі, що всі авторизовані користувачі повинні мати доступ до конфіденційної інформації.

Досить порушити одне з властивостей захищеної інформації, щоб використання системи стало безглуздом.

### **Загрози конфіденційності інформаційних ресурсів**

Загроза - це можливі або дійсні спроби завладіти захищеними інформаційними ресурсами.

Джерелами загрози безпеці конфіденційних даних є компанії-конкуренти, зловмисники, органи управління. Мета будь-якої загрози полягає в тому, щоб вплинути на цілісність, повноту і доступність даних.

Загрози бувають внутрішніми або зовнішніми. Зовнішні загрози є спробами отримати доступ до даних ззовні і супроводжуються зломом серверів, мереж, акаунтів працівників і зчитуванням інформації з технічних каналів витоку (акустичне зчитування за допомогою жучків, камер, наведення на апаратні засоби, отримання віброакустичної інформації з вікон і архітектурних конструкцій).

Внутрішні загрози мають на увазі неправомірні дії персоналу, робочого відділу або управління фірми. В результаті користувач системи, який працює з конфіденційною інформацією, може видати інформацію стороннім. На практиці така загроза зустрічається частіше за інших. Працівник може роками «зливати» конкурентам секретні дані. Це легко реалізується, адже дії авторизованого користувача адміністратор безпеки не кваліфікує як загрозу.

Інформація - це один з найцінніших і важливих активів будь-якого підприємства і повинна бути належним чином захищена. Отже, захист інформації повинен здійснюватися комплексно, відразу по декількох напрямках. Чим більше методів буде задіяно, тим менше ймовірність виникнення загроз і витоку, тим стійкіше положення компанії на ринку.

### **Література:**

1. Соловей С. Забезпечення безпеки інформації [Електронний ресурс] / Сергій Соловей – Режим доступу до ресурсу: <https://intercert.com.ua/articles/posts/224-informacionnaya-bezopasnost-obuchenie-personala>.

2. Інформаційна безпека підприємства: ключові загрози та способи запобігання [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: <https://www.kp.ru/guide/informatsionnaja-bezopasnost-predprijatija.html>.

*Mykytas Anton Oleksandrovych*  
*Kharkiv National University of Radio Electronics, Kharkiv*  
*«Computer Engineering and Management», student*  
*Kononenko Oleksandr Mykolaiovych*  
*Kharkiv National University of Radio Electronics, Kharkiv*  
*«Computer Engineering and Management», student*  
*Bratyshchenko Mykyta Ruslanovych*  
*Kharkiv National University of Radio Electronics, Kharkiv*  
*«Computer Engineering and Management», student*

## СОЦІАЛЬНА ІНФОРМАТИКА

Небагато факторів так впливають на соціальну сферу товариств, як інформатизація. Розвиток нових інформаційних технологій і їх швидке проникнення в усі сфери життя породило новий напрямок у сучасній інформатиці - соціальну інформатику.

Соціальна інформатика є характерним прикладом нового міждисциплінарного наукового напрямку, який формується на стику ряду природних і гуманітарних наук під впливом інтеграційних факторів, та виникла в останні роки за соціальною необхідністю формування наукової бази нової постіндустріальної цивілізації - інформаційного суспільства.

Предметом вивчення соціальної інформатики як науки є процеси інформатизації суспільства, а також їх вплив на соціальні процеси, в тому числі - на розвиток і становище людини в суспільстві під впливом інформатизації. Соціальна інформатика - це наука, що вивчає комплекс проблем, пов'язаних з проходженням інформаційних процесів в соціумі.

Соціальна інформатика розглядає такі проблеми:

- закономірності і проблеми становлення інформаційного суспільства;
- інформаційні ресурси як фактор соціально-економічного та культурного розвитку суспільства;
- розвиток особистості в інформаційному суспільстві;
- інформаційна культура;
- інформаційна безпека та інші.

Завданнями соціальної інформатики є:

- формування вміння правильно орієнтуватися в новій інформаційній реальності як у світі в цілому, так і в своїй країні;
- формування уявлення про загальну потребу оволодіння інформаційною культурою, без чого неможливо органічне включення в сучасну інформаційну середу і активне сприяння її розвитку;

- методологічна підготовка до подальшого вивчення, освоєння і участі в розробці інформаційних технологій у відповідній предметній області: соціології, психології, економіці, соціальній роботі, журналістиці, правовій сфері та інших.

Соціальна інформатика як будь-яке наукове знання має багаторівневу структуру:

1 рівень - теоретико-методологічний (основні категорії, поняття і закономірності проходження інформаційних процесів в суспільстві);

2 рівень - середній (соціальні, економічні, правові, психологічні та інші аспекти інформатизації);

3 рівень - емпіричний (соціальні аспекти створення, впровадження та адаптації інформаційних технологій у відповідних предметних областях).

Соціальна інформатика грає методологічну роль для так званих галузевих інформатик: економічної, правової, психологічної, соціологічної інформатики та інших.

У будь-яку галузеву інформатику, крім свого предметного поля, входить другий і третій рівень соціальної інформатики як наукового знання, так, наприклад, правова інформатика неминуче займається соціальними зрізами правових аспектів інформатизації та соціальними аспектами створення та впровадження правових інформаційних технологій.

#### **Література:**

1. Урсул А. Д. Інформатизація суспільства: Введення в соціальну інформатику / А. Д. Урсул., 1990. – 191 с.
2. Соціальна інформатика та інформаційна безпека [Електронний ресурс] – Режим доступу до ресурсу: [https://иванов-ам.рф/informatika\\_kabinet/inf\\_soz/index.html](https://иванов-ам.рф/informatika_kabinet/inf_soz/index.html).

***Mykytas Anton Oleksandrovykh***

*Kharkiv National University of Radio Electronics, Kharkiv  
«Computer Engineering and Management», student*

***Kononenko Oleksandr Mykolaiovych***

*Kharkiv National University of Radio Electronics, Kharkiv  
«Computer Engineering and Management», student*

***Bratyshchenko Mykyta Ruslanovych***

*Kharkiv National University of Radio Electronics, Kharkiv  
«Computer Engineering and Management», student*

## **ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ (IoT)**

У сімдесяті роки минулого століття, з того часу, коли комп'ютери перестали бути поодинокими і унікальними виробами, почалася масова автоматизація за двома практично незалежними напрямками. Одне – автоматизація бізнес-процесів, яку ми називаємо інформаційними технологіями (IT, Information Technology). Інше – автоматизація технологічних процесів,

названа операційними технологіями на противагу ІТ (ОТ, Operational Technology).

Слід зауважити, ІТ мають справу не з інформацією, а з даними, тому їх варто було б називати «технології даних». ІТ об'єднують в собі комп'ютери, системи зберігання даних і мережі з процесами створення, обробки, зберігання, забезпечення безпеки і обміну будь-якими формами електронних даних. ОТ – це теж комплекс апаратного і програмного забезпечення, але призначеного для контролю та управління фізичними процесами.

Понад сорок років ІТ і ОТ розвивалися незалежно і за цей час набули рис, які істотно розрізняють їх. Але в другому десятилітті ХХІ століття під впливом ряду факторів, зокрема сенсорної революції, розвитку мережевих технологій, хмарного комп'ютингу, аналітики великих даних і інших сучасних трендів, почався процес конвергенції, який об'єднує два підходи – орієнтацію на дані і орієнтацію на події в фізичному світі.

Термін «Інтернет речей» позначає мережу фізичних предметів («речей»), підключених до Інтернету і взаємодіючих між собою або з зовнішнім середовищем. Одним з перших відомих IoT-пристроїв став вендинговий апарат с прохолодними напоями, модернізований американськими студентами у 1982 році. Він дозволяв віддалено перевіряти наявність напоїв, а також інформацію чи охолонули вони.

У 90-і роки вже була закладена теоретична база IoT, заснована на ідеях бездротової передачі даних, мобільності і штучного інтелекту. У 2000-х роках технології розвивалися стрімко, з'явилися перші реалізовані проекти IoT, будувалися масштабні плани про розумні міста та повної автоматизації рутинні процеси.

У наш час мільярди пристроїв обмінюються інформацією між собою. Світ Інтернету речей зростає, освоює нові технології, а розвинені країни навіть готують правову базу, яка регулюватиме новий інформаційний простір.

Спектр можливих технологій, що використовується для передачі трафіку «Інтернету речей», охоплює як бездротові, так і провідні мережі. Для бездротової передачі даних особливо важливу роль в побудові Інтернету речей грають такі якості, як ефективність в умовах низьких швидкостей, відмовостійкість, адаптивність, можливість самоорганізації.

Бездротові мережі для Інтернету речей підрозділяються на наступні типи:

- Low Power Short Range Networks – енергоефективні мережі малого радіусу дії;
- Low Power Wide Area Networks (LPWAN) – енергоефективні мережі великого радіусу дії;
- Cellular Network – технології, засновані на використанні стандартів стільникових мереж в діапазоні, де є дозвіл.

Успішна реалізація рішень на базі всеосяжного інтернету – не ізольований і незалежний процес. В Cisco вважають, що для цього потрібно технічна і комерційна платформа, на якій можна буде легко вибудовувати різні рішення для раціонального і ефективного досягнення обіцяних комерційних переваг. В основі такої платформи інтернету лежать надійний зв'язок і технологічна

інфраструктура, операційні та управлінські сервіси, а також ряд вертикальних і горизонтальних рішень.

Сучасна концепція Інтернету речей має на увазі, що всі сучасні пристрої незалежно від платформи повинні мати можливість спільно функціонувати з іншими пристроями і сервісами, утворюючи єдину взаємопов'язану екосистему, а не існувати ізольовано.

**Використані джерела:**

1. Боцман Я. А. Інтернет-речей / Я. А. Боцман. – 2016.
2. Лекторій. Що таке інтернет речей і навіщо він потрібен? [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: <https://techno.nv.ua/popscience/chto-takoe-internet-veshchej-1326653.html>.

# Зміст

## Частина 1

### Секція 1. Інформаційні системи і технології

**Абрамова А.О., Кравець П.В.**

Розроблення схеми автоматизації процесу очищення побутових стічних вод....3

**Бабич Є.Ю.**

Технології застосування штучного інтелекту в Україні.....5

**Баловсяк С.В., Гнатюк Ю.А.**

Прогнозування значень автомобільного трафіку за допомогою штучної нейронної мережі.....7

**Баловсяк С.В., Пайлик А.В.**

Система керування освітленням розумного будинку з використанням нечіткої логіки.....8

**Баловсяк С.В., Псарюк С.М.**

Розпізнавання та аналіз зображень друкованих текстів засобами месенджера Telegram.....10

**Батурин Г.С.**

Аналіз показателів схожості зображень в задаче тестирования динамического пользовательского интерфейса.....11

**Бердник М.Г., Морозов Д.О.**

Комп'ютерне моделювання власних чисел і функцій в циліндричній системі координат.....14

**Бідасюк Н.В.**

Мобільні технології на заняттях з англійської мови.....16

**Бобович Ю.В.**

Методи оптимізації Html5 canvas.....18

**Бугаєва Л.М., Безносик Ю.О., Сидоренко І.А.**

Застосування методів інтелектуального аналізу до баз даних Scada систем.....19

**Верстяк О.М.**

Оцінка глобальних проблем сьогодення.....21



<b>Возняк Ю.Р., Тушницький Р.Б.</b> Програмне забезпечення для генерування аудіовідбитків та пошуку за ними аудіозаписів у сховищі даних.....	23
<b>Войтюк. А.І., Лісовенко. І.Д.</b> Особливості паралельної реалізації задачі формування розкладу занять у ВНЗ на основі генетичного алгоритму.....	25
<b>Галактіонов І.О.</b> Сучасний стан проблеми оцінки компетенцій фахівців з інформаційних технологій.....	28
<b>Галактіонов І.О.</b> Використання моделі Раша при розробці автоматизованої системи оцінки компетентності іт-спеціалістів.....	30
<b>Гиря А.О.</b> Огляд інструментарію Fritz ai для імплантування елементів машинного навчання у мобільні додатки.....	33
<b>Голіней Д.В.</b> Веб-плагін імпорту CSV/XML - файлів.....	35
<b>Голяна М.Р., Балоба С.І.</b> Аналіз алгоритмів розпізнавання та відстеження рухомих об'єктів.....	37
<b>Довгань Д.В., Воробець Г.І.</b> Кросплатформна система трекінгу для громадського транспорту.....	39
<b>Дубук В.І., Коцун В.І., Чорний М.В.</b> Програмна реалізація захищених засобів управління графічного людино-машинного інтерфейсу інформаційної системи.....	43
<b>Дуницька Д.Ю., Чумак Л.І.</b> Математичне моделювання процесу випалювання вапняку.....	48
<b>Дячкова В.Б.</b> Применение компьютерно–ориентированных форм обучения в процессе формирования математических знаний и навыков.....	50
<b>Зверев О.А., Гапак О.М.</b> Криптосистема на основі еліптичних кривих.....	53
<b>Калай М.Ю., Самусь Є.І.</b> Технологія прогресивних веб-додатків.....	55

<b>Катренко А.В., Семенів Я.О.</b> Засади створення інформаційних систем обслуговування територіальних лікувальних закладів.....	57
<b>Кіріл А.М.</b> Використання методів віднімання фону в OpenCV.....	59
<b>Клименко М.В., Безверщенко Є.І.</b> Мережевий аналізатор на базі мікрокомп'ютера Raspberry Pi.....	63
<b>Ковтун А.А.</b> Огляд технології Flutter.....	64
<b>Когут Є.Ю.</b> Управління ризиками проекту створення розумного будинку.....	66
<b>Крикунова Г.Д.</b> Використання протоколу OAuth2 для автентифікації користувача у мобільних додатках.....	69
<b>Кропенко Д.О., Ходаковський О.В.</b> Захист шифрованого бездротового зв'язку пристроїв введення інформації від атак по стороннім каналам.....	71
<b>Кузьмініх В.О., Пивовар Н.О.</b> Система аналізу збіжності текстової інформації для оцінки плагіату.....	74
<b>Лук'янова Г.Ю.</b> Формування професійних компетенцій майбутнього педагога за допомогою інформаційно-комунікаційних технологій.....	76
<b>Мазниченко Н.І.</b> Методи та засоби захисту комп'ютерної інформації обмеженого доступу в юридичній діяльності.....	77
<b>Мартовицкий В.А., Осипова Д.Ю.</b> Шаблон QRС в современных web-приложениях.....	80
<b>Медведєв Р.Б., Складанний Д.М., Крайнік А.Р.</b> Алгоритм виявлення пари у теплоносії першого контуру водо-водяного реактора АЕС.....	84

<b>Міхєєв О.С.</b> Децентралізація функцій служби каталогів мультиагентної системи енергетичної інфраструктури з метою підвищення горизонтальної масштабованості та стабільності системи.....	86
<b>Ніколаєнко Р.С.</b> Захищена P2P комунікація на основі технології Blockchain.....	87
<b>Палюх В.М.</b> Імітаційне моделювання рекреаційної діяльності парку «Шевченків гай».....	89
<b>Прокопович-Ткаченко Д.І., Стелюк Б.Б., Солянніков В.Г.</b> Підходи до авторизації та автентифікації безпроводового доступу комунікаційних систем.....	93
<b>Рихтюк Е.Ю.</b> Автоматизований сервіс підбору ІТ-персоналу в компанії.....	95
<b>Рожков Є.І., Новікова Н.В.</b> Числа Фібоначчі в вебдизайні.....	97
<b>Савін М.С.</b> Алгоритм пошуку елементів на сторінці зі змінюваною структурою.....	99
<b>Сав'як Н.Т., Задорожна А.В.</b> Огляд перспективних фреймворків та бібліотек для розробки веб-сайтів.....	101
<b>Самойлов В.В.</b> Опис текстового редактора Sublime Text 3.....	102
<b>Сапіжак І.М.</b> Розробка сервіс-орієнтованої системи в інтернет-медіа сфері.....	104
<b>Сусуловська М.Р.</b> Комп'ютерний переклад медичних термінів.....	107
<b>Танасюк Ю.В., Гарвасюк Р.В.</b> Алгоритм для формування навчального розкладу.....	110
<b>Танасюк Ю.В., Головайко Р.А.</b> Віртуальний тур по навчальному корпусу чернівецького національного університету імені Юрія Федьковича.....	112

<b>Тарбай Б.В., Воропаєва С.Л., Поповецька Л.І.</b> Дослідження можливостей інтеграції C# та AutoCAD при тривимірному моделюванні.....	115
<b>Телишева Т.О., Камінський О.В.</b> Автоматизація процесу визначення IBAN в банківських системах.....	117
<b>Фуцур Д.А., Далекорей А.В.</b> Технологія “blockchain” для зберігання персональних даних.....	121
<b>Шлапак С.С.</b> Порівняння стандартів безпеки комп'ютерних мереж.....	123
<b>Шматок В.В., Святюк О.Я.</b> Технологія доповненої реальності.....	124
<b>Юскович-Жуковська В.І., Соловей Л.Я.</b> Напрямки використання соціальних мереж у підготовці IT-фахівців.....	126
<b>Муkytas А.О., Kononenko О.М., Bratyshchenko M.R.</b> Інформаційна безпека.....	128
<b>Муkytas А.О., Kononenko О.М., Bratyshchenko M.R.</b> Соціальна інформатика.....	130
<b>Муkytas А.О., Kononenko О.М., Bratyshchenko M.R.</b> Технології інтернету речей (IoT).....	131

## *Частина 2*

### *Секція 2. Економічні науки*

<b>Ахмедов О.А.</b> Впровадження інновацій: сучасні проблеми та шляхи їх подолання.....	3
<b>Бик О.Я.</b> Ілюзія вибору, або використання інструментів психологічного впливу в політичному маркетингу.....	6
<b>Городецький М.А.</b> Діджиталізація емоційних компонентів прийняття рішень як інструмент управління бізнес-процесами.....	7

<b>Жакун В.В.</b> Професійна діяльність з управління активами ІСІ в Україні.....	9
<b>Ідізада Сіяр Гулам</b> Використання категорійного менеджменту для підвищення ефективності збуту на підприємстві.....	11
<b>Імшенецький Ю.І.</b> Місії та цілі підприємства.....	13
<b>Кітченко О.М., Білошкурєнко Н.Г.</b> Таргетована реклама в інтернет бізнесі.....	15
<b>Крук О.В.</b> Управління якістю як одним з основних факторів конкурентоспроможності продукції підприємства.....	17
<b>Кузьмінський В.Ю., Воронін А.В.</b> Процес управління збутовою діяльністю підприємства.....	18
<b>Лиськова Л.М.</b> Співпраця України та ЄС в інноваційній сфері.....	20
<b>Ляшко І.І., Єременко О.М.</b> Ухвалення управлінських рішень як чинник ефективності виробництва.....	23
<b>Неводнічик А.Я.</b> Довірче управління активами та капіталом в Україні.....	25
<b>Потьомкіна Н.Ю.</b> Особливості кількісних та якісних методів оцінки ризиків у діяльності нафтогазових підприємств.....	27
<b>Таюк О.І.</b> Фінансова стратегія страхових компаній в Україні.....	28
<b>Ткачук Г.О.</b> Концепція безпечності трансформаційних перетворень на підприємствах харчової промисловості.....	31
<b>Туболец І.І., Горєлов Є.В.</b> Концептуальні основи антикризового фінансового управління підприємством.....	33

<b>Утенкова К.О.</b> Принципи системи економічної безпеки аграрного сектору.....	35
<b>Ушакова О.А., Кирилюк О.А.</b> «Тіньові» проблеми економічного розвитку України.....	37
<b>Федина В.В., Саламаха Ю.В.</b> Аналіз сучасного стану ринку банківських послуг в Україні.....	38
<b>Чебан В.Д., Церковна А.В.</b> Актуальні інструменти управління транспортною логістикою на підприємстві.....	41
<b>Шапоренко О.О.</b> Система факторів впливу на управління видатками бюджету.....	43
<b>Шинденков Ю.О., Воронін А.В.</b> Управління ризиками, як елемент системи управління підприємством.....	46

### *Секція 3. Технічні науки*

<b>Ахмедов О.А.</b> Використання сучасних засобів вимірювальної техніки для обліку та контролю споживання природного газу.....	48
<b>Божко К.М.</b> Отримання вольт-фарадної характеристики сонячної батареї за осцилограмами перехідного процесу.....	49
<b>Гриценко Т.А.</b> Сучасне обладнання для полегшення роботи майстра під час надання послуг з манікюру.....	51
<b>Діброва І.Є.</b> Рекреаційне районування Закарпаття.....	52
<b>Загоржевський В.І., Божко К.М., Чорнуха А.В.</b> Вдосконалення еквівалентних схем фотоелектричних сонячних батарей.....	54
<b>Золотовська О.В., Пивовар В.І.</b> Випробування вакуумної трубки сонячного колектора.....	55

<b>Іваницький В.П., Чичура І.І., Ямельницький І.В.</b> Оптимізація метрологічних характеристик приладів вимірювання частоти електричних процесів.....	58
<b>Косухіна О.С., Кузьмін І.О.</b> Application of wavelet transforms to digital signal processing.....	59
<b>Медведєв Р.Б., Складанний Д.М., Пустовий Д.О.</b> Моделювання зміни концентрації окисників у першому контурі реактора ВВЕР-1000.....	61
<b>Скиба Г.О.</b> Як визначити натуральну зубну пасту.....	63
<b>Скоркін О.Ю., Алістратова Т.С.</b> Інтелектуальна система вимірювання відстані.....	65
<b>Стоянова О.В., Котелевська В.Д.</b> Дослідження рецептури овочевих маринадів.....	68
<b>Цендра О.О.</b> Можливості розвитку велосипедної інфраструктури на укріплених берегах річок Закарпаття.....	70
<b>Штонда І.Ю., Далекорей А.М.</b> Сучасні методи вирішення проблем дощових систем водовідведення.....	72

**[www.konferenciaonline.org.ua](http://www.konferenciaonline.org.ua)**

***Міжнародна наукова інтернет-конференція***

**"Інформаційне суспільство: технологічні,  
економічні та  
технічні аспекти становлення"  
(випуск 43)**

***14 листопада 2019 р.***

***Частина 1***





Підписано до друку 22.11.2019  
Формат 60x84/16. Папір офсетний. Друк на дублікаторі.  
Умов.-друк. арк. 4,5. Обл.-вид. Арк 4,95.  
Тираж 100 прим.

Віддруковано ФО-П Шпак В.Б.  
Свідоцтво про державну реєстрацію № 073743  
СПП № 465644  
Тел. 097 299 38 99  
E-mail: [tooums@ukr.net](mailto:tooums@ukr.net)

